Центральноукраїнський національний технічний університет
Центр заочної та дистанційної освіти
Кафедра кібербезпеки та програмного забезпечення

”Допущено до захисту”
Завідувач кафедри цілісності та безпеки
критичних компонентів АСУ ТП
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
“____” _____ 2026 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за другим (магістерським) рівнем вищої освіти
на тему
“Дослідження та програмна реалізація системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП”

Виконав здобувач вищої освіти
ІІ курсу, групи КІ-25МЗ
ОПП «Комп’ютерна інженерія»
спеціальності F7 «Комп’ютерна інженерія»
_____ Гресько І.С.
«____» _____ 2026 р.

Керівник проекту
кандидат фізико-математичних наук, доцент
_____ Якименко Н.М.
«____» _____ 2026 р.

Нормоконтроль проекту
_____ Коваленко А.С.
«____» _____ 2026 р.

Рецензент _____
_____

Підписано КЕП
Центральноукраїнський національний технічний університет
ГРЕСЬКО ІГОР СЕРГІЙОВИЧ
Сертифікат: 5E984D526F82F38F0400000010752F01F14F2B07
Дійсний з 06.02.2026 09:53:47 по 07.02.2027 01:59:59

Центральноукраїнський національний технічний університет
Центр *Заочної та дистанційної освіти*
Кафедра *кібербезпеки та програмного забезпечення*
Рівень вищої освіти *магістр*
Галузь знань _F_____*"Інформаційні технології"*_____
Спеціальність F7 *"Комп'ютерна інженерія"*
Освітньо-професійна (освітньо-наукова) програма _*"Комп'ютерна інженерія"*_

ЗАТВЕРДЖУЮ
Завідувач кафедри
д.т.н., проф.
_____ Олексій СМІРНОВ
« 1 » вересня 2026 року

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ДРУГИМ (МАГІСТЕРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Греську Ігорю Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження та програмна реалізація системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП*

2. Керівник роботи *Якименко Наталія Миколаївна, кандидат фізико-математичних наук, доцент*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 43-13 від 17.08.2026 року

3. Строк подання студентом роботи до захисту *2.12.2026 р.*

4. Мета та завдання випускної кваліфікаційної роботи*: Метою розробки є дослідження та програмна реалізація системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП*

5. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Призначення та область використання.	*5. Впровадження системи в промислову експлуатацію*
2. Перегляд аналогічних існуючих систем.	*6. Наукова новизна.*
3. Опис і обґрунтування проектних рішень.	*7. Заходи з охорони праці та техніки безпеки.*
4. Етапи програмування системи.	*8. Висновки.*

6. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Наукова новизна	*1 аркуш*
Структурна схема системи	*1 аркуш*
Функціональна схема системи	*1 аркуш*
Діаграма процесів	*1 аркуш*
Блок-схема алгоритму роботи додатку	*2 аркуша*

7. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Марченко К.М., к.т.н., доцент	06.10.2026	16.11.2026

8. Дата видачі завдання « 1 » вересня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти	Строк виконання етапів випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти	Примітка
1.	Аналіз існуючих систем	10.10.2026 р.	
2.	Постановка задачі, оформлення ТЗ	15.10.2026 р.	
3.	Розробка моделі компонента	20.10.2026 р.	
4.	Розробка структур даних	25.10.2026 р.	
5.	Розробка алгоритмів системи	30.10.2026 р.	
6.	Програмування алгоритмів	10.11.2026 р.	
7.	Розрахунки з охорони праці та техніки безпеки	15.11.2026 р.	
8.	Оформлення ПЗ	17.11.2026 р.	
9.	Попередній захист роботи	2.12.2026 р.	

Дата видачі завдання
« 1 » вересня 2026 р.

Підпис керівника

_____ _____
(прізвище та ініціали)

Завдання прийнято до виконання
« 1 » вересня 2026 р.

Підпис здобувача

_____ _____
(прізвище та ініціали)

АНОТАЦІЯ

Гресько І.С. Дослідження та програмна реалізація системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП. F7 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Метою розробки є дослідження та програмна реалізація системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Об'єктом дослідження є процес апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Предметом дослідження є методи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Методи дослідження базуються на методах Інтернету речей, методах математичної статистики, методах розробки програмного забезпечення.

Результат роботи – програмна реалізація системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

Програма може використовуватися на ПЕОМ з ОС Windows 10/11.

Програму розроблено в середовищі Visual C++.

Ключові слова: комп'ютерна інженерія, апаратно-програмний комплекс, забезпечення цілісності та безпеки, критичні компоненти, АСУ ТП

ABSTRACT

Hresko I.S. Research and Software Implementation of a Hardware-Software System for Ensuring the Integrity and Security of Critical Components in Automated Process Control Systems (APCS). F7 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

This master's-level final qualification thesis presents the development of software designed for a hardware-software system aimed at ensuring the integrity and security of critical components within Automated Process Control Systems (APCS).

The objective of this development is the research and software implementation of a hardware-software system for ensuring the integrity and security of critical components in APCS.

The object of the research is the process involving a hardware-software system for ensuring the integrity and security of critical components in APCS.

The subject of the research consists of the methods used within a hardware-software system for ensuring the integrity and security of critical components in APCS.

The research methodology draws upon techniques from the Internet of Things (IoT), mathematical statistics, and software development.

The outcome of the work is the software implementation of a hardware-software system for ensuring the integrity and security of critical components in APCS.

During the development of the software model, an analysis of existing hardware and software tools was conducted. All components of the developed software are described in detail.

A user-friendly interface has been developed, and instructions for operating the software tools are provided.

The software is designed for use on personal computers running the Windows 10/11 operating system. The program was developed in the Visual C++ environment.

Keywords: computer engineering, hardware-software system, integrity and security assurance, critical components, automated process control systems (APCS)

ВІДОМІСТЬ ПРОЕКТУ

		Текстові документи			
1	А4	Пояснювальна записка	99	–	
2	А4	Робоча програма	39	–	Додаток А
		Графічні документи			
3	А4	Наукова новизна	1	–	
4	А4	Структурна схема	1	–	
5	А4	Функціональна схема роботи системи	1	–	
6	А4	Діаграма взаємодії процесів	1	–	
7	А4	Блок-схема основної програми	1	–	
8	А4	Блок-схема роботи підпрограми	1	–	

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ 9
ВСТУП..... 10
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ 13
1.1 Призначення системи..... 13
1.2 Область застосування 14
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ 19
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти..... 19
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування 29
2.3 Розгорнута постановка завдання 31
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ 32
3.1 Опис функціонування системи 32
3.2 Розробка структурної схеми..... 36
3.3 Розробка функціональної схеми 47
3.4 Розробка діаграми процесів 51
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ 55
4.1 Розробка блок-схем та опис алгоритмів функціонування системи 55
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ..... 72
6 НАУКОВА НОВИЗНА 77

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ 78
7.1 Вступ 78
7.2 Шкідливі і небезпечні фактори при роботі з комп’ютером 79
7.3 Аналіз умов праці 80
7.4 Техніка безпеки та протипожежна профілактика 84
7.5 Розрахункова частина 86
8 ОСНОВНІ ВИСНОВКИ 89
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 91

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ЕН	–	електронний нотаріус
ЕЦП	–	електронний цифровий підпис
СУБД	–	система управління базами даних
УЦ	–	удостовірюючий центр
CRL	–	список відкликаних сертифікатів
DVCS	–	Data Validation and Certification Server Protocols
http	–	HyperText Transfer Protocol – протокол передачі гіпертексту
HTTPS	–	розширення протоколу HTTP, підтримуюче шифрування
IMAP	–	протокол доступу до електроної пошти Інтернету
MAC	–	код автентифікації повідомлення
OCSP	–	Online Certificate Status Protocol
PKI	–	інфраструктура відкритих ключів
POP3	–	Post Office Protocol Version 3 – протокол поштового відділення
SMTP	–	простий протокол передачі пошти
SSL	–	Secure Sockets Layer – рівень захищених сокетів
SQL	–	Structured Query Language – мова структурованих запросів
TCP	–	протокол управління передачею
TLS	–	криптографічний протокол, захищаючий передачу даних
TSP	–	Time-Stamp Protocol
URL	–	єдиний показник ресурсів
XMPP	–	росширяємий протокол обміну повідомленями й інформацією про присутність

ВСТУП

Актуальність теми. Промислове забезпечення цілісності та безпеки критичних компонентів АСУ ТП переходить до захисту на рівні пристроїв, комунікації на основі ідентифікації, виявлення за допомогою штучного інтелекту та стандартів безпеки за проектуванням. У міру зближення IT/OT середовищ, заводи повинні посилювати застарілі системи, сегментувати мережі та впроваджувати стійкі архітектури, які захищають операції без шкоди для безвідмовної роботи.

Забезпечення цілісності та безпеки критичних компонентів АСУ ТП в промисловому середовищі зазнає значних змін, оскільки захист переходить від периметральних засобів захисту до надійних, захищених за конструкцією пристроїв.

Водночас, штучний інтелект змінює як атаку, так і захист, прискорюючи розвідку для супротивників, водночас забезпечуючи швидше виявлення аномалій та поведінкову аналітику для захисників. Регуляторний тиск, включаючи Закон ЄС про кіберстійкість та IEC 62443, підштовхує виробників до послідовних, орієнтованих на життєвий цикл практик безпеки в системах від багатьох постачальників. Мережа нульової довіри, безпечний віддалений доступ, сегментація та уніфікований моніторинг стають важливими в міру зростання конвергенції IT/OT. Мета зрозуміла: захистити виробництво, підтримувати надійність та створити кіберстійкі операції, здатні безпечно підтримувати сучасне підключення та інновації в інтелектуальному виробництві.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

– Дослідження системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

– Програмна реалізація системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Об'єктом дослідження є процес апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Предметом дослідження є методи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Методи дослідження базуються на методах Інтернету речей, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

– Розроблено вітчизняний продукт апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Робота апробована на LVIII науково-технічній конференції здобувачів вищої освіти «Наука-виробництву», основні положення випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти надруковані у статті збірника праць молодих науковців ЦНТУ, випуск №17.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

З огляду на значні ризики безпеки та атаки на промислові системи керування (ІКС), що використовуються в критично важливих секторах інфраструктури, що зростають у обсягах та все частіше висвітлюються в засобах масової інформації, потрібні фірми, які пропонують та впроваджують комплексні рішення. Фінансові та правові наслідки порушення ІКС зростають у всьому світі, і регуляторні органи дедалі більше зацікавлені у здатності організації захищатися від кібератак та у проведенні нею оцінки кіберризиків.

Фрагментація часткових рішень та складна інтеграція цих критично важливих елементів є надто поширеним явищем і стає витратами та ризиком, які власники рішуче налаштовані зменшити. Кіберрішення не можуть бути розроблені таким чином, щоб спробувати відповідати ІКС. Натомість вони повинні бути спроектовані, протестовані та охоплювати стандартні операційні процедури, інтегровані в діяльність з експлуатації та технічного обслуговування ІКС.

Загрози та кіберінциденти – зловмисні та випадкові – трапляються щодня в промислових мережах керування, і користувачі повинні бути про це обізнані. Ці системи є невід'ємною частиною критичної інфраструктури, яка сприяє роботі в життєво важливих секторах, таких як виробництво електроенергії, нафта і газ, водопостачання, транспорт, харчова, фармацевтична та хімічна промисловість.

1.2 Область застосування

Урядові організації, приватні компанії та державно-приватні партнерства, що керують критично важливою інфраструктурою, стикаються зі значними ризиками для безпеки, оскільки атаки на промислові системи керування (ІКС) зростають. Системи керування стають більш взаємопов'язаними, а архітектури на основі Ethernet є більш поширеними для компаній, незважаючи на підвищені потенційні ризики для безпеки. ІКС є невід'ємною частиною критично важливої інфраструктури, яка сприяє роботі в життєво важливих галузях, від яких люди покладаються щодня. Розробка кіберекосистеми, яка охоплює більше, ніж просто чотири стіни компанії, має вирішальне значення для зменшення загрози, яка зростає з кожним днем.

Загрози та кіберінциденти – зловмисні чи випадкові – трапляються щодня в промислових мережах керування. Зараз легше, ніж будь-коли, використовувати вразливості в промислових протоколах, мережах та обладнанні. Останні шість років мали б стати сигналом тривоги для галузі промислової автоматизації. ІКС стали основною ціллю для таких кібератак, як Stuxnet, Night Dragon та Shamoon. Збільшення обсягу атак вимагає ефективніших операційних кіберрішень, які агрегують, аналізують та співвідносять дані з кількох платформ у візуалізацію майже в режимі реального часу, яка відображає будь-які потенційні загрози, що виникають. Організації повинні дивитися за межі власного периметра та співпрацювати зі своїми корпоративними партнерами, постачальниками та продавцями щодо потенційного впливу кібератаки. Однак усі ці складні системи взаємодіючих пристроїв, мереж, організацій та людей роблять її потенційною загрозою, а також перевагою.

Корпорації та урядові організації повинні співпрацювати для подальшої розробки рішень для захисту критичної інфраструктури, які роблять більше, ніж просто відповідають мінімальним вимогам. Рішення повинні бути орієнтовані на фахівців, яким доручено підтримувати роботу критичної інфраструктури, а також створювати бізнес-обґрунтування для зниження ризиків. У минулому

протоколи зв'язку та ізольоване середовище робили ІКС значною мірою несприйнятливими до шкідливих атак, спрямованих на корпоративні інформаційно-технологічні (ІТ) мережі.

Однак, оскільки системи стають більш взаємопов'язаними, досягнення комплексної безпеки має бути багатопостачальним, організаційним процесом, що створює кіберекосистему. Спеціалізовані загрози, розроблені кваліфікованими кіберзлочинцями, хактивістами та урядами, більше ніж будь-коли раніше зосереджуються на критичній інфраструктурі та її допоміжних системах. Наслідки цих атак виходять далеко за межі периметра цільових об'єктів, що робить безпеку важливішою, ніж будь-коли.

Міністерство внутрішньої безпеки США (DHS) визначило три основні принципи розвитку кіберекосистем: автоматизація, сумісність та автентифікація.

– Автоматизація – забезпечення швидкого виявлення інцидентів та реагування на них. Автоматизація – це стратегія, яка включає прийняття рішень із заданими діями у відповідь на кіберситуації зі швидкістю машини, а не зі швидкістю людської реакції.

– Взаємодія – забезпечення розподіленого виявлення загроз на різних пристроях. Взаємодія повинна усунути технічні обмеження для організацій, щоб вони могли безперешкодно співпрацювати в автоматизації кіберзахисту.

– Автентифікація – забезпечення надійного зв’язку для автоматизованої співпраці безпечним способом. Під час прийняття автоматизованих рішень автентифікація гарантує автентичність залучених партнерів.

Підтримка цілісності ICS вимагає глибокого розуміння стандартів зв'язку, що використовуються між усіма різними компонентами ICS для забезпечення безпечної та ефективної роботи. На цьому кіберфізичному рівні може бути важко виявити помилки зв'язку, загрози цілісності та безпеці критичних компонентів АСУ ТП та проблеми з поганим станом мережі. Симптоми очевидні: повільні оновлення людино-машинного інтерфейсу (HMI), незрозумілі зупинки та небезпечні збої компонентів ICS. Надійна та справна мережа операційних технологій (ОТ) є ключем до запобігання цим збоям.

Потенційні ризики ICS

Зростає попит на багато ІКС та сенсорних даних для зв'язку з іншими комерційними та корпоративними системами в корпоративній мережі. Це створює нові ризики та виклики, з якими власники повинні зіткнутися та пом'якшити їхні наслідки. Їм потрібно просіяти так багато даних, і не вистачає кваліфікованої робочої сили, яка б допомогла їм їх обробити, а це означає, що працівники, які не мають кваліфікації, стають ненавмисним ризиком для цілісності та безпеки критичних компонентів АСУ ТП.

Перші повідомлення про кібератак до ICS надходили понад 15 років тому. Відтоді загальний обсяг зростав експоненціально і набагато перевищує показники новин. Поширені сумніви та втрата довіри громадськості до цих приватних та державних організацій призводять до навмисного приховування інформації про атаки; але погане поширення інформації серед громадськості також може призвести до імпульсивних реакцій та рішень, які можуть бути не найкращими. Повідомлення про кібератак регуляторним органам, галузевим колегам та організаціям підтримки є більш розумним варіантом. Це допомагає створювати рішення, зменшувати ризик майбутніх атак та розробляти сильніші захисні стратегії.

Безпека, розроблена з самого початку

Історично склалося так, що, оскільки безпека була несуттєвою проблемою, цілісність та безпека критичних компонентів АСУ ТП не була розроблена та впроваджена в ICS. Тепер вона має бути невід'ємною частиною будь-якого проекту. Сектор критичної інфраструктури повинен тісно співпрацювати з власниками, галуззю, інтеграторами, регуляторами та постачальниками, щоб ефективні заходи цілісності та безпеки критичних компонентів АСУ ТП могли бути інтегровані в ICS з самого початку.

Загалом, промисловому сектору потрібно перестати думати про безпеку як про щось, що потрібно впроваджувати після встановлення систем. Безпеку потрібно розробляти на самому початку та керувати нею на всіх рівнях підприємства. Найважливішим кіберкомпонентом в ІКС є самі пристрої, а

цілісність та безпека критичних компонентів АСУ ТП ІКС має бути зосереджена на забезпеченні безпеки та надійної роботи цих пристроїв.

Кіберзагрози, спрямовані на ІКС, змінюються та зростають, оскільки кіберзлочинці постійно шукають нові цілі, а злочинне вимагання зростає. Безпека ІКС більше не зосереджена лише на запобіганні хакерам чи наявності надійного фізичного периметра. Підпільна цифрова економіка забезпечує багатомільярдний стимул для потенційних корпоративних конкурентів або супротивників використовувати вразливості ІКС. Більше компаній повинні будуть детально описати свій підхід до цілісності та безпеки критичних компонентів АСУ ТП та детально описати, який аналіз та оцінку вони провели для своїх постачальників технологій та послуг. Уряди усвідомлюють, що цілісність та безпека критичних компонентів АСУ ТП є однією з найсерйозніших економічних та національних проблем безпеки, з якими вони стикаються, і активізують свої зусилля щодо захисту вразливостей критичної інфраструктури.

Ініціативи постачальників ІКС щодо зниження ризиків безпеки для систем керування призводять до того, що фахівці з автоматизації можуть ефективніше захищати свої промислові процеси завдяки поєднанню проектування систем керування та передових практик, технологій та професійних послуг. Оскільки ІКС є основою виробництва, процеси цілісності та безпеки критичних компонентів АСУ ТП повинні враховувати як внутрішні, так і зовнішні загрози за допомогою кількох рівнів захисту, які пом'якшують різні типи ризиків.

Постачальники ICS та фахівці з автоматизації повинні бути прагненням надавати постійно оновлюваний набір продуктів та послуг, які допомагають зменшувати ризики та покращувати безпеку виробничих активів. Рішення також повинно включати аналітику ризиків, яка збирає та співвідносить дані на платформі, що забезпечує практичну видимість сліпих зон цілісності та безпеки критичних компонентів АСУ ТП. Це сприяє ефективному управлінню кіберризиками та створює сильнішу позицію в галузі цілісності та безпеки

критичних компонентів АСУ ТП. Рішення повинні дозволяти організаціям розуміти своє поточне бізнес-середовище та забезпечувати контекстуальне усвідомлення того, як їхні співробітники, ланцюги поставок, клієнти та зловмисники взаємодіють з їхніми системами управління, даними, об'єктами та додатками. У глобально взаємопов'язаному світі загроза може виходити і виходить звідусіль.

Зробіть цілісність та безпеку критичних компонентів АСУ ТП частиною культури організації

Традиційні підходи до цілісності та безпеки критичних компонентів АСУ ТП є необхідними, але недостатніми для належного захисту організацій. Організації необхідно спонукати інвестувати в найкращі технології, розуміти свою екосистему та співпрацювати з надійними партнерами для спільного захисту екосистеми. Організації повинні розуміти необхідність періодичного проведення оцінок вразливостей через цінність, яку вони надають. Це дозволяє співробітникам компанії бачити бізнес-процеси, а також програми та дані, що їх підтримують, а також картографувати інфраструктуру, яка з'єднує обладнання.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

2.1 Огляд існуючих систем, технологій, архітектур, програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти

Відомо, що засновані на стандартах, відкриті, сумісні та безпечні системи архітектури автоматизації процесів працюють або розробляються в ExxonMobil, Reliance Industries, Shell та Texas A&M.

Ппрограмно-визначеної автоматизації (ПВАП) недостатньо для забезпечення відкритості, сумісності або відповідності стандарту Open Process Automation System (O-PAS) – це «стандарт стандартів», розроблений Форумом з відкритої автоматизації процесів (OPAF) . Експерти, що беруть участь у цій 10-річній ініціативі зі стандартизації, рекомендують вказувати відповідність OPA в будь-якому запиті на пропозицію системи автоматизації процесів. Деякі фахівці, близькі до цієї ініціативи, припускають, що постачальники автоматизації підтримують стандарт або втрачають частку ринку на користь тих, хто його підтримує.

Інтерес виходить за межі нафти і газу; OPAF заявила, що інтерес включає харчову промисловість та напої, металургію та гірничодобувну промисловість, нафтохімічну, фармацевтичну, целюлозно-паперову промисловість, комунальні послуги та інші компанії, що використовують архітектури розподілених систем керування (DCS) та промислових систем керування (ICS).

Проєкти OPA реальні та розширюються

Прогрес у сфері автоматизації процесів (OPA) є результатом десятиліття роботи. OPA реальний, як описано в проекті ExxonMobil, детально поясненому минулого року, де головний інженер, відповідальний за проект, відвідав галузевий форум ARC лише через кілька тижнів після запуску.

У минулому він би не пішов після стартапу. Зараз ми розширюємо

відкриті екосистеми для меншої інженерії, багаторазового використання інтелектуальної власності та системної інтеграції. Тепер ми без жодних проблем розгортаємо нову систему на основі OPA на резервуарному парку хімічного терміналу Батон-Руж Анкоридж (ACT).

Минулого літа в Індії розпочався проект на основі OPA, розгортання якого очікується у 2027 році, сказав Макконнелл. Серед стандартів, що використовуються, є стандарт IEC 61499 Control Runtime Standard-Open та стандарт контролерів IEC 61131. У стандарті IEC 61499 функціональні блоки інкапсулюють інструкції та мають власний подієвий автомат станів, що дозволяє інтеграцію програмного та апаратного забезпечення від різних постачальників, бібліотеки функцій, структурований зв'язок з іншими пристроями та системами. Використовуючи аналогію з магазином додатків, стандарт забезпечує портативність та повторне використання (людина-машинний інтерфейс, сигналізація, історія подій) для більших можливостей та гнучкості. Немає потреби в надмірно складній системі.

Відкриті системи підвищують ефективність завдяки структурованій інкапсуляції, що дозволяє створювати складені блоки з елементів повторного використання, а не типові логічні блоки.

Контроль на основі станів та візуальне представлення логіки та потоку даних можна безпосередньо переносити на інші системи, якщо вони відповідають стандарту.

Контейнерні конструкції забезпечують швидке розгортання з апаратною незалежністю. Логіку можна призначити іншим контролерам за потреби під час збою.

Керування на основі послідовності/умов може співіснувати в контролерах. Розподілена логіка дозволяє розробляти стійкі до відмов стратегії керування, займаючи лічені хвилини замість тижнів чи місяців, як це було раніше. Можлива простіша інтеграція типів керування з очікуваними в майбутньому легшими оновленнями.

UniversalAutomation.org (UAO) налічує понад 100 членів (включаючи директорів ASRock, ExxonMobil, Intel, Kongsberg Marine, Kyland Group, Novo Nordisk, Schneider Electric, Wood Group та Yokogawa); ця некомерційна організація контролює спільну екосистему портативного, сумісного програмного забезпечення, що забезпечує простоту підключення, що демонструє шалений успіх IEC 61499.

Тестування та сертифікація допомагають у впровадженні OPA

10-річні зусилля створили стандартизовану, відкриту, сумісну, безпечну систему архітектури автоматизації процесів з компонентами O-PAS. Заходи з тестування та сертифікації O-PAS допомагають забезпечити працездатність продуктів. Тестові стенди та виробничі системи з 2017 по 2024 рік демонстрували постійне вдосконалення в циклі зворотного зв'язку.

Варіанти: Розподілений вузол керування, гібридні застосування, заміна

Зараз увага зосереджена на впровадженні OPA, а не на тестуванні чи демонстраціях. Шляхи використання OPA: 1) використання лише розподіленого вузла керування [DCN], 2) гібридне застосування або 3) копіювання та заміна. Останній варіант найменш ймовірний.

Більше комерційних компонентів OPA, доступні навички

Технології дозріли, і з'явилося більше комерційних пропозицій. Невеликі проекти можуть допомогти «розвинути навички» на шляху до встановлення великих систем. Ми спираємося на успіхи, щоб впливати на ринок.

Розгортання застосовує автоматизацію там, де її не було. Це менша система, але комерційний проект, сказав він, з бізнес-потребами, що виходять за рамки дослідницької та розробницької реалізації проекту Lighthouse, описаного минулого року. У запиті пропозицій для ACT згадувалося OPA. Системний інтегратор допоміг з впровадженням. Заводські приймальні випробування (FAT) проведено, і система готова до виробництва у другому кварталі. Серед постачальників – OSI, Phoenix Contact, ASI та Phoenix Micro. Системи OPA не потребують проміжного програмного забезпечення, стійкі до залежності від

постачальника та готові до використання з полиці.

Системи OPA: деякі компроміси до досягнення критичної маси

Хоча переваги вже доступні, існують деякі компроміси між традиційними пропозиціями DCS та системами OPA. Традиційні системи керування швидко розгортаються, мають перевірену надійність і мають команди підтримки для виправлень, оновлень безпеки та дорожніх карт продукту. Комерційні системи OPA мають максимальну гнучкість проектування без прив'язки до постачальника, адаптивність, а проекти можуть точно відповідати вимогам, обмеженням та інноваціям. Нові системи усувають проміжне програмне забезпечення та необхідність «чарівного пилу зверху, щоб вони працювали», – сказав Ітон. Він додав, що OPA зменшує компроміси та тягар доказування надійного виконання та системної інтеграції, особливо з мережевими та реагуваннями на збої.

OPA та екосистема, що базується на стандартах

Метою комітету OPAF та партнерів по співпраці є розробка екосистеми систем на основі відкритих стандартів, яка може включати:

– Ethernet розширеного фізичного рівня (APL).
– Модель даних OPC UA FX.
– L2 BPCS.
– EN MCS.
– IEK 61850.
– IEK 62714.
– OPC UA (PA DIM, MDIS).
– Безпека IEC 62443.
– Програмно-визначені системи (такі як пропозиції COPA).
– Використання хмари на рівні L3 як відкритого середовища.

Інтеграційний канал OPA в IT-простір базується на робочих стандартах та відкритих архітектурах від O-PAS та зацікавлених сторін.

Мотивацією для використання системи автоматизації відкритих процесів є уникнення застарівання операційної системи, високі витрати на зворотну

сумісність, вимоги до прибутку та ризики традиційних систем управління системами.

Відкрита автоматизація процесів у Reliance Industries дозволяє уникнути ризиків

Мотивація для використання Open Process Automation:

– Часте старіння операційних систем Microsoft без встановлення патчів та пов'язані з цим вразливості безпеки.

– Висока вартість зворотної сумісності

– Високі вимоги до прибутку

– Ризики традиційної DCS.

Цілі тестового стенду включають сумісність між кількома постачальниками, включаючи Schneider Electric, Yokogawa, ZabbiX, ASRock, Stahl, Omega та Stardom. Архітектура програмного забезпечення на першому етапі включає сумісність DCN, функціональні блоки, цілісність та безпеку критичних компонентів АСУ ТП, магістральну мережу OPC UA та відповідність O-PAS.

Фаза 2 удосконалень та розширене тестування з приблизно 250 входами/виходами, інтеграцією з п'ятьма протоколами (HART, Fieldbus Foundation, Modbus, Profibus, Ethernet APL), безпекою 2-го рівня та оцінкою загальної вартості володіння.

Контролер Phoenix Contact може бути частиною системи COPA 500 (або можна використовувати інший контролер). Моделі процесів на основі штучного інтелекту доступні для керування за допомогою розширених DCN. Агент Redfish від Ignition знаходиться на DCN I/O. Усі п'ять частин системного ПЛК перетворені на систему автоматизації процесів, як пояснила на форумі лідерства ARC 2026 консультативна група ARC.

Елементи системи OPA: зв'язок, опції контролера

COPA 500 може використовувати контролер Phoenix Contact, але не обов'язково. Моделі процесів на основі штучного інтелекту доступні для керування за допомогою розширених DCN. Агент Redfish від Ignition

знаходиться на DCN I/O. Усі п'ять частин системного програмованого логічного контролера (ПЛК) перетворюються на систему автоматизації процесів.

Для отримання доступу до підключення програм до PLCnext Edge Gateway через налаштовувану веб-сторінку не потрібно нічого вивчати. Протягом години комфорт дорівнює використанню того, що є в хмарі. Орієнтований на клієнта продукт не має програмного коду. Стажер може керувати ним так само легко, як і людина з 40-річним досвідом. За словами Дурбіна, блоки коду використовують ті ж концепції, що й навчання програмуванню для третьокласників.

COPA 500, розроблений для 100–1000 вводів/виводів, використовує програмне забезпечення для автоматизації запалювання від Inductive Automation, як пояснила консультативна група ARC на форумі лідерства ARC 2026 року. Апаратне забезпечення, програмне забезпечення та компоненти сумісні в системах OPA.

COPA 500 використовує програмне забезпечення для автоматизації запалювання від Inductive Automation. COPA 500 розрахована на 100-1000 входів/виходів. COPA 50 обробляє менші системи або конструкції блоків з 10-100 входами/виходами.

Програмно-визначена автоматизація (ПВАП) – це впровадження віртуалізації та технології контейнерів, тоді як Стандарт відкритої автоматизації процесів (OPA) приймає віртуалізацію та контейнери та виходить за рамки цього, щоб визначити галузеві стандарти інтерфейсів даних, інформаційних моделей та інтерфейсів управління системами для ключових атрибутів якості – модульності, сумісності та взаємозамінності.

Техаський університет A&M використовує COPA та OPA-S для свого теплообмінника на невеликому модульному ядерному реакторі в Коледж-Стейшн. Також очікується, що проект терміналу ExxonMobil у Порт-Аллені поблизу Батон-Руж буде введено в експлуатацію у березні; FAT – у січні.

Оскільки багато традиційних систем управління системами керування (DCS) наближаються до застарілості, O-PAS знижує вартість традиційних

рішень, додав він.

Як програмно-визначена автоматизація допомагає ОРА

Оскільки цифрова трансформація допомагає виробничим операціям, SDA стає фундаментальним фактором гнучкості, масштабованості та інновацій. Переваги SDA можуть включати швидше розгортання, покращену сумісність систем та підвищену швидкість реагування. Це допомагає впоратися з ринковими та операційними змінами з особливим акцентом на цілісність та безпеку критичних компонентів АСУ ТП, інтеграцію застарілих технологій та готовність робочої сили.

Раніше вузьким місцем були ПЛК та проводка. Тепер це управління змінами та мережі. Програмно-визначена автоматизація – це як терапія для пар для команд операційних технологій та інформаційних технологій (ОТ та ІТ).

Програмно-визначена автоматизація розділяє програмне та апаратне забезпечення

SDA розділяє логіку керування та власне обладнання. Логіка може працювати на будь-якому обладнанні або віртуальних контролерах. SDA, якщо відповідає стандартам, може уникнути обмежень застарілих систем, а системи, пов'язані з власним обладнанням, перешкоджають масштабованості та інноваціям. Традиційна автоматизація стає ще дорожчою в обслуговуванні, оскільки кваліфіковані інженери виходять на пенсію.

SDA забезпечує гнучкість, спритність та стійкість. Цифрові зусилля на цьому не можуть зупинитися. Трансформація вимагає змін у бізнесі. Цифрові архітектури сприяють цифровій трансформації.

Об'єкти потребують уваги до IT/OT та цілісності та безпеки критичних компонентів АСУ ТП. Програмні платформи можуть мати мікросервери та відкриті й віртуалізовані системи автоматизації. Відкриті та віртуальні контролери пропонують більше можливостей і використовуються дедалі ширше. Не зосереджуйтесь настільки на технологіях, щоб забути про корисні суспільні зміни.

Open Process Automation пропонує відкриті, безпечні системи на основі

стандартів, які прискорюють інновації та створення цінності. OPA підвищує конкуренцію постачальників, зменшує бар'єри для нових технологій, знижує витрати на інтеграцію та життєвий цикл, повторно використовує програми керування в різних системах, а також є безпечною та адаптивною за своєю суттю.

Сертифікація OPA гарантує, що прості пристрої можуть працювати зі складнішими, знижуючи витрати на інтеграцію та життєвий цикл. Цього року Open Process Automation Forum виповнюється 10 років, і з'являється більше варіантів та можливостей вибору. Доступно більше комерційних продуктів.

Що таке система на основі O-PAS? До її атрибутів належать стандартна інформаційна модель, розв'язання обчислень та вводу/виводу, а також програмного та апаратного забезпечення. Програмно-визначене резервування для середовища виконання логіки керування та програмно-визначена архітектура. Сертифікація компонентів триває.

Де ж місце займає SDA? Воно знаходиться на стандартній схемі архітектури керування процесами: обчислення DCN, платформа розширених обчислень, мережевий ввід/вивід та маршалінг, а також програма виконання IEC 61499.

Сам по собі програмно-визначений характер не означає сумісності

SDA не обов'язково означає сумісність або портативність, хоча SDA може досягти обох цілей. OPA використовує SDA як основний принцип, як показано в комерційному проекті ExxonMobil Light House (див. посилання вище).

Діяльність партнерів ExxonMobil та інших членів O-PAF демонструє цінність.

Дивіться далі маркетингового галасування та будьте розумним споживачем. На цьому етапі відповідність OPA має бути пунктом каталогу, а не дорожньою картою. Повідомте про ці потреби постачальників. Відкритість має бути в компонентах автоматизації, які ми купуємо. SDA дозволяє оркестрацію та зниження витрат, полегшуючи навантаження на кінцевих користувачів.

Відкрита та стандартизована модель даних забезпечує легшу інтеграцію, варіанти вибору продуктів та відкриває ринок більшої потенційної клієнтської бази, зацікавленої в OPA.

SDA використовує сучасні концепції програмної інженерії з взаємозамінністю програмного забезпечення та портативністю додатків. Кінцеві користувачі повинні повідомляти про свої потреби. Це комерційно продемонстровано та рекомендовано для майбутніх впроваджень.

Бібліотеки керування розроблені, спільно використовуються

Shell Scotford має двох операторів хімічного заводу, який займається уловлюванням вуглецю та сонячними електростанціями.

У 2008 році, коли завод запустили, на ньому працювало сім операторів і не було жодного простою. Ремонт на основі ноутбуків займав тиждень, «часу, якого у нас не було». Система почала перевантажуватися через збій на хімічному заводі минулого року. У:

У 2021 році було встановлено стрічковий прес із застарілим ПЛК.

У 2023 році було використано осушувач повітря, щоб довести, що SDA та UAO можуть працювати на різних платформах.

Випробувальний стенд проекту біоочисної установки 2024 року з понад 300 входами/виходами продемонстрував високу надійність.

Бібліотеки продовжують розроблятися та поширюватися. Існує потреба в процедурній автоматизації, послідовному управлінні, подієво-орієнтованому підході, сумісності з IEC 61499 та іншими стандартами (S88, ISA-106 та PackML), а також у новому налаштованому кінцевому автоматі.

Іноді потрібно зробити щось за п'ять хвилин, не встигаючи документувати. Ми хочемо взяти ці процедури, і забезпечити їх впровадження з досвідом найдосвідченішої людини в нашому персоналі.

Композитні типи автоматизації (CAT) забезпечують відображення графа стану вибраної моделі. Блоки, згенеровані за стандартом IEC 61499, є результатом автоматично згенерованого коду. HMI також генерується автоматично.

Для демонстрації потрібно було, щоб SDA використовувала CAT та розташовувалася поверх існуючої DCS. Для зв'язку використовуватиметься клієнт-серверний зв'язок OPC UA. Моделювання емулює поведінку DCS за допомогою HMI, згенерованого SDA.

Симулятор імітує реальний завод та 90% можливих помилок до розгортання. Вам не потрібно позбавлятися старих систем». Експерти можуть виконати перехід, спочатку працюючи над невеликими успіхами, а потім співпрацювати з керівництвом та іншими людьми для розширення, сказав він. Адаптація до сучасних систем (SDA) може бути швидшою, дешевшою та безпечнішою.

Не дозволяйте SDA замінити переваги сумісності OPA

«Фраза «програмно-визначена автоматизація» почала з’являтися в маркетингових повідомленнях постачальників систем управління близько двох років тому, приблизно у 2024 році:

– Schneider Electric: «відкрита програмно-визначена автоматизація» з EcoStruxure Automation Expert [1].

– Rockwell Automation: «програмно-визначена автоматизація» з Automation DevOps та FactoryTalk [2].

– Emerson: «програмно-визначені можливості» з DeltaV версії 16 та Boundless Automation [3].

– Siemens: «програмне забезпечення визначило все» з Industrial Operations X та Industrial Edge[4].

– Honeywell: «програмно-визначені висновки» з Aptica, Forge та Experion [5].

– ABB: «програмно-визначена автоматизація» з Automation Extended [6].

– Yokogawa: «програмно-визначені системи керування», що безпосередньо посилаються на системи на основі стандарту відкритої автоматизації процесів (O-PAS) [7].

– Для повноти картини також зазначимо, що існує компанія під назвою Software Defined Automation. [8].

Порівняння SDA з Open Process Automation, як визначено у стандарті O-PAS:

– Коротко кажучи, програмно-визначена автоматизація – це впровадження віртуалізації та контейнерних технологій.

– На відміну від цього, O-PAS використовує віртуалізацію та контейнери, а також виходить за рамки цього, щоб визначити стандартні галузеві інтерфейси даних, інформаційні моделі та інтерфейси управління системами для ключових атрибутів якості – модульності, сумісності та взаємозамінності.

Кінцеві користувачі повинні поставити три запитання постачальнику, який пропонує SDA:

1. Чи буде система SDA постачальника сумісною з системою SDA іншого постачальника?

2. Чи зможу я перенести свої програми з системи SDA одного постачальника на систему SDA іншого постачальника без перезапису?

3. Чи буде економія коштів постачальника SDA від використання апаратного забезпечення загального призначення передана мені для зниження початкової та загальної вартості володіння?

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Для реалізації програмного забезпечення апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП було використано середовище розробки Visual C++. Сучасні програмні системи управління технологічними процесами та контролю захищеності характеризуються надзвичайно високими вимогами до надійності, швидкодії та детермінованості виконання завдань, що робить розробку подібного софту виключно за допомогою базових інструментів трудомістким процесом. Для нівелювання цих складнощів, оптимізації створення інтерфейсів операторів та

стандартизації взаємодії з операційною системою застосовуються спеціалізовані об’єктно-орієнтовані бібліотеки класів, зокрема MFC (Microsoft Foundation Classes).

У контексті архітектури безпеки АСУ ТП критично важливим є забезпечення мінімальних затримок під час обробки неперервних потоків телеметричних даних, перевірки цілісності конфігурацій промислових контролерів та реагування на кіберінциденти. Бібліотека MFC виступає структурованим каркасом (framework), який інкапсулює низькорівневі системні виклики Windows API, спрощуючи розробку багатопотокових служб, взаємодію з локальними базами даних журналювання та інтеграцію захисних механізмів у єдиний апаратно-програмний комплекс.

Головними перевагами застосування Visual C++ та MFC у розробці системи забезпечення цілісності АСУ ТП є:

– Висока продуктивність і низькі накладні витрати: компільований код на C++ гарантує максимальну швидкість виконання операцій у реальному часі, що є життєво необхідним для промислових середовищ, де неприпустимі затримки обробки аварійних сигналів.

– Інкапсуляція та модульність: об'єднання складних інтерфейсів API та системних протоколів у логічну ієрархію класів значно спрощує підтримку коду, його розширення та аудит безпеки.

– Багаторазове використання коду (Reusability): за рахунок механізмів спадкування розробник може швидко створювати стандартизовані компоненти для перевірки контрольних сум, аналізу стану критичних вузлів та генерації тривожних сповіщень.

– Автоматизація прототипування: вбудовані засоби генерації додатків дозволяють оперативно формувати базову структуру багатооконних панелей оператора-технолога та диспетчерських пультів моніторингу безпеки.

Таким чином, використання мови Visual C++ спільно з ієрархією класів MFC забезпечує створення надійного, продуктивного, стійкого до збоїв та масштабованого програмного ядра для апаратно-програмного комплексу захисту критичних компонентів АСУ ТП.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускну кваліфікаційну роботу за другим (магістерським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

В процесі розробки випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти необхідно виконати наступний обсяг роботи:

а) провести аналіз існуючих систем-аналогів для виявлення їх позитивних і негативних якостей. Результати аналізу врахувати в подальших розробках;

б) вибрати та обґрунтувати методику побудови системи контролю роботи технологічного обладнання на виробництві в автоматизованому режимі. Розробити функціональну та структурну схеми системи;

в) розробити програмне забезпечення системи, що дозволить реалізувати поставлену технічним завданням задачу. Побудувати блок-схеми алгоритмів програми та підпрограми;

г) організувати інтерфейс користувача з метою формування та виводу на екран ЕОМ повідомлень про некоректні дії користувача та нестандартні ситуації в роботі технологічного обладнання;

д) розробити рекомендації по організаційних та методичних заходах, які забезпечать впровадження системи в промислову експлуатацію та її подальшу успішну експлуатацію;

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

ж) розробити заходи по охороні праці при впровадженні та експлуатації системи, а також розробити заходи з цивільного захисту;

з) сформувати висновки про виконаний обсяг робіт та одержані результати.

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Оскільки рішення з цілісності та безпеки критичних компонентів АСУ ТП все частіше інтегруються в операції та політики організацій, існують ключові складові, які можуть сприяти впровадженню цільових рішень для середовища ICS:

1. Аудит та застосування політик і процедур безпеки, розроблених спеціально для мережі системи управління та її пристроїв.

2. Контроль доступу через локальну мережу (LAN), глобальну мережу (WAN) та фізичні периметри, доповнений безпечною передачею даних.

3. Виявлення загроз аномальної та шкідливої активності на всіх рівнях інфраструктури ICS.

4. Управління ризиками та зменшення їхнього впливу на можливі атаки за допомогою встановленого пакету продуктів безпеки, які покращують та регулюють ICS без порушення контрольованого процесу – віртуалізовані функції та апаратні засоби.

5. Безпека та автентифікація датчиків процесів.

6. Вирішення ключових проблем безпеки, що вимагає тісний зв'язок з постачальниками.

Вищезгадані товари зазвичай пропонуються через три або чотири компанії; це суміш виробників оригінального обладнання (OEM), консультантів та постачальників програмного забезпечення. Група найкращих у своєму класі відповідних компаній надасть кінцевим користувачам найкраще у своєму класі рішення, універсальний магазин.

Розгляньте внутрішні та зовнішні загрози цілісності та безпеці критичних компонентів АСУ ТП без обмежень

Ініціативи постачальників ІКС щодо зниження ризиків безпеки систем керування у відповідь на зростаючі кіберзагрози призводять до того, що фахівці з автоматизації ефективніше захищають свої промислові процеси завдяки поєднанню проектування систем керування та передового досвіду, технологій та професійних послуг. Оскільки ІКС є основою виробництва, процеси цілісності та безпеки критичних компонентів АСУ ТП повинні враховувати як внутрішні, так і зовнішні загрози за допомогою кількох рівнів захисту, що пом'якшує різні типи ризиків; методологія глибоко поглибленого електронного та фізичного захисту з урахуванням ризиків.

Постачальники ICS та фахівці з автоматизації повинні бути прагненням надавати постійно оновлюваний набір продуктів і послуг, які допомагають зменшувати ризики та покращувати безпеку виробничих активів. Інформаційні силоси, що існують в організаціях сьогодні, призводять до того, що інформація про безпеку рідко використовується спільно. Постачальники комплексних рішень будуть купувати, інтегрувати та сприяти впровадженню нових технологій цілісності та безпеки критичних компонентів АСУ ТП та надавати кінцевим користувачам необхідний комплексний продукт безпеки.

Шість ключових складових можуть сприяти розробці цільових рішень для середовища ICS:

1. Аудит та застосування політик і процедур безпеки.

2. Контроль доступу з безпечною передачею даних.

3. Виявлення загроз аномальної та шкідливої активності на всіх рівнях інфраструктури ICS.

4. Управління ризиками та їх пом'якшення.

5. Безпека та автентифікація датчиків процесів.

6. Вирішення ключових проблем безпеки, що вимагають тісний зв'язок з постачальниками. Надано: MG Strategy+, Control Engineering.

Акцент на цілісності та безпеці критичних компонентів АСУ ТП промислових датчиків

Раніше ІКС задовольняли потреби безпеки завдяки ізоляції від корпоративних систем та фізичній безпеці. З огляду на сучасний попит на можливості віддаленого доступу, підключення бізнес-систем та проектування зі стандартним галузевим обладнанням та програмним забезпеченням, ці системи тепер мають ширшу поверхню для атак. Організації більше не можуть просто контролювати цифровий периметр; їм потрібно контролювати, де можна знайти свої дані, а також в межах автоматизованих бізнес-процесів та вертикальних каналів, які можуть зашкодити надійності, безпеці та цілісності організації у разі порушення.

Застарілі технологічні датчики не мають захисту від цілісності та безпеки критичних компонентів АСУ ТП

Мільйони застарілих датчиків процесів використовуються в критично важливих секторах інфраструктури без цілісності та безпеки критичних компонентів АСУ ТП, автентифікації чи файлів журналів, і навряд чи вони будуть оновлені для підвищення рівня безпеки. Ця екосистема датчиків, комунікаційних протоколів та вбудованих технологій створює перешкоду для цілісного управління кібербезпекою.

Ініціатива щодо цілісності та безпеки критичних компонентів АСУ ТП промислових систем управління, оголошена урядом США у липні 2021 року, спрямована на сприяння впровадженню технологій та систем, що забезпечують мережевий підхід до видимості загроз, індикаторів, виявлення та попереджень без урахування польових пристроїв (датчиків тиску, температури, напруги).

Датчики, виконавчі механізми та електричні приводи – це інженерні системи, а не «мережеві» пристрої. Вони були розроблені для задоволення експлуатаційних вимог до процесів, а також для забезпечення надійності та безпеки. Ці датчики передають вхідні дані до ICS та її мережі, де створюється враження, що вхідні дані датчиків не скомпрометовані та правильні.

Коли вхідні дані датчиків не автентифіковані, накопичувачі та

контролери, що отримують сигнали датчиків, не мають засобів автентифікації походження сигналів датчиків і тому приймають вхідні дані датчиків і реагують відповідно; це вразливість, яку зловмисники можуть використовувати, використовуючи бекдори в обладнанні електромережі та інших подібних пристроях. Існує дефіцит кіберкриміналістики на рівні датчиків, що ускладнює визначення того, чи були інциденти зловмисними чи випадковими.

Моніторинг фізичного рівня заохочує співпрацю IT/OT

Постійна увага зацікавлених сторін [інформаційних технологій (IT) та операційних технологій (OT) та інших] до забезпечення промисловості точними, безкомпромісними та автентифікованими вимірюваннями датчиків процесів є основною вимогою для моніторингу обладнання, безпеки процесів, контролю процесів та цілісності та безпеки критичних компонентів АСУ ТП, оскільки це впливає на стійкість, якість продукції, цифрових двійників та аналітику великих даних.

Моніторинг фізичного рівня процесу за допомогою датчиків, а не підхід «зверху вниз» до вразливостей мережі, заохочує співпрацю між мережевими та інженерними командами для виявлення відхилень у роботі датчиків, таких як дрейф, порушення ланцюга поставок або цілісність та безпека критичних компонентів АСУ ТП, що може забезпечити повернення інвестицій (ROI) шляхом оптимізації технологічних операцій, перевірки цифрових двійників та переходу до прогнозного обслуговування.

Датчики надають дані, на основі яких приймаються рішення щодо контролю, і тому повинні належати до категорії критичних активів для представлення процесу. Якщо продукт забруднюється або система контролю реагує негативно через зловмисні маніпуляції хакерами параметрами датчиків, це може призвести до пошкодження обладнання, травмування персоналу, недовіри громадськості або поєднання всіх трьох факторів.

Вразливість водопровідної системи, порушення, автентифікація

У 2020 році ізраїльські ЗМІ повідомили, що хакери проникли в комп'ютерну мережу об'єктів, які контролюють систему водопостачання Ізраїлю,

та вивели з ладу датчик, який виявляє рівень хлору. Без цього критично важливого датчика рівень хлору в питній воді міг би досягти токсичного рівня або впасти достатньо низько, щоб спричинити появу бактерій у воді. Хоча атака була невдалою, вона спонукала до масштабної ініціативи, спрямованої на забезпечення надійності сенсорних пристроїв та їхньої наявності процесу автентифікації. Виявлення аномалій процесу виявляє будь-яку аномалію незалежно від причини, а також прогнозує вихід з ладу компонентів.

Постачальники датчиків та програмного забезпечення для цілісності та безпеки критичних компонентів АСУ ТП співпрацюють над розробкою рішень, які не зосереджені на аномаліях мережі, а також виявляють аномалії процесу керування або датчиків шляхом моніторингу ситуаційної обізнаності про процес незалежно від мережі – контрольно-вимірювальні системи проти мереж Ethernet. Економічно ефективні та ефективні рішення, що забезпечують безпеку промислових об'єктів, мають вирішальне значення для майбутнього світової економіки.

3.2 Розробка структурної схеми

Поради щодо цілісності та безпеки критичних компонентів АСУ ТП промислових систем управління (ІСУ), найкращі практики

Катастрофічна катастрофа може бути результатом ненадійних практик промислової цілісності та безпеки критичних компонентів АСУ ТП. Дивіться шість поширених точок входу для атак, вісім запобіжних заходів цілісності та безпеки критичних компонентів АСУ ТП для атак за типом та чотири кроки для покращення.

Хоча цілісність та безпека критичних компонентів АСУ ТП завжди була серйозною проблемою для будь-якої галузі, поширеною думкою було те, що загроза стосувалася втрати конфіденційних даних, стати жертвою шпигунства та зіткнутися з припиненням роботи. Однак атака Triton (також відома як Trisis або HatMan) у 2018 році показала інший бік цієї дуже серйозної загрози: потенційно

катастрофічну катастрофу. Дізнайтеся про поширені точки входу атаки, запобіжні заходи та способи покращення.

Традиційно, промислові системи керування (ІКС) проектувалися для роботи ізольовано у власних мережах керування, де мало хто міг передбачити загрозу з боку цілісності та безпеки критичних компонентів АСУ ТП. Однак, з розвитком інших технологій навколо промислових об'єктів, включаючи інтелектуальні датчики, бездротові шлюзи, дистанційно керовані системи, віртуалізацію, хмарні обчислення, смартфони та різні потреби бізнес-аналітики, шанси на те, що ці промислові системи залишаться вільними від зовнішнього втручання, з кожним днем зменшуються.

Першим випадком зовнішнього маніпулювання ІКС став Stuxnet у 2010 році – скрипт, навмисно розроблений для саботажу промислових контролерів, що керують центрифугами. Після цього у 2013 році відбулася атака Havex, спрямована на електромережі та енергетичні компанії; через неї було зібрано велику кількість даних для шпигунства та саботажу.

У 2015 році існувало дві загрози: BlackEnergy, яка знищувала дані та файли на робочих станціях, спричиняючи значні перебої з електропостачанням в Україні, та IronGate, яку було виявлено у відкритих джерелах і яка виконувала ту саму функцію, що й Stuxnet. Industroyer також спричинив хаос в Україні у 2016 році за допомогою шкідливого програмного забезпечення, яке видаляло дані та виконувало розподілені атаки типу «відмова в обслуговуванні» (DDoS) на мережу, що призвело до відключення українських електромереж.

Атаку Triton було виявлено у 2017 році. Її виявлення запобігло тому, що могло б стати серйозною катастрофою. Це шкідливе програмне забезпечення могло заразити контролери безпеки Triconex, надаючи хакеру доступ до зміни параметрів безпеки. Зловмисна атака могла вимкнути встановлені значення безпеки для промислового обладнання, що потенційно могло спричинити інцидент такого ж масштабу, як вибух на хімічному заводі Jiangsu Tianjiayi, який стався в Китаї у березні 2019 року.

Розуміння джерел атак

Першим кроком у боротьбі з цією загрозою цілісності та безпеці критичних компонентів АСУ ТП є розуміння того, звідки можуть виникати атаки, оскільки зловмисники використовують розвідку як перший крок для оцінки та розуміння слабких місць цілей протягом певного періоду. У довгостроковій перспективі організація може використовувати аналіз векторів загроз, щоб визначити різні методи, які може використовувати зловмисник, або до яких може бути схильна система. Все це має ґрунтуватися на ризику, що виникає в результаті аналізу впливу активів компанії на бізнес. Користувачі можуть захотіти взяти деякі готові інструменти оцінки та використовувати їх для відокремлення та раціоналізації критичних активів від некритичних та провести оцінку прогалин у них для початку.

Шість поширених точок входу для зловмисників:

1. Вхідні атаки із зовнішніх мереж, інтернету та віддалених з’єднань через програмне забезпечення для планування ресурсів підприємства (ERP), шлюзи, сховища даних і документів та онлайн-архіви.

2. Неправильно налаштовані брандмауери та шлюзи.

3. Доступ користувачів до робочих станцій та комп’ютерів керування через викрадені або фішингові облікові дані.

4. Фізичні атаки, спрямовані на виробничі системи, у більшості випадків це людино-машинні інтерфейси (HMI), робочі станції інженерів та операторів, а також фактичні контролери безпеки процесів.

5. Латеральні мережеві атаки, спрямовані на мережі керування та використовують промислові комунікаційні протоколи для виявлення інших пристроїв у мережі та поширення шкідливого коду.

6. Атаки соціальної інженерії, які зосереджені на використанні особистої інформації для обману інсайдерів, щоб вони надали доступ, відкрили шлюзи та ненавмисно запустили скрипти.

Вісім запобіжних заходів у цілісності та безпеці критичних компонентів АСУ ТП

Кожен тип атаки має свій власний набір запобіжних заходів. Ось деякі з них:

1. Сегрегація та сегментація

Хоча це може здатися очевидним, ретельна оцінка прогалин у мережі керування за допомогою інструментів та кваліфікованого персоналу часто може виявити багато неконтрольованих точок доступу, які ігноруються під час дотримання стандартних практик захисту мережі керування. Ці загрози можуть виникати з:

– Необмежений доступ до робочих місць інженерів/операторів.

– Застаріле виявлення шкідливого програмного забезпечення.

– Сторонні програми та конектори, які не були захищені або перевірені.

– Відсутність демілітаризованих зон (DMZ) або діодів передачі даних під час експорту даних з мереж керування.

– Критично важливі ресурси, підключені до спільного домену.

2. Керування контролем доступу користувачів

Це завдання охоплює вжиття заходів для обмеження несанкціонованого доступу, а також відстеження та припинення будь-якої діяльності, пов’язаної з несанкціонованим доступом. Це включає:

– Погіршення доступу для неавторизованого персоналу.

– Керування політиками та їх оновлення за чітким графіком.

– Увімкнення багатофакторної автентифікації в організації.

– Білий список, додавання попередньо затверджених адрес, місцезнаходжень та сигналів тривоги на основі портів для ідентифікації персоналу, який отримує доступ до систем

– Зміна налаштувань за замовчуванням для всіх паролів і кодів доступу, а також періодичне оновлення паролів користувачів.

3. Часто оновлюйте патчі

Оновлення всього обладнання керування та безпеки до найновіших

версій прошивки має бути періодичною діяльністю. Хоча звичайні неінвазивні оновлення мають бути основним рішенням для всіх критично важливих контролерів, принаймні оновлення слід виконувати під час кожного щорічного циклу технічного обслуговування.

4. Виконайте перевірки валідації

Перевірки програми, логіки та виконуваних файлів гарантують, що зміни в логіці, кодах та скриптах є змінами, навмисно внесеними уповноваженою особою. Емульовані середовища перевірки допомагають контролювати будь-які небажані зміни в логіці та параметрах, а також допомагають операторам навчатися роботі на обладнанні, не ризикуючи реальними фізичними системами. Доступні інструменти для автоматичного виявлення будь-яких змін на логічному рівні, і будь-які такі зміни виконуються в контрольованому середовищі з резервною копією, готовою до відновлення у разі компрометації контролера або системи.

5. Додайте фізичну безпеку

З огляду на нещодавні загрози цілісності та безпеці критичних компонентів АСУ ТП, деякі постачальники систем керування тепер включають фізичні блокування на свої контролери, які запобігають виконанню будь-якого додаткового коду на контролері без попереднього проходження рівня фізичної безпеки.

6. Навчання з цілісності та безпеки критичних компонентів АСУ ТП

Критично важлива частина кіберзагрози походить від зловмисників, які покладаються на помилки, допущені персоналом заводу. Жоден захід цілісності та безпеки критичних компонентів АСУ ТП не може бути повністю впроваджений без залучення всіх зацікавлених сторін та усвідомлення ними своїх обов'язків. Це включає навчання персоналу тому, як виявляти атаки, як захищати свою особисту інформацію та як захистити себе від атак. Таке навчання має проводитися на всіх рівнях управління, керівників, системних адміністраторів операційних технологій (ОТ) та користувачів.

7. Створіть план реагування на інциденти

У випадку, якщо випадкова помилка чи недогляд залишають лазівку для потенційних зловмисників, впровадження цілісності та безпеки критичних компонентів АСУ ТП повинно включати практичний план для персоналу у разі порушення безпеки або виявлення загрози. Ці плани, після розробки, необхідно регулярно практикувати на практиці та надавати всім відповідальним співробітникам, щоб забезпечити швидке реагування у разі порушення безпеки.

8. Ведіть оновлений реєстр активів

Щоб зменшити ризик, ведіть актуальний облік усіх перелічених інвентарних активів ОТ, включаючи комутатори, маршрутизатори, брандмауери, різні веб-сервіси, програмне забезпечення для контролю та збору даних (SCADA), сервери історії, контролери або будь-які пристрої з адресацією за інтернет-протоколом (IP), оскільки всі вони можуть залишати прогалини для зловмисників, щоб вони могли використовувати некеровану систему. Активи можна контролювати через мережу на наявність оновлень останніх версій, а виправлення та будь-які вразливості можна контролювати за допомогою різних інструментів.

Чотири фази ініціативи з цілісності та безпеки критичних компонентів АСУ ТП

Запуск ініціативи з цілісності та безпеки критичних компонентів АСУ ТП для промислових систем не є таким складним завданням чи великою інвестицією, як може здатися на перший погляд. Компроміс у запобіганні можливому збитку робить безглуздим для компаній не розглядати можливість інвестування в цілісність та безпеку критичних компонентів АСУ ТП.

Як і будь-яка успішна ініціатива в масштабах всієї компанії, цілісність та безпека критичних компонентів АСУ ТП також потребує внутрішніх відповідальних осіб, які допомагають компанії впроваджувати необхідні політики та процедури. У більшості випадків найкращим шляхом вперед є визначення відповідальних за цілісність та безпеку критичних компонентів АСУ ТП бізнес-мережі та контроль цілісності та безпеки критичних компонентів АСУ

ТП мережі. Цілісність та безпека критичних компонентів АСУ ТП має бути загальнозаводською ініціативою. Вона впроваджується у чотири етапи:

Фаза 1: Дизайн та фреймворк

Розробка системи управління кібербезпекою є найкомплекснішим етапом, який вимагає найбільших інвестицій часу та зусиль. Багато консалтингових фірм з питань цілісності та безпеки критичних компонентів АСУ ТП зосереджуються на допомозі компаніям у розробці інфраструктури, політик та процедур цілісності та безпеки критичних компонентів АСУ ТП. Це завдання включає ідентифікацію всіх систем та персоналу, пов'язаних з кібербезпекою, визначення їхніх ролей, визначення прав доступу та контролю, а також розробку політик на основі цих параметрів для забезпечення безпечної роботи. Етап проектування цілісності та безпеки критичних компонентів АСУ ТП вимагає значного внутрішнього поштовху та підтримки зацікавлених сторін для забезпечення його успішного завершення.

Фаза 2: Оцінка прогалин

Етап оцінювання в основному полягає в огляді проекту цілісності та безпеки критичних компонентів АСУ ТП та виявленні потенційних вразливостей і ризиків залежно від впливу на бізнес. Виявлені прогалини усуваються та оновлюються в проекті. Оцінювання може проводитися за допомогою досвідченого персоналу та різних інструментів, які перехоплюють пакети на мережевому рівні та виявляють аномальну поведінку та прогалини в системному зміцненні.

Фаза 3: Впровадження

Ця частина полягає в фактичному впровадженні політик, процедур та практик цілісності та безпеки критичних компонентів АСУ ТП. Часто зовнішня допомога на цьому етапі може допомогти пришвидшити процес впровадження та забезпечити позначку всіх контрольних списків. Ключовим методом впровадження є посилення системи.

Фаза 4: Аудит

Аудит цілісності та безпеки критичних компонентів АСУ ТП охоплює такі завдання, як комплексне тестування на проникнення, щоб переконатися, що впровадження цілісності та безпеки критичних компонентів АСУ ТП досягає бажаних результатів. Спеціалізовані аудиторські компанії зазвичай беруться за це завдання та допомагають забезпечити надійну цілісність та безпеку критичних компонентів АСУ ТП. Ця частина вимагає найбільшої кількості зовнішньої експертизи для нового плану впровадження. Однак, якщо внутрішня команда аудиту цілісності та безпеки критичних компонентів АСУ ТП проходить навчання на всіх етапах, ця команда може використовувати свої знання та досвід для аудиту інших заводів та об'єктів компанії.

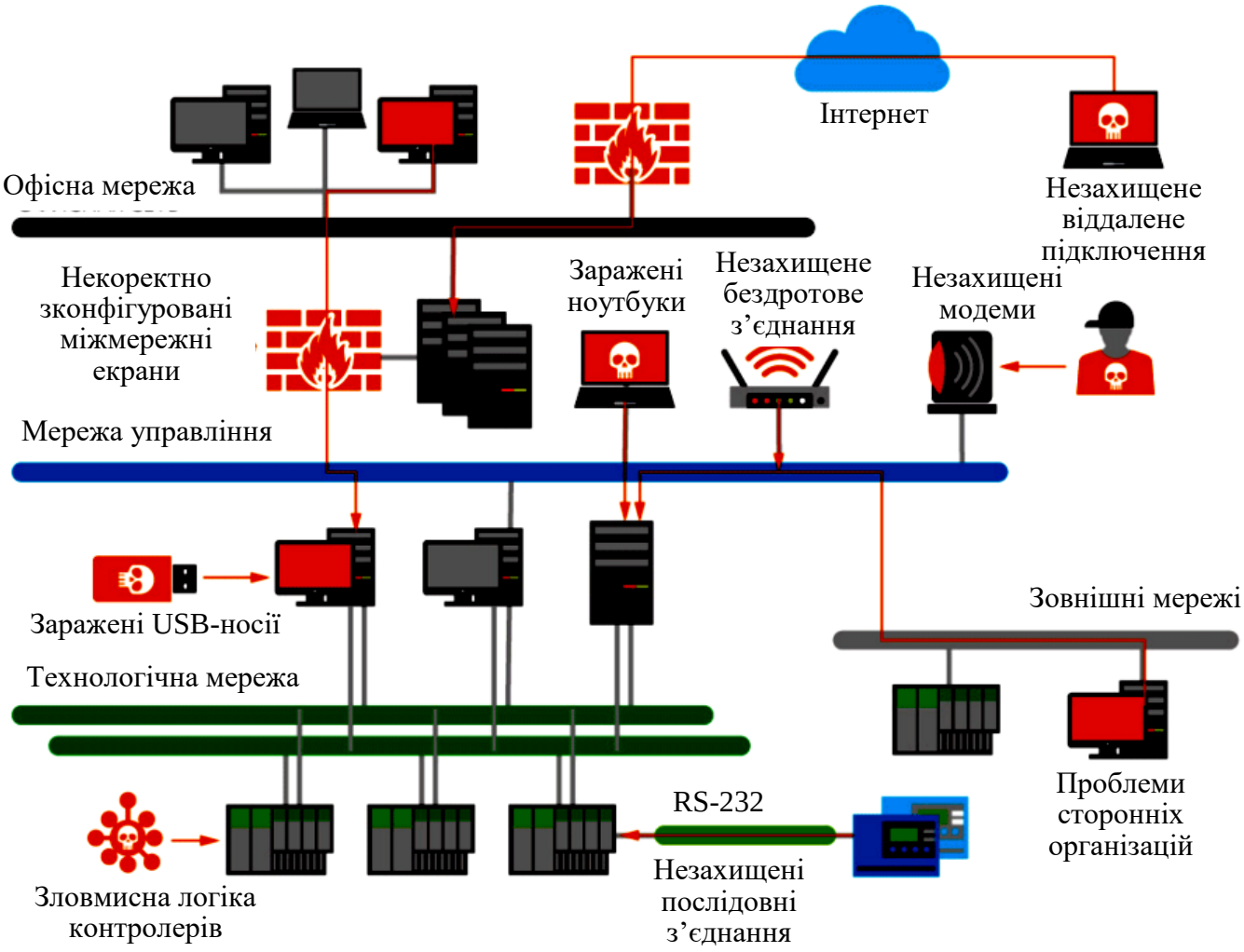

Рисунок 3.1 – Структурна схема системи

Ключові компоненти та стратегії безпеки для промислових систем управління

Промислові системи керування (ІКС) стають дедалі частішою мішенню кібератак, і компанії, що працюють у життєво важливих галузях промисловості, повинні вживати заходів для запобігання або зменшення ризику катастрофічних подій.

Значні ризики безпеки та атаки на промислові системи керування (ІКС) зростають в обсязі, і потрібні комплексні рішення. Фінансові та правові наслідки порушення ІКС зростають у всьому світі, і регуляторні органи дедалі більше зацікавлені у здатності компанії захищатися від кібератак. Фрагментація часткових рішень та їх складна інтеграція стають витратами, які власники ризиків хочуть зменшити.

Загрози та кіберінциденти – зловмисні та випадкові – проти ІКС трапляються щодня. Ці системи є критично важливою частиною інфраструктури, яка забезпечує роботу в життєво важливих галузях, таких як виробництво електроенергії, нафта і газ, транспорт, фармацевтика та хімічна промисловість. У минулому ІКС працювали в середовищі, яке здавалося безпечнішим, оскільки вони були фізично ізольовані та використовували власні протоколи керування з налаштованим апаратним та програмним забезпеченням.

П'ять факторів цілісності та безпеки критичних компонентів АСУ ТП

Рішення з цілісності та безпеки критичних компонентів АСУ ТП все частіше розробляються для операцій та політик, і існує п'ять ключових складових, які можуть стимулювати цільові рішення для ІКС:

1. Аудит та застосування політик і процедур безпеки, розроблених спеціально для мережі системи управління та її пристроїв.

2. Контроль доступу через локальну мережу (LAN), глобальну мережу (WAN) та фізичні периметри, доповнений безпечною передачею даних.

3. Виявлення загроз аномальної та шкідливої діяльності на всіх рівнях.

4. Управління ризиками та зменшення їхнього впливу на можливі атаки за допомогою встановленого пакету засобів безпеки, розробленого для покращення регулювання ICS без порушення контрольованого процесу.

5. Вирішуйте ключові проблеми безпеки, які вимагають налагодження тісний зв'язок з постачальниками.

ІКС є основою виробництва, а це означає, що процеси цілісності та безпеки критичних компонентів АСУ ТП повинні враховувати внутрішні та зовнішні загрози за допомогою кількох рівнів захисту, які пом'якшують різні ризики.

Ініціативи постачальників ICS щодо зниження ризиків безпеки систем керування у відповідь на зростання цілісності та безпеки критичних компонентів АСУ ТП призводять до того, що фахівці з автоматизації підвищують ефективність захисту своїх промислових процесів. Однак постачальники ICS та фахівці з автоматизації повинні бути прагненням надавати набір продуктів і послуг, які зменшують ризики та забезпечують безпеку виробничих активів. Крім того, інформаційні силоси, що існують в організаціях, означають, що інформація рідко обмінюється. Постачальники комплексних рішень будуть купувати, інтегрувати та сприяти впровадженню технологій цілісності та безпеки критичних компонентів АСУ ТП та надавати продукт кінцевим користувачам.

Оскільки ІКС схильні до кібератак і дедалі частіше стають ціллю атак, постачальники автоматизації співпрацюють з постачальниками послуг безпеки інформаційних технологій (IT) для розробки надійніших рішень. Хоча багато вразливостей пов'язані з технологіями, варто зазначити, що деякі слабкі місця виникають через брак персоналу або недостатню обізнаність. Ці зміни можуть вимагати культурних змін та механізмів співпраці для зменшення помилок, спричинених людським фактором.

Практика управління ризиками в організації повинна бути пропорційною наявним ризикам. Організації не повинні запитувати: «Чи існує ризик?», а радше: «З якими ризиками ми стикаємося та який рівень інвестицій для їх

пом’якшення?». Навчання керівників та персоналу не встигає за постійно мінливими загрозами цілісності та безпеці критичних компонентів АСУ ТП. Корпорації повинні брати участь у робочих групах, які обговорюють поточну ситуацію з кібербезпекою у своєму секторі, описують ключові стратегічні елементи для підвищення рівня безпеки та підтримують працівників інструментами та інструкціями.

Хоча промисловий сектор поступово усвідомлює наявність більшого ризику для цілісності та безпеки критичних компонентів АСУ ТП ІКС, управління ризиками є складним через високі витрати, пов'язані з кожним ризиком, та відсутність історичної статистики для визначення ймовірності виникнення сценарію. Компанії повинні мати економічно ефективні та дієві рішення, які забезпечать безпеку промислових об'єктів. Це має вирішальне значення для світової економіки.

Ось чому організації повинні мати свої політики та процедури, а також розробляти та впроваджувати заходи безпеки в середовищі ICS, перш ніж робити будь-яку подальшу інтеграцію в інші мережі. Бізнес-кейс, стан безпеки та план управління ризиками визначають протоколи та методологію системної інтеграції.

Ще одним фактором, який слід враховувати в цій загальносистемній інтеграції, є те, що фахівці з IT-безпеки не розуміють належним чином промислових процесів, які використовують ІКС, а фахівці з ІКС не розуміють належним чином сучасних ризиків IT-безпеки. Це може призвести до недостатньої обізнаності та запобіжних заходів, що позбавить переваг, яких прагнули досягти завдяки інтеграції бізнес-систем та систем управління, коли трапляється один серйозний інцидент з ІКС.

Підтримка цілісності та безпеки критичних компонентів АСУ ТП

З огляду на це, для підтримки компонентів безпеки ICS слід досягти наступних цілей:

1. Структура, яка надає огляд та визначає основні елементи.

2. Корпоративне управління для забезпечення послідовного та належного управління ризиками безпеки.

3. Глибоке розуміння ризиків, з якими стикаються, та здатність обґрунтувати необхідні заходи щодо їх пом'якшення.

4. Управління життєвим циклом ICS, що відповідає процесу інженерії безпеки.

5. Підвищена обізнаність щодо безпеки ICS по всій організації.

6. Постійний перегляд заходів захисту, які можна обрати та впровадити.

7. Процедури, що забезпечують достатню реакцію на нові вразливості та зміни в середовищі загроз.

8. Ефективне управління ризиками третіх сторін, які можуть вплинути на організацію.

3.3 Розробка функціональної схеми

Вступ та актуальність захисту АСУ ТП

Системи диспетчерського управління та збору даних (SCADA), а також суміжні автоматизовані системи технологічного управління (АСУ ТП) є критичною основою сучасної інфраструктури. Вони забезпечують функціонування енергомереж, транспортування палива, водопостачання, систем «розумного міста» та об'єктів атомної енергетики. Масштаби впровадження таких рішень стрімко зростають із кожною модернізацією промислового виробництва.

Попри тривалі дискусії у профільній літературі щодо безпеки АСУ ТП, суттєвого прогресу в захисті систем цього класу протягом останнього десятиліття досягнуто не було, що зумовлено специфікою їх архітектури та характером загроз.

Особливості загроз і мотивація порушників

Основна частина інформації в АСУ ТП складається з технологічних даних (параметрів фізичних процесів, станів обладнання) та керівних впливів. На

відміну від фінансових систем, володіння цими даними без прямого доступу до технологічного об'єкта рідко дозволяє отримати пряму монетарну вигоду, що обмежує коло зовнішніх зловмисників. Здебільшого ризики шахрайства пов'язані з діями внутрішнього персоналу (інсайдерів).

Серед монетизованих зовнішніх атак переважають промислове шпигунство та рідкісні замовні акції проти конкурентів, тоді як більшість інших інцидентів носять немонетизований характер (наприклад, помилки персоналу чи деструктивні дії). Водночас низька ймовірність класичних зовнішніх атак не зменшує актуальності проблеми. Загальна актуальність загрози визначається добутком ймовірності її реалізації на потенційний збиток. Для АСУ ТП такий збиток охоплює не лише фінансові втрати, а й екологічні катастрофи, зупинку життєзабезпечення цілих регіонів, а також загрози життю та здоров'ю людей.

Уроки кіберцифрової ери: прецедент Stuxnet

Показовим прикладом вразливості промислових мереж управління став виявлений у 2010 році шкідливий код Stuxnet, націлений на інфраструктуру компанії Siemens. Вірус реалізував багатовекторну атаку:

– на рівні ОС Windows (експлуатуючи одразу кілька вразливостей нульового дня);

– на рівні ПЗ SCADA (Siemens WinCC/PCS 7);

– на рівні контролерів програмованої логіки (PLC S7-300), які керували частотними перетворювачами електромоторів.

Модифікуючи робочі частоти приводів і приховуючи зміни від операторського ПЗ, шкідливий код здатний виводити обладнання з ладу, імітуючи нормальний режим роботи. Цей інцидент продемонстрував реальність цілеспрямованих атак на критичну інфраструктуру.

Нормативно-правова база захисту

У міжнародній практиці існує низка галузевих стандартів (NERC, ChemITC, NIST, ISA), проте обов'язкові критерії безпеки для комерційних підприємств часто мають рекомендаційний характер. У правовому полі України ключовими є поняття об'єктів критичної інфраструктури та ключових систем

інформаційної інфраструктури – систем, що управляють чутливими процесами, порушення яких веде до надзвичайних ситуацій (у нафтогазовій галузі, енергетиці, екологічно небезпечних виробництвах).

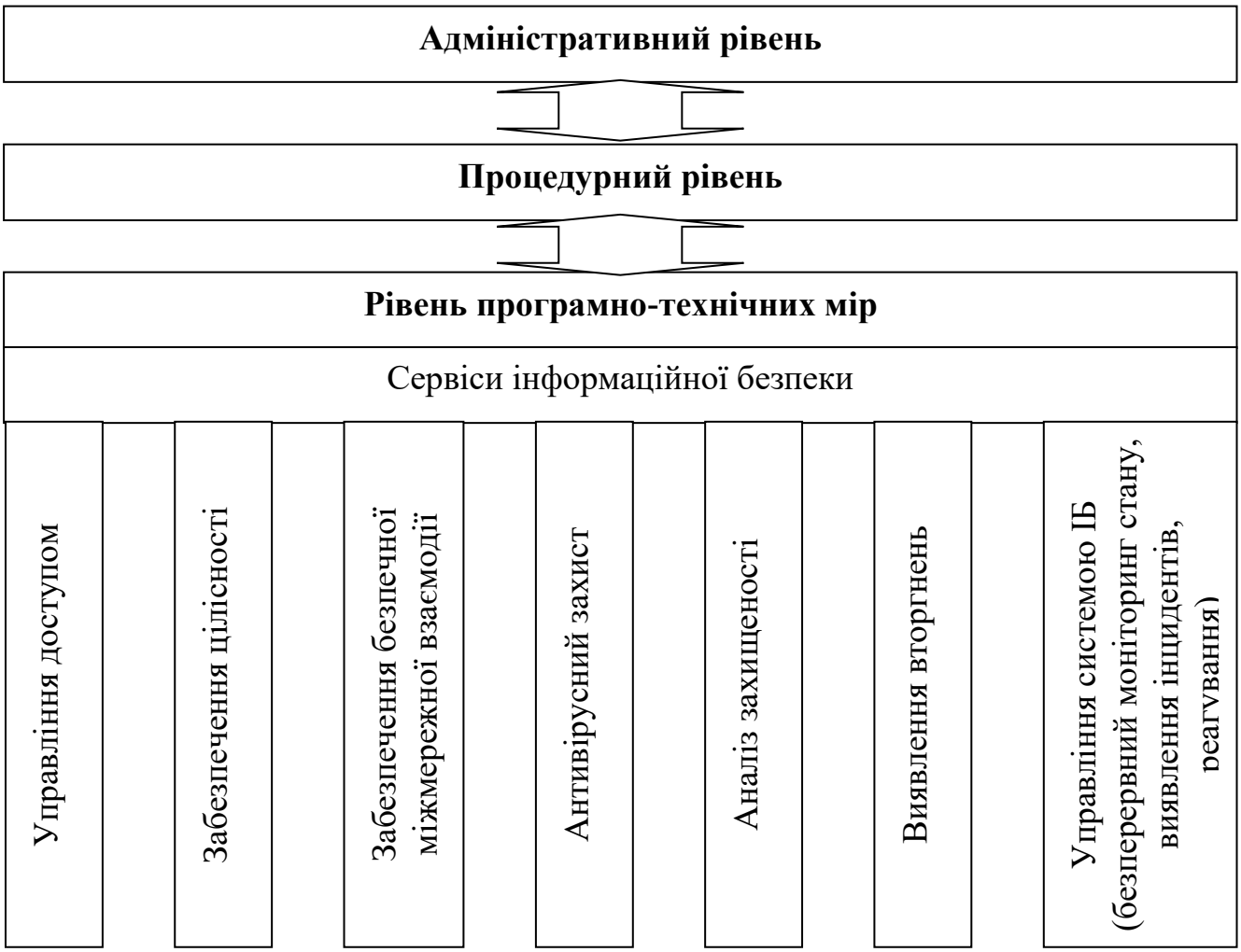

Рисунок 3.2 – Функціональна схема системи

Класифікація загроз і підходи до побудови системи безпеки

Забезпечення безпеки АСУ ТП вимагає комплексної нейтралізації загроз трьох основних класів:

1. Техногенні загрози: фізичні впливи на компоненти системи (нейтралізуються засобами контролю фізичного доступу).

2. Антропогенні загрози: навмисні або ненавмисні помилки персоналу і

служб обслуговування.

3. Загрози несанкціонованого доступу: пов'язані з інтеграцією АСУ ТП з корпоративними мережами підприємств (локальними обчислювальними мережами – ЛОМ), що вимагає використання виділених мережевих сегментів, міжмережевих екранів та криптографічного захисту каналів.

Архітектура захисту реалізується на трьох рівнях:

– Адміністративний: розробка політик, регламентів і концепцій безпеки керівництвом підприємства.

– Процедурний: організаційні заходи, орієнтовані на управління «людським фактором».

– Програмно-технічний: основний рубіж захисту, що включає управління доступом, забезпечення цілісності, безпечну міжмережеву взаємодію, антивірусний захист, аналіз захищеності, виявлення вторгнень та централізований моніторинг (SIEM/SOC).

Сервіси та механізми забезпечення безпеки

– Управління доступом: реалізується на мережевому рівні (створення демілітаризованих зон – DMZ, де корпоративна мережа розглядається як недовірений сегмент) та прикладному рівні (спеціалізовані засоби захисту СУБД та операційних систем).

– Забезпечення цілісності: контроль вірогідності даних і надійності транзакцій на рівнях ОС і СУБД шляхом обчислення контрольних сум.

– Безпечна міжвнежева взаємодія: використання промислових комутаторів Ethernet із захистом від прослуховування трафіку, підміни MAC/IP-адрес, атак на протокол STP, а також застосування стандарту автентифікації пристроїв 802.1x.

– Антивірусний захист і виявлення вторгнень: застосування мережевих і хостових систем запобігання вторгненням (HIPS), здатних функціонувати в умовах обмеженості ресурсів контролерів та АРМ АСУ ТП.

– Управління системою ІБ: централізований збір логів, аудит подій та кореляція інцидентів безпеки в реальному часі.

Висновок

З огляду на тенденції розвитку кібервійни та появу спеціалізованих військових підрозділів у провідних країнах світу (таких як USCYBERCOM, ARCYBER), рівень загроз для стратегічної інфраструктури постійно зростає. Оскільки системи АСУ ТП розраховані на тривалий цикл експлуатації, розроблювані апаратно-програмні комплекси забезпечення їхньої цілісності та безпеки повинні володіти високим потенціалом адаптації до майбутніх викликів.

Розглянувши усі блоки функціональної схеми перейдемо до розгляду діаграми взаємодії процесів, які відбуваються у системі.

3.4 Розробка діаграми процесів

Діаграму процесів розробленої системи наведено на рисунку 3.3. Її детальний аналіз дозволяє простежити логіку взаємодії внутрішніх компонентів та маршрутизацію потоків інформації в межах апаратно-програмного комплексу забезпечення цілісності й безпеки критичних елементів АСУ ТП. У процесі проєктування застосовується модель графічного представлення потоків даних (Data Flow Diagram, DFD), яка відображає рух і трансформацію даних в інформаційній системі.

Діаграми взаємодії процесів є базовим інструментом структурного проєктування для візуалізації обробки даних. Традиційно розробка розпочинається з побудови контекстної діаграми потоків даних, яка ілюструє загальну взаємодію системи захисту АСУ ТП із зовнішнім середовищем. Надалі ця модель деталізується шляхом поетапної декомпозиції процесів і потоків даних з метою повної та всебічної демонстрації архітектури розроблюваного комплексу.

Згідно з методологією DFD, такі діаграми базуються на чотирьох основних елементах:

– процеси – трансформації та обробка даних у межах описуваної системи захисту;

– сховища даних – репозиторії для збереження інформації (наприклад, журнали подій, бази правил та контрольних сум);

– зовнішні сутності – джерела та споживачі даних поза системою (оператори-технологи, зовнішні сервери, промислові контролери);

– потоки даних – канали передачі інформації між зазначеними елементами.

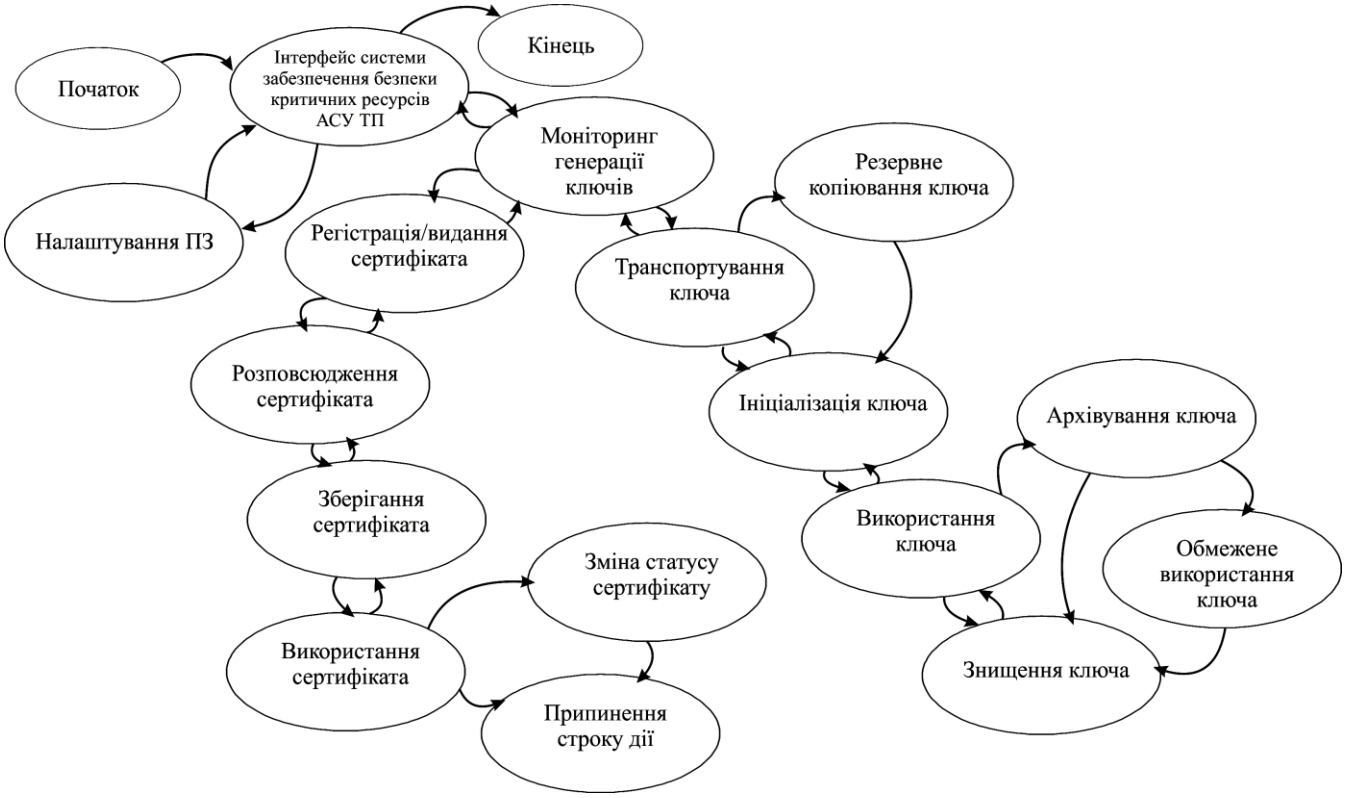

Рисунок 3.3 – Діаграма взаємодії процесів

Порядок функціонування модулів та процедури TLS Handshake у захищеному контурі АСУ ТП

Взаємодія компонентів розподіленої системи управління та хмарних вузлів на основі криптографічного протоколу TLS здійснюється за такою послідовністю:

1. Ініціація сеансу (ClientHello): Клієнтський модуль відправляє запит на встановлення захищеного з'єднання, зазначаючи актуальну версію протоколу

TLS, випадково згенероване число, а також перелік підтримуваних методів шифрування та алгоритмів стиснення.

2. Відповідь хмарного сервісу (ServerHello): Сервер хмарного сегмента обробляє запит та формує відповідь, що містить узгоджену версію протоколу, отримане від клієнта випадкове число, обраний алгоритм симетричного шифрування AES та підтримувані параметри стиснення.

3. Ідентифікація вузла (Certificate): Сервер передає клієнту власний цифровий сертифікат для підтвердження автентичності та перевірки довіри в межах інфраструктури.

4. Взаємна автентифікація (опціонально): За потреби сервер хмарного сервісу може ініціювати запит клієнтського сертифіката для реалізації двосторонньої (взаємної) автентифікації сторін.

5. Завершення етапу квитування (ServerHelloDone): Сервер надсилає службове повідомлення про завершення передачі параметрів рукостискання (handshake).

6. Обмін ключами (ClientKeyExchange): Клієнт формує повідомлення, що містить відкритий ключ алгоритму Діффі-Хеллмана (Diffie-Hellman / PreMasterSecret).

7. Генерація сеансового ключа: Використовуючи значення PreMasterSecret та згенеровані випадкові числа, клієнт і сервер обчислюють єдиний спільний секретний ключ, на основі якого надалі генеруються всі похідні криптографічні ключі для захисту сеансу.

8. Активація захисту (ChangeCipherSpec): Клієнт надсилає повідомлення рівня записів (тип 20), яке інформує про перехід на шифрування всього подальшого трафіку за допомогою узгодженого алгоритму AES та спільного секретного ключа.

9. Формування підтвердження (Finished): Клієнт відправляє контрольне повідомлення, що містить криптографічний хеш (MD5) та код автентичності повідомлень (MAC), сформовані на основі попередніх етапів рукостискання.

10. Перевірка з боку сервера: Сервер розшифровує отримане

повідомлення та верифікує контрольні значення хешу та MAC. У разі виявлення розбіжностей процес квитування переривається, а з'єднання аварійно скидається.

11. Фіналізація з'єднання: Сервер надсилає власне повідомлення ChangeCipherSpec та зашифрований блок Finished, після успішної перевірки якого клієнтом процедура вважається повністю завершеною.

Після успішного завершення процедури handshake весь подальший інформаційний обмін між компонентами системи переходить у захищений режим (тип пакетів 23), забезпечуючи повне шифрування даних за допомогою криптоалгоритму AES.

4 РЕАЛІЗАЦІЯ ПРОЕКТУ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

4.1 Блок-схеми та опис алгоритмів функціонування системи

Алгоритмічне забезпечення апаратно-програмного комплексу захисту критичних компонентів автоматизованих систем керування технологічними процесами (АСУ ТП) призначене для контролю цілісності програмного забезпечення, виявлення несанкціонованих змін конфігурації та моніторингу подій інформаційної безпеки. Основними об'єктами контролю є програмовані логічні контролери (ПЛК), операторські станції HMI, сервери SCADA, інженерні робочі станції та мережеві пристрої промислової інфраструктури. Особливістю досліджуваного комплексу є поєднання апаратних засобів спостереження з програмними алгоритмами перевірки стану критичних компонентів. Такий підхід дозволяє організувати контроль технологічної інфраструктури з урахуванням обмежень, пов'язаних із безперервністю виробничих процесів.

Загальну послідовність роботи апаратно-програмного комплексу відображено на рисунку 4.1. Основний алгоритм передбачає ініціалізацію системи моніторингу, визначення контрольованих компонентів, отримання відомостей про їхній стан та перевірку відповідності встановленим еталонним характеристикам. Після збору інформації виконується аналіз цілісності програмних файлів, конфігурацій та доступних характеристик мережевої взаємодії. У разі виявлення відхилення формується подія безпеки, яка передається до модуля оцінювання ризику. Результати перевірок реєструються в журналі аудиту та використовуються для визначення необхідності додаткового аналізу або реагування.

Архітектура комплексу передбачає функціональне розділення засобів спостереження, аналізу та керування.

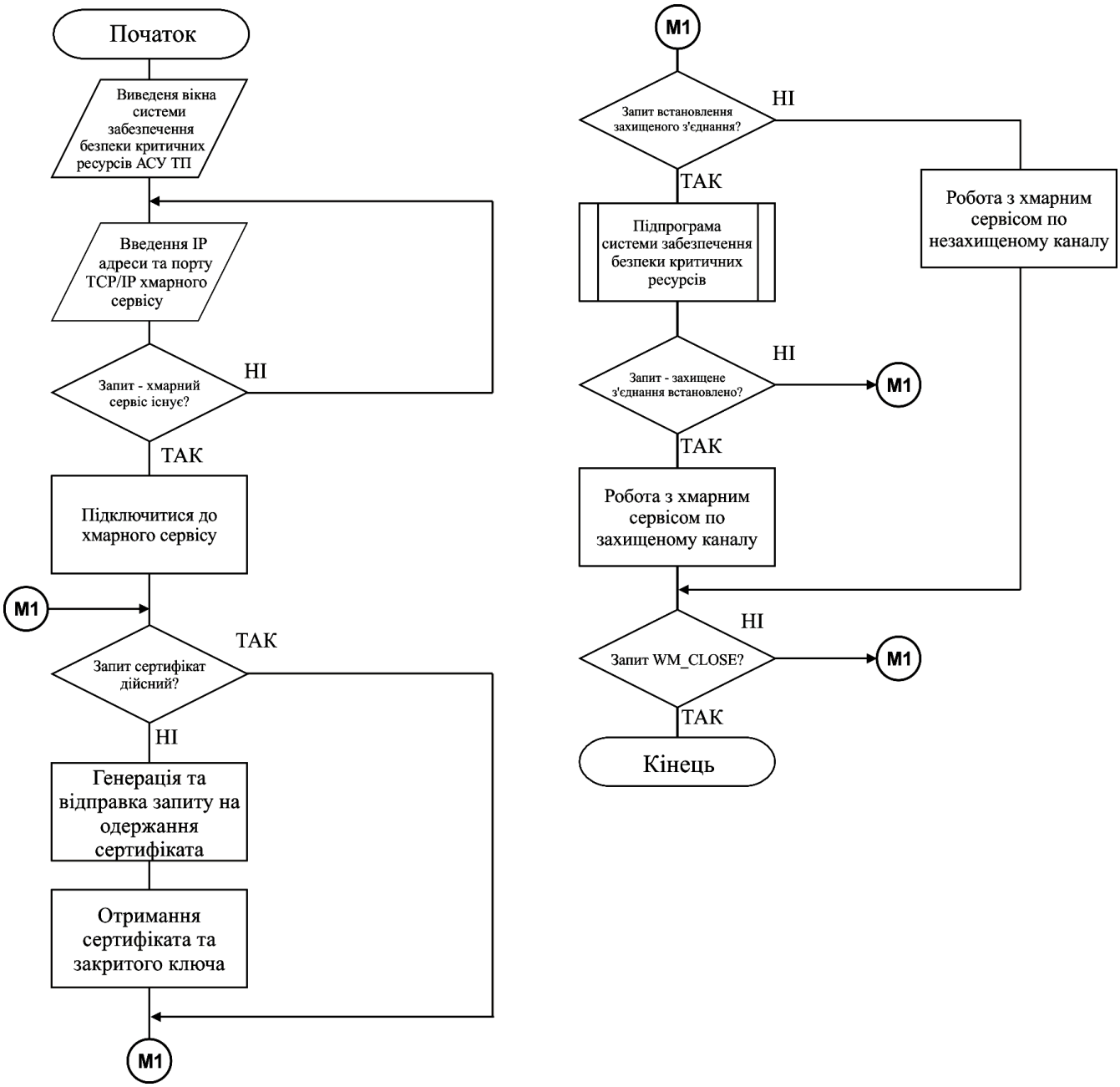

Рисунок 4.1 – Блок-схема основної програми

Апаратна частина може включати окремий обчислювальний вузол моніторингу, мережеві адаптери, пристрої отримання копій трафіку та засоби контролю стану обладнання. Програмна частина забезпечує отримання телеметрії, перевірку контрольних значень, аналіз мережевих подій, зіставлення результатів і формування повідомлень про порушення. Керувальний компонент відповідає за зберігання конфігурації, еталонних станів і правил безпеки. Розміщення основних

засобів аналізу поза критичними контурами керування дозволяє обмежувати їхній вплив на роботу технологічного обладнання.

Принциповою вимогою до алгоритмів є збереження працездатності технологічного процесу. На відміну від звичайних корпоративних інформаційних систем, АСУ ТП безпосередньо взаємодіє з фізичним обладнанням. Неконтрольоване сканування ПЛК, перезапуск служб або блокування мережевих з'єднань може порушувати виконання технологічних операцій. Тому основним режимом спостереження доцільно обрати пасивне отримання інформації. Операції, які потребують звернення до контролерів або зміни їхнього стану, повинні виконуватися лише за наявності відповідної підтримки виробника та погодження відповідальних фахівців.

Окремим функціональним блоком є підпрограма перевірки цілісності критичного компонента, алгоритм якої представлено на рисунку 4.2. Вона отримує ідентифікатор контрольованого ресурсу, визначає доступну еталонну конфігурацію та виконує порівняння з поточним станом. Для програмних файлів можуть використовуватися криптографічні контрольні значення. Для конфігурацій обладнання застосовується зіставлення параметрів або перевірка підписаного еталонного представлення. У разі невідповідності алгоритм визначає характер зміни та перевіряє наявність відповідного погодження. Непідтверджені відхилення реєструються як потенційні порушення цілісності.

Під час побудови захисних механізмів необхідно враховувати вимоги промислової кібербезпеки. Серія стандартів ISA/IEC 62443 визначає підходи до захисту промислових систем автоматизації та керування, зокрема розмежування захищених зон і каналів взаємодії. Рекомендації NIST SP 800-82 Rev. 3 також приділяють увагу особливостям операційних технологій, для яких важливими є безпечність, надійність і доступність. Відповідні принципи використовуються як методологічна основа вибору алгоритмів моніторингу та реагування. Наявність окремих захисних функцій не означає автоматичної відповідності всього комплексу зазначеним стандартам.

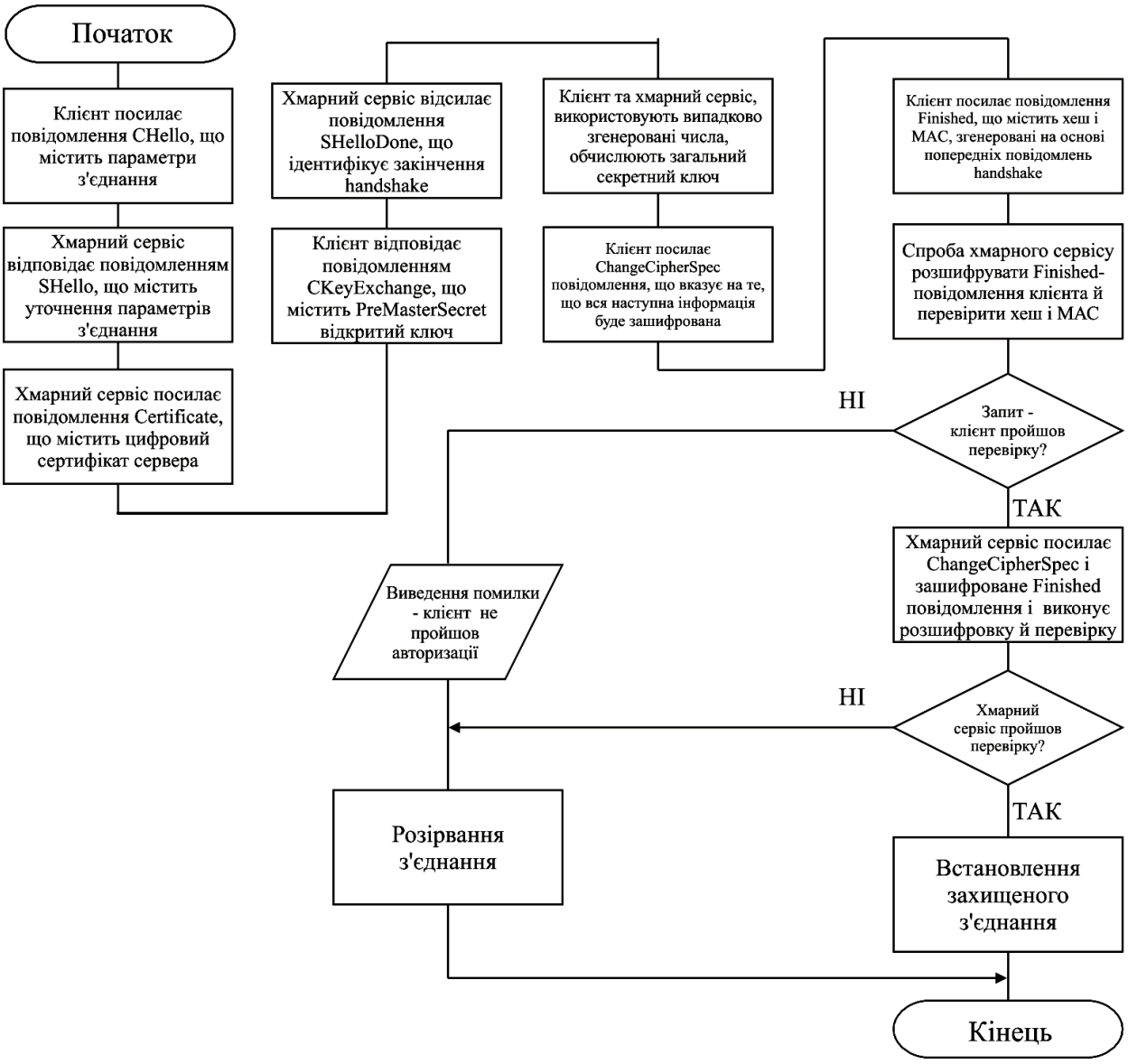

Рисунок 4.2 – Блок-схема роботи підпрограми

Алгоритм інвентаризації критичних компонентів АСУ ТП

Початковим етапом функціонування комплексу є формування актуального переліку технічних і програмних ресурсів, які потребують контролю. У промисловій інфраструктурі можуть використовуватися пристрої різних виробників із неоднаковими можливостями отримання службової інформації. Тому алгоритм інвентаризації повинен враховувати характеристики кожного типу обладнання.

Вхідними даними алгоритму є відомості про топологію технологічної мережі, перелік контрольованих пристроїв, їхні ідентифікатори та доступні способи моніторингу. Для ПЛК можуть визначатися модель, серійний номер,

версія прошивки та належність до технологічної ділянки. Для серверів SCADA й операторських станцій додатково фіксуються операційна система, встановлені програмні компоненти та мережеві параметри.

На першому етапі перевіряється наявність ресурсу в реєстрі. Якщо пристрій уже зареєстрований, отримані характеристики порівнюються з попередніми. У разі появи нового компонента створюється відповідний запис. Повторне надходження інформації не повинно спричиняти дублювання одного фізичного пристрою.

Для кожного ресурсу доцільно визначати рівень критичності. ПЛК, який безпосередньо керує небезпечним технологічним процесом, може потребувати суворіших правил контролю, ніж допоміжна інженерна станція. Однак оцінка критичності повинна ґрунтуватися на функціональному призначенні обладнання, а не лише на його типі.

Окремо встановлюється допустимий спосіб отримання інформації. Для серверів може бути доступний програмний агент моніторингу. Для ПЛК, які не підтримують безпечне отримання службових параметрів, доцільно використовувати попередньо підготовлені конфігураційні копії та пасивний мережевий аналіз.

Результатом алгоритму є реєстр критичних компонентів із визначеними характеристиками, рівнями важливості та дозволеними процедурами перевірки.

Алгоритм ініціалізації апаратних засобів моніторингу

Апаратна частина комплексу забезпечує отримання інформації про мережеву взаємодію та стан доступних технічних компонентів. Для цього може використовуватися окремий сервер моніторингу, який підключається до технологічного сегмента через спеціально визначені інтерфейси.

На початковому етапі перевіряється доступність мережевих адаптерів і відповідність їхньої конфігурації встановленим параметрам. Для пасивного спостереження може використовуватися Network TAP або копіювання трафіку через SPAN-порт керованого комутатора.

Важливо враховувати відмінності цих способів підключення. SPAN забезпечує передавання копій пакетів на визначений порт комутатора, але за перевантаження можливі втрати. Network TAP дозволяє отримувати копію трафіку через окремий апаратний засіб. Конкретні гарантії повноти та незалежності спостереження залежать від конструкції пристрою й мережевої топології.

Після ініціалізації інтерфейсів запускається програмний механізм отримання пакетів. Для цього може використовуватися libpcap або сумісний засіб захоплення мережевого трафіку. Отримані пакети передаються до компонента попереднього аналізу.

Окремо перевіряються характеристики апаратного вузла моніторингу. До контрольованих параметрів належать використання оперативної пам'яті, завантаження процесора, стан накопичувачів і доступність службових компонентів.

У разі відмови сенсора система повинна повідомляти про втрату спостереження. При цьому апаратний компонент не повинен створювати залежність, за якої його відмова автоматично припиняє передавання технологічних команд.

Результатом алгоритму є підготовлений засіб моніторингу з контрольованими параметрами працездатності.

Алгоритм формування еталонного стану компонентів

Для перевірки цілісності необхідно мати достовірне представлення дозволеного стану кожного критичного ресурсу. Таким представленням може бути набір контрольних значень програмних файлів, опис конфігурації або підписаний пакет інженерного проєкту.

Алгоритм формування еталона починається з отримання погоджених вихідних матеріалів. Для операторської станції це можуть бути виконувані файли, бібліотеки та службові конфігурації. Для ПЛК еталоном може виступати затверджена версія керувальної програми або її експортований образ.

На першому етапі перевіряється походження матеріалів. Еталон повинен формуватися на основі довіреної версії програмного забезпечення. Якщо поточний стан компонента вже скомпрометований, його автоматичне прийняття як еталона призведе до закріплення небезпечної конфігурації.

Для файлових об'єктів можуть застосовуватися криптографічні хеш-функції, зокрема SHA-256. Вони дозволяють отримувати контрольне значення, яке залежить від вмісту файлу. У разі зміни даних результат обчислення зазвичай відрізняється від попереднього.

Для конфігураційних файлів необхідно враховувати можливість змін, які не впливають на функціональне значення параметрів. Наприклад, перестановка незалежних записів або зміна формату представлення можуть змінити хеш. Тому для структурованих конфігурацій доцільно використовувати визначене канонічне представлення або аналіз окремих параметрів.

Після формування контрольних значень створюється еталонний маніфест. Він містить ідентифікатор компонента, версію конфігурації, перелік контрольованих об'єктів та відповідні результати обчислення.

Для захисту маніфесту доцільно передбачити цифровий підпис або інший механізм підтвердження його достовірності. Саме зберігання хешів у звичайному файлі не гарантує захисту від порушника, який може змінити і контрольований об'єкт, і його еталон.

Результатом алгоритму є затверджений еталонний стан, який використовується під час періодичних перевірок.

Алгоритм перевірки цілісності програмних файлів

Перевірка програмних файлів є одним з основних механізмів виявлення несанкціонованих змін на інженерних станціях, серверах SCADA та інших обчислювальних компонентах.

Вхідними даними алгоритму є перелік контрольованих файлів, довірений еталонний маніфест та параметри доступу до відповідної файлової системи.

На першому етапі визначається доступність контрольованого об'єкта. Якщо файл відсутній, формується повідомлення про порушення очікуваної

конфігурації. Якщо доступ до нього неможливий, результат позначається як неповний.

Після відкриття файлу виконується послідовне зчитування його вмісту та обчислення контрольного значення. Для великих файлів доцільно використовувати блокове зчитування, яке не потребує завантаження всього вмісту в оперативну пам'ять.

Отримане значення порівнюється з еталоном. Якщо вони збігаються, перевірка підтверджує відповідність поточного вмісту зафіксованому стану. Якщо значення відрізняються, формується запис про виявлену зміну.

Важливо враховувати, що збіг контрольних значень не підтверджує відсутності всіх можливих загроз. Наприклад, зловмисний код може виконуватися лише в оперативній пам'яті або використовувати легітимний програмний файл без його зміни. Тому контроль цілісності повинен доповнюватися іншими механізмами спостереження.

Результатом алгоритму є перелік перевірених об'єктів із визначеним станом цілісності.

Алгоритм контролю керувальних програм ПЛК

Програмовані логічні контролери є критичними компонентами АСУ ТП, оскільки безпосередньо забезпечують виконання алгоритмів керування обладнанням. Несанкціонована зміна їхніх програм може призвести до порушення технологічних режимів.

Для контролю цілісності ПЛК необхідно використовувати способи отримання інформації, які підтримуються конкретним виробником. Не всі контролери дозволяють отримувати повний образ керувальної програми або обчислювати його криптографічне контрольне значення.

Одним із можливих підходів є порівняння затвердженої версії інженерного проєкту з конфігурацією, отриманою через офіційне програмне середовище. Така перевірка повинна виконуватися відповідно до експлуатаційних обмежень обладнання.

Якщо контролер підтримує безпечне отримання контрольного значення програми або підписаної інформації про її версію, ці дані можуть використовуватися для автоматизованого аналізу.

За відсутності відповідного інтерфейсу можливе порівняння погоджених резервних копій проєкту. У такому випадку необхідно розуміти, що перевірка копії не підтверджує безпосередньо поточний стан пам'яті ПЛК. Вона засвідчує лише цілісність відповідного збереженого артефакту.

Під час аналізу необхідно розрізняти зміну програмної логіки та зміну робочих параметрів. Частина технологічних значень може змінюватися під час нормального функціонування. Тому їх не слід включати до незмінного еталона без урахування функціонального призначення.

Якщо виявлено невідповідність керувальної програми погодженій версії, система реєструє відповідну подію. Автоматичне перезаписування пам'яті контролера не допускається без окремої процедури погодження та перевірки технологічної безпеки.

Результатом алгоритму є визначення стану цілісності керувальної програми в межах можливостей конкретного обладнання.

Алгоритм контролю цілісності прошивок обладнання

Прошивка визначає базові функції промислового пристрою. Її несанкціонована зміна може впливати на механізми виконання команд, мережеву взаємодію та засоби захисту.

Для контролю прошивок алгоритм використовує відомості про встановлені версії, доступні криптографічні ідентифікатори та офіційно підтверджені характеристики програмних пакетів.

На початковому етапі визначається поточна версія прошивки. Джерелом можуть бути службовий інтерфейс пристрою, інженерне програмне забезпечення або журнал оновлень.

Після отримання інформації виконується порівняння з погодженою конфігурацією. Якщо встановлена версія відрізняється від очікуваної, перевіряється наявність зареєстрованого оновлення.

Необхідно враховувати, що збіг номерів версій не є повноцінною криптографічною перевіркою цілісності. Для достовірнішого підтвердження потрібні механізми перевірки підпису прошивки, довіреного завантаження або апаратної атестації, якщо вони підтримуються пристроєм.

За відсутності таких можливостей результат обмежується контролем версій і конфігураційних відомостей. Система не повинна формувати висновок про криптографічно підтверджену цілісність лише на основі текстового ідентифікатора прошивки.

Результатом алгоритму є оцінка відповідності програмного забезпечення обладнання погодженому стану з указанням способу підтвердження.

Алгоритм контролю операторських та інженерних станцій

Операторські станції HMI та інженерні робочі місця забезпечують взаємодію персоналу з технологічним обладнанням. Через них можуть виконуватися зміни програм ПЛК, налаштування параметрів і перегляд стану виробничого процесу. Тому контроль їхнього програмного середовища має важливе значення.

Вхідними даними алгоритму є еталонні відомості про встановлені програми, контрольовані файли, служби операційної системи та параметри доступу.

На першому етапі перевіряється наявність основних програмних компонентів. До них можуть належати середовище програмування контролерів, HMI-застосунок, драйвери промислових протоколів і засоби обміну даними.

Далі виконується контроль цілісності визначених виконуваних файлів і конфігурацій. Якщо виявлено зміну, алгоритм зіставляє її з реєстром погоджених оновлень.

Окремо можуть перевірятися спроби запуску невідомих програм. Для такого контролю використовуються підтримувані операційною системою механізми журналювання запуску процесів або контролю виконуваних файлів.

У Linux-середовищі за відповідної підтримки можуть застосовуватися механізми Integrity Measurement Architecture (IMA). Вони дозволяють вимірювати

цілісність файлів і, за визначеної конфігурації, перевіряти допустимість їхнього використання. Однак увімкнення блокувальних механізмів без попереднього тестування може порушити роботу технологічних застосунків.

Результатом алгоритму є контрольований стан програмного середовища операторських та інженерних станцій.

Алгоритм пасивного моніторингу промислового мережевого трафіку

Мережеве спостереження дозволяє виявляти зміни взаємодії між компонентами АСУ ТП без безпосереднього втручання в технологічний процес.

Вхідними даними алгоритму є копії мережевих пакетів, отримані апаратним сенсором. На першому етапі визначаються джерело та адресат передавання, транспортний протокол, порти й часові характеристики з'єднання.

Далі виконується визначення типу промислового протоколу. У технологічних мережах можуть використовуватися Modbus TCP, OPC UA, PROFINET, EtherNet/IP та інші способи обміну. Підтримка кожного протоколу потребує відповідного аналізатора, який враховує його структуру.

Для протоколів, які передають дані без шифрування, можуть аналізуватися доступні службові поля повідомлень. Для захищених з'єднань обсяг доступної інформації обмежується параметрами, видимими без дешифрування.

Окремо формується перелік характерних мережевих взаємодій. Для кожного пристрою визначаються звичайні адресати, дозволені протоколи та типові напрямки передавання.

Якщо сенсор спостерігає нове підключення до ПЛК з невідомого вузла, така подія може бути передана до механізму оцінювання ризику. Водночас поява нового з'єднання не доводить факт атаки. Воно може бути пов'язане з дозволеними інженерними операціями.

Результатом алгоритму є потік структурованих мережевих подій, придатний для кореляції з іншими джерелами інформації.

Алгоритм виявлення небезпечних керувальних операцій

Для забезпечення цілісності технологічної конфігурації необхідно контролювати не лише факт мережевого підключення, а й характер доступних керувальних операцій.

Вхідними даними алгоритму є події промислових протоколів, журнали інженерного програмного забезпечення та доступні відомості про адміністративні дії.

На першому етапі визначається тип операції. До особливо значущих можуть належати змінювання програми контролера, оновлення прошивки, модифікація конфігурації та зміна режиму роботи обладнання.

Якщо протокол дозволяє достовірно визначити відповідну команду, вона зіставляється з установленою політикою. Для кожного пристрою можуть визначатися дозволені джерела адміністративних операцій та відповідні періоди технічного обслуговування.

За відсутності відкритого прикладного вмісту алгоритм використовує інші доступні джерела. Наприклад, серверний журнал інженерного середовища може містити відомості про завантаження нової програми.

Якщо підтверджено виконання критичної операції поза погодженим регламентом, формується подія підвищеної важливості. При цьому моніторинговий компонент не повинен самостійно надсилати ПЛК команди зупинки або відновлення без погодженої процедури.

Результатом алгоритму є перелік керувальних дій, які потребують перевірки відповідності установленим правилам безпеки.

Алгоритм виявлення відхилень від штатної взаємодії

У промисловій мережі характер обміну даними часто визначається технологічним циклом. Частина повідомлень передається періодично, а інші виникають у відповідь на зміну стану обладнання.

Для визначення потенційних аномалій може використовуватися аналіз історичних характеристик мережевої активності.

На початковому етапі формується базовий профіль взаємодії. До нього можуть входити звичайна кількість пакетів, частота обміну, перелік активних вузлів та характерні часові інтервали.

Після формування профілю поточні показники порівнюються з попередніми спостереженнями. Наприклад, різке збільшення кількості запитів до ПЛК може розглядатися як відхилення від штатної взаємодії.

Однак необхідно враховувати зміну технологічних режимів. Під час запуску виробничої лінії або аварійного переходу кількість повідомлень може закономірно збільшуватися.

Тому для підвищення достовірності доцільно враховувати доступний технологічний контекст. Він може містити поточний режим роботи обладнання та інформацію про заплановані операції.

Результатом алгоритму є виявлені аномалії, які передаються до модуля оцінювання ризику без автоматичного ототожнення з підтвердженою атакою.

Алгоритм перевірки погоджених змін конфігурації

Не кожна зміна програмного забезпечення або параметрів обладнання є порушенням. Протягом експлуатації АСУ ТП виконуються планові оновлення, налаштування та технічне обслуговування.

Для розмежування дозволених і невідомих змін передбачається алгоритм зіставлення результатів контролю цілісності з реєстром погоджених операцій.

Вхідними даними є подія зміни, ідентифікатор компонента, час виявлення та доступна інформація про нову конфігурацію.

На першому етапі перевіряється наявність чинного погодження. Якщо відповідна операція зареєстрована, визначається її допустимий обсяг. Зміна повинна відповідати саме тому компоненту та версії, які зазначені в погодженні.

Окремо контролюється час виконання. Операція, дозволена лише під час зупинки обладнання, не повинна автоматично вважатися погодженою поза визначеним технологічним вікном.

Після зіставлення визначається статус зміни. Вона може бути погодженою, непідтвердженою або такою, що потребує уточнення.

Навіть дозволена зміна повинна супроводжуватися оновленням еталонного стану лише після підтвердження правильності нової конфігурації. Автоматичне перезаписування еталона за фактом виявленої зміни створює ризик приховування несанкціонованого втручання.

Результатом алгоритму є встановлення відповідності змін експлуатаційним регламентам.

Алгоритм оцінювання ризику порушень цілісності

Після виявлення відхилення необхідно визначити його значущість для конкретного компонента АСУ ТП. Однакова зміна може мати різні наслідки залежно від функціонального призначення обладнання.

Вхідними даними алгоритму є характеристика відхилення, категорія компонента, результат перевірки погодження та доступні ознаки підозрілої активності.

На першому етапі визначається тип події. Невідповідність контрольного значення виконуваного файлу розглядається інакше, ніж зміна звичайного журналу або тимчасового параметра.

Далі враховується критичність компонента. Для ПЛК, який керує важливим технологічним процесом, непідтверджена зміна програми може потребувати негайного повідомлення відповідальним фахівцям.

Окремо перевіряється наявність супутніх ознак. Наприклад, зміна конфігурації після підключення невідомої інженерної станції може мати вищу значущість, ніж аналогічна зміна під час документованого технічного обслуговування.

Для комплексного оцінювання доцільно використовувати багатокритеріальну модель, яка враховує тип відхилення, критичність обладнання, достовірність джерела та результат перевірки погодження.

На основі отриманих характеристик визначається пріоритет події. Конкретні порогові значення повинні встановлюватися після перевірки алгоритму на контрольованих сценаріях.

Результатом є оцінка ризику з поясненням чинників, які вплинули на прийняте рішення.

Алгоритм кореляції подій інформаційної безпеки

Окрема невідповідність контрольного значення не завжди дозволяє встановити причину зміни. Тому для підвищення інформативності моніторингу доцільно зіставляти події цілісності з мережевою активністю та журналами доступу.

Вхідними даними є повідомлення файлового моніторингу, події промислових протоколів, результати перевірки погоджень і доступні записи автентифікації.

На першому етапі виконується нормалізація часових позначок та ідентифікаторів компонентів. Далі події групуються за спільними ресурсами й часовими інтервалами.

Наприклад, підключення невідомої інженерної станції до ПЛК, подальша адміністративна операція та виявлена зміна керувальної програми можуть розглядатися як пов'язана послідовність.

При цьому необхідно враховувати достовірність кожного джерела. Мережевий сенсор може підтверджувати факт з'єднання, але не завжди здатний визначити його прикладний зміст.

Якщо події мають достатні спільні ознаки, вони об'єднуються в один логічний інцидент. За недостатньої інформації зберігається невизначений стан кореляції.

Результатом алгоритму є пов'язані групи подій, які використовуються для уточнення ризику та проведення подальшого аналізу.

Алгоритм безпечного реагування на виявлені порушення

Реагування на інциденти в АСУ ТП повинно враховувати можливі наслідки для технологічного процесу. Дії, які є допустимими в корпоративних інформаційних системах, не завжди можуть застосовуватися до промислових контролерів.

Вхідними даними алгоритму є підтверджені або потенційні порушення цілісності, оцінка ризику та інформація про поточний стан технологічного обладнання.

На першому етапі визначається критичність події. Для невисокого рівня небезпеки може бути достатньо створення запису аудиту та повідомлення адміністратора.

Якщо виявлено непідтверджену зміну програми критичного ПЛК, доцільно сформувати термінове сповіщення відповідальним фахівцям із технологічної та інформаційної безпеки.

Автоматичне блокування мережевого з'єднання, перезапуск контролера або повернення попередньої програми повинні виконуватися лише за наявності спеціально погодженої процедури. Безпосереднє втручання в керування технологічним обладнанням може мати небезпечні фізичні наслідки.

Для локалізації інциденту можуть використовуватися організаційні та технічні заходи, які не порушують безпечного стану процесу. Наприклад, тимчасове обмеження адміністративного доступу до інженерної станції може бути допустимим після оцінювання залежностей від відповідного вузла.

Результатом алгоритму є визначена реакція, яка відповідає критичності події та умовам безпечної експлуатації.

Алгоритм збереження та захисту журналів аудиту

Для подальшого аналізу необхідно забезпечити централізоване зберігання результатів моніторингу. Відповідні записи повинні дозволяти встановлювати час виявлення відхилення, контрольований компонент і причину спрацювання.

На початковому етапі подія перетворюється до структурованого представлення. До нього включаються ідентифікатор компонента, категорія порушення, джерело інформації та результат перевірки.

Після формування запис передається до захищеного сховища. У разі тимчасової недоступності центрального компонента може застосовуватися обмежена локальна буферизація.

Для забезпечення достовірності журналів необхідно обмежувати можливість їхньої зміни. За потреби можуть використовуватися криптографічний контроль цілісності, цифрові підписи або сховища з обмеженням модифікації раніше записаної інформації.

Окремо необхідно захищати журнали від розкриття службових відомостей. Вони можуть містити внутрішні адреси, назви ПЛК, конфігураційні параметри та іншу інформацію про структуру технологічної мережі.

Результатом алгоритму є доступна для аналізу історія подій із визначеними механізмами контролю цілісності та доступу.

Алгоритм контролю відмов і працездатності комплексу

Працездатність захисного комплексу повинна контролюватися незалежно від стану основних технологічних компонентів. Відмова системи моніторингу не повинна автоматично створювати небезпечний стан АСУ ТП.

Вхідними даними алгоритму є стан апаратних сенсорів, програмних агентів, колекторів і централізованого сховища.

На першому етапі перевіряється доступність компонентів. Далі аналізується час останнього успішного отримання телеметрії та стан внутрішніх черг.

Якщо мережевий сенсор перестав передавати події, система повинна визначити можливість порушення каналу спостереження. Відсутність повідомлень не слід автоматично трактувати як відсутність загроз.

Для розподілених компонентів можуть використовуватися службові повідомлення про працездатність. Вони дозволяють контролювати стан навіть за низької інтенсивності звичайної технологічної телеметрії.

За тимчасової втрати зв'язку накопичені події можуть передаватися після його відновлення. При цьому необхідно зберігати початковий час виникнення, щоб уникати помилок кореляції.

Результатом алгоритму є актуальна інформація про стан комплексу та повноту доступного спостереження.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Апаратно-програмний комплекс забезпечення цілісності та безпеки критичних компонентів автоматизованих систем керування технологічними процесами (АСУ ТП) призначений для контролю стану промислового обладнання, виявлення несанкціонованих змін програмного забезпечення та моніторингу подій інформаційної безпеки. Програмна частина комплексу забезпечує перевірку еталонних конфігурацій, аналіз мережевої активності, реєстрацію відхилень і формування повідомлень про потенційні порушення. Головне вікно програми показане на рисунку 5.1.

Практичне впровадження комплексу передбачає підготовку апаратного середовища моніторингу, встановлення програмних компонентів, налаштування взаємодії з контрольованими ресурсами та перевірку працездатності. Особливістю експлуатації є необхідність збереження безперервності технологічних процесів. Тому засоби спостереження доцільно розміщувати поза критичними контурами керування. Будь-які операції, здатні змінити стан технологічного обладнання, повинні виконуватися відповідно до погоджених експлуатаційних процедур.

Апаратна частина комплексу може включати окремий сервер моніторингу, мережеві адаптери та засоби отримання копій промислового трафіку. Для підключення до технологічної мережі доцільно використовувати Network TAP або SPAN-порт керованого комутатора. Такий спосіб дозволяє отримувати відомості про мережеві з'єднання без безпосереднього передавання керувальних команд до промислових контролерів. Конкретна конфігурація обладнання визначається топологією мережі та вимогами до пропускної здатності.

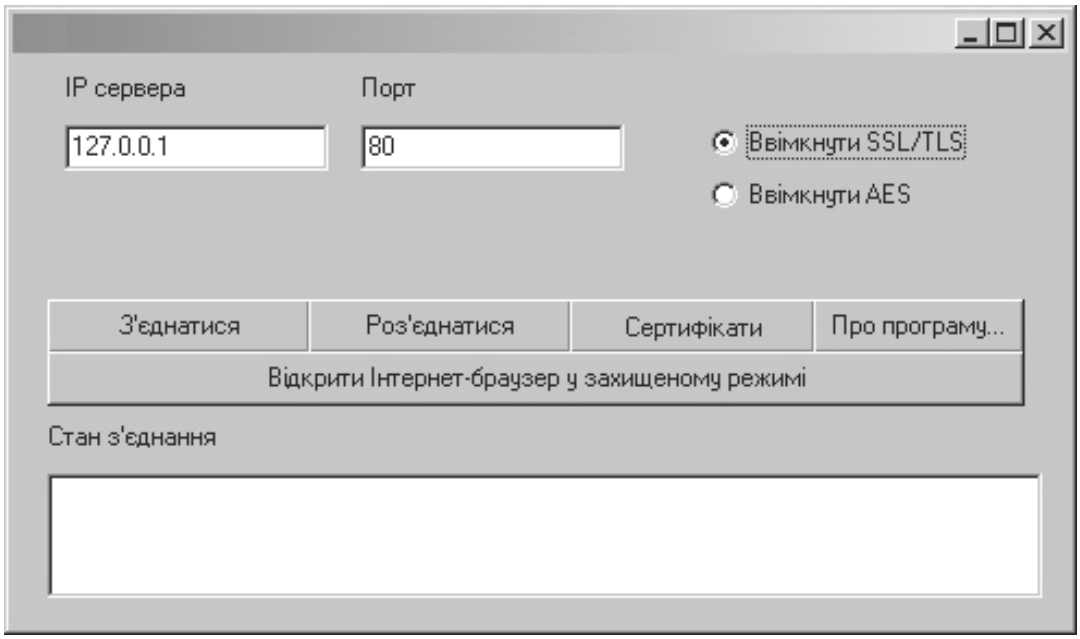

Рисунок 5.1 – Головне вікно ПЗ

Вимоги до обчислювальних ресурсів залежать від кількості контрольованих пристроїв, інтенсивності мережевого обміну та обсягу збережених подій. Особливу увагу необхідно приділити продуктивності мережевого інтерфейсу та накопичувачів. Для забезпечення стабільної роботи доцільно відокремити ресурси, призначені для приймання телеметрії, від компонентів її подальшого аналізу. За потреби можуть використовуватися окремі вузли збору та централізованого зберігання.

Підготовка середовища починається з визначення переліку критичних компонентів АСУ ТП. До них можуть належати програмовані логічні контролери, операторські станції HMI, сервери SCADA, інженерні робочі місця та промислове мережеве обладнання. Для кожного компонента необхідно встановити його призначення, мережеві параметри, версію програмного забезпечення та допустимі способи моніторингу. Отримані відомості використовуються для формування реєстру контрольованих ресурсів.

Наступним етапом є підключення апаратного сенсора до визначеної ділянки промислової мережі. Якщо використовується SPAN, налаштовується копіювання трафіку з відповідних портів або VLAN. Після підключення

необхідно перевірити наявність пакетів в обох напрямках і контролювати показники їхньої втрати. Для зменшення обчислювального навантаження можуть застосовуватися фільтри захоплення, які обмежують аналіз необхідними мережевими потоками.

Після налаштування мережевого спостереження виконується підготовка механізмів контролю цілісності. Для серверів SCADA та інженерних станцій визначається перелік виконуваних файлів, бібліотек і конфігурацій, які підлягають перевірці. Як можливий механізм контролю використовується обчислення криптографічних хешів SHA-256. Результати зберігаються в еталонному маніфесті, який повинен формуватися на основі попередньо перевіреної та погодженої конфігурації.

Для захисту еталонних даних необхідно обмежити можливість їхньої модифікації. Доцільно передбачити окремі права доступу до створення, перегляду та оновлення маніфестів. За потреби застосовуються цифрові підписи або інші механізми підтвердження достовірності. Оновлення еталонного стану допускається лише після перевірки змін і відповідного погодження. Автоматичне прийняття поточної конфігурації за новий еталон після виявлення невідповідності є небажаним.

Контроль програмованих логічних контролерів потребує окремого налаштування. Для кожної моделі необхідно визначити можливість безпечного отримання відомостей про встановлену програму та прошивку. Якщо виробник підтримує відповідні інтерфейси, можуть використовуватися ідентифікатори версій, контрольні значення або результати перевірки цифрового підпису. За відсутності таких можливостей доцільно контролювати затверджені резервні копії інженерних проєктів. Така перевірка не повинна видаватися за безпосереднє підтвердження поточного вмісту пам'яті ПЛК.

Після підготовки джерел налаштовується модуль аналізу мережевої активності. Для нього визначаються контрольовані IP-адреси, промислові протоколи та дозволені напрямки взаємодії. Залежно від підтримуваних аналізаторів можуть оброблятися повідомлення Modbus TCP, OPC UA та інших

промислових протоколів. У разі використання захищених з'єднань система аналізує доступні метадані без спроб несанкціонованого дешифрування.

Окремо встановлюються правила виявлення порушень. До них можуть належати невідповідність контрольних значень, зміна версії прошивки, поява невідомого мережевого вузла та виконання непогоджених адміністративних операцій. Для кожного правила визначається категорія критичності й умови формування сповіщення. Порогові значення для виявлення аномальної мережевої активності доцільно уточнювати з урахуванням штатних режимів роботи технологічного обладнання.

Для коректного зіставлення подій необхідно забезпечити узгоджені часові позначки. Системи моніторингу та доступні серверні компоненти повинні використовувати погоджене джерело синхронізації часу. Водночас зміна часових налаштувань промислових контролерів без відповідного дозволу не допускається. За потреби необхідні перетворення часових позначок виконуються безпосередньо в програмному компоненті оброблення подій.

Рекомендована послідовність запуску починається з перевірки працездатності апаратного вузла та доступності сховища аудиторських даних. Далі активується компонент отримання мережевої телеметрії. Після перевірки надходження повідомлень запускаються модулі нормалізації та контролю цілісності. Наступним етапом є активація механізмів оцінювання ризиків, кореляції подій і формування сповіщень. Завершується запуск перевіркою доступності користувацького інтерфейсу.

Первинне тестування доцільно проводити на лабораторному стенді або в іншому ізольованому середовищі. Для перевірки цілісності використовуються контрольовані копії програмних файлів і конфігурацій. Після формування еталонів до окремих тестових файлів вносяться зміни. Повторна перевірка повинна визначити невідповідність контрольних значень і сформувати відповідний запис аудиту. Окремо необхідно перевірити оброблення недоступних файлів та некоректних еталонних даних.

Для перевірки мережевого моніторингу можуть використовуватися тестові ПЛК, програмні симулятори або попередньо підготовлені записи промислового трафіку. Контролюється правильність визначення мережевих вузлів, протоколів і доступних характеристик обміну. Додатково перевіряється формування сповіщень у разі появи непередбаченого підключення. Такі випробування не повинні передбачати зміну режимів реального технологічного обладнання.

Для ідентифікації програмного продукту передбачається надання відомостей про його розробника. Вони використовуються для встановлення авторства, документування походження програмного забезпечення та організації його подальшого супроводження. Авторські дані апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП представлені на рисунку 5.2.

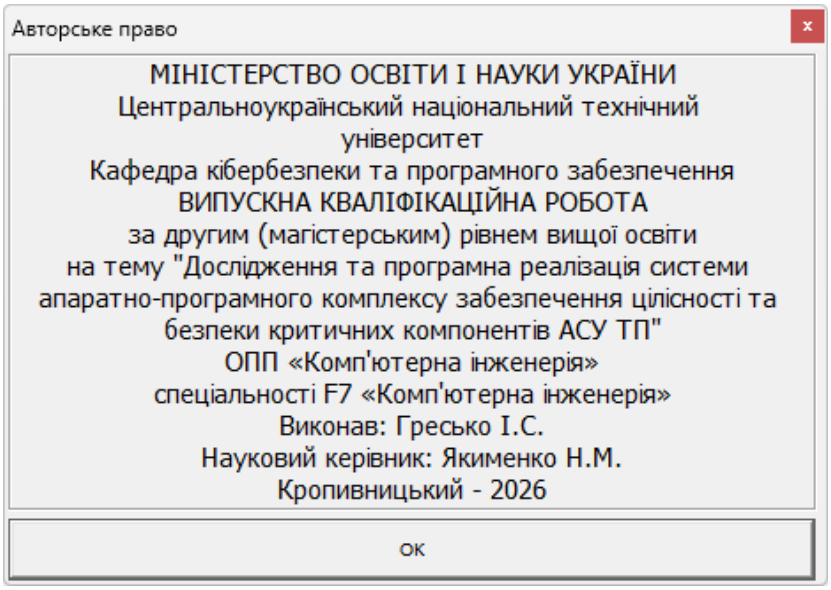

Рисунок 5.2 – Авторське право

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Метою розробки є дослідження та програмна реалізація системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Об'єктом дослідження є процес апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Предметом дослідження є методи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Методи дослідження базуються на методах Інтернету речей, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

– Розроблено вітчизняний продукт апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП, який має більш широкі можливості, на відміну від існуючих аналогів.

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

7.1 Вступ

Зі становленням та розвитком інформаційного суспільства спостерігається масове впровадження комп’ютерних технологій в усіх сферах життя і діяльності людини. Застосування персональних комп’ютерів і ЕОМ дозволило значно підвищити продуктивність праці, змінити характер і зміст праці.

Впровадження комп'ютерних технологій принципово змінило характер праці різних категорій фахівців. Програмісти у процесі роботи отримують негативний вплив на органи зору, а також мають значну розумову напругу і нервово-емоційне навантаження. Руки (м’язи рук та суглоби пальців) при роботі з клавіатурою мають теж істотне навантаження. До шкідливих факторів, які впливають на робітників галузі інформаційних технологій фахівці відносять високочастотні електромагнітні коливання під час роботи апаратної частини ЕОМ та виділення шкідливих газів [1, 2].

Ці шкідливі фактори можуть привести до професійних захворювань.

До недоліків умов праці користувачів комп’ютерної техніки можна віднести:

– недостатню площу і обсяг виробничого приміщення;

– недотримання вимог мікроклімату на робочих місцях;

– низький рівень освітленості у приміщеннях і на робочих поверхнях апаратури;

– підвищений рівень низькочастотних магнітних полів від моніторів;

– порушення вимог організації робочих місць;

– недотримання вимог до режимів праці та відпочинку;

– надмірне виробниче навантаження працівників;

– відсутність навичок зниження впливу психоемоційної напруги.

Відповідно до ст. 14 Закону «Про охорону праці» [3] на роботодавця покладено обов'язок забезпечити: безпеку працівників при експлуатації устаткування; застосування засобів індивідуального захисту працівників; відповідні вимоги охорони праці, умов праці на кожному робочому місці; дотримання режиму праці та відпочинку працівників; навчання безпечним методам і прийомам виконання робіт; інструктаж з охорони праці; організацію контролю над станом умов праці на робочих місцях; проведення атестації робочих місць за умовами праці.

Максимально зменшити кількість шкідливих впливів на людину при високій продуктивності праці, створити комфортні умови для роботи людей – головна задача охорони праці [5].

7.2 Шкідливі і небезпечні фактори при роботі з комп'ютером

Електронно-обчислювальні машини (ЕОМ) та інше офісне обладнання є джерелами небезпеки ураження електричним струмом. Оскільки робота програміста характеризується істотним зоровим навантаженням, то вимагає належного освітлення. У приміщенні, в якому працюють ІТ-працівники, необхідно створити належний мікроклімат, параметри якого регламентуються, Державними санітарними правилами і нормами, зокрема ДСанПіН 3.3.2.007-98 [2].

Шкідливими факторами при роботі з персональним комп'ютером є іонізуюче випромінювання промислової частоти, підвищене нервово-емоційне навантаження на оператора, підвищене навантаження на органи зору та дрібні стереостатичні рухи кінцівок.

Ці фактори можуть викликати у працівника певні розлади здоров'я, зокрема підвищення артеріального тиску, кон'юктивіти, тендовагініти ті інші захворювання.

Комп'ютер, як і будь-який електричний прилад, особливо при його неправильному підключенні, може бути джерелом ураження оператора

електричним струмом. Саме тому всі працівники, які працюють з персональним комп’ютером, повинні мати першу (або другу) групу допуску з електробезпеки.

Через наявність зазначених факторів працівники, які працюють з персональними комп’ютерами, підлягають попередньому та періодичному медичному огляду згідно з пунктом 6.2.3 додатку 4 до наказу Міністерства охорони здоров’я України “Про затвердження Порядку проведення медичних оглядів працівників певних категорій” від 21 травня 2007 року №246 [8].

7.3 Аналіз умов праці

Приміщення розташоване на третьому поверсі п'ятиповерхового будинку. У приміщенні розташовані 3 робочих місця з комп'ютерами (далі ПК). Відповідно до норм «Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-98 [4] площа, яка відводиться для робочого місця з комп'ютером повинна бути не менше 6 м^2, об'єм не менше 20 м^3. Розміри даного приміщення складають: довжина – 6 м, ширина – 4,5 м, висота – 3,5 м, тобто загальна фактична площа складає 27 м^2. Необхідна площа на 3 робочих місця із установленими ПК складає 18 м^2, що не перевищує нормативну. Об’єм приміщення на одного працюючого складає 31,5м^3, отже відповідає нормі ДСанПіН 3.3.2-007-98 – не менше 20 м^3.

При роботі з ПК людина може підпадати під вплив шкідливих та небезпечних факторів. Під шкідливими виробничими факторами розуміють фактори, тривалий вплив яких викликає розвиток професійних захворювань. Небезпечні виробничі фактори це ті, вплив яких на працюючого викликає травму, тобто пошкодження організму. Шкідливі і небезпечні чинники, з якими стикається працівник при роботі з ПК, приведені в таблиці 7.1.

За категорією вибухо- і пожежонебезпеки дане приміщення відноситься до категорії В – пожежонебезпечне, тому що присутні тверді матеріали, що горять, такі як дерев'яні столи, папір та інше. Виходячи з категорії

пожежонебезпеки і поверховості будинку, ступінь вогнестійкості будівлі II. Згідно з ДБН В 1.1-7-2016 «Пожежна безпека об’єктів будівництва» [5] ЕОМ повинні розташовуватись в будівлі не менше ніж II ступню вогнестійкості.

Таблиця 7.1 – Перелік шкідливих та небезпечних виробничих чинників

Найменування чинників	Можливі джерела їх виникнення	Характер дії
Небезпека ураження електричним струмом	Мережа живлення	Небезпечний
Пожежонебезпечність приміщень	Наявність матеріалів, що згорають і джерел запалення (електроапаратура)	Небезпечний та шкідливий
Іонізація повітря	Статична електрика випромінювання	Шкідливий
Підвищений рівень шуму	Шум створюється перетворювачем напруги ЕОМ, її технічною периферією, а також людьми, що працюють в приміщенні	Шкідливий
Несприятлива освітленість	Недостатнє штучне і природне освітлення	Шкідливий
Незадовільні параметри мікроклімату	Незадовільний стан системи опалення і вентиляції	Шкідливий
Психофізіологічні напруження	Монотонність праці, перенапруженість зорових аналізаторів, розумова напруженість, незручність і статичність пози	Шкідливий

За ступенем небезпеки поразки людей електричним струмом відділ класифікується як приміщення з підвищеною небезпекою, тому що не виключена можливість одночасного дотику людини до маючих з'єднання з

землею конструкцій будинку, з одного боку, і до металевих корпусів електроустаткування, що можуть опинитися під напругою – з іншого.

Для забезпечення оптимальних мікрокліматичних умов у приміщенні передбачена система опалення (загальне парове) в холодний період, та вентиляція і кондиціонування в теплий період року згідно ДБН2.5–67–2013 «Опалення, вентиляція та кондиціонування» [6]. При виконанні замірів параметрів мікроклімату, значення їх відповідали оптимальним та допустимим параметрам відповідно до ДСанПіН3.3.2.007 – 98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно – обчислювальних машин».

Припустимий рівень іонізації повітря помешкання відповідно до СН 21.52-80 повинен складати 1500 – 3000 один./м^3.

Нормування освітлення здійснюється відповідно до ДБН В.2.5 – 28 – 2006 «Природне та штучне освітлення». [7]

Відділ забезпечений комбінованим освітленням. В темний час доби передбачається загальне і/або місцеве рівномірне штучне освітлення, а в світлий – бокове одностороннє природне освітлення два віконних прорізи.

Одним з найбільш поширеніших чинників зовнішнього середовища, який несприятливо впливає на людину, є шум. Вплив шуму на організм людини залежить від рівня звукового тиску, частотних характеристик, тривалості дії, а також індивідуальних особливостей людини.

При тривалій дії шуму у оператора ЕОМ виявляються симптоми утомленості, нервового збудження, що сприяють погіршенню працездатності і допущенні помилок при роботі. Для уникнення шкідливої дії шуму на організм працюючого, необхідне дотримання нормованих параметрів, які не повинні перевищувати допустимих величин. При роботі на комп'ютері рівень шуму не повинен перевищувати 50 дБА. Приміщення розташоване вікнами у двір і знаходиться далеко від проїжджої частини вулиці. Основними джерелами шуму в приміщенні є устаткування і люди. Розглянута кімната не призначена для

прийому відвідувачів і тому в ній не спостерігається великого скупчення людей. Тому основним джерелом шуму є комп'ютерна техніка.

Джерелами шуму при роботі ЕОМ є механічні частини принтера, що рухаються, і вентилятори(Lпк = 35 дБА, , Lprn = 48 дБА.) При роботі вентиляційної системи, що забезпечує оптимальний температурний режим електронних блоків ЕОМ і вмонтована в задню панель, створюється аеродинамічний шум. Шум, створюваний працюючим комп'ютером, може бути охарактеризований як широко смуговий постійний з аперіодичним посиленням при роботі принтера. Час роботи ПЕОМ – 6 – 8 год. за добу; принтери працюють не більш 1,5-2 год. за добу.

При наявності великої кількості джерел шуму еквівалентне значення шуму $L_{ЕКВ}$, дБА розраховують по наступній формулі:

$$L_{ЭКВ} = 10 \cdot \lg\left(\frac{1}{T}\sum_{i=1}^{n}\left(t_i \cdot 10^{0.1 \cdot L_i}\right)\right) \qquad (7.1)$$

де

L_i – рівень шуму і-го джерела (пристрою),

ti – час роботи і-го джерела (пристрою),

T – загальний час роботи,

n – кількість джерел шуму даного типу;

Для даного приміщення необхідні змінні складають:

Загальний час роботи – робочий день, тобто T=8 годин.

Для фонового шуму (вентиляторів):

L1 = 35 дБА, T1 = 8 годин, n1=15 (5x3);

Для лазерного принтера Lexmark Jet:

L2 = 48дБА, T2 = 2 години, n2=1, для сканера L3 = 46дБА, T3 = 2 години.

Підставляємо отримані величини у формулу (7.1):

$$L_{ЭКВ} = 10 \cdot \lg\left(\frac{1}{8} \cdot \left(15 \cdot 8 \cdot 10^{0.1 \cdot 35} + 1 \cdot 2 \cdot 10^{0.1 \cdot 48} + 1 \cdot 2 \cdot 10^{0.1 \cdot 46}\right)\right) = 46{,}3 \text{ дБА}$$

Таким чином, еквівалентний рівень шуму в приміщенні за робочий день $L_{екв}$ = 46,3 дБА, що не перевищує норму 50 дБА.

7.4 Техніка безпеки та протипожежна профілактика

Відповідно ДБН В 1.1-7-2016 «Пожежна безпека об’єктів будівництва» будинок можна віднести до II групи по ступені вогнестійкості й до категорії Д по ступені пожежонебезпеки.

Від розподільного щита по праву й ліву сторони встановлені кондиціонери, зовнішня електропроводка, поміщена в ізольований кабель. Висота проводки становить 2,2 м від рівня підлоги. Біля кожного стола організований розподільний щит, розташований на текстолітовій пластинці, закріпленій на стіні на рівні 1м від підлоги. Усього до складу входять п'ять розеток і дві клеми заземлення. Всі обчислювальні машини з'єднані із клемами заземлення. Чотири з п'яти розеток забезпечують подачу напруги 220 V, а одна, забезпечує подачу напруги в 36 V. Про це є відповідні написи на кожному розподільному щиті.

Робота обслуговуючого персоналу полягає в інсталяції необхідного програмного забезпечення й наступному його використанні в діалоговому режимі роботи з ЕОМ. Іноді може виникати необхідність написання допоміжних програм для поліпшення роботи вузла або для зниження витрат. З погляду забезпечення умов праці й вимог техніки безпеки для роботи програміста необхідно наступне: достатнє освітлення екрану дисплея й робочого місця; повна технічна справність устаткування, його електробезпечність; достатня пожежобезпечність приміщення; оптимальний мікроклімат, що сприяє продуктивній роботі; відповідність робочого місця вимогам ергономіки. До небезпечних і шкідливих факторів, дії яких піддається програміст, можна віднести: можливість поразки електричним струмом, при несправності устаткування, порушенні заземлення або техніки безпеки; робота в мікрокліматі з неприпустимими параметрами; робота при недостатній освітленості екрану дисплея й робочого місця.

Відповідно НПАОП 40.1-1.21-98 “Правил безпечної експлуатації електроустановок споживачів” [8], приміщення можна віднести до приміщень

без підвищеної небезпеки, оскільки це приміщення, сухе, з нормальною температурою й ізолюючими підлогами, що не має заземлених металоконструкцій.

Персональні ЕОМ можна віднести до першого класу електротехнічних виробів по способі захисту людини від поразки електричним струмом, оскільки їхні корпуси зроблені з ізолюючої пластмаси й кожен пристрій має заземлення. Відповідно правилам пристрою електроустановок ЕОМ можна віднести до електроустановок з робочою напругою до 1000 В.

Однією з причин пожежі в приміщенні з обчислювальною технікою може бути коротке замикання, що спричиняє спалах електропроводки. Для його попередження вся обчислювальна техніка, а також інші електричні пристрої повинні бути обладнані плавкими запобіжниками, а на вході електромережі повинен бути передбачений автомат захисту. Не слід користуватися електричними подовжувачами й трійниками, що не мають сертифікатів відповідності вимогам безпеки.

Необхідно передбачити наявність у межах досяжності первинних засобів гасіння пожежі (вогнегасників) для локалізації вогню власними силами до приїзду команди пожежної охорони. Повинен бути розроблений план екстреної евакуації персоналу при виникненні загоряння. Кількість евакуаційних виходів повинна бути не менше двох. Допускається використання одного евакуаційного виходу, якщо відстань найбільш віддаленого робочого місця до цього виходу не перевищує 25 м.

7.5 Розрахункова частина

Запорукою безпечної роботи є виконання вимог електричної безпеки, оскільки все офісне обладнання заживлюється від електричної мережі. Одним з необхідних засобів електричної безпеки є встановлення захисного заземлення.

Початкові дані, необхідні для розрахунку захисного заземлення:

– допустимий опір розповсюдженню струму в землі від заземлювального

пристрою $R_{зн}$ = 10 Ом;

– питомий опір грунту в місці встановлення заземлювача $\rho_з$ = 100 Ом/м;

– тип грунту – суглинок;

– тип заземлювача – труба, діаметром d=0.06 м і довжиною l =1.7 м;

– конструкція заземлювача – розташування заземлювачів по контуру. Розрахунок проводимо за стандартною методикою [7].

Визначимо розрахунковий опір землі:

$$\rho_{рз} = \phi \cdot \rho_З$$

де ϕ – коефіцієнт сезонності, що враховує коливання питомого опору при зміні вологості ґрунту протягом року; при використанні заземлювача довжиною l = 1.7 м при глибині закладання від вершини h = 0.65 м ϕ = 1.1 для четвертої кліматичної зони.

Схема розташування заземлювачів показана на рисунку 7.1.

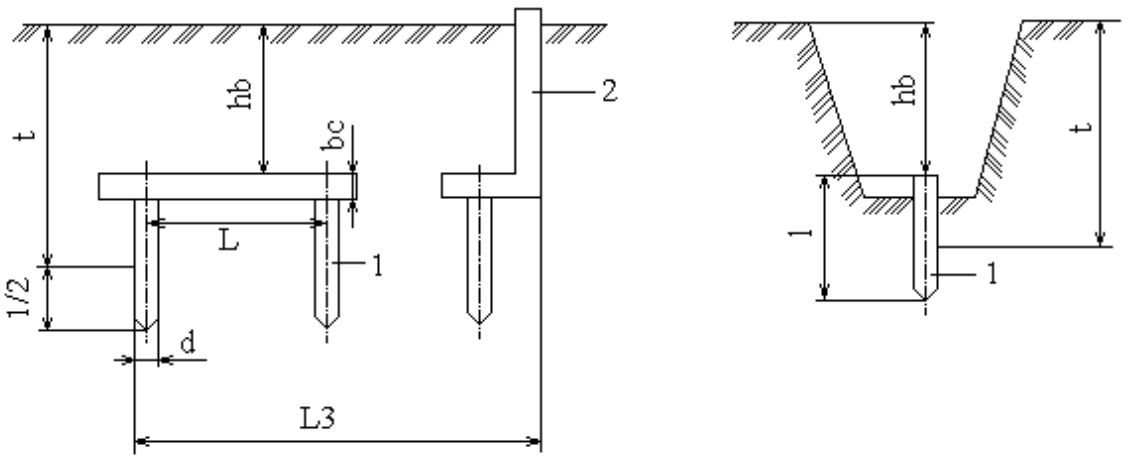

Рисунок 7.1 – Схема розташування заземлювачів

Опір землі:

$$\rho_{рз} = 1{,}1 \cdot 100 = 110 \text{ Ом·м}$$

Опір Rв, розповсюдженню струму в землі від одного вертикального заземлювача:

$$R_B = \frac{\rho_{рз}}{2\pi \cdot l}\left(\ln\frac{2\cdot l}{d} + 0.5\ln\frac{4t+l}{4t-l}\right)$$

де

l – довжина заземлювача (l = 1.7 м);

d = 0.06 м – діаметр заземлювача при U<1 кВ та при S<100 кВА;

t – відстань від поверхні до середини заземлювача:

$$t = h + l/2 = 0.65 + 1.7/2 = 1.5 \text{ м.}$$

$$R_в = \frac{110}{2\cdot 3.14\cdot 1.7}\left(\ln\left(\frac{2\cdot 1.7}{0.06}\right) + 0.5\cdot\ln\left(\frac{4\cdot 1.5+1.7}{4\cdot 1.5-1.7}\right)\right) = 45.17 \text{ Ом}$$

Визначаємо потрібну кількість заземлювачів:

$$n' = \frac{R_в}{R_{зн}} = \frac{45.17}{10} = 4.5 \approx 5 \text{ шт.}$$

Коефіцієнт використання вертикальних заземлювачів враховує ефект екранування. При вибраному значенні k = a/l, де a – відстань між вертикальними заземлювачами, м; k = 1 при a = 2.4 м.

Таким чином, коефіцієнт використання вертикального заземлювача за довідковими даними дорівнює $\eta_В = 0{,}6$.

Кількість вертикальних заземлювачів з урахуванням коефіцієнту використання $\eta_В$ приблизно складає

$$n = \frac{R_в}{R_{зн}\cdot\eta_в} = \frac{45.17}{10\cdot 0.6} = 7.53 \approx 8 \text{ шт.}$$

Довжина горизонтального заземлювача, необхідна для розміщення вертикальних заземлювачів по контуру

$$L = a\cdot n = 2.4\cdot 8 = 19.2 \text{ м}$$

Опір горизонтального заземлювача $R_Г$, Ом, прокладеного на глибині h = 0.65 м від поверхні землі буде

$$R_г = \frac{R_{рз}}{2\cdot 3.14\cdot L}\cdot\ln\frac{2\cdot L^2}{b\cdot h} = \frac{110}{2\cdot 3.14\cdot 19.2}\cdot\ln\frac{2\cdot 19.2^2}{0.06\cdot 0.65} = 10.61 \text{ Ом}$$

де b = 0.04 м – ширина сталевої смуги, з якої виготовлений заземлювач.

Обчислюємо загальний опір:

$$R_з = \frac{R_в \cdot R_г}{n \cdot R_г \cdot \eta_в + R_в \cdot \eta_г} = \frac{45.17 \cdot 10.61}{6 \cdot 10.61 \cdot 0.6 + 45.17 \cdot 0.34} = 8.33 \text{ Ом}$$

де $\eta_Г$ – коефіцієнт використання горизонтального заземлювача ($\eta_Г = 0.34$).

Маємо 7.33 < 10 Ом (за потужності генераторів та трансформаторів 100 кВт і менше), отже нормативне обмеження $R_з < R_{з.норм}$ виконується.

8 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

В межах України в недостатній мірі представлені вітчизняні розробки в цій області.

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти наведені теоретичне узагальнення й рішення наукового завдання дослідження методів апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

– Досліджена система апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

– На основі отриманих результатів досліджень створена програмна реалізація системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП.

Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем.

Програма реалізована на мові високого рівня Visual C++. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

Програма призначена для виконання під управлінням багатозадачної операційної системи Windows 10/11.

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гресько І.С. Дослідження та програмна реалізація системи апаратно-програмного комплексу забезпечення цілісності та безпеки критичних компонентів АСУ ТП // Збірник праць молодих науковців ЦНТУ. – Вип. 17. – Кропивницький: ЦНТУ, 2027.

2. Технології інтернету речей. Навчальний посібник [Електронний ресурс]: / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 12,5 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.

3. Greg Dunko, Joydeep Misra, Josh Robertson, Tom Snyder “A reference guide to the Internet of Things” / 2017 Bridgera LLC, RIoT.

4. Donald Norris “Programming with STM32. Getting started with the Nucleo Board and C/C++” 416 p. 2018.

5. Neil Kolban “Kolban’s book on ESP32”. Texas, USA. 951 p.

6. Vintenko, B., Myronets, I., Smirnov, O., Smirnova, T. «Enhancing the Reliability of Input Data for Nuclear Power Plant Operator Support Systems». *International Conference on Sensors, Devices and Systems. SDaS 2025. Lecture Notes in Electrical Engineering*, 2026. vol 1617. pp 3-12 Springer, Cham.

7. Богаченко, С., Смірнов, О., Буравченко, К., Смірнова, Т., Конопліцька-Слободенюк, О., Якименко, Н., Смірнов, С. «Обмеження ресурсів мобільних та edge-платформ при розробці програмного забезпечення для реалізації та оптимізації моделей машинного навчання». *Електронне фахове наукове видання «Цілісність та безпека критичних компонентів АСУ ТП: освіта, наука, техніка»*, 2026, т. 2 № 34, С. 677-686.

8. Вінтенко Б.Ю., Смірнова Т.В., Миронець І.В., Смірнов О.А., Буравченко К.О. «Метод оцінки функціональної стійкості комп'ютерно-орієнтованих процедур системи підтримки оперативного персоналу АЕС». *Системи управління, навігації та зв’язку*, 2026, вип. 2(84), С. 62-69.

9. Смірнова Т.В., Усік П.С., Лисенко І.А., Буравченко К.О., Смірнов О.А. «Методологія підтримки технологічних процесів у критичній інфраструктурі з забезпеченням безпеки інформації на основі хмарних технологій». *Безпека інформації.* 2025. Том 31 № 1. С. 49-60.

10. Смірнова Т.В., Буравченко К.О., Добринчук О.А., Смірнов С.А., Якименко Н.М., Смірнов О.А. «Хмарна технологія моніторингу ключових індикаторів ефективності технологічних процесів у критичній інфраструктурі». *Центральноукраїнський науковий вісник. Технічні науки.* 2025. № 12(43), ч. II. С. 36-54.

11. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». *Cybersecurity Defensive Walls in Edge Computing*, 2025. pp. 21-61.

12. Вінтенко, Б.Ю., Миронець, І.В., Смірнов, О.А., Коваленко, О.В., Усік, П.С., Буравченко, К.О., Лисенко, І.А. «Логіко-структурна модель комп'ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». *Цілісність та безпека критичних компонентів АСУ ТП: освіта, наука, техніка*. 2025. Том 2 № 30. С. 413-427, 2025.

13. Смірнова, Т.В. «Дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави». *Цілісність та безпека критичних компонентів АСУ ТП: освіта, наука, техніка*. 2025. Том 2 № 30. С.195-208, 2025.

14. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 193–224.

15. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257.

16. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A.,

Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622.

17. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». *Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка»* (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.

18. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». *International Review on Modelling and Simulations* 18 (1), 2025. pp. 32-42.

19. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». *Центральноукраїнський науковий вісник. Технічні науки.* 2025. Вип. 11(42), ч. II. С.52-62.

20. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості інтелектуальних систем підтримки оператора». *VIII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології",* м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – 2025. – С. 44-46.

21. Вінтенко, Б., Миронець, І., Смірнов, О., Коваленко, А., Конопліцька-Слободенюк, О., Смірнова, Т., Константинова, Л. «Дослідження застосування систем підтримки оперативного персоналу об'єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000». *Електронне фахове наукове видання «Цілісність та безпека критичних компонентів АСУ*

ТП: освіта, наука, техніка», 2024. № 2(26), С. 6-26.

22. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення цілісності та безпеки критичних компонентів АСУ ТП хмарних сервісів IaaS, PaaS та SaaS». *Цілісність та безпека критичних компонентів АСУ ТП: освіта, наука, техніка.* 2024. №4(24), С. 6-27.

23. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз цілісності та безпеки критичних компонентів АСУ ТП програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Цілісність та безпека критичних компонентів АСУ ТП: освіта, наука, техніка.* 2024. №3(23), С. 111-131.

24. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.

25. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the Age of ASIC Resistance». *CEUR Workshop Proceedings*, 2023, 3628, pp. 93-105.

26. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.

27. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». *Lecture Notes on Data Engineering and Communications Technologies*, 2023, 178, pp. 208–223.

28. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023,

вип. 3(73), С. 155-166.

29. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи,* 2023, том 7, № 2, С. 49-56.

30. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.

31. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління,* № 2(70). 2022. С. 28-37.

32. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку,* 2022, № 3(69). С. 93-98.

33. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»,* № 2 (307). С. 46-52. 2022.

34. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67). С. 84-89.

35. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M.

«Cloud-Based Cyber Incidents Response System and Software Tools». *Communications in Computer and Information Science*, 2021, vol 1486. Springer, Cham. pp 169-184.

36. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings*. Volume 2740, 2020, Pages 102-114.

37. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.

38. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 172-177.

39. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.

40. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 125-136.

41. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 366-379.

42. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», *CEUR Workshop Proceedings* Volume 2608, 2020, Pages 633-645.

43. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». *International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019*; Odessa; Ukraine; 9-13 September 2019. P.22-28.

44. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.

45. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T),* Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.

46. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T),* Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.

47. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». *CEUR Workshop Proceedings*, Vol 2588, P. 90-106, 2019.

48. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», *2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019*/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.

49. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 353-358.

50. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O.,

Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 347-352.

51. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», *CEUR Workshop Proceedings* Volume 2353, *CEUR Workshop Proceedings* 2019, Pages 618-629.

52. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», *Telecommunications and Radio Engineering*. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.

53. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». *Сучасні інформаційні системи*. 2021. Т. 5, № 4. С. 79-95

54. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» *Вісник Черкаського державного технологічного університету. Технічні науки.* №4. С. 103-110. 2020.

55. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», *Цілісність та безпека критичних компонентів АСУ ТП: освіта, наука, техніка*. № 3(7). С. 43-62. 2020.

56. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.

57. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у *Цілісність та безпека критичних компонентів АСУ ТП та інформаційні технології: монографія.* – Х. : ТОВ

«ДІСА ПЛЮС», 2020.С. 122-135.

58. Смірнов О.А., Дрєєва Г.М., Дрєєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». *Центральноукраїнський науковий вісник. Технічні науки.* № 2(33). с. 161-172, 2019.

59. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.

60. Smirnov, O., Kuznetsov, A., Kuznetsova., K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).

61. Смірнов О.А., Дрєєва Г.М. Метод генерування фрактального трафіку за допомогою моделі генератора на графі. Монографія: Інформаційна безпека та інформаційні технології : монографія / за заг. ред. В. С. Пономаренка. – Х. : Вид. Рожко С.Г. 2019. С. 123-139

62. Дрєєва Г.М., Смірнов О.А., Дрєєв О.М. Метод генерування фрактальноподібної числової послідовності на основі скінченного автомату для моделювання трафіку у мережі. Центральноукраїнський науковий вісник. Технічні науки. № 1(32). с. 173-183, 2019.