Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: Засоби захисту автоматизованої системи керування технічними процесами енергетичних систем

Виконавець: студента IV курсу, групи КБ-41

_____ **Максим СІРЕНКО**
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Сергій ДАКОВ	

Нормоконтроль	Інна МИХАЛЬЧУК	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-41** (група) **Максиму Миколайовичу Сіренку** (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Засоби захисту автоматизованої системи керування технічними процесами енергетичних систем

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Концепція впровадження розроблених рівнів кібербезбеки.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з автоматизованими системами керування, класифікаціїю та організаційною структурою. Проаналізувати модель порушника та можливі загрози, на основі цього розробити стратегію та програму забезпечення захисту, розробити рівні кібербезпеки для захисту АСУ на атомних станціях.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рівні кібербезпеки для захисту різних автоматизованих систем керування на атомних станціях.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ (підпис) Сергій ДАКОВ (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Максим СІРЕНКО (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 22.01.2023	*виконано*
2	Аналіз літератури	29.01.2023 – 11.02.2023	*виконано*
3	Обгрунтування вибору рішення	12.02.2023 – 15.02.2023	*виконано*
4	Аналіз автоматизованих систем керування	16.02.2023 – 04.03.2023	*виконано*
5	Аналіз нормативно правової бази та стандартів МАГАТЕ	05.03.2023 – 21.03.2023	*виконано*
6	Дослідження вразливостей та загроз	22.03.2023 – 08.04.2023	*виконано*
7	Розробка рівнів кібербезпеки та рекомендацій захисту АСУ ТП в ядерних установках	09.04.2023 – 10.05.2023	*виконано*
8	Оформлення пояснювальної записки	11.05.2023 – 27.05.2023	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2023 – 12.06.2023	*виконано*

Завдання видав _____ (підпис) Сергій ДАКОВ (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Максим СІРЕНКО (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Пояснювальна записка дипломної кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 81 сторінку основного тексту, 6 таблиць та 11 рисунків. Список використаних джерел містить 21 найменування і займає 2 сторінки.

Метою роботи є розробка засобів захисту автоматизованої системи керування технічними процесами енергетичних систем.

Об'єктом дослідження є процес захисту автоматизованої системи керування в АС.

Предметом дослідження є механізми та засоби, реалізації методів захисту автоматизованих систем керування.

Методи дослідження:

- аналіз відкритих та закритих джерел;
- аналіз атак та профілів виконавців;
- розробка засобів кіберзахисту АСУ ТП.

Практична цінність роботи полягає в розробці рівнів кібербезпеки для автоматизованих систем керування на атомних станціях.

Ключові слова: Кібербезпека, SCADA, енергетика, автоматизовані системи управління, функціональна система автоматизації, контрольно-вимірювальні прилади, системи управління та захисту, МАГАТЕ, ядерні установки.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

АСУ ТП	–	Автоматизовані системи управління технічними процесами
РФН	–	Рівень функціональної надійності
МЗ	–	Математичне забезпечення
ФСА	–	Функціональна система автоматизації
КВП	–	Контрольно-вимірювальні прилади
СУЗ	–	Системи управління та захисту
МАГАТЕ	–	Міжнародне агентство з атомної енергії
SDA	–	Sensitive digital assets
МПК	–	Мікропроцесорний контролер
ОП	–	Оперативний персонал
ОЗ	–	Організаційне забезпечення
VPN	–	Virtual Private Network
АС	–	Атомна електростанція
ІКС	–	Інформаційно-комунікаційна система
ПЗ	–	Програмне забезпечення
ПКБ	–	Програма комп'ютерної безпеки
МРЧІ	–	Мітка радіочастотної ідентифікації
ТЗ	–	Технічні засоби

ЗМІСТ

ВСТУП

Автоматизовані системи керування технічними процесами в енергетичних системах відіграють вирішальну роль у забезпеченні ефективності, надійності та безпеки експлуатації. Захист таких систем від потенційних загроз та зловмисного втручання стає все більш актуальною проблемою у сучасному цифровому середовищі. Інтенсивний розвиток інформаційних технологій та зростання кількості кібератак на автоматизовані системи створюють необхідність у використанні ефективних засобів захисту. Ця дипломна робота присвячена вивченню та аналізу різних засобів захисту автоматизованих систем керування технічними процесами енергетичних систем. Основною метою дослідження є виявлення та оцінка ефективності застосування таких засобів у контексті забезпечення безпеки та надійності роботи енергетичних систем. У роботі будуть проаналізовані різні методи та технології захисту, такі як аутентифікація, авторизація, мережеві файрволи та інші. Також будуть вивчені сучасні загрози та атаки на автоматизовані системи керування технічними процесами енергетичних систем, щоб визначити найбільш уразливі місця та пропонувати відповідні заходи захисту. Результати дослідження допоможуть розробити рекомендації та рекомендувати оптимальні засоби захисту для автоматизованих систем керування технічними процесами енергетичних систем. Це сприятиме покращенню безпеки та надійності роботи енергетичних систем, зменшенню ризиків зловмисного втручання та забезпеченню стабільного функціонування в умовах сучасного цифрового середовища. Актуальність даної дипломної роботи обумовлена кількісним та якісним зростанням загроз та ризиків, яким піддаються автоматизовані системи керування технічними процесами в енергетичних системах. В сучасному світі, де цифрові технології використовуються все ширше, з'являється все більше потенційних загроз з боку хакерів, кіберзлочинців та навіть державних акторів, які намагаються отримати несанкціонований доступ до систем енергетичних підприємств. В разі успішного вторгнення або атаки на автоматизовані системи керування технічними процесами енергетичних систем

можуть виникнути серйозні наслідки, такі як порушення роботи енергетичних об'єктів, небезпека для життя та здоров'я людей, а також значні економічні збитки. У зв'язку з цим, розробка та впровадження ефективних засобів захисту є надзвичайно важливою задачею.

Дослідження засобів захисту автоматизованих систем керування технічними процесами в енергетичних системах є актуальним, оскільки воно спрямоване на виявлення та оцінку різних методів та технологій захисту, а також на розробку рекомендацій щодо покращення безпеки та надійності роботи енергетичних систем. Це дозволить зменшити ризики зловмисного втручання, забезпечити стійкість до кібератак та забезпечити безперебійне функціонування енергетичних систем в умовах постійно зростаючих загроз.

Метою роботи є розробка засобів захисту автоматизованої системи керування технічними процесами енергетичних систем.

Для досягнення мети дипломної роботи поставлено наступні **завдання**:

- аналіз автоматизованих систем атомної станції керування технічними процесами
- дослідження вразливостей, моделі загроз та порушників на АСУ ТП в ядерних установках
- розробка засобів захисту автоматизованої системи керування технічними процесами в АС

Об’єктом дослідження є процес захисту автоматизованої системи керування в АС.

Предметом дослідження є механізми та засоби, реалізації методів захисту автоматизованих систем керування.

Методи дослідження:

· аналіз відкритих та закритих джерел;

· аналіз атак та профілів виконавців;

· розробка засобів кіберзахисту АСУ ТП.

Практична цінність роботи полягає в розробці рівнів кібербезпеки для автоматизованих систем керування на атомних станціях.

РОЗДІЛ 1
АНАЛІЗ АВТОМАТИЗОВАНИХ СИСТЕМ КЕРУВАННЯ ТЕХНІЧНИМИ ПРОЦЕСАМИ

1.1 Визначення автоматизованих систем керування технічними процесами

Перш ніж заглибитися в основні поняття, що використовуються в автоматизованих системах управління технологічними процесами, важливо дати чітке визначення терміну «система», який останнім часом використовується досить широко. Різні автори пропонують тлумачення та визначення, але загалом вони погоджуються, що система – це сукупність взаємодіючих елементів. Проте деякі стверджують, що система — це не просто сукупність елементів зі спільними характеристиками, але вона також демонструє певну цілісність, досягнуту завдяки зв'язкам і взаємодії між її елементами. Кожна система характеризується єдиною ціллю, результатом якої є цілеспрямована взаємодія між її елементами.

Система не існує ізольовано, а існує в зовнішньому середовищі, яке взаємодіє з системою в цілому або з окремими її елементами. Взаємодія між елементами системи та її зовнішнім середовищем вносить певний рівень невизначеності щодо меж системи та ускладнює її локалізацію. Тому виникає необхідність визначити релевантні зв'язки, які слід враховувати, не враховуючи несуттєві, які мають мінімальний вплив на функціонування системи та точність її математичних моделей. У міру розвитку нашого розуміння системи та розробки більш точних математичних моделей виникає необхідність переоцінити межі системи та її взаємозв'язки із зовнішнім середовищем, удосконалюючи таким чином наше початкове уявлення про систему.

З незліченної кількості типів систем ми зупинимося саме на одному класі — системах технологічного керування процесами виробництва та споживання унікальної продукції на підприємствах міського господарства. До цього класу також відносяться інженерні системи міського господарства, такі як централізоване

теплопостачання, водонагрівання, гаряче та холодне водопостачання, вентиляція та кондиціювання повітря, газопостачання, водовідведення, електропостачання. Однак наш головний інтерес полягає в їх ролі як об'єктів управління в ширшому контексті технологічних систем управління.

Основним рішенням для вирішення сучасних управлінських завдань є використання автоматизованих систем управління технологічними процесами . Ці системи, відомі як автоматизовані системи керування, поєднують центральну та вирішальну роль людського досвіду та творчості з широким застосуванням сучасних математичних методів та засобів автоматизації, включаючи мікропроцесорні контролери.

Відповідно до Держстандарту України (ДСТУ) АСУ ТП віднесено до людино-машинних систем. Це полегшує автоматизований збір інформації з перетворювачів первинного або передавального сигналу та її початкову обробку. Ця обробка включає такі завдання, як фільтрація сигналу, а також перетворення сигналів у значення фізичних параметрів, таких як температура (°С), тиск (Па), об’єм (м³/кг) тощо. АСУ ТП обчислює, формує та здійснює керуючі впливи на об'єкт управління відповідно до встановлених критеріїв управління. Він працює в режимі реального часу, синхронізуючи технологічний процес, і забезпечує комплексний контроль над усім об'єктом. Технічні засоби в складі АСУ ТП сприяють розробці управлінських рішень. Варто зазначити, що АСУ ТП якісно відрізняється від традиційних систем автоматичного керування, які автоматизують виключно окремі дії в межах ділянок технологічного процесу. На відміну від цього, АСУ ТП включає в себе автоматизований процес прийняття рішень для управління всім технологічним процесом. Це стало можливим завдяки використанню різноманітного «інтелектуального» обладнання для автоматичної обробки інформації, насамперед передових багатофункціональних і високопродуктивних мікропроцесорних контролерів. Отже, АСУ ТП характеризується єдністю та взаємодією трьох основних компонентів:

об'єкт керування (ОК) - це технологічний процес з агрегатами, аппаратами, установками та установкою. Тоді вони - це технологічні дії, які складаються з технологічного обладнання, матеріалів, комплектуючих тощо.

технічні засоби (ТЗ) - апаратура автоматичної обробки інформації, в тому числі (МПК);

оперативний персонал (ОП) - оператори технологічного відділу, експлуатаційні оператори.

АСУ ТП для того, щоб отримати уявлення про особливості та характер функціонування, розглянемо його спрощену загальну структуру (рис. 1.1)

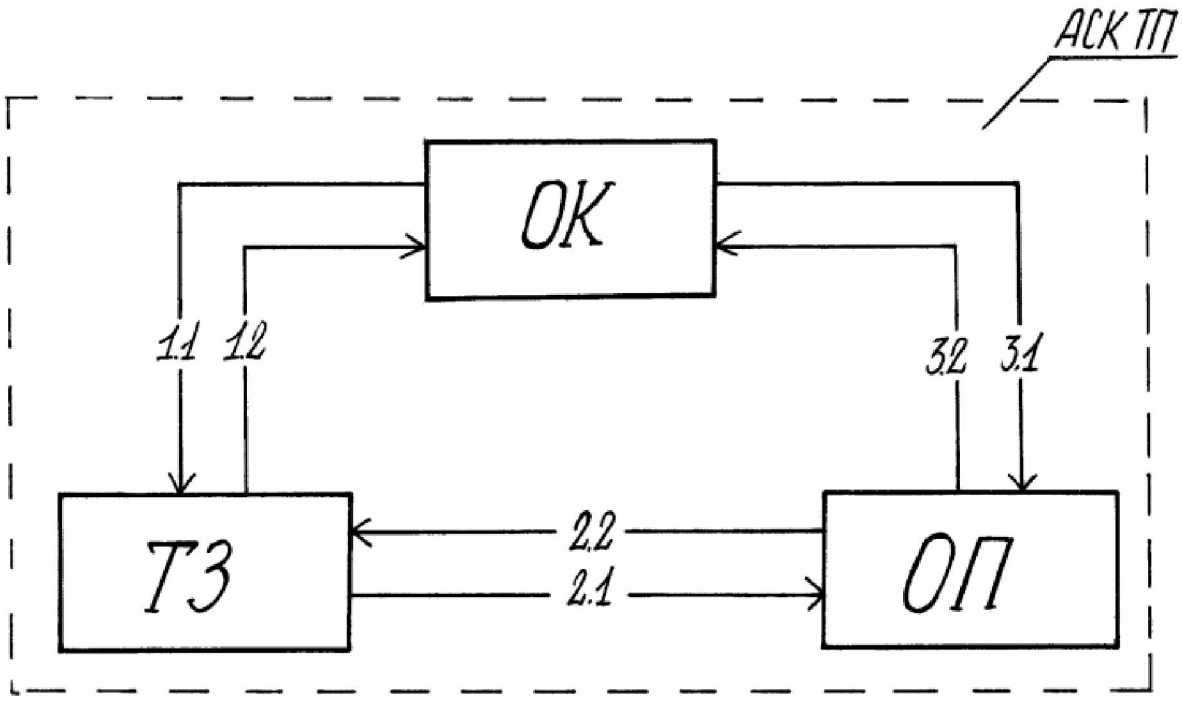

Рисунок 1.1 - Потоки інформації, сигнали в автоматичному режимі

Потоки інформації зображенні на (рис. 1.1). 1.1 - Сигнали від попереднього контролера (ПП) та поточного контролера про стан об'єкта керування. 1.2 - Сигнали, які впливають на об'єкт керування для забезпечення необхідної реакції. 2.1 - Сигнали, що уточнюють значення певних параметрів. 2.2 - Сигнали для корекції параметрів налаштування відповідних регуляторів при необхідності. 3.1 - Дані аналітичного контролю об'єкта. 3.2 - Віддалене керування окремими параметрами об'єкта.

Роль людини як невід'ємної складової в структурному каркасі АСУ ТП є важливою. Участь людей і призначені їм ролі в процесі управління об'єктами характеризують організацію цього процесу. У свою чергу, розподіл завдань між людьми та автоматизованим обладнанням визначає апаратний склад системи керування. Оптимальний розподіл обов'язків між людьми та автоматизованим обладнанням не може бути визначено заздалегідь, оскільки залежить від конкретних умов на об'єкті, що управляється, якості автоматизованого обладнання та рівня технічної підготовки операторів і технологів, залучених до процесу управління. Це питання виникає на етапі проектування АСУ ТП, де стоїть завдання визначити оптимальний розподіл функцій між людьми та обладнанням. Обсяг інформації, яку необхідно отримувати та швидко опрацьовувати для формування ефективних керуючих впливів, значно зріс у сучасних системах управління, перевершуючи можливості окремої людини. Отже, управління складними об'єктами покладається на команду людей. Існує критична точка, коли координація та обмін керуючими впливами та спільне прийняття рішень між членами команди вимагають інтенсивних інформаційних потоків у самій системі керування. Тому основним інструментом для вирішення сучасних завдань управління фізичними об'єктами є АСУ ТП. Він поєднує важливу роль і творчі здібності людини з широким використанням сучасних математичних методів і засобів автоматизації, включаючи МПК.

1.2 Функції, цілі, критерії керування АСУ ТП

У наведеному визначенні АСУ ТП підкреслюється, що ця система обробляє як технологічну, так і техніко-економічну інформацію з основною метою оптимізації роботи об'єкта керування на основі прийнятих критеріїв керування шляхом вибору відповідних керуючих впливів .

Критерій контролю в АСУ ТП являє собою комплексний показник, який кількісно характеризує загальну якість роботи об'єкта управління. Він враховує чисельні значення керуючих впливів, розрахованих, виданих і реалізованих системою керування. Отже, критерії, що визначають параметри АСУ ТП, можуть охоплювати

як технологічні показники, такі як температура, тиск і споживання, так і техніко-економічні показники, такі як собівартість продукції при конкретному рівні якості та продуктивність об'єкта керування. Математично критерій керування АСУ ТП визначає мету створення даної системи.

Існують певні обмеження, які необхідно враховувати при виборі керуючих впливів. Ці обмеження можна розділити на два типи: фізичні обмеження, які не повинні порушуватися незалежно від вибору керуючих впливів, і умовні обмеження, які можуть бути порушені, але призводять до значних втрат, які не враховуються критерієм контролю. Як наслідок, під час впровадження АСУ ТП найважливіші фактори часто враховуються через обмеження, а не покладаються виключно на критерії управління.

При проектуванні АСУ ТП важливо визначити конкретні цілі та функції системи. Конкретні цілі роботи АСУ ТП можуть включати:

Оптимізація витрат палива, енергетичних ресурсів та інших ресурсів з метою зниження їх питомих значень.

Покращення якості виробленої продукції.

Зменшення затрат на людський фактор робочої сили.

Забезпечення безпеки функціонування об'єкта керування.

Досягнення раціонального використання обладнання.

Досягнення оптимальних режимів роботи обладнання з точки зору визначеного критерію.

Кожне з перерахованих вище завдань для конкретного АСУ ТП може бути метою системи. Система досягне цього будь-яким способом. Виконуючи свої функції, АСУ ТП може досягти поставлених цілей. Функції АСУ ТП — це набір системних дій, що ґрунтується на діях, спрямованих на досягнення мети функціонування. В інформаційному, контрольному та допоміжному розділах АСУ ТП є три види функцій.

1.2.1 Інформаційні функції

У тому числі сюди входять функції АСУ ТП, а також його функції. Результати передають оператору-технологу або зовнішньому користувачеві інформацію про стан контролю технологічного процесу для себе і не тільки йому, але й іншим особам. До основних інформаційних функцій можна віднести: Автоматичний контроль параметрів технологічного процесу, таких як температура, тиск, тиск, витрати та ін., автоматизовано за допомогою. Якщо оператор-технолог повідомлений про невідповідності, то можна продовжити перевірку на відповідність параметрів процесу вимогам і постійну перевірку його відповідності необхідним умовам; постійно перевіряти правильність технологічних даних технологічного процесу по всіх компонентах.

Оператор-технолог запропонував вимірювання або реєстрацію за його бажанням тих параметрів технологічного процесу, які його цікавлять у процесі управління об'єктом; також можлива реєстрація, вимірювання або реєстрація на вимогу оператора-технолога таких параметрів технологічного процесу, які його цікавлять; За словами оператора-технолога, за запитом можна повідомити про виробничу ситуацію на будь-якій ланці об'єкта управління в поточний момент.Час відхилення деяких параметрів технологічного процесу, з метою фіксації часу відхилення деяких параметрів технологічного процесу за допустимими технологічними регламентами величини, визначається шляхом фіксації часу відхилення деяких; За бажанням оператора-технолога надаються деякі комплексні показники, які безпосередньо не контролюються автоматично, але вони характеризують або якість вихідної продукції, або інші важливі показники технологічного процесу, і вони можуть бути розраховані за його бажанням. Деякі комплексні показники, які безпосередньо не контролюються автоматично, але характеризують або якість вихідної продукції, або інші важливі показники технологічного процесу; Оперативний розрахунок досягнутих техніко-економічних показників технологічного процесу тобто в реальному масштабі часу, а також

оперативний аналіз для досягнення техніко-економічного показника технологічного процесу.

Періодично ведеться реєстрація автоматично контрольованих і розрахованих даних про хід технологічних систем або розрахункових показників. Є можливість регулярно реєструвати автоматично контрольовані (передаварійні, аварійні) стани; виявлення та сигналізація про небезпечні (перед аварійні, аварійні) ситуації тощо.

1.2.2 Керуючі функції

До функцій АСУ ТП входять: завдання з розрахунку, виробництва та реалізації керуючих впливів на об'єкт управління. Відповідно до цього розрахунок означає обчислення математичних формул керуючих впливів, виробництво – визначення раціональних керуючих впливів на основі отриманої інформації, а реалізація – це процес визначення раціональних керуючих впливів. Реалізація включає дії, що забезпечують передачу раніше отриманих керуючих впливів і передачу їх відповідним виконавчим механізмам. Основними функціями управління є:

Автоматичне керування параметрами технологічного процесу можливе автоматичне керування параметрами технологічного процесу в системі.

Технологічні нормативи, програмне забезпечення, зміна режимів процесу, які встановлені технологією; програмна зміна режимів технологічного процесу відповідно до заданої закономірності.

Однотактне логічне керування операціями технологічного процесу або апаратами; автоматичний захист обладнання від аварій; автоматичний захист обладнання від травм;

Формування та реалізацію керуючих впливів, що забезпечують досягнення або дотримання оптимальних за технологічними або техніко-економічними критеріями управління режимів процесу, необхідно здійснювати за допомогою керуючих впливів.

Перехідні технологічні процеси раціонально управляються шляхом раціонального управління процесом перехідного періоду;Технологічний блок

відрізняється розподілом матеріальних потоків і навантаження у вигляді матеріальних потоків і навантажень, а також розподілом;Автоматичне керування блоками старт/стоп; автоматичне керування пуском/зупинкою агрегатів;

Також можливий автоматичний пуск/зупинка електродвигунів технологічного обладнання або кількість обертів цих електродвигунів, але змінювати кількість обертів цих електродвигунів не потрібно.Адаптивне управління об'єктом управління в цілому і т.д. можливе шляхом адаптивного управління об'єктом управління в цілому.

1.2.3 Допоміжні функції

Ці функції служать для вирішення внутрішньосистемних завдань АСУ ТП, в першу чергу зосереджуючись на забезпеченні безперебійної роботи технічних засобів АСУ ТП.

Існує два режими реалізації функції АСУ ТП, а саме автоматичний та автоматизований, в залежності від залучення обслуговуючого персоналу. Допоміжні функції виконуються виключно в автоматичному режимі. Як правило, інформаційні функції також здійснюються в автоматичному режимі, тоді як операції, пов'язані з аналітичним контролем окремих параметрів технологічних процесів, виконуються в автоматизованому режимі.

Для функцій управління визначено три автоматизованих і два автоматичних режими реалізації. Визначено наступні автоматизовані режими реалізації функцій управління:

«Ручний» режим, де технічні засоби АСУ ТП надають необхідну інформацію оператору-технологу (ОТ) про стан об'єкта керування. ОТ відповідає за вибір і виконання керуючих дій.

Режим «Порадник», коли технічні засоби АСУ ТП формують рекомендації щодо управління об’єктом управління, а ОТ приймає рішення щодо їх реалізації та здійснює відповідні дії.

Режим «Діалог», де ОТ має можливість коригувати параметри та умови будь-якої задачі, що вирішується АСУ ТП.

Режим диспетчерського (диспетчерського, опосередкованого) керування полягає у регулюванні технічними засобами АСУ ТП установок та/або параметрів місцевих автоматичних регуляторів за заздалегідь заданим алгоритмом.Нормальний (безпосередній) режим управління здійснюється шляхом здійснення керуючих впливів виключно на виконавчі механізми через технічні засоби АСУ ТП.

При побудові АСУ ТП часто виникає необхідність розбити його на підсистеми. Ці підсистеми є окремими частинами загальної системи, що відрізняються або функціональними, або структурними характеристиками.

Функціональна особливість дає можливість декомпозиції АСУ ТП на інформаційну та керуючу підсистеми або на підсистеми, призначені для виконання конкретного завдання.Структурна особливість дозволяє розбити АСУ ТП на підсистеми, що відповідають за управління конкретними частинами об'єкта.

1.3 Класифікація АСУ ТП

АСУ ТП можна класифікувати за різними суттєвими факторами та показниками, кожен з яких може служити класифікаційною ознакою. Існує п’ять основних класифікаційних ознак АСУ ТП, які наведені в табл. 1.1 - 1.5.

Таблиця 1.1

Класифікація АСУ ТП за рівнем, який вона посідає в організаційно-виробничій структурі.

Назва АСУ ТП за рівнем	Код класу	Об'єкти керування, які відповідають ознаці
нижній рівень	1	Технологічні агрегати, установки, ланки виробництва, які не мають в своєму складі других АСУ ТП нижнього рівня
верхній рівень	2	Групи технологічних установок, цехи виробництва, які не мають в своєму складі АСУ ТП нижнього рівня
багаторівневі	3	Групи технологічних установок, цехи виробництва, які мають в своєму складі АСУ ТП нижнього рівня

Таблиця 1.2

Класифікація АСУ ТП за характером протікання технологічного процесу (ТП) за часом.

Назва АСУ ТП за характером протікання ТП	Код класу	Характер протікання технологічного процесу
неперервної дії	н	Технологічні процеси неперервної дії з практично беззупинковою подачею енергії, палива, реагентів, сировини тощо, наприклад, теплопостачання при опаленні рівня

Продовження таблиці 1.2

Назва АСУ ТП за характером протікання ТП	Код класу	Характер протікання технологічного процесу
перервної (періодичної) дії	п	Поєднання технологічних процесів із неперервним і перервним режимами функціонування, наприклад, фільтр швидкісний при нормальному режимі і промивці
дискретної дії	д	Дискретні технологічні процеси, як правило, підприємств із несуттєвою для керування тривалістю технологічних операцій

Таблиця 1.3

Класифікація АСУ ТП за "умовною інформаційною потужністю" (УІП), яку характеризують числом, яке дорівнює сумі параметрів автоматичного контролю і керуючих впливів.

Назва АСУ ТП за "УІП"	Код класу	Число "УІП" АСУ ТП	
АСУ ТП із найменшою "УІП"	1	10	40
АСУ ТП із малою "УІП"	2	41	160
АСУ ТП із середньою "УІП"	3	161	650
АСУ ТП із підвищеною "УІП"	4	651	2500
АСУ ТП із великою "УІП"	5	2501	не обмежене

Саме ця характеристика дозволяє кількісно оцінити системи автоматичного керування та автоматизовані системи управління технологічними процесами, оскільки в САК рідко значення «УІП» перевищує 7.

Таблиця 1.4

Класифікація АСУ ТП за рівнем функціональної надійності (РФН) .

Назва АСУ ТП за РФН	Код класу	Характеристика РФН
мінімальним РФН	1	РФН АСУ ТП практично не регламентують, не ставлять вимоги на його підвищення
середнім РФН	2	РФН АСУ ТП регламентують, але відмовлення в АСУ ТП не приводе до зупинки об'єкта керування (ОК)
високим РФН	3	РФН АСУ ТП жорстко регламентують, тому що відмовлення в АСУ ТП можуть привести до зупинки ОК або аварії

Таблиця 1.5

Класифікація АСУ ТП за сукупністю інформаційних і керуючих функцій, тобто за режимом функціонування (РФ) АСУ ТП

Назва АСУ ТП за РФ	Код класу	Об'єкти керування, які відповідають ознаці
АСУ ТП із інформаційним РФ	1	В автоматичному режимі виконують інформаційні функції, рішення по керуванню приймає оператор-технолог

Продовження таблиці 1.5

Назва АСУ ТП за РФ	Код класу	Об'єкти керування, які відповідають ознаці
АСУ ТП із локальноавтоматичним РФ	л	В автоматичному режимі виконують інформаційні функції і функції локального керування окремими параметрами. Рішення по керуванню об'єктом приймає і реалізує ОТ
АСУ ТП із РФ "порадника"	п	В автоматичному режимі виконують інформаційні функції і функції локального керування окремими параметрами. За допомогою математичних моделей об'єкта керування АСУ ТП формує поради для вибору ОТ керуючих впливів відповідно до критерію керування
АСУ ТП із автоматичним РФ	а	Інформаційні і керуючі функції АСУ ТП виконують в автоматичному режимі відповідно до критерію керування

Надані ознаки класифікації та їх відповідні коди для класів АСУ ТП використовуються при розробці технічного завдання на створення таких систем. Сам код АСУ ТП складається з кодів класів, представлених символами з першого по п’ятий. Наприклад, якщо код АСУ ТП «1н33п», це означає, що система нижчого рівня, працює безперервно, має середню умовну інформаційну потужність, демонструє високий рівень функціональної надійності, працює в режимі «порадник».

1.4 Основні технічні умови на АСУ ТП та його основні складові.

Конфігурація та структура будь-якого АСУ ТП ретельно підбираються, щоб забезпечити відповідність системи основним технічним вимогам і конкретним вимогам, викладеним у Технічному завданні на її розробку. Загалом, як АСУ ТП в цілому, так і його підсистеми повинні відповідати наступним основним технічним вимогам:

Управління всім об'єктом в реальному часі.

Управління технологічними процесами на основі визначених критеріїв контролю.

Виконання всіх покладених на нього функцій відповідно до поставленої задачі та цілей управління.

Володіння необхідними показниками і характеристиками, такими як точність, надійність, швидкість реагування.

Дотримання ергономічних вимог щодо способів подання інформації, форм, розміщення технічних засобів тощо.

Адаптивність для безперебійної інтеграції з системами управління суміжних ієрархічних рівнів та іншими АСУ ТП, забезпечення технічної та інформаційної сумісності.

Володіння необхідними метрологічними характеристиками каналів вимірювання інформації.

Працездатність в умовах підвищеної вологості, запиленості повітря, підвищених температур і нестабільної сейсмічної активності.

Гарантія заданого терміну експлуатації системи (6-9 років) в умовах, що вимагають проведення ремонтних робіт.

АСУ ТП має передбачати потенційну модернізацію та розвиток у майбутньому.

Крім того, замовник і розробник можуть висувати особливі вимоги до систем АСУ ТП за їх згодою .

До основних компонентів будь-якої системи АСУ ТП відносяться: оперативний персонал та допоміжно-інформаційний, організаційний, математичний, програмний, технічний .

Технічне забезпечення охоплює необхідні технічні засоби, у тому числі перетворювачі первинного і передавального сигналів, виконавчі механізми, мікропроцесорні контролери, алгоритми, що забезпечують виконання всіх функцій АСУ ТП.

Математичне забезпечення складається з математичних методів, моделей та алгоритмів, які описують технологічні процеси об’єкта керування та є достатніми для реалізації всіх функцій АСУ ТП.

Програмне забезпечення охоплює сукупність комп’ютерних програм, необхідних для роботи та функціонування ТЗ в АСУ ТП. Програмне забезпечення можна класифікувати на загальні і спеціальні категорії.

Інформаційне забезпечення включає автоматично контрольовані параметри об'єкта керування у вигляді сигналів, а також системи класифікації та кодування інформації та масиви даних і документів, необхідні для реалізації програмного забезпечення АСУ ТП.

Організаційне забезпечення складається з описів функціональної, технічної та організаційної структур АСУ ТП, а також інструкцій і технологічних регламентів для оперативного персоналу.

Оперативний персонал складається з операторів-технологів, які здійснюють безпосереднє управління об'єктом, та оперативного персоналу, відповідального за утримання та обслуговування технічного обладнання, у тому числі МПК та програмних засобів.

Функціонування АСУ ТП можна охарактеризувати як цілеспрямований процес перетворення вхідної інформації у вихідну. Ця трансформація здійснюється спільними зусиллями двох складових: оперативного персоналу та технічної інфраструктури.Оперативний персонал і технічні засоби, в тому числі мікропроцесорний контролер, відіграють вирішальну роль як основних компонентів АСУ ТП як людино-машинної системи. Вони збирають вхідну інформацію від об'єкта

управління та зовнішніх джерел, обробляють і аналізують її, приймають рішення щодо управління об'єктом і реалізують ці рішення через керуючі впливи на об'єкт та інші сигнали. Оперативний персонал та технічні засоби спільними зусиллями забезпечують правильне функціонування АСУ ТП. Щоб оперативний персонал і технічні засоби могли ефективно працювати на основі прийнятих критеріїв управління, їх необхідно забезпечити відповідними правилами та інструкціями. Для оперативного персоналу це завдання виконує організаційно-допоміжна документація АСУ ТП, а як інструкції до основних технічних засобів – програмне забезпечення. Інші технічні засоби реалізують свої алгоритми апаратними методами, а отже, не потребують додаткових інструкцій.

Під час роботи між компонентами АСУ ТП відбувається інтенсивна взаємодія. Організаційна та програмна складові визначають поведінку оперативного персоналу та МПК відповідно. Крім того, оперативний персонал активно взаємодіє з технічною підтримкою та при необхідності налаштовує програмне забезпечення. Ці взаємодії відбуваються всередині системи АСУ ТП та із зовнішнім середовищем, насамперед через обмін інформацією у формі сигналів, даних, повідомлень, текстів тощо. Цей обмін інформацією спирається на певне розуміння щодо форм і можливих значень інформаційних елементів. Сукупне розуміння цих аспектів становить інформаційне забезпечення, яке сприяє процесам обміну інформацією всередині АСУ ТП та із зовнішнім середовищем.

1.5 Оператори, структура, організаційно-технічне забезпечення АСУ ТП

Організаційне забезпечення АСУ ТП, яке складається зі збірки документів, що встановлюють процедури та правила для оперативного персоналу . До таких документів відносяться технологічні інструкції та регламенти, що описують технологічний процес, інструкції з експлуатації АСУ ТП, а також описи його функціональної, технологічної та організаційної структури або аналогічні документи. Роль організаційної підтримки є вирішальною, оскільки вона регулює всю людську діяльність в АСУ ТП, починаючи від планових завдань з технічного обслуговування

до складних і критичних дій, таких як оптимізація технологічного процесу. Важливо мати чіткі та суворі правила в рамках організаційної підтримки та розпоряджень, яких необхідно суворо дотримуватися, водночас дозволяючи певний ступінь свободи в діяльності ОП, щоб заохочувати їхню творчість та покращувати процес управління об'єктом.

Загальні вимоги до організаційного забезпечення АСУ ТП є простими. Він повинен містити набір правил і розпоряджень, які регулюють взаємодію ОП і технічних засобів, а також їх взаємодію між собою під час роботи системи. Крім того, він повинен надати всю необхідну інформацію про порядок роботи АСУ ТП, включаючи заходи щодо забезпечення точності та надійності. Інструкція з експлуатації АСУ ТП повинна висвітлювати дії ОП у звичайних, передаварійних і аварійних ситуаціях.

Оперативний персонал АСУ ТП складається з операторів-технологів, які здійснюють безпосередній контроль і управління системою, та оперативного персоналу, який забезпечує роботу системи в заданому режимі, включаючи всі технічні засоби та програмні компоненти.

Одним із головних завдань у АСУ ТП є досягнення оптимальної взаємодії «людина-машина», що передбачає організацію інформаційних потоків до та від оперативного персоналу таким чином, щоб максимально збільшити їх творчий потенціал. Тому при розробці АСУ ТП та відповідних технічних засобів взаємодії «людина-машина» важливо враховувати психофізіологічні особливості та можливості людини. Елементи конструкції, що полегшують цю взаємодію, такі як індикатори відображення інформації та командні пристрої, повинні бути зручними для користувача, вимагати від оператора мінімальної уваги та зусиль. Крім того, вимоги також повинні включати забезпечення комфортного середовища для оптимальної роботи людини на робочому місці.

Як інформаційний процесор людину можна порівняти з універсальним обчислювальним пристроєм. Хоча люди можуть не зрівнятися з комп'ютерами за швидкістю, вони володіють унікальними здібностями, такими як інтуїтивне вирішення проблем, адаптивність у невизначених ситуаціях і здатність до творчого

прийняття рішень. Однак надійність людини в роботі поступається технічним засобам через такі фактори, як втома та вплив психологічних аспектів. Тим не менш, за сприятливих умов праці, коли люди можуть контролювати навколишнє середовище за допомогою сенсорного сприйняття, передбачати події, навчатися та адаптуватися до змін, їх інтеграція в АСУ ТП може значно підвищити надійність їхньої роботи.

Розглядаючи, як ефективно використовувати творчі здібності людей як основний компонент АСУ ТП, першочерговим завданням є визначення оптимального розподілу функцій між людьми та машинами. На машини можуть бути покладені повторювані та рутинні завдання, що передбачають прості управлінські обов'язки, такі як контроль параметрів технологічного процесу на певному рівні або на основі заздалегідь визначеної програми, або автоматичний захист обладнання за допомогою стандартизованих алгоритмів. З іншого боку, завдання, які не мають формалізованих алгоритмів або вимагають можливостей, які зараз неможливі для автоматизації, призначені для участі людини. Крім того, люди відповідають за резервне копіювання на випадок збою автоматичного пристрою.

Організаційна структура АСУ ТП визначається складом його оперативного персоналу та взаємовідносинами, що встановлюються між ними. У цій структурі є посадові особи, які є або виробничим, або адміністративним персоналом, відповідальним за управління технологічним об'єктом, або групи таких посадових осіб, організовані за відповідними критеріями. Ключові зв'язки в організаційній структурі АСУ ТП узгоджуються з оперативними відносинами та співпідпорядкованістю між цими працівниками, які є важливими для процесу управління. Якщо необхідно, організаційну структуру АСУ ТП можна проілюструвати за допомогою діаграми, яка також вказує на географічне розміщення оперативного персоналу в АСУ ТП та їх взаємодію з персоналом з інших систем або рівнів управління.

Технічна підтримка АСУ ТП охоплює набір технічних ресурсів і алгоритмів, призначених для виконання всіх функцій АСУ ТП. Склад технічного забезпечення змінювався з плином часу, починаючи з 1960-х років і до останнього часу, в залежності від технічних засобів, що випускаються промисловістю країни. Історично

до складу технічного забезпечення АСУ ТП входили пристрої збору, перетворення, передачі та відображення інформації, а також обчислювальні, керуючі та виконавчі пристрої. Він охоплював повний набір контрольно-вимірювальних приладів, засобів автоматизації. У технічну підтримку АСУ ТП також входять прилади та обладнання, необхідні для налаштування, тестування працездатності технічних засобів, запасні пристрої. Технічні характеристики всіх ресурсів АСУ ТП повинні передбачати взаємозамінність специфікацій для однотипного обладнання з урахуванням факторів зовнішнього середовища та забезпечення безпечної роботи системи.

Сукупність технічних ресурсів АСУ ТП, представлена конструктивно незалежними пристроями, вузлами та обладнанням, утворюють технічну структуру АСУ ТП. Ця структура відображає первинні самостійні компоненти технічних ресурсів системи. З'єднання між цими компонентами представлено фізичними лініями, такими як електричні дроти та кабелі, які з'єднують окремі ресурси автоматизації у функціонуючий комплекс. У процесі розробки та впровадження АСУ ТП змінювалися технічні конструкції на основі технічних засобів, що випускаються промисловістю країни.

Технічні структури АСУ ТП також значною мірою залежать від надійності технічних засобів та їх стандартизації та уніфікації. Перш ніж описувати типові технічні структури АСУ ТП, розберемося спочатку з термінами «типізація» і «уніфікація». Типізація — це раціональний вибір і зведення різноманітних конструкцій машин, устаткування, пристроїв і т. п. в обмежене число оптимальних типів, що володіють істотними якісними характеристиками. По суті, це задача оптимізації з певними обмеженнями. Типізація передує уніфікації, яка передбачає зведення різноманітних видів виробів і процесів їх виготовлення до раціонального мінімуму за розмірами, формою, властивостями тощо. Уніфікація вигідна тим, що контрольно-вимірювальні прилади і керуючі комп'ютери є спільними. стандартизований вхід і/або вихід сигналів постійного струму з такими значеннями, як 0-5, 0-20 і 4-20 мА. У контексті АСУ ТП зазвичай використовуються уніфіковані сигнали постійного струму 4-20 мА.

1.6 Математичне забезпечення та алгоритми АСУ ТП

Математичне забезпечення АСУ ТП складається з набору математичних методів, моделей і алгоритмів, які використовуються при розробці та експлуатації цих систем. Оскільки обчислювальна технологія все більше інтегрується в АСУ ТП, значення її математичної підтримки разом із програмним забезпеченням, побудованим на ній, стає порівнянним, а іноді навіть перевершує вартість технічної підтримки тієї ж системи. У метафоричному сенсі математичне забезпечення можна розглядати як «ідеологічний зміст» або «м'який товар» АСУ ТП, на відміну від «твердого товару», який надає технічна підтримка. Управління об'єктом охоплює набір суттєвих операцій, необхідних для цілеспрямованого впливу на об'єкт. Ці операції включають такі завдання, як автоматичний контроль (отримання інформації), аналіз (прийняття рішень) і виконання (здійснення керуючих впливів). У сучасних АСУ ТП процеси інформаційного пошуку та здійснення керуючих впливів здійснюються автоматично за допомогою технічних засобів захисту. Коли мова йде про генерацію та прийняття рішень для управління об’єктами, як правило, необхідно визначити оптимальний (або принаймні раціональний) алгоритм їх реалізації. Щоб досягти цього, кожне завдання управління має бути сформульовано математично.

Математична постановка будь-якої задачі оптимального керування складається з двох компонентів: математичної моделі об’єкта та критерію керування. Математична модель являє собою систему математичних співвідношень, які описують поведінку керованого об'єкта та умови (включаючи збурення та обмеження), за яких він працює. Для аналітичного вираження моделі необхідні знання фізичної природи об’єкта керування, його структури та конструктивних характеристик. Хоча математична модель завжди є наближенням і не враховує всі явища, що відбуваються всередині об’єкта, її можна ефективно використовувати для визначення керуючих впливів на різні значення параметрів об’єкта керування. Це може бути досягнуто в синхронізації з розвитком технологічного процесу або шляхом випереджувального аналізу, якому сприяє висока швидкість сучасних систем обробки інформації. Якщо характеристики об'єкта управління зазнають змін, то адекватність

моделі об'єкта повинна постійно оцінюватися та оновлюватися на основі поточної інформації про стан об'єкта. За допомогою математичної моделі різноманітні керуючі впливи застосовуються для виявлення та реєстрації відповідей моделі з наступним відбором тих впливів, які найкраще задовольняють критерій контролю.

Обробка інформації в МПК передбачає виконання алгоритмів, які втілюють технологічні інструкції для здійснення процесу. Кожен алгоритм, який виконує МПК, певною мірою представляє міркування та розрахунки, які оператор-технолог виконував би за відсутності МПК. Такі алгоритмічні інструкції, виражені формальною мовою математичних формул і логічних умов, диктують послідовність дій, при чому кожна дія відповідає виконанню елементарної операції МПК. Ці елементарні операції охоплюють додавання, віднімання, множення, ділення, логічні операції.

Послідовність дій не довільна, вона дотримується певної методики вирішення завдань. Цей метод іноді спочатку формулюється як математична формула, іноді в словесній або описовій формі або навіть як складний набір логічних умов. У всіх випадках формулювання має бути точним і однозначним, не залишаючи місця для неправильного тлумачення. Мета полягає в тому, щоб отримати остаточний числовий або логічний (дискретний) результат після кінцевої кількості елементарних операцій. Коли ці умови виконуються, інструкція для розв’язування задачі, виражена формальною мовою математичних формул і логічних умов, називається алгоритмом розв’язування задачі. В АСУ ТП також використовуються алгоритми керування. Це формальні інструкції, які диктують, як обробляти інформацію про керований об’єкт для отримання відповідних керуючих впливів. Алгоритм управління, який відображає загальну мету системи управління, часто є складним і може бути розділений на численні підалгоритми, кожен з яких відповідає певному завданню або функції системи управління. Ці підалгоритми пов'язані між собою таким чином, що в різних виробничих сценаріях в дію вступають конкретні ланки загального алгоритму управління. Як результат, багато окремих підалгоритмів не працюють у фіксованій послідовності або хаотично. Замість цього вони організовані в різні ланцюжки на основі змін у виробничій ситуації.

Розроблена ФСА ТП (Функціональна система автоматизації технологічних процесів) дозволяє чітко зрозуміти план вирішення конкретної проблеми.

Алгоритмічна структура зображує алгоритм регулювання температури гарячої води, який для зручності розділений на два під алгоритми. Під Алгоритм А обробляє постійний автоматичний контроль температури гарячої води, представляючи частину процесу вирішення проблеми, що виконується в цьому режимі. З іншого боку, під алгоритм Б виконується за запитом оператора-технолога. Варто зазначити, що обидва під алгоритми взаємопов'язані через спільні дані, що забезпечує їх координацію та узгодженість.

Вирішальним кроком у розвитку цього підходу є побудова спрощеної алгоритмічної структури, зображеної у вигляді блок-схеми на (рис. 1.2).

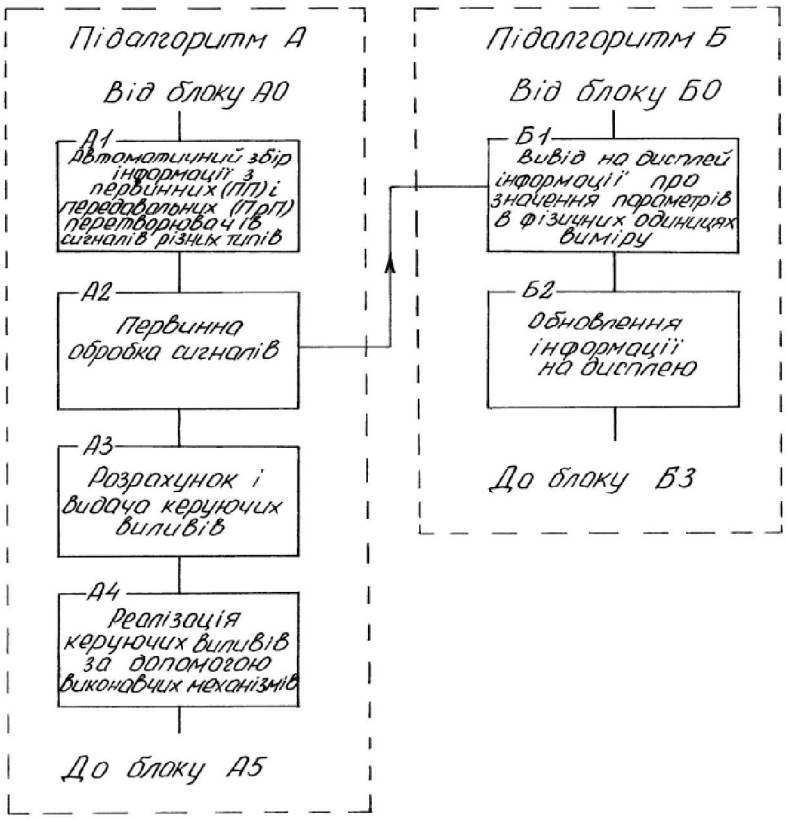

Рисунок 1.2 - Спрощена алгоритмічна структура задачі керування температурою

Зображення переходів дій між блоками в алгоритмічній структурі дотримується певних умовностей. Лінії традиційно використовуються для зображення переходів від одного блоку до іншого. Однак при переході зверху вниз або зліва направо стрілки

не використовуються. Натомість при переході в протилежному напрямку слід розміщувати стрілки. Графічно блоки зазвичай зображують у вигляді прямокутників або ромбів із співвідношенням висоти до ширини 1:1,5. Висота вибирається із серії: 10, 20 або 30 мм, а відстань між блоками завжди встановлюється 10 мм.

Алгоритмічну структуру задачі можна проілюструвати з різними рівнями деталізації. Кожен блок у структурі є спрощеним представленням, а більш детальним модулям відповідають більш детальні блок-схеми. Наприклад, на рисунку 1.3 наведено фрагмент блок-схеми одного з модулів спрощеної алгоритмічної структури, а саме блоку А2 – «Первинна обробка сигналів».

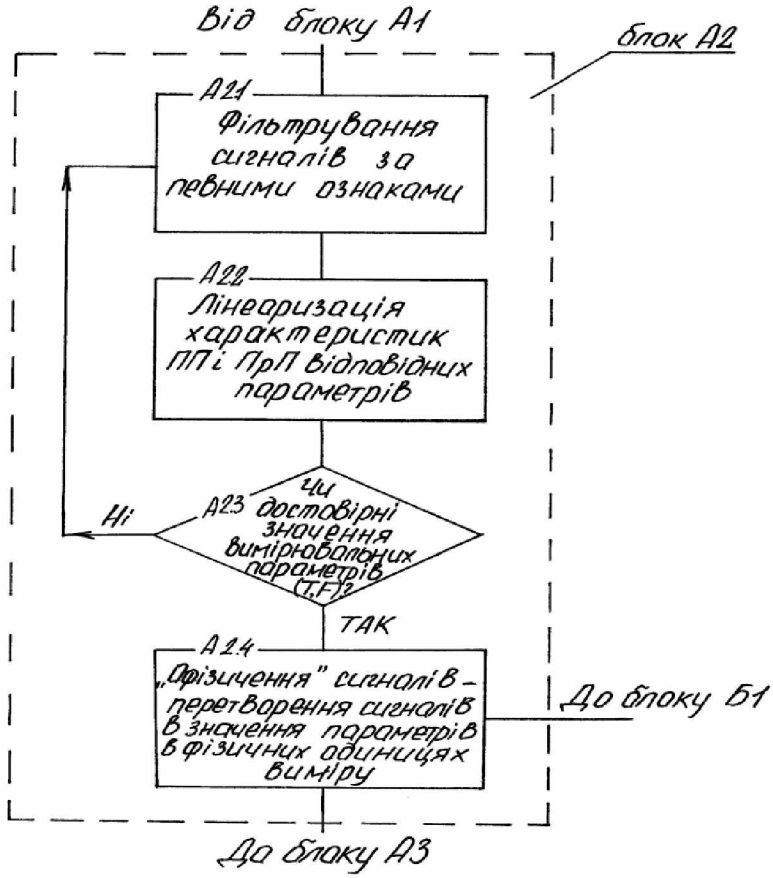

Рисунок 1.3 - Фрагмент блок-схеми спрощеного "Первинна обробка сигналів".

У міру подальшого розвитку алгоритму кожен новий блок описується детально. Це включає математичні формули, логічні умови, взаємозв'язки між ними та часові характеристики виконання окремих блоків. Документація алгоритму розв'язання задачі служить двом цілям.

По-перше, він охоплює концептуальні аспекти, такі як наміри та методи вирішення проблем. По-друге, він служить основою для наступного етапу детальної розробки алгоритму - трансформації прийнятих ідей в набір інтерактивних програм в рамках МПК.

1.7 Класифікація програмного забезпечення АСУ ТП

Програмне забезпечення АСУ ТП включає в себе набір програм, які полегшують виконання всіх функцій системи, забезпечують заплановану роботу технічної підтримки АСУ ТП і сприяють плановому розвитку системи. Кожна програма представляє конкретну реалізацію машинного алгоритму, призначеного для вирішення конкретних проблем. Рівень деталізації в описі програмного забезпечення АСУ ТП залежить від передбачуваного користувача опису. Оперативному персоналу АСУ ТП, особливо операторам-технологам, які можуть не володіти навичками програмування, детальні описи програм не потрібні. Операторам-технологам достатньо мати розуміння того, як працює відповідне обладнання та як виконуються програми на логічному рівні. Цей логічний рівень передбачає роботу з логічними аналогами явищ замість заглиблення в описи фізичного рівня. Таким чином, у спрощеній функціональній схемі ІПК логічний рівень умовно поділяється на три частини: обладнання для виконання програм, програми та дані (рис. 1.4).

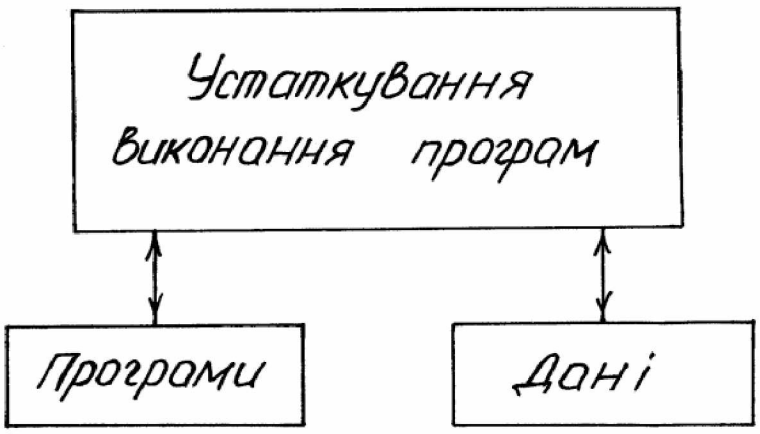

Рисунок 1.4 - Функціональна схема МПК

Використовуючи це спрощення, основна функція МПК зводиться до перетворення даних. Ці дані можна розділити на дві категорії: локальні дані, специфічні для однієї програми, і глобальні дані, застосовні до кількох програм або навіть до всіх конкретних програм у системі АСУ ТП. Приклади даних включають числа або тексти. Частина МПК, призначена програмам, містить набори команд, які визначають послідовність дій, що виконуються з даними для досягнення бажаної мети. По суті, програма складається з послідовності команд, які необхідно виконати для реалізації заданого алгоритму обробки даних.

Якщо програма виконує певну функцію в системі АСУ ТП, її називають функціональною програмою. Простим прикладом такої програми є програма, яка складається з двох команд: (а) введення сигналу від первинного перетворювача передачі для контролю температури відображення отриманого значення температури на дисплеї МПК.

Обладнання для виконання програм у МПК виконує команди програми послідовно. Ці команди підказують введення даних з відповідного обладнання (клавіатура, дисплей, перетворювач передачі тощо), виконують необхідні перетворення даних і виводять їх на різне обладнання (виконавчі механізми, дисплей тощо). Для опису послідовності команд використовуються спеціальні мови програмування, які можуть бути специфічними для певних МПК.

Незалежно від мови програмування, програми АСУ ТП мають три характерні особливості. По-перше, кожна програма АСУ ТП, особливо функціональна, має рекомендації щодо її впровадження. Ці вказівки охоплюють один або декілька з наступних чотирьох режимів виконання програми:

1) активація програми через регулярні проміжки часу;
2) активація програми в певний час доби;
3) активація програми на основі запиту іншої програми;
4) активація програми за запитом оператора-технолога;

Другою відмінною рисою програм АСУ ТП є їх велика кількість і велика кількість. Оскільки кожна програма активується відповідно до власних правил, бувають ситуації, коли кілька програм вимагають виконання одночасно. У таких

випадках обладнання для виконання програм визначає пріоритетність програм на основі їх важливості, надаючи пріоритет найважливішій програмі на даний момент.

Третя особливість програм АСУ ТП передбачає використання різних типів пам'яті для їх зберігання, включаючи енергонезалежне запам'ятовуюче обладнання, енергонезалежне запам'ятовуюче обладнання, магнітні диски, дискети та ін. Час виконання програм що зберігається в різних типах пам'яті обладнання значно відрізняється.

Термін «програмне забезпечення» або «програмне забезпечення в АСУ ТП» охоплює всі програмні засоби, що беруть участь у функціонуванні системи АСУ ТП. Програмне забезпечення АСУ ТП може складатися з багатьох елементів і мати складну логічну схему, яка регулює їх взаємодію. Проте спрощена схема програмного забезпечення АСУ ТП має простий вигляд і базується на введених раніше концепціях. Природно, що основними компонентами цієї схеми є «програми» і «дані» (див. рис. 1.5).

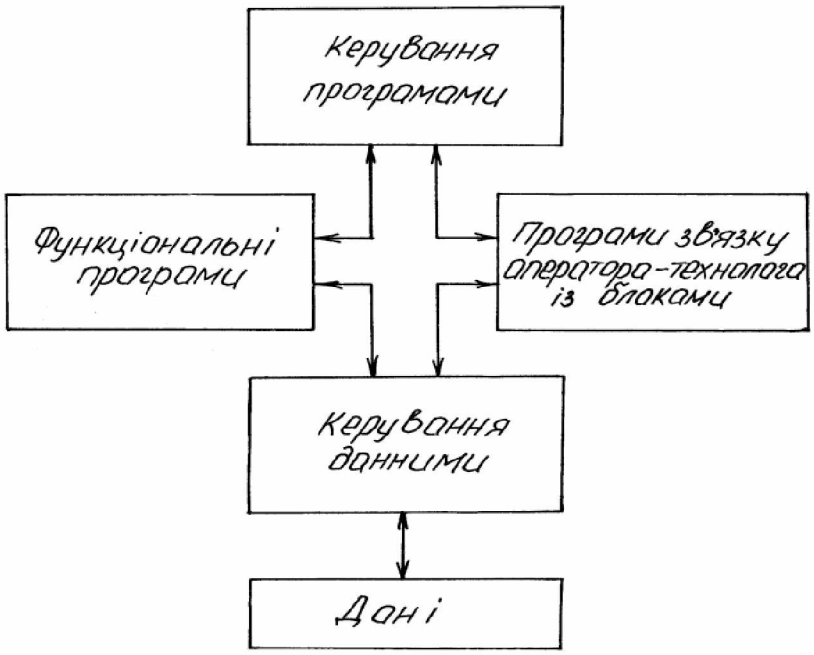

Рисунок 1.5 - Схема програмного забезпечення

Як згадувалося раніше, виконання програм обладнанням виходить за рамки простого виконання команд. Обладнання відповідає за виконання завдань, пов'язаних із виконанням великої кількості «функціональних програм» згідно з відповідними

правилами. Крім того, він виконує функції, пов'язані з підготовкою даних до обробки. Ці функції реалізовані програмно і є частиною програмного забезпечення АСУ ТП, яке можна розділити на два блоки: «керування програмою» і «керування даними». Блок «керування програмами» відповідає за організацію виконання та взаємодії всіх програм ПЗ АСУ ТП. З іншого боку, блок «керування даними» обробляє зберігання «даних» у відповідних пристроях пам'яті та надає «дані» «функціональним програмам» у необхідному форматі. Оператор-технолог взаємодіє з блоками «управління програмами» та «управління даними» через комунікаційні програми, які призначені для зручного спілкування оператора-технолога з МПК.

Програмне забезпечення АСУ ТП поділяється на дві категорії: загальне програмне забезпечення і спеціальне програмне забезпечення. Загальне програмне забезпечення – це складова програмного забезпечення, що постачається в комплекті з АСУ ТП і включає програми організації функціонування технічних засобів, сервісні програми, розробку спеціального програмного забезпечення для АСУ ТП. До складу ПЗ АСУ ТП входять такі програми:

Програма диспетчера відіграє вирішальну роль у координації роботи окремих програм та ефективній організації черг програм. Він відповідає за безперебійну роботу і своєчасне виконання різних програм.

Інші програми, що входять до загального ПЗ АСУ ТП:

Програми для керування конкретним обладнанням МПК: ці програми керують контролем та керуванням окремими компонентами обладнання.

Допоміжні програми: ці програми надають такі корисні функції, як створення таблиць, друк результатів розрахунків і виконання різних допоміжних завдань.

Стандартні підпрограми: ці підпрограми пропонують попередньо визначені обчислення для часто зустрічаються функцій, таких як натуральні логарифми, синуси тощо.

Перекладачі: ці програми сприяють перекладу алгоритмів, написаних алгоритмічними мовами, у формат, який може виконувати МПК. Програми тестування: ці програми призначені для перевірки та діагностики всіх пристроїв МПК

у безперервному та періодичному режимах, забезпечуючи їх належне функціонування.

Спеціальне програмне забезпечення АСУ ТП розроблено спеціально для реалізації інформаційно-управлінських функцій у конкретній системі АСУ ТП. Побудований на базі загального програмного забезпечення . Розробка спеціального програмного забезпечення продовжує процес алгоритмізації, використовуючи алгоритмічну систему, блок-схеми та фактичні алгоритми виконання функцій як вихідні дані.Під час створення спеціального програмного забезпечення необхідно звернути увагу на два основні аспекти.

По-перше, програмний комплекс структурується шляхом визначення складу програм та їх взаємодії. Слід зазначити, що кількість окремих спеціальних програм може не відповідати кількості функціональних завдань або виконаних алгоритмів. Алгоритми деталізуються до рівня, коли вони можуть бути виконані відповідно до заданих характеристик, в результаті чого складається програма і схема їх взаємодії.

Другий аспект передбачає організацію взаємодії між програмами, яка включає в себе одну програму ініціювання роботи іншої програми та обмін даними між програмами.Процес розробки спеціального програмного забезпечення для АСУ ТП є трудомістким і відповідальним завданням. Перекладачі відіграють важливу роль, дозволяючи програмістам писати окремі модулі або блоки різними мовами програмування, забезпечуючи ефективну розробку та продуктивність у реальному часі. Розробка функціональних програм, розроблених спеціально для АСУ ТП, передбачає використання мов програмування, однаково зрозумілих як програмістам, так і технологам-операторам.

1.8 Нормативно правова база

В ході виконання дипломної роботи я проаналізував нормативно-правову база, та стандарти МАГАТЕ які регламентують захист автоматизованих систем управління технологічними процесами (АСУ ТП) в енергетичних системах, включає такі закони та нормативні акти:

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (№ 2163-VIII від 05.02.2015) - цей закон встановлює загальні принципи та вимоги щодо захисту інформації в інформаційно-телекомунікаційних системах. Він стосується також захисту АСУ ТП від кібератак та інших загроз.
2. Закон України "Про критичну інфраструктуру" (№ 2258-VIII від 14.07.2017) - цей закон встановлює вимоги до захисту критичної інфраструктури, до якої можуть відноситись ядерні установки та АСУ ТП. Він передбачає необхідність розробки та впровадження заходів з кібербезпеки.
3. Постанова Кабінету Міністрів України "Про затвердження Правил забезпечення кібербезпеки критичної інфраструктури" (№ 594 від 06.06.2018) - ця постанова встановлює правила та вимоги щодо забезпечення кібербезпеки критичної інфраструктури, включаючи ядерні установки та АСУ ТП.
4. Нормативні документи та стандарти Національного інституту стандартів (Держстандарту), які стосуються кібербезпеки та захисту АСУ ТП. Деякі з них включають:

● ДСТУ ISO/IEC 27001:2015 "Системи управління інформаційною безпекою. Вимоги"

● ДСТУ ISO/IEC 27002:2015 "Системи управління інформаційною безпекою. Кодекс практики"

● ДСТУ ISO/IEC 27005:2015 "Системи управління ризиками інформаційної безпеки. Рекомендації з використання"

● ДСТУ ISO/IEC 27019:2018 "Системи управління інформаційною безпекою. Рекомендації щодо захисту інформації в галузі енергетики"

● ДСТУ ISO/IEC 15408:2015 "Системи управління інформаційною безпекою. Оцінка відповідності. Частини 1-3".

5. Закон України "Про ядерну енергетику" (№ 1636-VII від 06.02.2014) - цей закон встановлює загальні принципи, права та обов'язки у галузі ядерної енергетики. Він регулює управління технологічним процесом в ядерних установках, включаючи використання АСУ ТП.

6. Закон України "Про ядерну безпеку" (№ 250/95-ВР від 03.10.1995) - цей закон встановлює правила та вимоги щодо забезпечення ядерної безпеки в Україні. Він вимагає впровадження системи управління ядерною безпекою, включаючи АСУ ТП, для контролю технологічних процесів у ядерних установках.

7. Національні стандарти та норми в галузі ядерної енергетики, які включають вимоги до АСУ ТП, зокрема:

- ДСТУ IEC 60880:2014 "Системи контролю та автоматизації для ядерних об'єктів енергетики" - цей стандарт встановлює вимоги до систем контролю та автоматизації, включаючи АСУ ТП, для ядерних об'єктів енергетики.
- ДСТУ IEC 61513:2011 "Технологічні процеси ядерних установок. Вимоги до систем управління" - цей стандарт встановлює вимоги до систем управління технологічними процесами в ядерних установках, включаючи АСУ ТП.
- ДСТУ IEC 62566:2014 "Системи інформаційні технології для ядерних об'єктів енергетики" - цей стандарт встановлює вимоги до систем інформаційних технологій, включаючи АСУ ТП, для ядерних об'єктів енергетики.

8. Стандарти безпеки МАГАТЕ:

- Safety Series No. NS-G-1.1 "Радіаційна безпека для ядерних енергетичних установок" - цей стандарт встановлює загальні принципи та вимоги щодо радіаційної безпеки в ядерних енергетичних установках, включаючи використання АСУ ТП.
- Safety Series No. NS-G-1.3 "Процес безпеки у ядерних енергетичних установках" - цей стандарт надає рекомендації щодо управління безпекою в ядерних енергетичних установках, включаючи АСУ ТП та інші системи управління.

9. Рекомендації МАГАТЕ:

- Safety Series No. SSG-7 "Вимоги до автоматизованих систем управління ядерною безпекою" - ці рекомендації встановлюють вимоги до проектування, впровадження та експлуатації автоматизованих систем управління ядерною безпекою, включаючи АСУ ТП.
- Safety Series No. SSG-9 "Вимоги до безпеки кібербезпеки для ядерних установок" - ці рекомендації надають вимоги та рекомендації щодо кібербезпеки АСУ ТП для ядерних установок.

Ця нормативно-правова база, стандарти МАГАТЕ встановлють вимоги та рекомендації з кібербезпеки та захисту АСУ ТП в Україні, зокрема в ядерних установках, з метою забезпечення конфіденційності, цілісності та доступності інформації, а також захисту від кібератак та інших загроз.

Висновок до першого розділу

У даному розділі було розглянуто питання автоматизованих систем керування технічними процесами. Дослідження показали, що впровадження автоматизованих систем керування є важливим кроком у покращенні ефективності технічних процесів в різних сферах діяльності. Автоматизовані системи керування дозволяють замінити ручний контроль та управління технічними процесами на автоматичні методи, що забезпечує більш точний, швидкий і надійний контроль за роботою системи. Вони забезпечують збільшення продуктивності, зниження витрат і покращення якості виробництва. Одним з ключових переваг автоматизованих систем керування є можливість інтеграції з іншими технологіями та системами, такими як сенсори, мережі зв'язку та штучний інтелект. Це дозволяє створювати розумні системи, які можуть адаптуватися до змінних умов і оптимізувати свою роботу для досягнення максимальних результатів. Застосування автоматизованих систем керування технічними процесами має широкий спектр застосування, включаючи виробництво, енергетику, транспорт, медицину та багато інших галузей. Вони можуть бути успішно використані для контролю та керування різними процесами, від простих до складних.

Узагальнюючи, автоматизовані системи керування технічними процесами є важливим інструментом для досягнення оптимального контролю, ефективності та надійності в різних галузях діяльності. Впровадження таких систем може принести значні переваги, включаючи зниження витрат, покращення якості та збільшення продуктивності. Прогрес у розробці технологій, таких як штучний інтелект, сприяє появі нових можливостей для розвитку автоматизованих систем керування, що дає надію на подальше зростання їх ефективності та широке використання у майбутньому.

РОЗДІЛ 2
РЕАЛІЗАЦІЯ КОМП'ЮТЕРНОЇ БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ ТА ПОРУШНИКА, ВРАЗЛИВОСТІ АСУ ТП У ЯДЕРНИХ УСТАНОВКАХ

2.1 Політика, план та елементи комп'ютерної безпеки на АЕС

Політика забезпечення комп'ютерної безпеки встановлює в організації цілі комп'ютерної безпеки високого рівня. Ця політика має відповідати належним регулюючим вимогам. Вимоги політики забезпечення комп'ютерної безпеки слід детально викласти в документи нижчого рівня, які будуть використовуватися при здійсненні та контролі цієї політики. Крім того, ця політика має бути:

- здійсненної;
- досяжною;
- допускає аудит.

План забезпечення комп'ютерної безпеки розробляється з метою здійснення цієї політики у формі організаційних ролей, обов'язків та процедур. У цьому плані визначаються та детально описуються засоби досягнення цілей комп'ютерної безпеки на установці, і є частиною загального .У плані мають бути викладені основні дії у термінах сприйнятливості до вразливостей, захисних заходів, аналізу наслідків та заходів пом'якшення наслідків з метою встановлення та збереження на прийнятному рівні кібер-ризику на ядерній установці та сприяння поверненню в безпечний експлуатаційний режим.

Кожен індивідуальний елемент плану має на меті досягнення конкретних цілей та вирішення певних завдань відповідно до встановленою політикою забезпечення комп'ютерної безпеки. Мінімальний зміст та розбивка за пунктами ПЗКБ пропонуються у наступних нижче підрозділах:

а) Організація та обов'язки:

1) організаційні схеми;

2) відповідальні особи та обов'язки по звітності;

3) процес періодичного розгляду та затвердження.

b) Управління активами:

1) перелік всіх комп'ютерних систем;

2) перелік всіх програм, встановлених на комп'ютерних системах;

3) схема мережі, включаючи всі з'єднання із зовнішніми комп'ютерними системами.

c) Оцінка ризику, уразливості та дотримання вимог:

1) періодичність розгляду та повторної оцінки плану забезпечення безпеки;

2) самооцінка (включаючи процедури тестів на можливість проникнення у систему);

3) процедури аудиту та виявлення та усунення недоліків;

4) дотримання регулюючих та законодавчих вимог.

d) Проектування з урахуванням вимог безпеки та управління конфігурацією системи:

1) основні засади архітектури та проектування;

2) вимоги, пов'язані з різними рівнями безпеки;

3) формалізація вимог комп'ютерної безпеки для постачальників та виробників;

4) безпека всього життєвого циклу системи;

e) Експлуатаційні процедури безпеки:

1) контроль доступу;

2) безпека даних;

3) безпека ліній та каналів зв'язку:

4) безпека платформ та прикладних програм ;

5) моніторинг систем;

6) підтримка комп'ютерної безпеки;

7) дії у разі інцидентів;

8) забезпечення стійкості функціонування;

9) резервне копіювання системи.

f) Менеджмент персоналу:

1) перевірка;

2) навчання;

3) атестація;

4) припинення дії договору/кадрова перестановка.

Вищевикладені дані становлять основу розробки ПЗКБ. У доповнення до цієї основи є численні довідкові матеріали, причому основними міжнародними довідковими матеріалами є документи ISO 27001 для систем менеджменту інформаційної безпеки та ISO 27002 для рекомендацій з практичної реалізації. У той час як більшість перерахованих вище елементів однаково у планах забезпечення комп'ютерної безпеки для будь-яких видів діяльності чи галузей промисловості, існують певні нюанси їхньої практичної реалізації на ядерних установках.

2.1.1 Фізична безпека

План забезпечення фізичної безпеки та ПЗКБ мають доповнювати один одного. Для комп'ютеризованих активів існують вимоги до щодо фізичного контролю доступу, і так само, погіршення електронних характеристик може призвести до деградації або втрати певних функцій фізичного захисту. Сценарії атак цілком можуть включати координацію як електронної, і фізичної атаки. Групам, відповідальним за план забезпечення фізичної безпеки та ПЗКБ, слідує інформувати один одного та координувати свої зусилля з метою забезпечення узгодженості планів у процесі їх розробки та розгляду.

2.1.2 Кадрова безпека

Крім поінформованості та навчання, дуже важливими для забезпечення надійної комп'ютерної безпеки є також інші аспекти безпеки, які зазвичай розглядаються в області кадрової безпеки. Необхідні положення щодо організації відповідного рівня перевірки, зобов'язань щодо конфіденційності, процедур завершення дії контрактів та визначення необхідної професійної компетентності має бути скоординовані між керівництвом з комп'ютерних питань та керівництвом з питань кадрової безпеки. Зокрема для персоналу, виконує важливі обов'язки у сфері

безпеки (системні адміністратори, група безпеки), може знадобитися перевірка більш високого рівня

2.1.3 Класифікація комп'ютерних систем на АЕС

Комп'ютери та комп'ютерні системи означають обчислювальні, комунікаційні пристрої, контрольно-вимірювальну апаратуру та пристрої керування, є функціональними елементами ядерної установки. Комп'ютерними функціями, що становлять основний інтерес, є процеси управління та обробки даних, пов'язані з безпекою та фізичною безпекою. Інші комп'ютерні функції можуть представляти інтерес у зв'язку з підтримкою цих функцій та можливим погіршенням безпеки внаслідок вторинних чи непрямих ефектів або на загальну продуктивність установки. Нижче представлений далеко не вичерпний список комп'ютерних систем, які можуть бути на ядерних установках і стосуватися цілях цих керівних матеріалів. Вони класифіковані окремо відповідно до їх важливості з погляду безпеки та фізичної безпеки. Обидві ці класифікації слід брати до уваги при визначенні відповідного застосовного рівня безпеки та при аналіз з метою оцінки ризику. Слід також мати на увазі, що деякі функції явно перекриваються у плані актуальності з погляду безпеки та фізичної безпеки.

У нормах безпеки МАГАТЕ обладнання ядерних установок поділено на категорії згідно з його функціями, як показано на (рис 2.1).

Рисунок 2.1 - Устаткування станції з погляду функцій безпеки.

Обладнання станції

- Системи, важливі для безпеки
- Системи безпеки
- системи захисту: контрольно-вимірювальні прилади та системи управління та захисту (КВП та СУЗ), які використовуються для виконання автоматичних дій із захисту реактора та станції;
- системи обслуговування пристроїв безпеки: КВП та СУЗ, що здійснюють дії щодо забезпечення безпеки, ініційовані системами захисту та ручними спрацьовуваннями;
- Допоміжні засоби системи безпеки: КВП та СУЗ для систем аварійного енергопостачання.
- Системи, пов'язані з безпекою
- системи управління технологічними процесами: КВП та СУЗ для управління роботою станції;
- КВП та СУЗ у приміщенні щита управління, включаючи системи аварійної сигналізації;
- Комп'ютерні системи управління технологічними процесами, здійснюють збір та підготовку інформації для приміщення щита управління;
- КВП та СУЗ для поводження з паливом та його зберігання;
- протипожежні системи;
- Системи контролю доступу;
- Інфраструктура голосового зв'язку та передачі даних.
- Системи, не важливі для безпеки
- Системи керування для функцій, не важливих для безпеки (наприклад, знесолення).

Слід враховувати також комп'ютерні системи, які обов'язково входять до складу обладнання станції, але можуть впливати на безпеку. Устаткування, що не відноситься до технологічного обладнання станції:

- Засоби автоматизації діловодства

• Системи допусків до роботи та робочих завдань: Системи, що забезпечують координацію виробничої діяльності з метою створення сприятливої робочої обстановки.

• Інженерно-технічні системи та системи обслуговування: системи, що забезпечують виконання детальних операцій з експлуатації станції, операцій обслуговування та технічної підтримки.

• Системи керування конфігурацією: системи, що відстежують конфігурацію станції, включаючи моделі, версії та частини обладнання, встановлені на ядерній установці.

• Системи керування документацією: системи, що використовуються для зберігання та пошуку інформації про станцію, наприклад, креслень, протоколів нарад.

• Інтранет: система, яка забезпечує доступ до всієї документації станції – як технічної, так і адміністративної – згідно з принципом службової потреби. Доступ зазвичай надається тільки в режим зчитування інформації.

- Зовнішні канали зв'язку

• Електронна пошта: система, що використовується для обміну інформацією з зовнішніми партнерами.

• Відкритий веб-сайт: Система, яка використовується для надання користувачам Інтернету інформації про встановлення.

• Дистанційний доступ/доступ третіх осіб: системи, що дозволяють строго контрольований доступ ззовні до певних функцій на майданчику.

2.2 Рівні безпеки та поділ на зони

Рівні безпеки – це абстракція, яка визначає ступеня захисту фізичної безпеки, необхідні для різних комп'ютерні системи на установці. Для кожного рівня при диференційованому підході будуть потрібні різні набори захисних заходів, що задовольняють вимоги фізичної безпеки цього рівня. Деякі захисні заходи

застосовуються до всіх комп'ютерних систем всіх рівнях, у той час як інші є специфічними для певного рівня.

Модель рівня фізичної безпеки припускає більш просте розподіл захисних заходів для різних комп'ютерних систем на основі категоризації системи (віднесення її до певного рівня) та визначення набору захисних заходів, які відповідають цьому рівню. Рівні та пов'язані з ними захисні заходи мають бути належними чином документовані до ПЗКБ.

2.2.1 Зони

Зони – це логічне та фізичне поняття, що дозволяє групувати комп'ютерні системи для адміністративного управління, комунікації та застосування захисних заходів. Зональна модель дозволяє об'єднувати групи для цілей адміністрування та застосування захисних заходів комп'ютери, мають однакову або аналогічну важливість для безпечної та надійної експлуатації станції.

При застосуванні зональної моделі слід дотримуватися наступних рекомендації:

- кожна зона включає системи, що мають однакову або порівнянну важливість для фізичної безпеки та безпеки установки;
- системи, що належать до однієї зони, мають аналогічні потреби щодо захисних заходів;
- різні комп'ютерні системи, що належать до однієї зони, утворюють область надійного зв'язку для внутрішньої комунікації в межах цієї зони;
- зональні межі вимагають механізмів розв'язки для потоків даних на основі політики, яка залежить від конкретної зони;
-з метою покращення конфігурації зони можуть бути поділені на субзони.

Оскільки зони складаються із систем з однаковою чи порівнянною важливістю для безпеки та фізичної безпеки установки, кожної зоні може бути присвоєний рівень, що вказує на захисні заходи, що підлягають застосування всіх комп'ютерних систем у цій зоні. Однак зв'язок між зонами та рівнями не взаємно однозначна; у тих

випадках, коли для кількох зон потрібен однаковий ступінь захисту, однаковий рівень може бути присвоєний кільком зонам. Зони відображають логічне та фізичне групування комп'ютерних систем, тоді як рівні представляють ступінь необхідного захисту.

Зональна модель має бути належним чином документована в ПЗКБ, включаючи короткий огляд всіх комп'ютерних систем, всіх відповідних ліній зв'язку, всіх зональних перетинів та всіх зовнішніх підключень.

2.3 Проектна загроза та моделі порушників та атак.

Важливим інструментальним засобом, що використовується для визначення рівнів загрози та як основа для розробки засобів забезпечення Безпека, є проектна загроза. ПЗ є заяву про властивості та характеристики потенційних порушників (Внутрішніх або зовнішніх). ПЗ розробляється на основі надійної інформації, отриманої із застосуванням спеціальних засобів, але вона не призначена для того, щоб стати заявою про фактичні переважаючі погроз. Виходячи з сучасних уявлень про характер загроз, ПЗ є найбільш серйозною загрозою, на захист від якої повинна бути розрахований захист установки. Держави використовують ПЗ у свої системах регулювання для визначення належного розподілу ресурсів з метою захисту ядерного матеріалу та ядерних установок від ворожих дій. Слід розглянути можливість включення до таких сценаріїв загроз або автономних атак з використанням комп'ютерних систем/атак, спрямованих проти таких систем, або координованих атак, які включають використання комп'ютерних систем.

При розробці моделей атак можна враховувати різні можливі варіанти. Ядерна установка може зазнати атаки з метою:

- підготовки до подальшої координованої атаки, спрямованої на організацію саботажу на станції та/або вилучення ядерного матеріалу;
- Створення загрози здоров'ю людей або екологічної безпеки;
- Організації атаки, спрямованої проти іншого майданчика;
- Створення атмосфери хаосу та страху;

- Отримання фінансової вигоди для злочинного угруповання;

- Створення нестійкостей на основних ринках та досягнення прибутків для певних ринкових гравців.

Залежно від завдань чи цілей атаки виконавець атаки буде прагнути скористатися різними системними вразливістю. Такі атаки можуть призводити до:

- несанкціонований доступ до інформації (втрата конфіденційності);

- перехоплення та зміни інформації, програмного забезпечення, апаратних засобів і т.д. (Втраті цілісності);

- блокування ліній передачі даних та/або відключення систем (втраті працездатності);

- несанкціонованого проникнення в системи передачі даних або комп'ютери (втрата надійності).

Всі ці аспекти можуть мати серйозні наслідки для функціональних можливостей комп'ютерних систем та надавати на них серйозний вплив, що може створювати пряму чи непряму загрозу безпеці та фізичній безпеки установки. Під час розробки сценаріїв атак слід враховувати технологічні тенденції та легкість доступу при здійсненні атак на технології.

Далі буде представлено можливий набір профілів даних виконавців атак, основна увага приділяється внутрішнім загроз, що походять від внутрішніх

2.3.1 Внутрішні загрози АСУ ТП ядерних установок

Таємний агент.

Ресурси: Сприяння «соціальної інженерії».Доступ до системи на певному рівні.Є доступ до системної документації та експертним знанням.

Тривалість: Може бути різною, але, як правило, не може становити багато годин.

Інструментальні: Наявність доступу, знання програмування та системної архітектури: можливе знання паролів, що діють. Можливість впровадження спеціально розроблених програм «backdoor» та/або програм-троянів.

Мотивація: Розкрадання ділової інформації, технологічних секретів, особисті дані. Економічна вигода (продаж інформації).Шантаж.

Розгніваний службовець.

Ресурси: Середні/потужні ресурси. Доступ до системи на певному рівні. Наявність системної документації та експертних знань щодо конкретних видів діяльності та експлуатації систем.

Тривалість: Може бути різною, але, як правило, не може становити багато годин.

Інструментальні: Наявність доступу, знання програмування та системної архітектури. Можливе знання діючих паролів. Здатність вводити «дилетантські» інструментальні засоби або скрипти (потенційно більше складні у разі наявності певних комп'ютерних навичок).

Мотивація: Помста, руйнування, створення хаосу. Розкрадання ділової інформації. Здивувати роботодавця/ інших службовців. Завдати шкоди репутації або призвести до втрати довіри.

2.3.2 Зовнішні загрози АСУ ТП ядерних установок

Хакер-аматор.

Ресурси: Кваліфікація може бути різною, але, як правило, вона невисока. Слабке знання систем, крім пов'язаного з відкритою інформацією.

Тривалість: Значна, але з невисокою наполегливістю.

Інструментальні: Широкодоступні скрипти та інструментальні засоби. Можлива

певна доопрацювання інструментальних засобів.

Мотивація: Розваги, підтвердження статусу. Випадковий вибір мети. Можливість скористатися «легкою здобиччю».

Держава.

Ресурси: Великі ресурси та експертні знання. Діяльність зі збору інформації з використанням спецзасобів. Можливий досвід навчання / експлуатації в зв'язки із системою.

Тривалість: Різна.

Інструментальні: Групи підготовлених кіберекспертів. Складні інструментальні засоби. Можуть використовуватися колишні/ працюючі службовці. "Соціальна інженерія".

Мотивація: Збір інформації з використанням спецзасобів. Створення точок доступу для наступних дій. Розкрадання технології.

Войовничий противник ядерної енергетики.

Ресурси: Обмежені ресурси, але може бути фінансова підтримка таємних каналів. Доступ до інструментальним засобам кіберспільноти. Слабке знання систем, крім пов'язаного з відкритою інформацією.

Тривалість: Різна.

Інструментальні: Є комп'ютерні навички. Можлива підтримка зі сторони спільноти хакерів. "Соціальна інженерія".

Мотивація: Переконаність у місії порятунку світу. Розхитування громадської думки щодо певним питанням. Перешкода діловим операціям.

Терорист.

Ресурси: Різноманітні навички. Можливий досвід навчання / експлуатації в зв'язки із системою.

Тривалість: Значна, з дуже високою наполегливістю.

Інструментальні: Скрипти, інструментальні засоби власної розробки. Можуть бути використані "Наймані хакери". Можуть використовуватися колишні/ працюючі службовці. "Соціальна інженерія".

Мотивація: Збір інформації з використанням спецзасобів. Створення точок доступу

для наступних дій. Створення хаосу. Помста. Вплив на суспільна думка (Створення обстановки страху).

Тут наведено типи виконавців атак пов'язуються з наявними в них ресурсами, тривалістю атаки, інструментальними засобами, які, ймовірно, будуть використовуватися, та мотивацією виконавців атак. Профілі даних необхідно адаптувати з урахуванням конкретних типів установок. Тому необхідно організувати належний процес збору даних з використанням спеціальних засобів для забезпечення повноти та актуальності матриці даних про виконавців атак на кожній установці.

2.3.3 Приклади атак на АСУ ТП в ядерних установках та їх наслідки

У таблиці 2.1. наведено приклади систем, які можуть бути на ядерній установці. У ній вказані потенційні наслідки успішних атак на аналізовані системи, відповідні наслідки для встановлення.

Таблиця 2.1

Наслідки атак на типові системи на ядерених установках

Система	Наслідки для комп'ютерної безпеки	Потенційний вплив на систему
Система захисту реактора	Втрата цілісності критичних для безпеки програмного забезпечення/даних. Втрата функціональної готовності.	КРИТИЧНІ Погіршення безпеки станції, радіоактивний викид.

Продовження таблиці 2.1

Система	Наслідки для комп'ютерної безпеки	Потенційний вплив на систему
Система управління технологічним процесом	Втрата цілісності пов'язаних з управлінням програмного забезпечення/даних. Втрата функціональної готовності.	ЗНАЧНІ Погіршення експлуатації станції.
Система допусків до роботи та робочих завдань	Втрата цілісності даних та експлуатаційної готовності системи.	СЕРЕДНІ Неправильні дії у відносинах компонентів. Порушення нормального режиму експлуатації та обслуговування.
Система фізичного контролю доступу	Втрата експлуатаційної готовності та цілісності систем доступу на майданчику. Втрата конфіденційності даних про доступ.	ЗНАЧНІ Надання доступу особам, які не мають відповідного дозволу. Особи, яким дозволено доступ, не мають можливості отримати доступ до необхідних їм зон.

Продовження таблиці 2.1

Система	Наслідки для комп'ютерної безпеки	Потенційний вплив на систему
Система управління документообігом	Втрата конфіденційності, доступності та цілісності даних.	СЕРЕДНІ Інформація використовується для планування більше серйозних атак.
Електронна пошта	Втрата конфіденційності, цілісності та готовності.	НЕЗНАЧНІ Зростання адміністративною навантаження. Труднощі повсякденної роботи.

2.4 Моделі атак на АСУ ТП та ІКС у ядерних установках.

Як зазначено вище, характер та форма атак з використанням комп'ютерів, захист яких необхідно забезпечувати, може бути найрізноманітнішими. Хоча типи атак можуть відрізнятися, до їх наслідків
на високому рівні відносяться:

- несанкціонований доступ до інформації або її перехоплення (втрата конфіденційності);
- несанкціонована модифікація інформації, програмного забезпечення забезпечення, апаратних засобів і т.д. (втрата цілісності);
- блокування ліній передачі даних та/або відключення систем (втрата готовності).

При розробці профілактичних заходів, спрямованих проти комп'ютерних атак, дуже важливо розуміти характер атак та потенційних місць, які можуть використовуватися при атаці або виконавцями атак для отримання відповідної інформації та доступу до комп'ютерних системам, що є метою атак. Хоча наведені приклади атак є вигаданими, вони пов'язані з можливими сценаріями, розробленими на основі аналогічних атак, зафіксованих у інших галузях промисловості. Продумування таких сценаріїв – це хороший спосіб забезпечення того, щоб у плані забезпечення безпеки враховувалася динаміка мінливої обстановки щодо загроз.

Добре спланована комп'ютерна атака складається з низки етапів.Ці етапи включають:

- визначення мети;
- вивчення обстановки;
- доступ до системи / порушення її нормальної роботи;
- виконання атаки;
- приховування слідів на підтримку заперечення винності.

У наступних підрозділах перераховані три передбачуваних сценарію комп'ютерних атак. Перший сценарій, однією з цілей якого є збір інформації, що може розглядатися як підготовчого стосовно наступних двох сценаріїв.

2.4.1 Сценарій 1 – збір інформації на підтримку зловмисної дії

Мета атаки – отримати фізичний доступ до контрольованих (з обмеженим доступом) зон установки для того, щоб підтримати наступну атаку.

При цьому інтерес представляє особа, яка контролює карти доступу та визначальний порядок доступу. Для отримання фізичного доступу до зон обмеженого доступу необхідно порушити нормальну роботу комп'ютера, управляючого картами доступу, та порушити нормальну роботу системи керування кодами доступу. Виконавець атаки має намір діяти як субпідрядника, що постачає частини обладнання. Можливими цілями при збиранні інформації на підтримку атаки є:

- особиста інформація для подальшого здирництва або «соціальної інженерії»;

- проектна документація системи контролю доступу;
- стратегічні та інженерно-технічні плани систем безпеки або інших відповідних зон станції;
- графіки роботи - графік роботи станції, розпорядок дня, хто працює, коли вони працюють, хто у відпустці, коли відбуваються певні зміни;
- список постачальників та коли вони працюють на устаткуванні;
- інвентарні списки обладнання та деталей;
- паролі та заходи контролю доступу;
- адміністративно-технічні заходи контролю доступу;
- інформація про розробників програмного забезпечення та про поточні проекти;
- мережева архітектура;
- архітектура систем дистанційної передачі даних.

До потенційних методів збору цієї інформації відносяться:

- «Соціальна інженерія»;
- Пошук відкритої інформації в Інтернеті;
- Пошук корисної інформації в інформаційних відходах;
- war dialling (комп'ютерний перебір телефонних номерів з метою пошуку модему), war driving (пошук бездротових мереж шляхом пересування на автомобілі);
- Атаки електронної пошти - «фішинг» з метою отримання доступу до мереж, використання програм перехоплення, що вводиться з клавіатури інформації;
- Встановлення програмного забезпечення або пристроїв на хост-машини через жорсткий диск, картку пам'яті чи компакт-диск;
- Підслуховування введення паролів або введення кодів доступу (вручну, використанням засобів аудіо-або відеоспостереження).

Елементи атаки можуть включати:

- отримання картки доступу (контактної картки) та коду доступу;
- розкрадання/дублювання наявної картки доступу;
- доступ до програматора карт доступу з метою створення нової карти;
- створення вхідних даних про нового службовця;

- ототожнення з особистими даними нещодавно звільненого службовця;
- отримання бажаного рівня доступу.

Як тільки карта та коди отримані, виконавець атаки використовує отриману інформацію для організаційної діяльності з метою потайного проникнення на установку як особа, яка доставляє частини обладнання.

2.4.2 Сценарій 2 – атака з відключенням чи порушенням нормальної роботи однієї чи кількох АСУ ТП

Мета атаки – організувати саботаж на атомній електростанції та перешкодити негайному поверненню станції в експлуатацію.

У цьому прикладі в період зупинки субпідрядник проводить тести на системі управління подачею поживної води підрядник створює пункт віддаленого доступу для моніторингу та тестування системи зі свого офісу. Після того, як підрядник завершує роботу, точка доступу з недогляду продовжує діяти. Виконавець атаки зібрав на станції інформацію, яка вказує, що субпідрядник раніше працював на станції і є основною метою для отримання інформації щодо станції Виконавець атаки проводить фішинг-атаку на електронну пошту в офісі субпідрядника та впроваджує в систему руткіт, отримуючи адміністративний контроль. В результаті виконавець атаки отримує доступ до комп'ютерної мережі підрядників та дізнається плани тестування на станції, а також визначає порт віддаленого доступу, який не було заблоковано станцією.

Використовуючи цю інформацію, зловмисник має можливість організувати атаку з відмовою в обслуговуванні (DoS) на систему управління подачею поживної води шляхом заглушення мережі трафіком, що спричиняє збій системи. Система була розрахована на роботу лише за мінімального навантаження з трафіку.

Після того, як виконавець атаки отримав доступ, проаналізував мережу та визначив протокол зв'язку, він проводить атаку. Внаслідок атаки система управління подачею поживної води перестає реагувати на команди, що призводить до ручного аварійного зупинення станції. Причина збою системи управління подачею поживної

води не може бути визначена відразу ж, реактор залишається у режимі зупинки для розслідування інциденту.

2.4.3 Сценарій 3 – порушення нормальної роботи комп'ютерної системи як інструментальний засіб координованої атаки

Мета атаки – розкрадання ядерного матеріалу під час його переміщення між сховищами. Комп'ютерна атака використовується для внесення змін до системи контролю та відстеження інвентарної кількості з метою приховування втрати викраденого матеріалу.

В результаті розвідки та збору відомостей із застосуванням спецзасобів був визначено процес маркування та простеження переміщень радіоактивного матеріалу між сховищами Він включає встановлення на кожний предмет МРЧІ (мітки радіочастотної ідентифікації) з описом компонента та перерахуванням вмісту.

План атаки включає допомогу внутрішнього порушника з метою вилучення матеріалу під час його переміщенню. Етапи атаки такі:

- Перехоплення вантажу під час його переміщення;
- Вилучення невеликої кількості транспортованого радіоактивного матеріалу;
- Перепрограмування чіпа з метою введення інформації про кількості, що залишилася;
- Модифікація даних системи відстеження інвентарної кількості таким чином, щоб відобразити нову кількість, як відправляється, а викрадена кількість - як досі знаходиться на зберіганні у відправляючої установки.

Комп'ютерна атака націлена на отримання через мережу доступу до бази даних щодо інвентарних кількостей та модифікацію файлу реєстрації інвентарних кількостей та передач.

Висновок до другого розділу

У даному розділі була розглянута проблематика комп'ютерної безпеки в контексті автоматизованих систем керування технічними процесами в ядерних установках. Дослідження показали, що забезпечення безпеки в цих системах є критично важливим завданням, оскільки вони впливають на безпеку ядерних установок, а також на здоров'я людей та навколишнє середовище. Виявлено, що автоматизовані системи керування технічними процесами у ядерних установках піддаються різноманітним загрозам та вразливостям. Ці загрози можуть походити як зовні, так і зсередини системи, і включають такі фактори, як хакерські атаки, витік інформації, неправильне використання або зловживання правами доступу. Для забезпечення комп'ютерної безпеки в автоматизованих системах керування технічними процесами в ядерних установках необхідно впроваджувати комплексні заходи захисту. Ці заходи включають розробку і впровадження надійних систем аутентифікації та авторизації, шифрування даних, систем моніторингу та виявлення вторгнень, а також проведення регулярних аудитів та оновлення програмного забезпечення.

У результаті аналізу було встановлено, що реалізація програми комп'ютерної безпеки є важливим кроком у запобіганні можливим загрозам та вразливостям автоматизованих систем керування технічними процесами в ядерних установках. Ефективна програма комп'ютерної безпеки дозволяє забезпечити надійну та безпечну роботу системи, запобігти можливим аваріям та мінімізувати ризики для людей та навколишнього середовища.

Висновки цього розділу можуть бути використані як основа для розробки і впровадження ефективних заходів комп'ютерної безпеки в автоматизованих системах керування технічними процесами в ядерних установках. Дотримання цих заходів є важливим елементом для забезпечення безпеки ядерних установок та захисту від можливих загроз і вразливостей.

РОЗДІЛ 3
РОЗРОБКА СТРАТЕГІЇ, ПРОГРАМИ ТА РІВНІВ КІБЕРБЕЗПЕКИ ДЛЯ АСУ ТП В ЯДЕРНИХ УСТАНОВКАХ

3.1 Розробка рекомендації до стратегії кібербезпеки на ядерних установок.

Стратегія повинна бути здійсненною, досяжною та підлягати перевірці. Стратегія повинна включати такі пункти:

(a) Як виконується оцінка загроз, включаючи визначення можливих сценаріїв кібератак;

(b) Як визначаються цілі комп'ютерної безпеки;

(c) Як можуть бути визначені компетенції та рівні можливостей у сфері комп'ютерної безпеки;

(d) розподіл ролей і обов'язків у сфері комп'ютерної безпеки для всіх компетентних органів і операторів (і, можливо, для продавців, підрядників і постачальників);

(e) Виявлення та створення нових організацій або адаптація ролей комп'ютерної безпеки для існуючих організацій, де існують прогалини в можливостях;

(f) підходи до реалізації, інтеграції та координації діяльності компетентних органів і операторів з комп'ютерної безпеки;

(g) Заходи щодо підтримки можливостей комп'ютерної безпеки в рамках режиму ядерної безпеки.

Стратегія описує підготовчу діяльність, яку має здійснити держава та її орган з питань комп'ютерної безпеки, зокрема:

(a) Виконання оцінки загрози;

(b) Оцінка впливу кібератаки на ядерну безпеку;

(c) Визначення того, чи використовувати нормативний підхід чи підхід, що ґрунтується на продуктивності, для регулювання комп'ютерної безпеки, або комбінацію обох;

(d) Встановлення структури здібностей і компетенцій у сфері комп'ютерної безпеки;

(e) Впровадження (інтеграція та координація) діяльності органів та операторів з комп'ютерної безпеки.

3.2 Розробка програми комп'ютерної безпеки на ядерних установках

ПКБ для кожного компетентного органу та оператора визначає це роль організації в реалізації стратегії у формі організаційних ролей, обов'язків і процедур. ПКБ також визначає засоби, за допомогою яких компетентний орган або оператор прагне досягти цілей комп'ютерної безпеки та/або впровадити заходи комп'ютерної безпеки, визначені законодавством, положеннями, стандартами та вказівками його регулюючого органу та компетентного орган комп'ютерної безпеки.

Компетентний орган з питань комп'ютерної безпеки повинен забезпечити, щоб кожен орган або оператор розробляв і підтримував свій ПКБ, як зазначено в цьому розділі. ПКБ має бути встановлено в рамках загального плану безпеки об'єкта та в системі управління кожного об'єкта . Орган з питань комп'ютерної безпеки повинен забезпечити сприяння розвитку комп'ютерної безпеки як важливого компонента культури ядерної безпеки та повинен заохочувати відданість безперервному вдосконаленню шляхом прямого зобов'язання вищого керівництва кожного компетентного органу чи оператора. Рисунок 2.2 ілюструє приклад структури для ПКБ, включаючи супровідні та допоміжні документи.

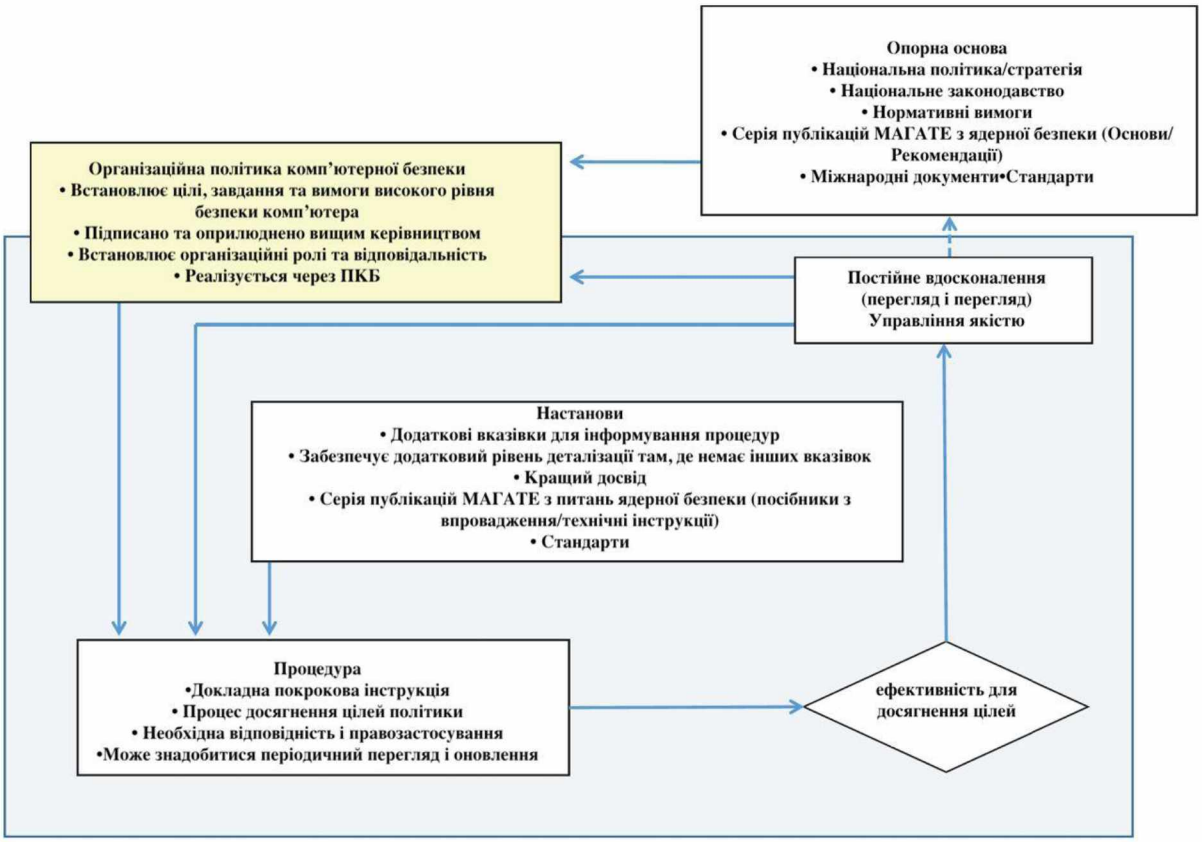

Рисунок 2.2 - Огляд програми комп'ютерної безпеки на АС.

ПКБ має описувати комп'ютерну безпеку в організації з точки зору сприйнятливості до вразливостей, заходів захисту, аналізу наслідків і заходів пом'якшення, щоб ідентифікувати та підтримувати прийнятний рівень ризику, що виникає внаслідок кібератак, і сприяти відновленню до безпечного робочого стану. Зміст ПКБ має включати щонайменше таке:

(a) Організація та обов'язки:

(1) Організаційні схеми;

(2) Відповідальні особи та обов'язки щодо звітності;

(3) Штрафи та коригувальні дії;

(4) Процес періодичної перевірки та затвердження;

(5) Інтерфейси з іншими програмами.

(b) Управління цифровими активами:

(1) Список усіх комп'ютерних систем;

(2) Список усіх комп'ютерних системних програм;

(3) діаграми потоку даних і мережі, включаючи всі підключення до зовнішніх комп'ютерних систем;

(4) Керування конфігурацією (апаратне забезпечення, прошивка, програмне забезпечення програми, стан обладнання та відповідні конфігурації);

(5) Класифікація цифрових активів та ідентифікація SDA, в тому числі класифікація важливості (тобто внесок у ядерну безпеку, ядерний функції безпеки та обліку та контролю ядерних матеріалів).

(c) Оцінка ризику, вразливості та відповідності:

(1) Періодичність перегляду та повторної оцінки ПКБ;

(2) Самооцінка (включаючи процедури активного та пасивного тестування);

(3) Періодична та реактивна переоцінка ризику та відповідна методологія;

(4) процедури аудиту та відстеження та виправлення недоліків;

(5) Огляд законодавчої та нормативної відповідності.

(d) Проект безпеки системи:

(1) Основні принципи архітектури та дизайну;

(2) Фундаментальні підходи до проектування безпеки;

(3) Формалізація вимог комп'ютерної безпеки для постачальників,

(4) Безпека повного життєвого циклу.

(e) Оперативні процедури безпеки:

(1) Контроль доступу;

(2) Безпека даних;

(3) безпека зв'язку;

(4) Безпека платформи та додатків (наприклад, захист, керування виправленнями, захист від шкідливих програм);

(5) моніторинг системи (включаючи керування журналами);

(6) Підтримка комп'ютерної безпеки;

(7) розгляд інцидентів;

(8) безперервність роботи та аварійне відновлення;

(9) Резервне копіювання системи.

(f) Управління персоналом:

(1) перевірки надійності (перевірка персоналу);

(2) підвищення обізнаності та навчання;

(3) Кваліфікація персоналу;

(4) Припинення найму або переведення персоналу.

ПКБ має бути інтегрованою та скоординованою частиною системи управління організацією. ПКБ може бути розділений на частини, які мають різні рівні класифікації безпеки, щоб полегшити використання плану ефективно та узгоджено з правилом «необхідності знати» та вимогами конфіденційності.

ПКБ слід регулярно переглядати та оновлювати, щоб відобразити відповідні нові знання всередині та поза режимом ядерної безпеки, включаючи таке:

(a) Нові технології, які можна використовувати в кібератаках або для захисту від них;

(b) Нові характеристики кіберзагроз, включаючи виявлені зміни в тактиці, техніки та процедури;

(c) Нові типи інцидентів комп'ютерної безпеки або події ядерної безпеки.

ПКБ має включати положення про регулярні тренування для підготовки учасників і підтвердити ПКБ, включаючи плани на випадок непередбачених обставин. У відповідних випадках ці вправи повинні бути інтегровані з іншими вправами безпеки, і повинні періодично проводити спільно з проти аварійними навчаннями.

3.2.1 Заходи комп'ютерної безпеки на АС

ПКБ визначає заходи комп'ютерної безпеки, які забезпечують функції запобігання, виявлення, затримки, реагування та пом'якшення, а також гарантують, що не зловмисні дії не призведуть до погіршення безпеки комп'ютера, що призведе до підвищеної сприйнятливості до кібератак. Конкретні заходи безпеки комп'ютера можна віднести до наступних трьох типів:

(a) Заходи технічного контролю: Апаратні та/або програмні рішення для захисту від вторгнення, виявлення, пом'якшення та відновлення після вторгнення або

інші зловмисні дії, спрямовані проти SDA. Переваги технічних заходів контролю, зокрема забезпечення безперервних і автоматичних захисних дій, слід враховувати при оцінці ефективності різних типів заходів.

(b) Фізичні заходи контролю: Фізичні бар'єри для захисту SDA від фізичного пошкодження та несанкціонованого фізичного доступу. Заходи фізичного контролю включають охорону та бар'єри, такі як замки, огорожі, ворота, фізичні оболонки, пристрої індикації втручання та ізолятори.

(c) Заходи адміністративного контролю: політика, процедури та практика призначений для захисту SDA шляхом контролю за діями та поведінкою персоналу. Заходи адміністративного контролю включають оперативно-управлінські заходів і, як правило, мають директивний характер, вказуючи, які працівники і сторонній персонал повинен і не повинен робити, але також включати заходи впливу, такі як просування сильної культури безпеки.

3.3 Розробка рівнів кібербезпеки для АСУ ТП на ядерних установках

Застосування рекомендацій на різних рівнях комп'ютерної безпеки представлено далі.

Базовий рівень, заходи базового рівня слід застосовувати щодо всіх комп'ютерних систем заходи, що відповідають кожному рівню, не є сукупними тому можливі повторення. Як показано на (рис. 3.1), рівні безпеки різні: від рівня 5 (необхідний найменший захист) та до рівня 1 (необхідний максимальний захист);

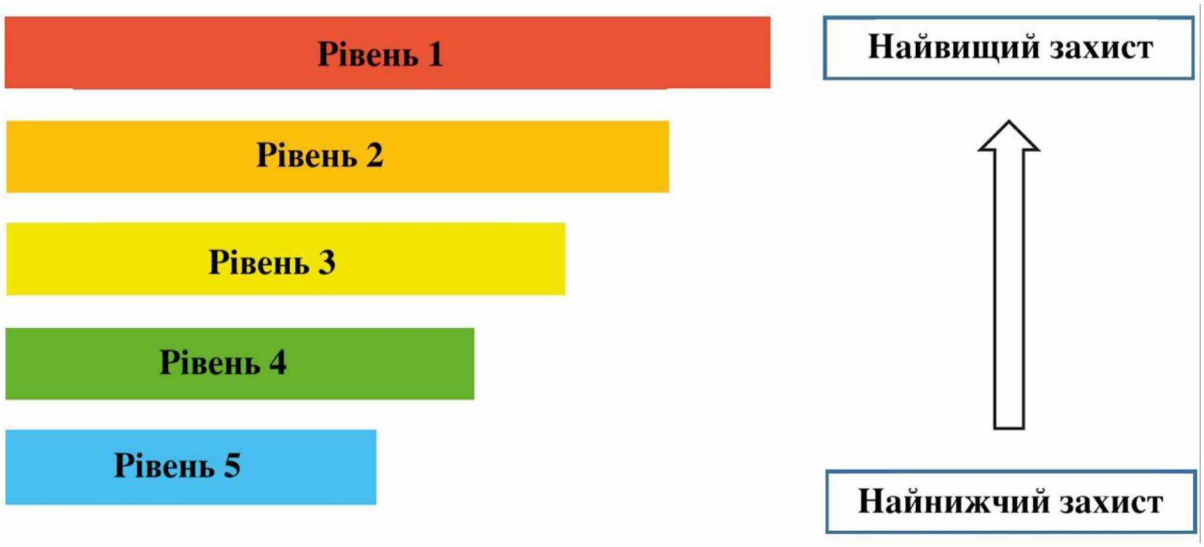

Рисунок. 3.1 - Рівні безпеки/суворість заходів.

Для систем та рівнів слід застосовувати наведені нижче заходи базового рівня:

- для кожного рівня визначаються політика та види практичної діяльності;
- експлуатаційні процедури безпеки викладаються в письмово з метою ознайомлення з ними всіх користувачів;
- персонал, якому дозволено доступ до системи, повинен мати відповідну кваліфікацію та досвід та у необхідних випадках повинен мати допуск до конфіденційної інформації;
- користувачам надається доступ тільки до тих функцій та тим систем, які їм необхідні для виконання робочих завдань;
- здійснюються належний контроль доступу та аутентифікація користувачів;
- діють системи або процедури виявлення аномалій;
- здійснюється моніторинг вразливостей прикладних програм та систем, та вживаються відповідні заходи;
- періодично проводяться оцінки вразливості систем;
- змінні носії повинні контролюватись відповідно до експлуатаційними процедурами фізичної безпеки;
- слід суворо дотримуватись регламентів технічного обслуговування компонентів, що забезпечують безпеку комп'ютерів та мереж;

- Сувора реєстрація та моніторинг компонентів, що забезпечують безпеку комп'ютерів та мереж (наприклад, шлюзів безпеки, систем виявлення проникнення, систем запобігання проникнення серверів віртуальних приватних мереж (VPN));

- діють належні процедури резервного копіювання/відновлення;

- фізичний доступ до компонентів та систем обмежений відповідно до їх функціями.

3.3.1 Рівень 1 - максимальний захист

Крім заходів базового рівня, захисні заходи рівня 1 слідують використовувати для систем, наприклад, систем захисту, які є життєво важливими для встановлення та вимагають найвищого рівня безпеки. Ці заходи включають:

- не повинно бути дозволено надходження до системи рівня 1 жодних мережевих потоків даних будь-якого виду (наприклад, підтверджень, сигналізації) від систем з нижчими рівнями безпеки. Повинна бути можливою лише суворо вихідна комунікація. Слід зазначити, що суворо одностороння комунікація такого роду сама по собі не гарантує надійності та цілісності даних (можна розглянути можливість резервування/виправлення помилок). Слід також враховувати, що це виключає будь-який вид протоколів "взаємної ідентифікації" (включаючи TCP/IP), навіть у разі контрольованих напрямів підключення. Винятки вкрай небажані і можуть розглядатися лише суворо індивідуальному порядку й у тому випадку, якщо вони підкріплені повним обґрунтуванням та аналізом ризику кібербезпеки;

- заходи щодо забезпечення цілісності та експлуатаційної готовності систем, як правило, пояснюються в обґрунтуваннях безпеки;

- дистанційний доступ з метою обслуговування не допускається;

- фізичний доступ до систем суворо контролюється;

- кількість працівників, яким надано доступ до систем, обмежена до абсолютного мінімуму;

- щодо будь-яких затверджених модифікацій, що виробляються в комп'ютерні системи, застосовується правило двох осіб;

- слід проводити реєстрацію та моніторинг усіх дій;
- кожне введення даних у системи затверджується та перевіряється на індивідуальну основу;
- щодо будь-яких модифікацій, включаючи обслуговування апаратних засобів, оновлення та модифікації програмного забезпечення, застосовуються суворі організаційні та адміністративні процедури.

Прикладом для впровадження рівня безпеки 1 є найголовніший комплекс АСУ ТП на ядерних установках - це система управління та захисту енергоблоку, структура зображена на (рис. 3.2).

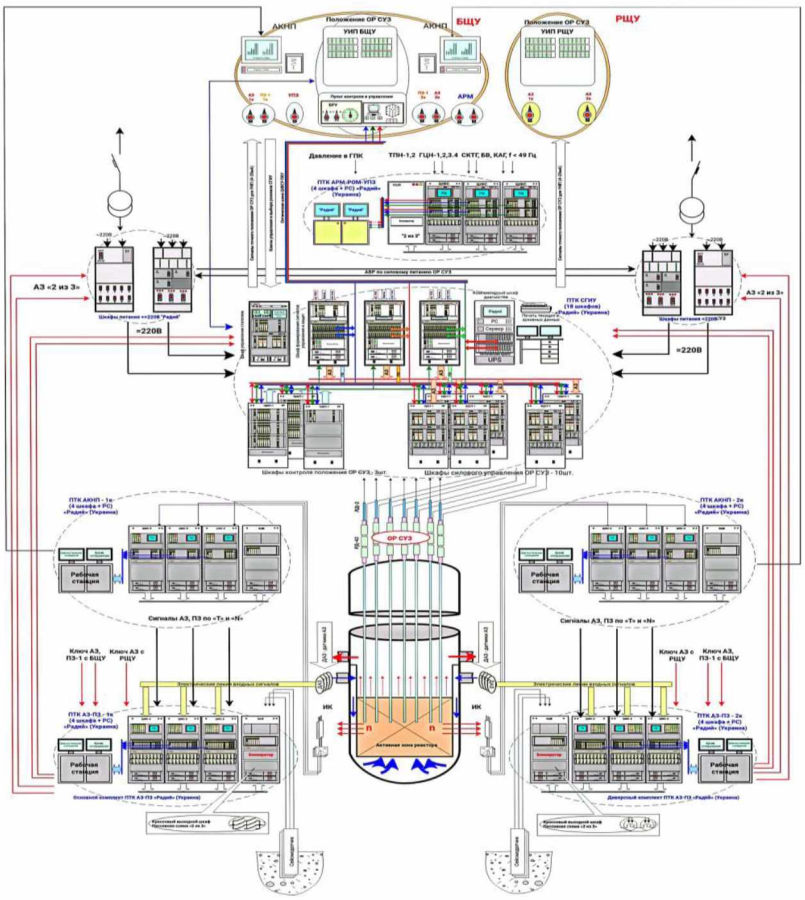

Рисунок 3.2 - Комплекс АСУ ТП система управління та захисту енергоблоку.

3.3.2 Рівень 2 - високий захист

Крім заходів базового рівня, захисні заходи рівня 2 слідують використовувати для систем, наприклад, систем оперативного управління, які потребують високого рівня безпеки. Ці заходи містять наступне:

- дозволяється лише вихідний, односторонній мережевий потік даних від систем рівня 2 до систем рівня 3. У протилежному (що входить) напрямі можуть прийматися лише необхідні повідомлення підтвердження або повідомлення про контрольовані сигнали (наприклад, для TCP/IP);
- дистанційний доступ з метою обслуговування може дозволятися тільки на індивідуальній основі та протягом певного робочого періоду. У разі використання він має бути захищений за допомогою ефективних заходів, і користувачі повинні дотримуватися політики забезпечення кібербезпеки;
- кількість працівників, яким надано доступ до систем, зведено до мінімуму, причому проводиться чітка різниця між користувачами та адміністративним персоналом;
- фізичні сполуки із системами слід суворо контролювати;
- вжито всіх розумних заходів щодо забезпечення цілісності та готовності систем;
- оцінка вразливості, що включає вплив на системи, може призводити до нестійкості станції або технологічного процесу та тому можливість її проведення слід розглядати тільки в у разі використання випробувальних стендів, запасних систем, під час заводських приймальних випробувань або тривалих запланованих періодів простою.

Для прикладу впровадження рівня безпеки 2 є АСУ ТП називається “Чорна скринька ”, вона відповідає за логування всіх інцидентів аварійного та перед аварійного стану реактору, схема якої зображена на (рис. 3.3)

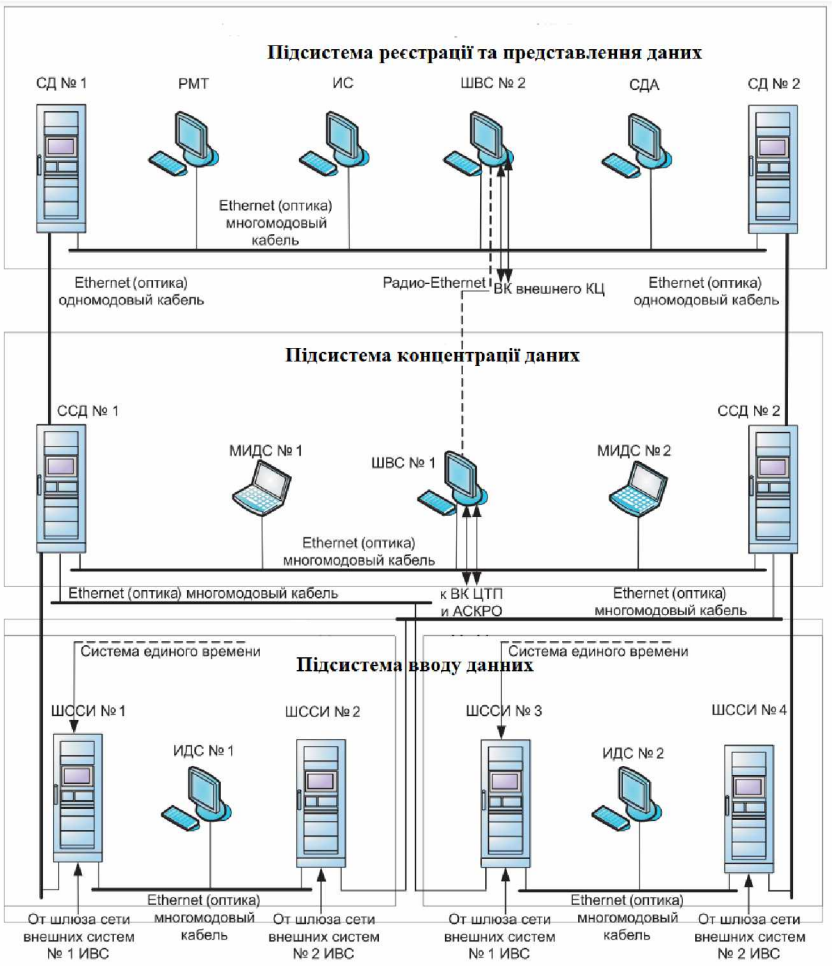

Рисунок. 3.3 - Система логування даних “Чорна скринька”.

3.3.3 Рівень 3 - середній захист

Крім заходів базового рівня, захисні заходи рівня 3 слід використовувати для систем диспетчерського управління в реальному часі, необхідних експлуатації, наприклад, систем диспетчерського управління технологічним процесом у реальному часі у приміщенні щита управління, що характеризуються середнім рівнем серйозності різних кіберзагроз. Ці захисні заходи включають:

- доступ до Інтернету із систем рівня 3 не дозволено;
- для ключових ресурсів здійснюється моніторинг реєстрації та контрольних слідів;
- для захисту цього рівня від неконтрольованих інформаційних потоків із систем рівня 4 та забезпечення лише певної та обмеженої діяльності передбачаються шлюзи безпеки;

- слід контролювати фізичні з'єднання із системами;
- дистанційний доступ з метою обслуговування дозволяється на індивідуальну основу за умови, що він надійно контролюється; віддалений комп'ютер і користувач повинні дотримуватися політики забезпечення безпеки, що обумовлюється в контракті;
- доступні користувачам системні функції контролюються з допомогою механізмів управління доступом та на основі принципу службової потреби

Для прикладу впровадження рівня безпеки 3 є АСУ ТП яка називається “АХК”, автоматичний хімічний контроль дозволяє операторам отримувати інформацію про концентрацію хімічних елементів в реальному часі, схема зображена на (рис. 3.4)

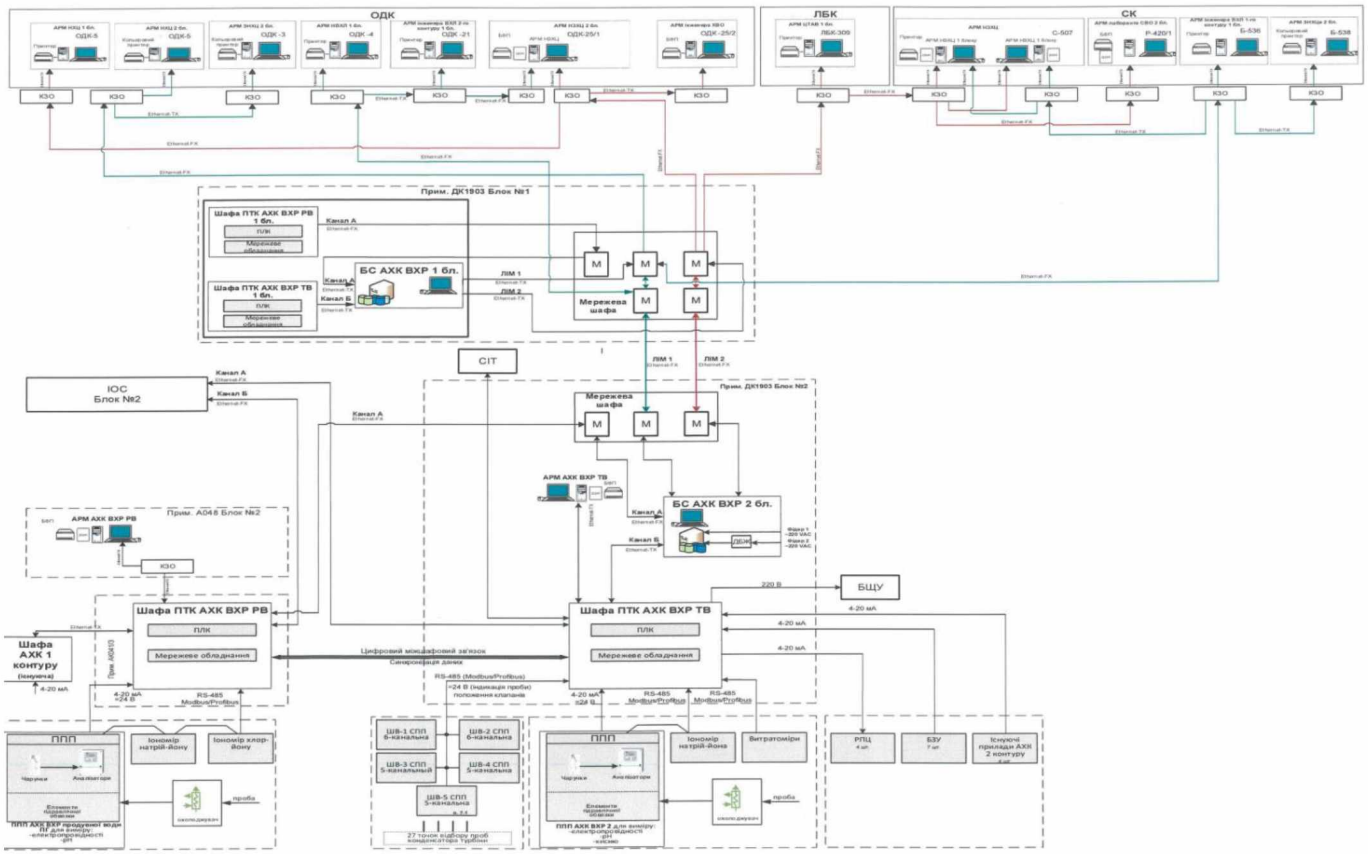

Рисунок 3.4 - Структурна схема системи “АХК”.

3.3.4 Рівень 4 - помірний захист

Крім заходів базового рівня, заходи рівня 4 слід використовувати для систем керування технічними даними, що використовуються для управління діяльністю з обслуговування чи експлуатації, пов'язаної з компонентами або системами, необхідними технічною специфікацією для експлуатації (наприклад, допуск до роботи, робочі замовлення, контрольований виведення з експлуатації, управління документацією), що характеризуються помірним рівнем серйозності різних кіберзагроз. Заходи рівня 4 включають таке:

- внесення модифікацій у системи дозволяється лише затвердженим та кваліфікованим користувачам;
- доступ до Інтернету із систем рівня 4 може надаватися. користувачам за умови застосування належних захисних заходів;
- для захисту цього рівня від неконтрольованих інформаційних потоків від зовнішніх мереж компанії або майданчика та забезпечення певної діяльності передбачаються шлюзи безпеки, які контролюються;
- слід контролювати фізичні з'єднання із системами;
- дистанційний доступ з метою обслуговування дозволяється та контролюється; віддалений комп'ютер і користувач повинні дотримуватися певну політику забезпечення фізичної безпеки, що обумовлюється в контракті та контрольовану;
- доступні користувачам системні функції контролюються з за допомогою механізмів контролю доступу. Будь-який виняток з цього принципу має бути ретельно вивчено та має бути забезпечено захист за допомогою інших засобів;
- дистанційний зовнішній доступ дозволено для затверджених користувачів за умови функціонування належних механізмів контролю доступу.

3.3.5 Рівень 5 - низький захист

Заходи рівня 5 слід використовувати для систем, що не є безпосередньо важливими для цілей технічного контролю або експлуатації, наприклад, систем автоматизації діловодства, що характеризуються низьким рівнем серйозності різних кіберзагроз. Заходи рівня 5 включають:

- внесення модифікацій у системи дозволяється лише затвердженим та кваліфікованим користувачам;
- доступ до Інтернету із систем рівня 5 дозволяється за умови застосування належних захисних заходів;
- дистанційний зовнішній доступ дозволяється затвердженим користувачам за умови функціонування належних заходів контролю.

З метою запобігання несанкціонованому доступу, а також поширення помилок із зони з нижчими вимогами захисту до зони з вищими вимогами, на межах зони потрібні механізми поділу потоків даних. Технічні та адміністративні заходи, що забезпечують поділ зон, повинні бути адаптовані до індивідуальних вимог захисних рівнів. Не повинен допускатися прямий канал з'єднання, що проходить через кілька зон.

3.4 Рекомендації для захисту АСУ ТП на ядерних установках

Виходячи з стандартів МАГАТЕ Safety Series No. SSG-7 та Safety Series No. SSG-9 що до кібербезпеки було розроблено рекомендації для захисту АСУ ТП на ядерних установках.

1. Політика кібербезпеки:
    - Розробка політики кібербезпеки, яка визначає цілі та принципи безпеки для АСУ ТП в ядерних установках.
    - Встановити вимоги до захисту систем АСУ ТП, включаючи вимоги до конфіденційності, цілісності та доступності даних.
2. Ідентифікація загроз:

- Виконати аналіз потенційних кіберзагроз, що можуть впливати на АСУ ТП, з огляду на їх імовірність та наслідки.
- Оцініти ризики та прийняти заходи для зниження впливу загроз на систему АСУ ТП.

3. Захист мереж та систем:
   - Встановити механізми аутентифікації, авторизації та контролю доступу для забезпечення обмеженого та керованого доступу до систем АСУ ТП.
   - Використовувати розроблені вище рівні кібербезпеки
4. Захист від кібератак:
   - Встановити системи моніторингу та виявлення кібератак для виявлення несанкціонованої активності та аномалій в системах АСУ ТП.
   - Розробити процедури реагування на кібератаки, включаючи відключення компрометованих систем та відновлення їх стану безпеки.
   - Використовути захисні мережеві брандмауери, інтра- та екстра-мережеві системи виявлення вторгнень для моніторингу мереж та виявлення аномальної активності.
5. Резервне копіювання та відновлення:
   - Регулярно резервувати дані та конфігурації систем АСУ ТП для можливого відновлення після інцидентів.
   - Розробити та тестувати плани відновлення після інциденту, включаючи процедури відновлення систем та даних з резервних копій.
6. Свідомість персоналу:
   - Навчати та регулярно тренувати персонал, що використовує АСУ ТП, з питань кібербезпеки, включаючи ідентифікацію фішингових атак, використання сильних паролів та усвідомлення потенційних загроз.
   - Залучити персонал до практики безпечних поведінкових звичок, таких як несвоєчасне відкриття невідомих електронних листів та повідомлень.

Висновок до третього розділу

У даному розділі було розглянуто питання розробки стратегії, програми та рівнів кібербезпеки для автоматизованих систем управління технологічним процесом в ядерних установках. Кібербезпека в ядерних установках є критично важливою, оскільки вразливість таких систем може мати серйозні наслідки для безпеки людей і навколишнього середовища. З метою забезпечення високого рівня кібербезпеки, було запропоновано розробку стратегії, яка визначає загальну спрямованість і принципи заходів з кібербезпеки в ядерних установках. Це включає аналіз загроз і ризиків, визначення мети та завдань кібербезпеки, розробку політик та процедур, а також встановлення відповідальностей та контролю за виконанням. Окрім стратегії, була розроблена програма комп'ютерної безпеки, яка включає конкретні технічні заходи для захисту АСУ ТП в ядерних установках. Це включає встановлення механізмів автентифікації та авторизації, контроль доступу, моніторинг та виявлення вторгнень, резервне копіювання та відновлення системи та інші заходи безпеки.

Також були розроблені рівні кібербезпеки для АСУ ТП на ядерних установках, що дозволяють класифікувати рівень захисту системи. Рівень 1 - Максимальний захист, є найвищим рівнем безпеки і передбачає використання передових технологій та найсуворіших заходів безпеки. Рівні 2-5 пропонують поступово менші рівні захисту, але все ще включають необхідні заходи безпеки для захисту системи від потенційних загроз. В цілому, розробка стратегії, програма та рівнів кібербезпеки для АСУ ТП в ядерних установках є важливим кроком у забезпеченні безпеки і надійності таких систем. Застосування цих заходів допомагає запобігти можливим кібератакам і зберегти інформацію та функціональність системи.

Розроблені рекомендації безпеки для АСУ ТП в ядерних установках надають важливі вказівки та вимоги для забезпечення ефективного захисту від кіберзагроз. Ці рекомендації охоплюють різні аспекти кібербезпеки, починаючи з розробки програми кібербезпеки та ідентифікації загроз, і до захисту мереж, захисту від кібератак та резервного копіювання. Виконання цих рекомендацій сприятиме створенню надійного інфраструктурного захисту для АСУ ТП в ядерних установках. Шляхом

встановлення механізмів аутентифікації, авторизації та контролю доступу, використання моніторингу систем на наявність аномалій, можна забезпечити конфіденційність, цілісність та доступність даних. Крім того, рекомендації з розробки рівнів кібербезпеки дозволяють класифікувати системи залежно від їх важливості та ризику. Встановлення відповідного рівня захисту допоможе приділити належну увагу найважливішим системам та виконати необхідні заходи безпеки. Завдяки розробленим рекомендаціям також рекомендується регулярно навчати та тренувати персонал, що використовує АСУ ТП, з питань кібербезпеки. Це допоможе забезпечити свідому поведінку персоналу та усвідомлення потенційних кіберзагроз.

ВИСНОВОК

В ході виконання дипломної роботи я провів аналіз автоматизованих систем керування технічними процесами (АСУ ТП) із особливим акцентом їх безпеку в контексті ядерних установок. Було досліджено визначення АСУ ТП, їх функції, цілі та критерії керування, а також класифікація, технічні умови та складові цих систем. Я розглянув питання комп'ютерної безпеки в контексті АСУ ТП на ядерних установках. Проаналізував політику, план та елементи забезпечення комп'ютерної безпеки, а також рівні безпеки та поділ на зони. Проаналізовано загрози та порушників, а також наведено приклади атак на АСУ ТП та їх можливі наслідки.

У третьому розділі розробив стратегію, програму та кібербезпеки для АСУ ТП в ядерних установках. Також розробив власні рівні кібербезпеки та рекомендації для захисту АСУ ТП на ядерних установках. Розроблені рівні кібербезпеки для АСУ ТП в ядерних установках представляють систематичний підхід до захисту цих систем від кіберзагроз. Класифікація на рівні 1 до рівня 5 надає можливість оцінити рівень захисту і прийняти необхідні заходи для підвищення безпеки системи.

Рівень 1 - Максимальний захист, встановлює найвищі стандарти безпеки та вимагає використання передових технологій і рішень. Цей рівень рекомендується для найкритичніших систем і передбачає впровадження комплексних заходів безпеки, таких як сильне шифрування, мережеві периметри, мультифакторна аутентифікація та постійний моніторинг.

Рівні 2 до 5 пропонують послідовно менші рівні захисту, але все ще включають необхідні заходи безпеки для ефективного захисту АСУ ТП. Вони забезпечують імплементацію різних контрольних механізмів, включаючи доступ на основі ролей і привілеїв, мережевий моніторинг, автоматичне виявлення вторгнень та системи відновлення після інцидентів.

Розроблені рівні кібербезпеки сприяють покращенню стійкості АСУ ТП в ядерних установках до потенційних кібератак. Впровадження цих рівнів рекомендується як частина комплексного підходу до кібербезпеки, що включає

розробку стратегії та політики безпеки, а також постійне оновлення і підтримку заходів безпеки.

Загалом, розроблені рівні кібербезпеки створюють основу для стабільної та надійної роботи АСУ ТП в ядерних установках, забезпечуючи захист від сучасних кіберзагроз і допомагаючи зберегти цінну інформацію та безпеку оперативного процесу. Отже, дипломний проект зосереджений на важливих аспектах безпеки автоматизованих систем керування технічними процесами в ядерних установках. Результати дослідження дають можливість розробникам та операторам ядерних установок зрозуміти загрози та ризики, пов'язані з використанням АСУ ТП, а також розробити стратегію та програма комп'ютерної безпеки для їх захисту. Рекомендації, наведені у дипломному проекті, можуть бути використані для покращення безпеки та захисту АСУ ТП в ядерних установках. Продовження досліджень в цьому напрямку може сприяти подальшому удосконаленню систем керування технічними процесами і забезпеченню найвищого рівня безпеки в ядерній енергетиці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

2. Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (1980); Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1/Mod.1, IAEA, Vienna (2016).

3. INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/ Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

4. INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

5. EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

6. INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

7. INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (in preparation).

8. INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

9. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Information Technology — Security Techniques — Information Security Risk Management, ISO/IEC 27005:208, ISO, Geneva (2018).

10. INTERNATIONAL ATOMIC ENERGY AGENCY, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No. 10-G (Rev. 1), IAEA, Vienna (2021).

11. INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

12. INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).

13. Kim Zetter. Countdown to Zero Day. Stuxnet and the Launch of the World`s First Digital Weapon - Published in the United States by Crown Publishers, an imprint of the Crown Publishing Group, a division of Random House LLC, a Penguin Random House Company, New York. – 2016. – 319p.

14. Gabrielle Desarnaud. Cyber Attacks and Energy Infrastractures. Anticipating Risks - Etudes de l'Ifri – 2017.-60p.15. Eric D. Knapp Industrial Network Security - 225 Wyman Street, Waltham, MA 02451, USA – 2015.- 360p

15. APT-атаки на паливно-енергетичний комплекс: огляд тактик и технік [Електронний ресурс] – Режим доступа: World Wide Web. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-energy-2019

16. Чому захист АСУ ТП став сьогодні критично важливий? [Електронний ресурс] – Режим доступа: World Wide Web. – URL: https://www.securitylab.ru/analytics/484730.php

17. Безпека від кібератак в АСУ ТП [Електронний ресурс] – Режим доступа: World Wide Web. – URL: https://automation-system.ru/main/11-asutp/asu-tp/468-security-asutp.html

18. NERC Critical Infrastructure Protection (CIP), NERC CIP [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.nerc.com/pa/Stand/Pages/CIPStandards. aspx

19. NIST SP 800-82 [Електронний ресурс] – Режим доступу: World Wide Web. URL: https://csrc.nist.gov/publications/detail/sp/800-82/archive/2011-06-09#:~:text=NIST%20Special%20Publication%20(SP)%20800,control%20system%20configurations%20such%20as

20. Nuclear Regulatory Commission Regulation 5.71 [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.nrc.gov/docs/ML0903/ML090340159.pdf

21. Довгуша І.М., Кітура О.В. Безпека автоматизованих систем управління технологічними процесами / Довгуша І.М., Кітура О.В. // Актуальні проблеми кібербезпки: всеукраїнська наукова конференція, тези доп. – К., 2020. С.91-92.