Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
магістр
(ступінь вищої освіти)

на тему Дослідження специфіки моніторингу безпеки систем індустріального контролю ОТ-мереж
(назва теми)

Виконав(ла): студент(ка) IIого курсу,
групи БК-814м
Спеціальності 125 Кібербезпека та захист інформації
(код і найменування спеціальності)
Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних систем
ФАРИЛЮК Д.Р.
(ПРІЗВИЩЕ та ініціали)

Керівник КАРПУКОВ Л.М.
(ПРІЗВИЩЕ та ініціали)

Рецензент МОРОЗ Г.В.
(ПРІЗВИЩЕ та ініціали)

2025

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
Кафедра інформаційної безпеки та наноелектроніки
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
(код і найменування)
Освітня програма (спеціалізація) Безпека інформаційних та комунікаційних систем
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ
Завідувач кафедри ІБтаН
Андрій КОРОТУН
«____» _____2025року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

ФАРИЛЮК Дар'ї Романівні
(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Дослідження специфіки моніторингу безпеки систем індустріального контролю ОТ-мереж
Research into the specifics of security monitoring of industrial control systems for OT networks

керівник проєкту (роботи) д.т.н., професор КАРПУКОВ Леонід Матвійович.
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом закладу вищої освіти від « 26» листопада 2025 року № 530
2. Строк подання студентом проєкту (роботи) 10.12.2025
3. Вихідні дані до проєкту (роботи) Аналіз специфіки ОТ-мереж, їх вимог, методів і засобів захисту інформації та сучасних програмних та апаратних рішень захисту інформації
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Загальний опис промислових систем управління (ICS); ключові сектори та застосування ICS, огляд компонентів і архітектури ICS, основні вразливості та загрози в середовищах ICS, мережева архітектура ICS, Модель Пердью
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)
Презентація доповіді (в MS PowerPoint), 17 слайдів.

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1 – 3	КАРПУКОВ Л.М., завідувач кафедри ІБтаН	02.09.2025	05.12.2025
Нормоконтроль	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН		09.12.2025

7. Дата видачі завдання «02» вересня 2025року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1.	Вибір теми. Затвердження плану і завдання кваліфікаційної роботи.	02.09.25 – 16.09.25	виконано
2.	Аналіз завдання, пошук та огляд літературних джерел за темою роботи.	17.09.25 – 23.09.25	виконано
3.	Огляд специфіки роботи ICS та OT мереж, правила та методи взаємо OT мережі з іншими мережами.	24.09.25 – 29.09.25	виконано
4.	Дослідження та аналіз безпечних мережевих моделей підприємств та інших рекомендацій з метою покращення рівня захисту інформації.	30.09.25 – 05.10.25	виконано
5.	Опис та аналіз протоколів OT мережі у порівнянні з IT мережею, аналіз рівня інформаційної безпеки сучасних протоколів у порівнянні з більш поширеними старішими протоколами.	06.10.25 – 15.10.25	виконано
6.	Розробка списку рекомендацій для підвищення рівня інформаційної безпеки у індустріальних мережах, огляд сучасних апаратних та програмних рішень, опис та порівняння широкопрофільних апаратних та програмних рішень та вузькопрофільних рішень розроблених тільки для специфіки OT та ICS.	16.10.25 – 31.10.25	виконано
7.	Оформлення пояснювальної записки.	01.11.25 – 13.11.25	виконано
8.	Здача на перевірку та підпис кваліфікаційної роботи керівнику.	14.11.25 – 19.11.25	виконано
9.	Проходження перевірки на плагіат та нормоконтроль кваліфікаційн роботи.	20.11.25 – 30.11.25	виконано
10.	Допуск завідувачем кафедри до захисту кваліфікаційної роботи.		
11.	Захист дипломної роботи		

Студент(ка) _____ Дар'я ФАРИЛЮК
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ Леонід КАРПУКОВ
(підпис) (Ім'я ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до дипломної кваліфікаційної роботи магістра: 77 с., 14 табл., 7 рис., 1 дод., 29 джерел.

ПІДПРИЄМСТВО, ІНФОРМАЦІЙНА БЕЗПЕКА, ПРОТОКОЛ, БЕЗПЕКА СИСТЕМ ІНДУСТРІАЛЬНОГО КОНТРОЛЮ, ОТ МЕРЕЖІ, МОДЕЛЬ ПЕРДЬЮ, ПРОГРАМНІ ТА АПАРАТНІ РІШЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ ICS, SCADA, MICRO - SCADA.

Об’єкт дослідження — Інформаційна безпека у системах індустріального контролю.

Предмет дослідження – Методи та засоби забезпечення інформаційної безпеки у системах індустріального контролю.

Мета роботи – Розробка списку рекомендацій щодо підвищення рівня захисту індустрії.

У роботі розглянуто специфіку роботи ICS та OT мереж, правила та методи взаємодії інших мереж з OT мережею. Було проаналізовано і досліджено безпечні мережеві моделі підприємств та інші рекомендації з метою покращення рівня захисту інформації підприємств.

У роботі розглянуто в порівнянні протоколи OT та IT мереж та основні відмінності цих мереж як у пріорітетах КЦД, так і у вимогах до побудовии цих мереж.

Практичне значення одержаних результатів полягає у розробці рекомендацій щодо підвищення рівня безпеки інформації на підприємствах.

ABSTRACT

Explanatory note to the master's thesis: 77 p., 14 tables, 7 figures, 1 appendix, 29 sources.

ENTERPRISES, INFORMATION SECURITY, PROTOCOL, SECURITY OF INDUSTRIAL CONTROL SYSTEMS, OT NETWORKS, PERDUE MODEL, SOFTWARE AND HARDWARE SOLUTIONS FOR INFORMATION SECURITY ICS, SCADA, MICRO - SCADA.

Object of research — Information security in industrial control systems.

Subject of research — Methods and means of ensuring information security in industrial control systems.

Purpose of work — Development of a list of recommendations for increasing the level of industry protection.

The paper considers the specifics of the operation of ICS and OT networks, rules and methods of interaction of other networks with the OT network. Secure enterprise network models and other recommendations were analyzed and researched to improve the level of enterprise information protection.

The paper compared the protocols of OT and IT networks and the main differences between these networks in both the priorities of the CCD and the requirements for building these networks.

The practical significance of the results obtained lies in the development of recommendations for increasing the level of information security in enterprises.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ICS — Industrial Control Systems — Промислові системи керування;

SCADA — Supervisory Control and Data Acquisition — Надійний контроль та збирання даних;

IT — Information Technology — Інформаційні технології (IT);

PERA — Purdue Enterprise Reference Architecture — Еталонна архітектура підприємства Пердью;

OSI — Open Systems Interconnection — Модель взаємодії відкритих систем;

TCP/IP — Transmission Control Protocol / Internet Protocol — Протокол керування передачею / Інтернет-протокол;

HTTP — HyperText Transfer Protocol — Протокол передачі гіпертексту;

FTP — File Transfer Protocol — Протокол передачі файлів;

SMTP — Simple Mail Transfer Protocol — Простий протокол передачі пошти;

Modbus — Modular Digital Bus — Модульна цифрова шина;

Profinet — Process Field Net — Мережа польового рівня для процесів.

EtherCAT — Ethernet for Control Automation Technology — Ethernet для технологій автоматизації керування.

DNP3 — Distributed Network Protocol 3 — Розподілений мережевий протокол 3.

КЦД — Конфіденційність, Цілісність, Доступність — Вимірювана модель інформаційної безпеки.

IEC — International Electrotechnical Commission — Міжнародна електротехнічна комісія.

OPC UA — Open Platform Communications Unified Architecture — Уніфікована архітектура відкритих платформ зв’язку.

DMZ — Demilitarized Zone — Демілітаризована зона.

IDS — Intrusion Detection System — Система виявлення вторгнень.

IPS — Intrusion Prevention System — Система запобігання вторгненням.

SIEM — Security Information and Event Management — Керування інформацією та подіями безпеки.

SOC — Security Operations Center — Центр операцій безпеки (ЦОБ).

VLAN — Virtual Local Area Network — Віртуальна локальна мережа.

ERP — Enterprise Resource Planning — Планування ресурсів підприємства.

DCS — Distributed Control System — Розподілена система керування.

PLC — Programmable Logic Controller — Програмований логічний контролер.

RTU — Remote Terminal Unit — Віддалений термінал.

IED — Intelligent Electronic Device — Інтелектуальний електронний пристрій.

HMI — Human-Machine Interface — Людино-машинний інтерфейс.

OT — Operational Technology — Операційна технологія.

CPS — Cyber-Physical Systems — Кібер-фізичні системи.

SIS — Safety Instrumented Systems — Інструментальні системи безпеки.

MES — Manufacturing Execution System — Система керування виробництвом.

BMS — Building Management System — Система управління будівлями.

IIoT — Industrial Internet of Things — Промисловий Інтернет речей.

BPCS — Basic Process Control System — Базова система управління процесами.

NIST — National Institute of Standards and Technology — Національний інститут стандартів і технологій.

MTU — Master Terminal Unit — Головний термінал.

CPU — Central Processing Unit — Центральний процесор.

IOA — Input/Output Address — Адреса введення/виведення.

ASDU — Application Service Data Unit — Блок даних служби додатків.

ВСТУП

Актуальність теми дослідження обумовлено тим, що вимоги до середовища мережей операційних технологій (ОТ) набагато вищі аніж у мережах інформаційних технологій (ІТ), невеличкі затримки чи перебої у обробці та передачі інформації можуть нести за собою величезні збитки, руйнування та найголовніше можуть нанести фізичну шкоду працівникам промисловості.

Результатом нанесення шкоди промисловості та створення перебоїв у їх штатному режимі можуть мати за метою зловмисники, котрі атакують промисловість через канали передачі інформації за допомоги вразливостей протоколів, мереж, почтових сервісів і інших можливих точок доступу, з метою потрапляння до мережі ОТ і завдання значної шкоди через зміну різноманітних атрибутів промислових машин.

Зазвичай, найпріорітетнішою ціллю для зловмисників у промисловості становлять системи SCADA, котрі дозволяють змінювати параметри індустріальних машин та контролювати та реагувати на різноманітні події, тому у випадку несанкціонавоного доступу до системи SCADA зловмисник отримає прямий доступ до найкритичніших систем підприємтсва.

У рамках дослідження планується вивчити оптимальні моделі побудови мереж та іншої мережової інфраструктури у рамках промисловості, а також дослідити різноманітні апаратні та програмні рішення, котрі дозволяють значно підвищити рівень кіберзахисту промислових систем, у яких, зазвичай, найкоротші простої у роботі несуть за собою величезні наслідки.

Метою дослідження у кваліфікаційній роботі є аналіз і дослідження оптимальної побудови мережей ICS, підвищення рівня кіберзахисту на промислових об’єктах, розробка та порівняння комплексу рекомендацій щодо підвищення захищеності промислових об’ктів.

Дослідження даної теми є не тільки теоретично важливим, але й практично значущим, оскільки дозволяє виробити стратегії для підвищення захищеності промислових інформаційних систем, що врешті-решт сприятиме збереженню конфіденційності, цілісності та доступності інформації в умовах сучасних кіберзагроз.

Завданнями дослідження є:

- вивчити теоретичні основи комп'ютерних систем промисловості;
- розглянути оптимальні моделі побудови мереж і міжмережової комунікації у промисловості;
- проаналізувати протоколи промислових мереж, порівняти ступінь захищеності цих протоколів та розробити рекомендації щодо використання більш захищенних протоколів;
- розробити комплекс рекомендацій щодо захисту промислових систем керування та критичних мереж промисловості;
- зробити порівняльний аналіз сучасних апаратних та програмних рішень з точки зору профільності щодо саме мереж ОТ, та широкопрофільних рішень.

Об'єкт дослідження — Інформаційна безпека у системах індустріального контролю. Розробка рекомендацій щодо захисту систем промисловості.

Предмет дослідження — методи та механізми роботи промислових систем, відмінності протоколів ОТ та ІТ мереж.

Практична значимість результатів полягає у тому, що проаналізовані дані та результати представлені у пропозиційній частині кваліфікаційної роботи можуть бути використані для удосконалення рівня захисту інформації промислових систем керування, несанкціонований доступ до яких може нести за собою катастрофічні наслідки.

Наукова новизна роботи полягає у розробці списку рекомендацій щодо захисту систем промисловості у сучасному світі, коли технології розвиваються з неймовірною швидкістю, у багатьох процесах починається залучатися

штучний інтелект та обсяг інформації котра передається та обробляється продовжує зростати.

Усі ці критерії приводять нас до висновку того, що у найкритичніших систем - перешкодження штатної роботи яких можуть мати величезні наслідки не тільки для самого підприємства, а і для усієї країни (у випадку критичної інфраструктури), розвиток та впровадження найсучасніших рішень кіберзахисту повинно мати найвищий пріорітет.

Методологія дослідження охоплює аналітичний огляд наукової літератури, теоретичний аналіз вразливостей промислових протоколів, порівняння захисту інформації у різноманітних протоколах промислової специфіки та розробку рекомендацій щодо захисту промисловості за допомоги сучасних апаратних та програмних методів і засобів захисту інформації.

1 ПРИНЦИПИ, ВИДИ ТА ЕЛЕМЕНТИ ФУНКЦІОНУВАННЯ ІНДУСТРІАЛЬНИХ СИСТЕМ КОНТРОЛЮ

1.1 Принципи функціонування індустріальних систем контролю

Індустріальні системи контролю (Industrial Control Systems, ICS) є фундаментальним елементом сучасних виробничих процесів, що забезпечують автоматизацію, керування та моніторинг технологічних об’єктів у промисловості [1]. Основною метою таких систем є забезпечення стабільної, безпечної та ефективної роботи обладнання, процесів і технологічних ліній. Вони поєднують апаратні й програмні компоненти, які здійснюють збір, обробку, передавання та аналіз даних про стан технологічних процесів у реальному часі, дозволяючи операторам та інженерам приймати обґрунтовані рішення щодо керування виробництвом.

Функціонування ICS базується на ієрархічній структурі, яка зазвичай включає кілька рівнів: польовий рівень (датчики, виконавчі механізми, контролери), рівень керування (PLC, DCS або SCADA-системи) та рівень диспетчерського управління і планування (MES, ERP тощо). На нижньому рівні системи відбувається безпосередня взаємодія з фізичним середовищем через сенсори, що збирають дані про температуру, тиск, витрату, напругу та інші параметри. Ці дані передаються до програмованих логічних контролерів (PLC) або віддалених термінальних пристроїв (RTU), які аналізують вхідні сигнали й формують керуючі дії для виконавчих механізмів. Таким чином забезпечується замкнутий цикл керування технологічним процесом [3].

На рівні SCADA (Supervisory Control and Data Acquisition) здійснюється централізований моніторинг стану системи, архівування даних, візуалізація параметрів і дистанційне керування обладнанням. SCADA-системи взаємодіють із контролерами через промислові мережі та протоколи зв’язку, такі як Modbus, Profinet, EtherCAT чи DNP3. Вищі рівні — MES (Manufacturing Execution System) і ERP (Enterprise Resource Planning) — інтегрують інформацію з

виробничих процесів із бізнес-процесами підприємства, забезпечуючи ефективне планування ресурсів, контроль продуктивності та якість виробництва.

Однією з ключових характеристик індустріальних систем контролю є вимога до високої надійності та безперервності функціонування. Будь-який збій у роботі системи може призвести до порушення технологічного процесу, фінансових втрат або навіть аварійних ситуацій. Тому ICS мають спеціальні механізми резервування, діагностики та захисту, які мінімізують ризики зупинки виробництва. Водночас сучасні тенденції розвитку промислових систем — таких як цифровізація, впровадження Industrial Internet of Things (IIoT) та інтеграція з інформаційними мережами (IT) — призвели до підвищення рівня взаємопов’язаності між виробничими та корпоративними сегментами. Це, у свою чергу, створює нові виклики в аспектах інформаційної безпеки та потребує розроблення ефективних підходів до моніторингу OT-мереж і виявлення кіберзагроз [5].

Отже, принципи функціонування індустріальних систем контролю базуються на інтеграції апаратних і програмних засобів для безперервного керування технологічними процесами, обміну даними між різними рівнями автоматизації та забезпечення надійності функціонування виробництва. Глибоке розуміння цих принципів є необхідною основою для подальшого дослідження специфіки моніторингу безпеки OT-мереж, оскільки дозволяє чітко ідентифікувати критичні компоненти, канали обміну інформацією та потенційні вектори атак у промисловому середовищі [2].

1.2 Архітектура індустріальних систем контролю

Архітектура індустріальних систем контролю (Industrial Control Systems, ICS) визначає логічну структуру, взаємозв’язки та принципи організації апаратних і програмних компонентів, що забезпечують автоматизацію технологічних процесів. Вона формує основу для ефективного функціонування

систем керування, інтегруючи різнорівневі елементи — від датчиків і виконавчих механізмів до аналітичних платформ і корпоративних інформаційних систем. Основною метою побудови архітектури ICS є створення надійної, масштабованої та безпечної інфраструктури, здатної забезпечити стабільне функціонування виробничого процесу у реальному часі [8].

На рисунку 1.1 зображена логічна модель розмежування архітектури ICS - обов'язкова частина моделі Пердью і один із найголовніших принципів забезпечення інформаційної безпеки між мережами індустрії.

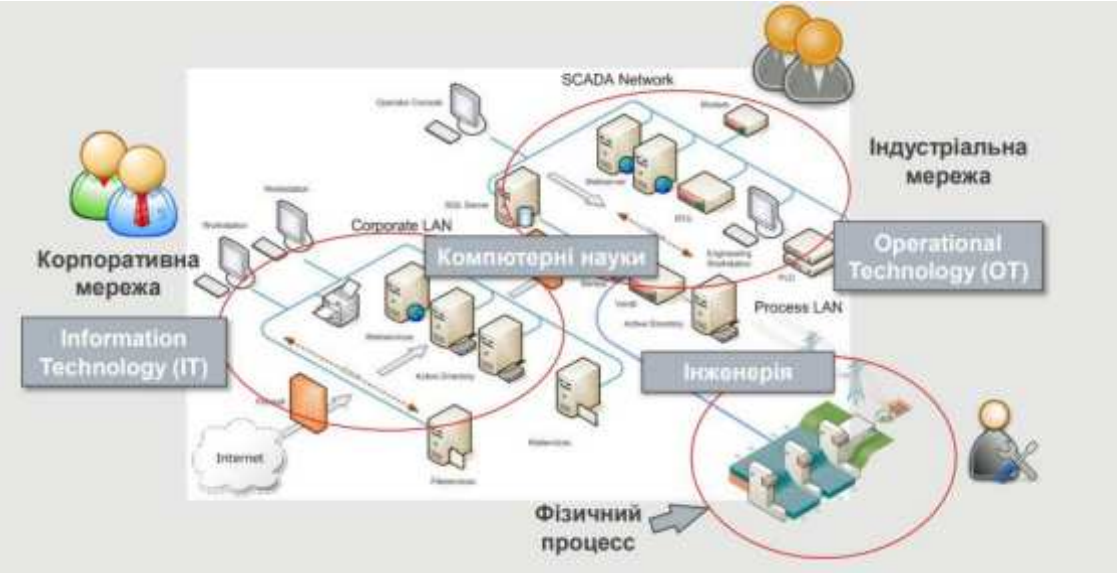

Рисунок 1.1 – Типова модель розмежування архітектури індустріальних систем контролю

Класичним підходом до моделювання архітектури ICS є еталонна модель Purdue Enterprise Reference Architecture (PERA), яка описує ієрархічну побудову промислових систем у вигляді взаємопов'язаних рівнів. Кожен рівень виконує специфічні функції у межах загальної системи керування:

- Рівень 0 (польовий) — фізичний рівень, що включає сенсори, датчики та

виконавчі механізми, які безпосередньо взаємодіють із технологічним процесом;

- Рівень 1 (керування) — містить програмовані логічні контролери (PLC),

віддалені термінальні пристрої (RTU) та інші елементи, що збирають дані з польового рівня і формують керуючі команди;

- Рівень 2 (моніторинг і візуалізація) — представлений системами SCADA

та HMI, які здійснюють централізований контроль, відображення технологічних параметрів і первинний аналіз даних;

- Рівень 3 (виробниче управління) — реалізується за допомогою систем

MES, які відповідають за координацію операцій, контроль якості, оптимізацію завантаження обладнання та відстеження виробничих показників;

- Рівень 4 (підприємницький) — охоплює ERP-системи, що забезпечують

планування ресурсів, управління логістикою, фінансами та інтеграцію виробничих процесів із бізнес-завданнями організації;

- Рівень 5 (аналітичний) — сучасне доповнення моделі, що включає хмарні сервіси, платформи штучного інтелекту та інструменти аналітики даних для прогнозування та оптимізації роботи виробництва [2,7].

На рисунку 1.2 схематично зображено власну теоритичну конфігурацію мережі згідно до моделі Пердью.

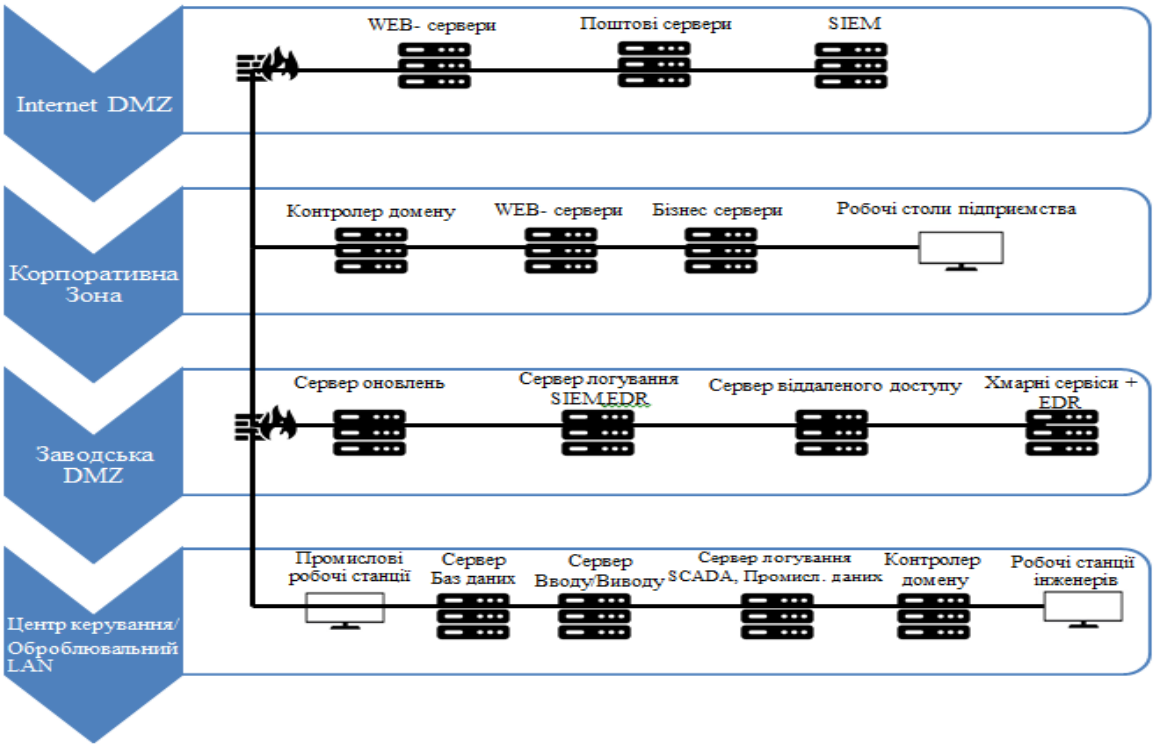

Рисунок 1.2 – Приклад топології промислових мереж за зразком моделі Пердью

Ієрархічна побудова ICS ґрунтується на принципі мережевої сегментації, коли кожен рівень функціонує у власному ізольованому середовищі, пов’язаному з іншими через стандартизовані шлюзи або комунікаційні протоколи. Критичним елементом є демілітаризована зона (DMZ), яка відділяє корпоративну IT-мережу від операційної OT-мережі, запобігаючи прямому обміну трафіком між ними та мінімізуючи ризик кіберінцидентів.

Комунікаційна взаємодія між компонентами ICS забезпечується за допомогою спеціалізованих промислових протоколів, розроблених для гарантованої надійності в умовах підвищених вимог до безперервності роботи [4]. Найбільш поширеними з них є Modbus, Profinet, EtherCAT, DNP3, OPC UA, які дозволяють передавати дані з мінімальними затримками та високим рівнем стійкості до збоїв. У сучасних системах дедалі частіше впроваджуються гібридні архітектурні рішення, що інтегрують промислові контролери з хмарними технологіями та пристроями Індустріального Інтернету речей (IIoT). Такий підхід розширює можливості моніторингу, аналітики та прогнозування стану виробництва у реальному часі.

Отже, архітектура індустріальних систем контролю являє собою багаторівневу, взаємопов’язану структуру, в якій апаратні, програмні та комунікаційні компоненти працюють узгоджено для досягнення високої ефективності, надійності та безпеки виробничих процесів. Її розуміння є ключовим для дослідження специфіки моніторингу безпеки OT-мереж, оскільки саме архітектурна структура визначає шляхи взаємодії між елементами системи, критичні вузли й потенційні точки уразливості [11].

1.3 Види та класифікація індустріальних систем контролю

Індустріальні системи контролю (ICS) охоплюють широкий спектр технологічних рішень, які застосовуються для автоматизації виробничих процесів у різних галузях промисловості - від енергетики й нафтогазового сектору до харчової промисловості та транспорту. Незважаючи на спільну мету - забезпечення надійного та безперервного функціонування технологічних процесів, - такі системи можуть істотно відрізнятися за архітектурою, функціональністю, масштабом і типом взаємодії з об’єктом керування. Для систематизації цього різноманіття використовують декілька підходів до класифікації ICS.

Найпоширенішою є класифікація за типом системи керування, що виділяє три основні групи:

- SCADA-системи (Supervisory Control and Data Acquisition) — призначені для централізованого моніторингу та диспетчерського управління розподіленими об’єктами. Вони забезпечують збір даних у реальному часі, їх обробку, архівування та відображення на інтерфейсі оператора. SCADA найчастіше застосовується в енергетичних мережах, транспортній інфраструктурі, системах водопостачання та телекомунікаціях;
- DCS-системи (Distributed Control Systems) — реалізують розподілене керування технологічними процесами в межах одного підприємства або виробничої ділянки. Кожна частина системи працює автономно, але узгоджено

з іншими, що підвищує гнучкість та надійність керування. DCS часто використовуються в хімічній, нафтохімічній і металургійній промисловості;

- PLC-системи (Programmable Logic Controller) — базуються на використанні програмованих логічних контролерів, які виконують локальні функції керування конкретними машинами або установками. Завдяки своїй модульності, простоті програмування та високій надійності PLC є універсальним рішенням для автоматизації невеликих і середніх процесів [12].

Окрім основних типів, сучасні виробництва дедалі частіше використовують гібридні або інтегровані системи, які поєднують властивості SCADA, DCS та PLC. Такий підхід дозволяє досягати більшої гнучкості, масштабованості й узгодженості даних між рівнями управління. Водночас з розвитком Індустрії 4.0 з’являються нові класи ICS, зокрема IIoT-платформи (Industrial Internet of Things), що забезпечують інтеграцію промислових пристроїв у єдине цифрове середовище та підтримують аналітику на основі великих даних [3].

Іншим критерієм класифікації є рівень інтеграції системи. За цим підходом виділяють:

- локальні системи керування, що охоплюють окремі машини або технологічні вузли;
- регіональні або дільничні системи, які координують взаємодію кількох виробничих установок;
- глобальні системи, що об’єднують комплексні технологічні процеси на рівні підприємства чи навіть цілої галузі.

Додатково ICS можна класифікувати за характером технологічного процесу — безперервні, дискретні або змішані. Безперервні процеси (наприклад, у нафтохімії чи енергетиці) потребують постійного контролю параметрів і коригування режимів роботи. Дискретні процеси (характерні для машинобудування, харчової чи легкої промисловості) передбачають циклічне виконання окремих операцій, тоді як змішані системи поєднують обидва типи керування [6].

Таким чином, індустріальні системи контролю можуть відрізнятися за масштабом, архітектурою, технологічною спрямованістю та функціональною роллю. Незалежно від різновидів, усі вони формують єдину екосистему промислової автоматизації, де збір, передавання, обробка й аналіз даних є ключовими передумовами для ефективного моніторингу, оптимізації процесів і забезпечення інформаційної безпеки ОТ-мереж.

1.4 Ключові елементи індустріальних систем контролю

Індустріальні системи контролю (Industrial Control Systems, ICS) є складними техніко-програмними комплексами, до складу яких входить безліч взаємопов’язаних компонентів. Кожен із них виконує специфічну функцію — від безпосереднього вимірювання параметрів технологічного процесу до аналітики, візуалізації та прийняття управлінських рішень. Розуміння структури та функцій ключових елементів ICS є необхідною умовою для оцінки їхньої надійності, ефективності й рівня захищеності в контексті кібербезпеки ОТ-мереж [10].

На рисунку 1.3 зображено ключові елементи індустріальних систем контролю.

Рисунок 1.3 – Ключові елементи індустріальних систем контролю

До основних компонентів ICS належать такі компоненти:

- Контролери (PLC, RTU, IED). Програмовані логічні контролери (PLC) та віддалені термінальні пристрої (RTU) є центральною ланкою польового та керуючого рівнів. Вони отримують інформацію від сенсорів, аналізують її за заданими алгоритмами й формують керуючі сигнали. PLC здебільшого застосовуються на локальних виробничих ділянках, тоді як RTU використовуються у розподілених системах, наприклад, у енергетичних мережах чи транспортній інфраструктурі. Інтелектуальні електронні пристрої (IED) поєднують функції збору, обробки та передачі даних, забезпечуючи більш гнучку й масштабовану взаємодію в межах OT-мережі;
- Людино-машинні інтерфейси (HMI). HMI забезпечують взаємодію оператора з технологічним процесом. За допомогою графічних панелей, екранів або спеціалізованих програм оператор може спостерігати за станом системи, змінювати параметри керування, переглядати історію подій і відстежувати аварійні сповіщення. Ефективність HMI безпосередньо впливає на швидкість реагування персоналу на відхилення та на рівень ситуаційної обізнаності під час моніторингу процесів;
- Системи диспетчерського контролю та збору даних (SCADA). SCADA-системи відіграють ключову роль у централізованому моніторингу, управлінні та архівуванні даних. Вони збирають інформацію з численних контролерів, аналізують її та передають оператору у зручній для сприйняття формі. SCADA також здійснює журналювання подій, формує звіти та може інтегруватися з іншими рівнями управління — MES чи ERP. У контексті безпеки SCADA є критичним елементом, адже компрометація її сервера або каналів зв’язку може призвести до зупинки виробництва чи спотворення технологічних параметрів;
- Системи виконання виробництва (MES). MES-системи є проміжною ланкою між виробничими процесами та корпоративним рівнем управління. Вони координують роботу обладнання, планують завантаження ресурсів, контролюють якість продукції та продуктивність операторів. Завдяки інтеграції

MES із нижчими рівнями (SCADA, PLC) підприємства отримують повну прозорість процесів і можуть оперативно реагувати на зміни умов виробництва;

- Комунікаційна інфраструктура та протоколи зв'язку. Передавання даних між компонентами ICS здійснюється за допомогою промислових протоколів, таких як Modbus, Profinet, EtherCAT, DNP3, OPC UA тощо. Ці протоколи розроблені для забезпечення стабільного обміну інформацією в реальному часі, проте більшість із них спочатку не передбачали механізмів захисту. Саме тому сучасні системи використовують шифрування, автентифікацію й сегментацію мережі (зокрема, DMZ) для підвищення безпеки передачі даних;
- Сервери та бази даних. Центральні сервери виконують функції зберігання, обробки й аналізу великих обсягів інформації. Вони можуть розміщуватися локально або у хмарному середовищі, залежно від архітектури підприємства. Серверна інфраструктура часто є ціллю кіберзагроз, тому до неї висуваються підвищені вимоги щодо резервування, контролю доступу та безперервності роботи [7,16].

У першому розділі було розглянуто теоретичні основи функціонування індустріальних систем контролю (ICS), їх архітектурну побудову, класифікаційні особливості та основні компоненти, що забезпечують ефективне управління технологічними процесами в OT-мережах.

Проаналізовано, що індустріальні системи контролю є основою сучасної промислової автоматизації, забезпечуючи безперервність, точність і безпеку функціонування виробництва. Їхнє призначення полягає у зборі, обробці та передачі даних про стан технологічних процесів у реальному часі, що дозволяє операторам здійснювати контроль і приймати оперативні рішення.

Розглянуто архітектуру ICS на основі еталонної моделі Purdue (PERA), яка передбачає ієрархічну структуру взаємопов'язаних рівнів — від польового обладнання до корпоративних систем управління. Така побудова дозволяє розмежувати функції між технічними, операційними та управлінськими рівнями, забезпечуючи цілісність і стабільність роботи промислового комплексу. Водночас саме архітектурна структура визначає ключові точки

взаємодії OT- і IT-середовищ, що є критичним аспектом для подальшого забезпечення кіберзахисту.

Було встановлено, що класифікація індустріальних систем контролю охоплює кілька основних типів — SCADA, DCS, PLC, а також сучасні гібридні рішення, інтегровані з технологіями Індустріального Інтернету речей (IIoT). Кожен тип має свої функціональні особливості, галузь застосування та рівень інтеграції з корпоративними мережами. Зокрема, SCADA забезпечує централізований моніторинг розподілених об’єктів, DCS — розподілене управління процесами, а PLC — гнучке локальне керування технологічними вузлами [9].

Окрему увагу приділено ключовим компонентам ICS, серед яких — польові пристрої, контролери (PLC, RTU, IED), системи SCADA та HMI, комунікаційні протоколи, серверна інфраструктура і MES-рівень. Визначено, що ефективна взаємодія між цими елементами є основою для стабільного функціонування OT-мереж, а також безпечного обміну інформацією в межах промислової екосистеми. Разом із тим, саме ці компоненти часто виступають потенційними точками уразливості, через які можливе проникнення або порушення роботи системи.

Узагальнюючи результати дослідження першого розділу, можна зробити висновок, що індустріальні системи контролю є багаторівневими, інтегрованими та критично важливими для безперервної діяльності промислових підприємств. Вони поєднують у собі технологічні процеси, інформаційні системи та комунікаційні технології, формуючи комплексну OT-інфраструктуру. Саме тому наступні розділи дослідження будуть присвячені питанням захисту, моніторингу та виявлення загроз у таких системах, адже кіберстійкість ICS є ключовим чинником їхньої безпечної та стабільної роботи.

2 СПЕЦИФІКА ПЕРЕДАЧІ ДАНИХ У РАМКАХ СИСТЕМ ІНДУСТРІАЛЬНОГО КОНТРОЛЮ, ПРОТОКОЛИ ЇХ ВРАЗЛИВОСТІ ТА ШИФРУВАННЯ

2.1 Промислові протоколи, їх розвиток та засоби захисту

Індустріальні системи контролю (ICS, Industrial Control Systems) забезпечують безперебійну роботу виробничих процесів, а обмін даними між їхніми компонентами здійснюється за допомогою спеціалізованих промислових протоколів. Ці протоколи розроблялися переважно для забезпечення стабільності, сумісності обладнання та оперативності передачі команд у реальному часі, а не для гарантування інформаційної безпеки. Однак із поступовим поєднанням технологічних (OT) і корпоративних (IT) мереж виникла потреба у посиленні захисту таких комунікаційних механізмів.

Перші промислові протоколи з’явилися у 1970–1980-х роках у межах концепції автоматизації виробництва. Вони були тісно прив’язані до конкретних виробників обладнання і мали закриту архітектуру. Наприклад, Modbus, розроблений компанією *Modicon* (тепер Schneider Electric) у 1979 році, став одним із перших відкритих протоколів для обміну даними між ПЛК (програмованими логічними контролерами) та пристроями управління. Інші ранні приклади — Profibus (Siemens), DeviceNet (Allen-Bradley) та CAN (Controller Area Network), які забезпечували надійну роботу навіть у середовищах із високим рівнем електромагнітних завад [13].

З часом розвиток мережевих технологій і стандартизація Ethernet привели до появи Ethernet-базованих протоколів: Modbus TCP, PROFINET, EtherNet/IP, BACnet/IP, DNP3 over TCP тощо. Вони забезпечили високу швидкість передачі даних, масштабованість і можливість інтеграції OT-систем з IT-інфраструктурою підприємства. Однак саме ця інтеграція створила нові вектори кібератак, оскільки більшість протоколів не мали вбудованих механізмів аутентифікації, шифрування чи контролю цілісності даних [18,6].

В таблиці 2.1 наведено порівняння індустріальних протоколів передачі даних та їх рівні захищеності та методи захисту.

Таблиця 2.1 – Порівняльна характеристика основних промислових протоколів

Протокол	Рік створення/ розробник	Тип передачі даних	Рівень безпеки (базовий / із розширеннями)	Підтримка шифрування / аутентифікації	Типова сфера застосування
1	2	3	4	5	6
Modbus RTU / TCP	1979, Modicon (Schneider Electric)	Послідовна або Ethernet (TCP/IP)	Низький / середній (із TLS-розширеннями)	Відсутня у базовій версії / TLS у Modbus Security	Загальне виробництво, SCADA, HVAC
PROFIBUS / PROFINET	1989, Siemens / PROFIBUS International	Послідовна / Ethernet (реальний час)	Середній	Обмежена підтримка (через безпечні шлюзи або VPN)	Автоматизація виробництва, робототехніка
EtherNet/IP	2001, ODVA (Allen-Bradley)	Ethernet (TCP/IP, UDP/IP)	Середній / високий (із CIP Security)	Шифрування TLS, аутентифікація користувачів	Машинобудування, логістичні системи
DNP3 / Secure DNP3	1993, Westronic / IEEE 1815	Послідовна / Ethernet	Середній / високий (із Secure Authentication)	Аутентифікація, контроль цілісності	Енергетика, водопостачання, транспорт
OPC UA	2006, OPC Foundation	Ethernet (TCP/IP, HTTPS, MQTT)	Високий	Вбудоване шифрування (TLS, AES), цифрові сертифікати, підпис повідомлень	Інтеграція OT-IT, SCADA, IIoT
BACnet / BACnet Secure Connect (BACnet/SC)	1995 / 2020, ASHRAE	Ethernet / IP / Wi-Fi	Середній / високий	TLS 1.3, сертифікати X.509	Будівельна автоматика, HVAC-системи
IEC 60870-5-104	1995, IEC	Ethernet (TCP/IP)	Низький / середній	Обмежене шифрування, можлива інтеграція з VPN	Енергетичні системи, диспетчерські центри

Сьогодні в системах ICS використовуються десятки протоколів, з яких найпоширенішими є:

- Modbus TCP/RTU — простий протокол «запит–відповідь», що

використовується у багатьох типах контролерів. Його головна перевага — сумісність між пристроями різних виробників, а головний недолік — відсутність захисту від перехоплення або модифікації даних;

- PROFINET — орієнтований на високу продуктивність у реальному часі, підтримує кілька рівнів пріоритизації трафіку, але потребує додаткових механізмів безпеки для захисту від атак типу «man-in-the-middle»;
- EtherNet/IP — заснований на стандартному протоколі TCP/IP, підтримує моделі обміну «Producer–Consumer» і сумісний із широким спектром пристроїв, що спрощує масштабування мережі;
- DNP3 (Distributed Network Protocol) — активно використовується в енергетиці, пізніше доповнений розширенням DNP3 Secure Authentication, яке забезпечує аутентифікацію повідомлень;
- OPC UA (Open Platform Communications Unified Architecture) найсучасніший протокол, який інтегрує функції безпечного обміну, моделювання даних і міжплатформової взаємодії. OPC UA реалізує шифрування, підпис повідомлень, а також аутентифікацію користувачів за сертифікатами [16].

Більшість «класичних» протоколів OT-мереж (Modbus, Profibus, DNP3 у базовій версії) проектувалися без урахування сучасних кіберзагроз. Їхні основні вразливості полягають у:

- відсутності шифрування переданих даних, що дозволяє зловмисникам здійснювати перехоплення трафіку;
- відсутності аутентифікації джерела команд — будь-який пристрій, який під’єднується до мережі, може надсилати команди управління;
- неможливості контролю цілісності даних, що відкриває можливості для атак типу spoofing або replay;
- недостатній сегментації мережі, через що компрометація одного вузла може призвести до зупинки всього виробничого процесу.

Для підвищення рівня захищеності промислових протоколів нині застосовуються такі підходи:

- Розширення протоколів безпечними версіями.

Наприклад, Secure DNP3, Modbus Security (TLS) або OPC UA Secure Channel. Вони реалізують криптографічний захист каналів (TLS/SSL), аутентифікацію учасників обміну та перевірку цілісності даних;

- Використання сегментації мережі та зонування (ISA/IEC 62443).

Поділ OT-інфраструктури на функціональні зони та рівні (рівень контролю, моніторингу, підприємства) з мінімальними точками перетину з IT-середовищем суттєво знижує ризики;

- Імплементація систем виявлення вторгнень (IDS/IPS) для OT-мереж.

Такі системи, як Nozomi Networks, Claroty, Dragos, або Security Onion ICS, дозволяють відстежувати аномальні дії в трафіку промислових протоколів;

- Застосування криптографічних методів шифрування та цифрового підпису.

Особливо актуально для протоколів на основі Ethernet або TCP/IP, де можливе впровадження TLS або IPSec без порушення сумісності з обладнанням;

- Сучасні підходи до оновлення та аутентифікації пристроїв.

Використання цифрових сертифікатів, керування ключами (PKI), безпечних оновлень прошивок і журналювання дій операторів [14].

Еволюція промислових протоколів від закритих та ізольованих систем до відкритих Ethernet-базованих стандартів значно розширила функціональність OT-мереж, але водночас зробила їх уразливими до кіберзагроз. Сучасна тенденція розвитку полягає у впровадженні механізмів безпеки на рівні протоколів — шифрування, аутентифікації та контролю цілісності. Проте навіть найновіші стандарти потребують комплексного підходу до захисту, який поєднує технологічні, організаційні та процедурні заходи, узгоджені з вимогами стандартів ISA/IEC 62443 та NIST SP 800-82 [15].

2.2 Вразливості протоколів систем індустріального контролю

Промислові протоколи, що використовуються в системах індустріального контролю (ICS/OT), історично розроблялися в умовах повної ізоляції технологічних мереж від зовнішніх IT-середовищ. Така модель «air-gap» передбачала, що загрози, притаманні корпоративним або публічним мережам, не становлять реальної небезпеки для виробничих процесів. У результаті більшість протоколів ICS були спроектовані з пріоритетом надійності передачі, синхронізації в реальному часі та сумісності обладнання, а не на забезпеченні конфіденційності чи аутентичності даних.

Сучасна інтеграція OT та IT, впровадження хмарних сервісів, віддаленого доступу та IIoT-рішень призвели до того, що вразливості промислових протоколів стали ключовим фактором ризику безпеки. Нижче розглядаються типові вразливості, характерні для найпоширеніших протоколів ICS [17].

В таблиці 2.2 наведено основні атаки та вразливості промислових протоколів.

Таблиця 2.2 – Основні типи атак на промислові протоколи та пов’язані вразливості

Тип атаки	Уразливі протоколи	Опис механізму атаки	Наслідки для ICS/OT
1	2	3	4
Перехоплення трафіку (Sniffing)	Modbus TCP, DNP3, IEC 60870-5-104, PROFIBUS	Відсутність шифрування дозволяє зчитування команд і параметрів процесу у відкритому вигляді.	Розкриття конфіденційних даних, підготовка складніших атак (MITM, spoofing).
Man-in-the-Middle (MITM)	Modbus, PROFINET, EtherNet/IP (без CIP Security), OPC Classic	Зловмисник підміняє або змінює трафік між контролером та пристроями.	Потайне втручання у роботу ПЛК, спотворення показників сенсорів, саботаж обладнання.
Replay Attack (повторна передача пакетів)	DNP3, Modbus, IEC 60870-5-104	Передача раніше записаних валідних команд або даних.	Хибні стани HMI/SCADA, повторне ввімкнення/вимкнення обладнання, аварійні ситуації.

Кінець таблиці 2.2

1	2	3	4
Command Injection (підміна або вставка команд)	Modbus, EtherNet/IP, PROFIBUS	Надсилання спеціально сформованих команд через відсутність аутентифікації джерела.	Зміна параметрів контролера, зупинка технологічної лінії, виведення обладнання з ладу.
Spoofing (підробка адреси або вузла)	Modbus TCP, PROFINET, EtherNet/IP	Імітація існуючого пристрою для надсилання команд або отримання даних.	Повне перехоплення ролі контролера чи сенсора, дезінформація оператора.
Denial of Service (DoS / DDoS)	Усі TCP/UDP протоколи ICS, особливо Modbus TCP, PROFINET	Перевантаження мережі або ресурсів ПЛК великою кількістю запитів чи неправильними пакетами.	Зупинка роботи контролерів, затримки у передачі даних, відмова SCADA.
Використання вендорних вразливостей	OPC Classic, DNP3 реалізації, Modbus шлюзи	Експлуатація помилок у драйверах, бібліотеках, прошивках або веб-інтерфейсі контролера.	Повний контроль над пристроєм, виконання коду, зміна логіки PLC.
Scanning & Enumeration (розвідка OT-мережі)	Більшість Ethernet-протоколів: Modbus TCP, Profinet, EtherNet/IP	Зловмисник збирає топологію мережі через прогнозовані відповіді пристроїв і широкомовні пакети.	Визначення критичних вузлів, вибір цілей для подальших атак.
Data Tampering (модифікація даних)	Modbus, DNP3, IEC 60870-5-104	Маніпулювання параметрами технологічного процесу на рівні пакетів.	Хибні команди регулювання, небезпечні зміни тиску, температури, швидкості обертів.
Саботаж через підміну конфігурацій PLC/HMI	Усі протоколи без аутентифікації	Зміна конфігурацій, таймерів, логіки, регістрів, координат керування.	Порушення технологічного процесу, аварії, тривалий простій системи.

Однією з найбільш критичних вразливостей класичних протоколів, таких як Modbus RTU/TCP, DNP3, IEC 60870-5-104, PROFIBUS, є повна відсутність шифрування даних. Інформація передається у відкритому вигляді, що дозволяє:

- перехоплювати повідомлення (sniffing);
- отримувати конфіденційні технологічні параметри;
- модифікувати або підміняти дані без виявлення системою контролю;
- здійснювати атаки на основі отриманої топології OT-мережі.

Це створює умови для атак типу man-in-the-middle, spoofing, а також дозволяє зловмиснику проводити розвідувальні дії без привернення уваги операторів [21,22].

Багато протоколів ICS не передбачають механізмів підтвердження правомірності джерела команд. У протоколах Modbus, PROFIBUS, EtherNet/IP (у базовій версії) будь-який пристрій, що отримав доступ до сегмента мережі, може надсилати команди управління обладнанням.

Наслідки:

- можливість несанкціонованої зміни параметрів ПЛК;
- запуск або зупинка технологічного процесу;
- створення аварійних ситуацій (перегрів, перенавантаження, неправильні значення у регуляторах);
- порушення логіки ПЛК без зміни його прошивки [19].

Деякі протоколи (наприклад, DNP3 Secure Authentication) отримали розширення із застосуванням цифрових підписів, але вони впровадлені далеко не в усіх промислових мережах.

Унаслідок відсутності механізмів контрольних сум, одноразових маркерів або часових міток, протоколи OT легко піддаються відтворенню старих коректних кадрів. Зловмисник може:

- повторно надіслати команду управління приводом чи клапаном;
- відтворити старі показники сенсорів, створюючи хибне уявлення про стан об’єкта;
- маніпулювати роботою SCADA, викликаючи помилкові дії оператора.

Replay-атаки особливо небезпечні в енергетичних системах та водопостачанні, де часова точність і актуальність даних є критично важливою.

Деякі протоколи ICS, зокрема EtherNet/IP у режимі UDP або PROFINET, передбачають широкомовну або мультикастну передачу даних. Це призводить до:

- зростання поверхні атаки;
- можливості перехоплення даних усіма пристроями в сегменті;

- легшого сканування мережі й визначення ролей пристроїв;
- ризику перевантаження мережі (Denial of Service).

Для зловмисника це спрощує процес навігації OT-інфраструктурою, оскільки топологія стає «прозорою».

Пакети більшості промислових протоколів мають:

- фіксовану структуру;
- мінімальну варіативність полів;
- відомі опкоди та функціональні коди.

Це дозволяє легко сформувати шкідливі пакети, що імітують легітимні запити. Наприклад, у Modbus достатньо знати адресу пристрою та функціональний код, щоб:

- змінити значення регістрів;
- ініціювати аварійну зупинку;
- чи змінити конфігурацію ПЛК.

Промислові контролери часто не ведуть детальний аудит дій, а протоколи не забезпечують механізмів логування. Це унеможливлює ефективне:

- відстеження підозрілих команд;
- аномалій у трафіку;
- розслідування інцидентів.

Навіть сучасні розширення безпеки часто покладаються на зовнішні засоби — IDS/IPS для OT, SIEM або системи поведінкового аналізу.

Поширені реальні вразливості у стеку промислових протоколів часто виникають не на рівні самого стандарту, а на рівні реалізації: драйверів, прошивок або стеків комунікацій. Типові приклади:

- неправильна обробка винятків і переповнення буфера;
- некоректна робота з TCP-сесіями;
- вразливі веб-інтерфейси керування ПЛК;
- небезпечні за замовчуванням налаштування (default credentials);
- неправильно реалізована аутентифікація у Modbus/TCP gateway.

Такі помилки роблять навіть сучасні протоколи наділені шифруванням уразливими.

Багато ПЛК, RTU, HMI та мережевих шлюзів мають обмежені ресурси. Зловмисник може спричинити відмову або нестабільність системи, надсилаючи:

- велику кількість TCP-запитів;
- часті широкомовні пакети;
- некоректні або спеціально сформовані кадри;
- фрейми з довгим часом обробки.

В наслідок цього критична інфраструктура може тимчасово втратити працездатність [26].

2.3 Шифрування та механізми захисту даних в OT-мережах

З розвитком промислових систем управління та інтеграцією OT-інфраструктури з корпоративними мережами зросла потреба у впровадженні надійних механізмів захисту переданих даних. Традиційні протоколи ICS, розроблені за часів ізольованості технологічних мереж, не мають вбудованих засобів шифрування, аутентифікації чи контролю цілісності. Це робить їх особливо вразливими до сучасних кіберзагроз, зокрема перехоплення трафіку, підміни команд, атак повтору та саботажу обладнання. У зв’язку з цим шифрування, захищена передача даних і контроль доступу стають ключовими компонентами комплексної безпеки OT-середовищ.

Рисунок 2.1 демонструє використання TLS у промислових системах (ICS) для захисту даних на різних рівнях.

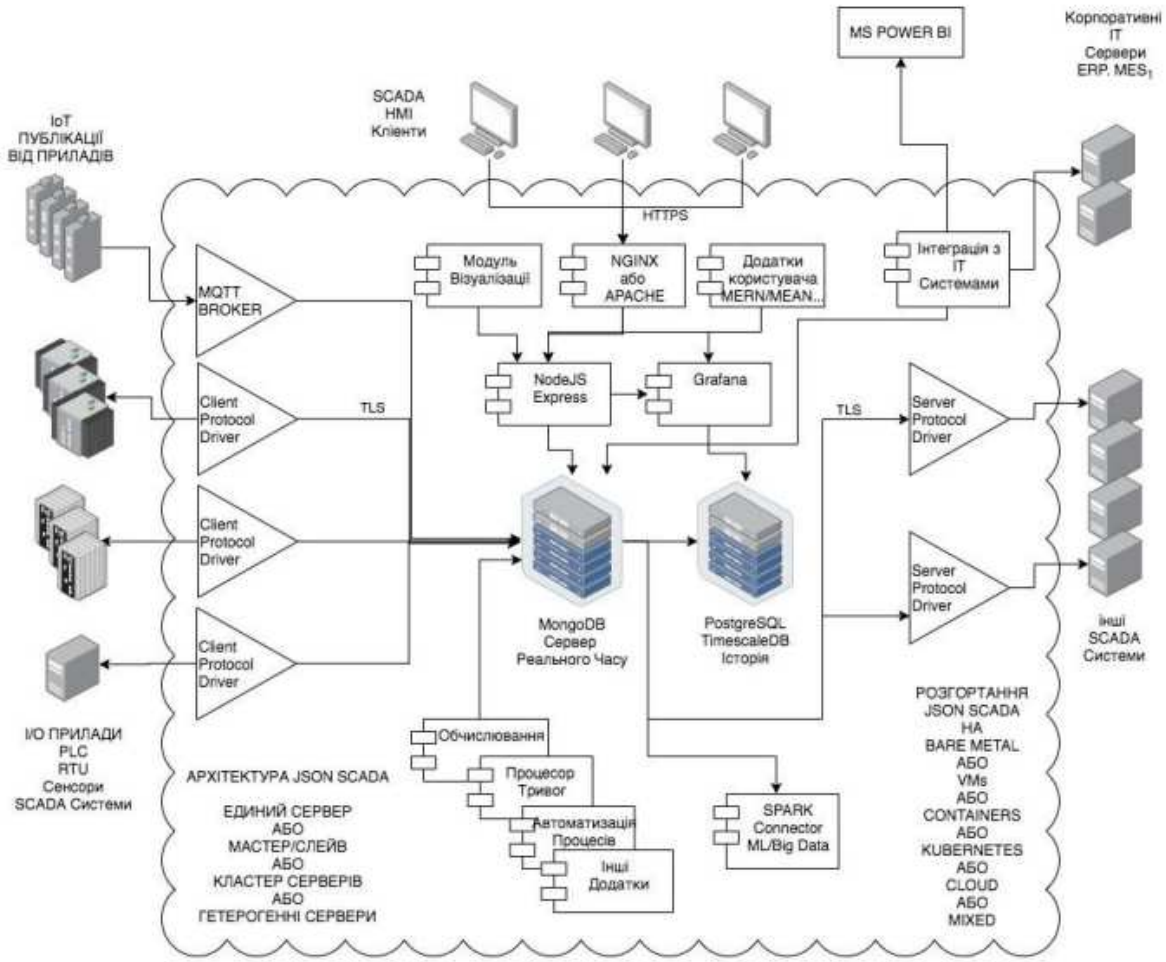

Рисунок 2.1 – Приклад реалізації TLS в ICS

TLS забезпечує шифрування з'єднань між MQTT Broker і сенсорами/пристроями, а також між клієнтами SCADA-систем через веб - інтерфейси (Node.js, NGINX). Система підтримує захищений обмін даними з базами даних (MongoDB, PostgreSQL) та інтеграцію з корпоративними IT - системами. Це гарантує конфіденційність і цілісність даних, критично важливих для обчислювальних процесів, моніторингу в реальному часі та автоматизації виробничих процесів [22].

Шифрування у промислових мережах виконує низку критично важливих функцій:

- забезпечення конфіденційності переданих даних, включно з технологічними параметрами та командами управління;
- гарантування цілісності пакетів, що виключає можливість непомітної модифікації;

- автентифікація джерела пакета або команди;
- захист від атак типу MITM та Spoofing під час передачі через TCP/IP;
- підвищення довіри між вузлами OT-мережі, особливо у гібридних архітектурах OT–IT.

Однак впровадження криптографічних технологій в OT-середовищі має свої виклики, пов’язані з обмеженістю ресурсів ПЛК, вимогами до роботи в реальному часі та високою вартістю модернізації старого обладнання [23].

На тлі зростання кіберзагроз виробничі стандарти почали впроваджувати криптографічні розширення. Найпоширеніші з них:

Modbus Security (TLS)

- Використовує TLS 1.2/1.3 для захисту трафіку Modbus TCP;
- Додає аутентифікацію пристроїв через сертифікати X.509;
- Захищає дані від MITM та знімає ризик підміни команд.

DNP3 Secure Authentication (SA)

- Реалізує криптографічні підписи, контроль цілісності та верифікацію команд;
- Використовується в енергетичних системах, де точність даних критично важлива.

OPC UA Secure Channel

- Один із найзахищеніших промислових протоколів;
- AES-256 для симетричного шифрування;
- RSA-2048/4096 для обміну ключами;
- SHA-256 для контролю цілісності;
- Сертифікати клієнта та сервера;
- Забезпечує захищене середовище «end-to-end».

CIP Security (EtherNet/IP)

- TLS;
- DTLS (для UDP);
- Цифрові сертифікати;
- Реалізує аутентифікацію пристроїв та контроль доступу.

BACnet Secure Connect (BACnet/SC)

- Використовує TLS 1.3;
- Автоматизує керування сертифікатами;
- Забезпечує захищені тунелі між вузлами будівельної автоматики.

Окрім вбудованих протоколів, застосовуються загальні криптографічні архітектури для підвищення безпеки ОТ:

VPN-тунелювання (IPSec, OpenVPN, WireGuard)

- шифрування між сегментами ОТ та зовнішніми мережами;
- приховування топології;
- захищений віддалений доступ до SCADA/PLC.

Переваги: можливість захистити протоколи, які не мають власного шифрування. Недоліки: затримки та потреба в додаткових обчислювальних ресурсах.

TLS/DTLS для ОТ-пристроїв

Дедалі більше сучасних контролерів підтримують TLS або DTLS на апаратному рівні. Це дозволяє:

- зменшити затримки завдяки блочним прискорювачам;
- забезпечити захист реального часу для критичних процесів.

IPSec на рівні шлюзів та межових пристроїв

Застосовується для захисту:

- міжсегментної передачі даних;
- зв’язку між виробничими майданчиками;
- взаємодії з хмарними платформами IIoT.

Окрім шифрування, захист ОТ-протоколів передбачає застосування низки немережевих і мережевих механізмів.

Аутентифікація та авторизація

- Сертифікати X.509;
- Контроль доступу за ролями (RBAC);
- Одноразові токени та маркери команд.

У промислових середовищах це забезпечує гарантію, що тільки довірені пристрої можуть надсилати команди керування.

Сегментація та зонування OT-мереж (ISA/IEC 62443)

Поділ мережі на:

- рівні (Levels 0–5);
- зони (Zones);
- кондуїти (Conduits).

Використання міжмережевих екранів для ICS

Спеціалізовані OT-firewall підтримують аналіз промислових протоколів (Modbus DPI, DNP3 DPI).

Вони здатні блокувати:

- небезпечні функціональні коди;
- маніпуляції регістрами;
- несанкціоновані широкомовні запити.

Системи виявлення аномалій та IDS/IPS для OT

Приклади: Nozomi Networks, Claroty, Dragos, Security Onion ICS.

Вони:

- відстежують шаблони поведінки протоколів;
- виявляють аномальні команди;
- фіксують підозрілі відхилення у роботі ПЛК.

Контроль цілісності (Integrity Monitoring)

Може включати:

- хеш-контроль конфігурацій ПЛК;
- моніторинг змін прошивок;
- перевірку валідності команд.

Попри зростаючу потребу, впровадження шифрування у промислових системах супроводжується низкою складностей:

- обмеженість ресурсів ПЛК та RTU — не всі контролери можуть обробляти AES/TLS у реальному часі;
- важливість мінімальної затримки — надмірне шифрування може

порушувати роботу систем управління;

- наявність великої кількості застарілого обладнання, що не підлягає модернізації;
- складність управління ключами в масштабних розподілених ОТ середовищах;
- ризики при оновленні прошивок, що може призвести до зупинки технологічних процесів.

Ці обмеження визначають необхідність грамотної адаптації криптографії та збалансованого підходу між безпекою та технологічною безперервністю [27].

Висновок: Застосування шифрування та сучасних механізмів захисту є критично важливим для безпеки ОТ-мереж, особливо у світлі інтеграції з корпоративними та хмарними системами. Хоча багато класичних протоколів ICS не мають вбудованого криптографічного захисту, сучасні розширення — Modbus Security, DNP3 SA, OPC UA, CIP Security, BACnet/SC — забезпечують високий рівень захищеності. Однак ефективний захист ОТ-інфраструктури не обмежується шифруванням: він вимагає комплексного впровадження сегментації, контролю доступу, моніторингу аномалій, захищених каналів зв’язку та відповідності стандартам ISA/IEC 62443.

3 ВИКОРИСТАННЯ БРАНДМАУЕРІВ І VPN ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОЇ ПЕРЕДАЧІ ДАНИХ, ПОРІВНЯННЯ ТИПІВ БРАНДМАУЕРІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ

Брандмауери є одним із ключових засобів захисту мережевих комунікацій, забезпечуючи контроль трафіку між сегментами мережі та запобігаючи несанкціонованому доступу. У контексті ОТ-мереж та систем індустріального контролю роль брандмауерів є особливо важливою, адже саме вони формують перший рубіж оборони між критичною інфраструктурою, корпоративною мережею та зовнішніми джерелами загроз. Еволюція цих засобів безпеки зумовлена зростанням складності атак, необхідністю глибшого

аналізу трафіку та потребою забезпечувати сегментацію технологічного та інформаційного середовищ [24].

На рисунку 3.1 зображені основні функції брандмауера, що може допомогти з вибором метода реалізації, функціоналу чи конкретного вендора.

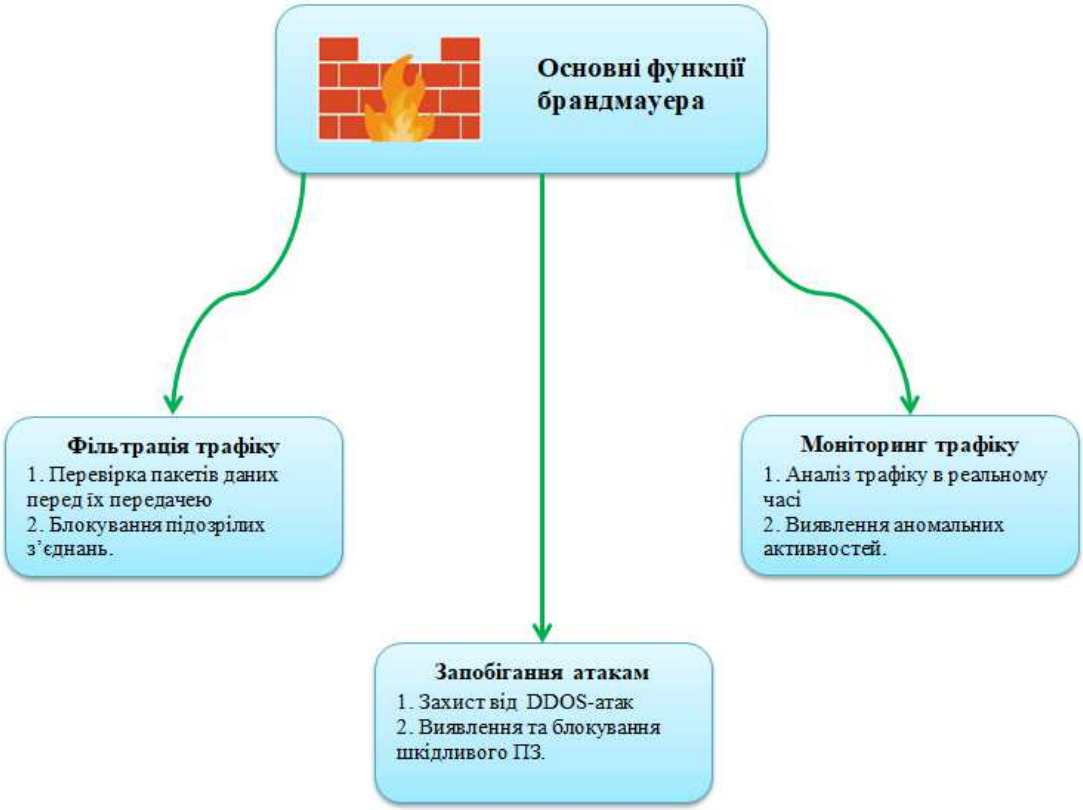

Рисунок 3.1 – Основні функції брандмауера

3.1 Опис технологій брандмауерів та їх типів

Перші брандмауери базувалися на принципах фільтрації пакетів і мали мінімальний функціонал, обмежений перевіркою полів заголовків. Це дозволяло створити базові політики доступу, однак не забезпечувало можливості аналізувати поведінкові особливості трафіку або виявляти приховані загрози.

Брандмауери першого покоління (packet-filtering firewalls) працювали на мережевому рівні моделі OSI та дозволяли/забороняли пакети на підставі IP-адрес, портів і протоколів. Їхні основні переваги — висока швидкодія та

простота, проте недостатня контекстність робила їх вразливими до сучасних атак.

На рисунку 3.2 зображено типи брандмауерів за методом реалізації

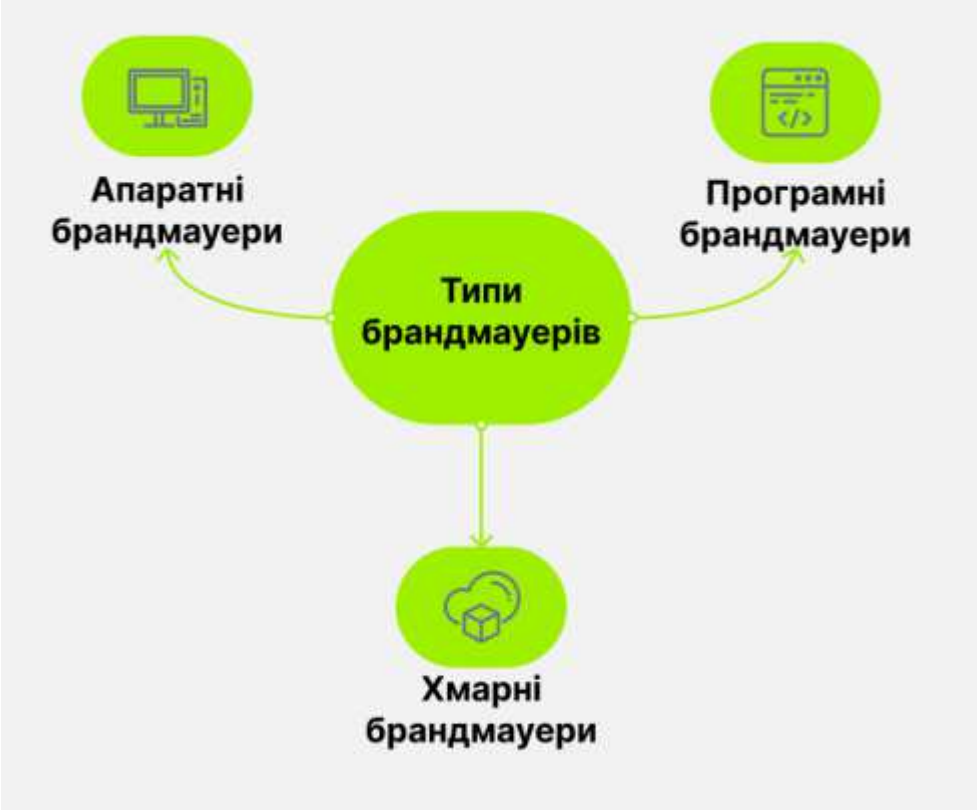

Рисунок 3.2 – Типи брандмауерів за методом реалізації

В таблиці 3.1 наведено порівняльні характеристики брандмауерів котрі відрізняються методами своєї реалізації, з цього можна зробити висновок що кожен із цих методів реалізаціє має своє місце у комплексній системі захисту інформації, а зачасту і інтеграцію комплексу декілької типів.

Таблиця 3.1 – Ключові характеристики брандмауерів за методом реалізації

Тип брандмауера	Ключові характеристики
1	2
Апаратні брандмауери	Використовуються для захисту цілих мереж. Встановлюються як окремі пристрої на межі мережі.
Програмні брандмауери	Працюють на рівні окремих пристроїв. Забезпечують захист конкретного комп’ютера або сервера.

Кінець таблиці 3.1

1	2
Хмарні брандмауери	Захищають дані в хмарних середовищах. Використовуються для безпеки SaaS-додатків.

Брандмауери другого покоління (stateful inspection firewalls) вже аналізували стан з’єднань, що значно підвищило рівень контролю. Вони підтримували таблиці активних сесій і відстежували коректність послідовності пакетів. Незважаючи на це, вони все ще не могли інспектувати вміст на прикладному рівні або працювати з зашифрованим трафіком [28,4].

Основним обмеженням класичних рішень є те, що вони не мають змоги розпізнавати складні загрози, що приховані в легітимному трафіку, а також не здатні забезпечувати детальний контроль OT-протоколів, таких як Modbus, DNP3 чи IEC 60870-5-104.

Зі зростанням кількості кібератак та їхньою складністю з’явилися брандмауери нового покоління (Next-Generation Firewalls, NGFW), які поєднують функції традиційних рішень із механізмами глибокої інспекції та інтелектуального аналізу [25].

3.2 Порівняльний аналіз різних типів брандмауерів і рекомендації щодо їх застосування

У сучасних корпоративних і промислових мережах брандмауери залишаються одним із ключових елементів побудови багаторівневої системи кіберзахисту. Зростання складності мережевих архітектур, поява хмарних сервісів, віддалених сегментів, OT-інфраструктур та гібридних середовищ вимагає від систем контролю трафіку значно ширших можливостей, ніж просте фільтрування пакетів. Сучасні брандмауери вже не обмежуються функціями класичних фільтрів; вони включають глибоку інспекцію пакетів, аналіз додатків, контроль ідентичностей, виявлення аномалій та інтеграцію з іншими системами безпеки.

В таблиці 3.2 наведено порівняння типів брандмауерів за їх функціональністю.

Таблиця 3.2 - Порівняння типів брандмауерів за їх функціональністю

Тип брандмауера	Опис
1	2
Традиційні брандмауери (FW)	Виконують базову фільтрацію трафіку на основі IP-адрес, портів і мережевих протоколів. Підходять для класичних IT-сегментів, але мають обмежені можливості для специфічних потреб OT-інфраструктури.
Брандмауери нового покоління (NGFW)	Підтримують поглиблену інспекцію трафіку (DPI), виявлення відхилень у поведінці та можуть працювати разом із антивірусними рішеннями. Забезпечують детальний контроль і аналіз промислових протоколів, таких як Modbus чи DNP3.
Універсальні захисні шлюзи (UTM)	Поєднують у собі функції брандмауера, VPN, систем виявлення та запобігання вторгненням (IDS/IPS), а також проксі-механізмів у єдиному рішенні. Спрямовані на комплексний мережевий захист.
Спеціалізовані OT-брандмауери (OTFW)	Створені для потреб промислових мереж та технологічних процесів. Забезпечують повне розуміння структури й команд OT-протоколів, що дозволяє виявляти і блокувати небезпечні операції.

До ключових характеристик NGFW належать:

- глибока інспекція пакетів (DPI) — здатність аналізувати вміст трафіку на рівні застосунків;
- ідентифікація та контроль застосунків (App-ID);
- вбудована система запобігання вторгненням (IPS);
- аналіз зашифрованого трафіку;
- кореляція подій та поведінковий аналіз;
- підтримка механізмів ZTNA та мікросегментації.

У контексті OT-мереж особливого значення набули спеціалізовані OT-брандмауери або розширення NGFW з підтримкою промислових протоколів.

Вони здатні:

- розпізнавати команди Modbus, DNP3, PROFINET, EtherNet/IP і блокувати

небезпечні операції;

- контролювати логіку взаємодії PLC та HMI;
- створювати політики, орієнтовані на технологічний процес, а не лише на мережеві параметри;
- виявляти аномалії у поведінці пристроїв.

Сучасні брандмауери також інтегруються з SIEM/SOAR-системами, що дозволяє автоматизувати реагування на загрози та корелювати події між OT і IT-середовищами.

Додатково брандмауери поділяються на периферійні та брандмауери внутрішньої сегментації.

Периферійні брандмауери:

- Забезпечують першу лінію оборони між ICS і зовнішніми мережами (корпоративною мережею чи Інтернетом);
- Захищають від зовнішніх атак та нелегітимного доступу.

Брандмауери внутрішньої сегментації:

- Розділяють мережу ICS на безпечні сегменти для обмеження ризиків;
- Запобігають поширенню атак всередині мережі у разі компрометації.

В таблиці 3.3 можна побачити порівняння традиційних брандмауерів та брандмауерів нового покоління.

Таблиця 3.3 – Порівняння традиційних фаєрволів та фаєрволів нового покоління (NGFW)

Характеристика	Традиційний фаєрвол	Фаєрвол нового покоління (NGFW)
1	2	3
Функціональність	Базова фільтрація пакетів, stateful inspection	Розширена безпека з глибоким аналізом пакетів (DPI)
Обізнаність	Працює з IP-адресами, портами й протоколами	Розуміння додатків, користувачів та вмісту трафіку
Інтеграція з IDS/IPS	Відсутня або реалізована окремо	Вбудовані механізми виявлення та запобігання вторгненням
Декодування SSL/TLS	Не підтримується	Повна підтримка аналізу зашифрованого трафіку

Кінець таблиці 3.3

1	2	3
Гранулярний контроль	Обмеження на рівні портів і протоколів	Деталізований контроль на рівні додатків та користувачів
Інтеграція з розвідкою загроз	Мінімальна або потребує ручного налаштування	Автоматичне підключення до зовнішніх джерел (threat intelligence feeds)
Антивірус / аналіз шкідливого ПЗ	Окремий модуль або стороннє рішення	Часто інтегрований у склад NGFW
Сценарії використання	Периметровий захист, базова фільтрація	Захист від складних загроз, сегментація, контроль доступу, видимість трафіку

За цією таблицею можна зробити висновок, що NGFW забезпечує глибший рівень контролю та захисту, підходить для сучасних IT-мереж та гібридних IT/OT середовищ [29,3].

UTM/NGFW — підходить для офісних чи змішаних середовищ, але не завжди розуміє OT-протоколи.

OT-фаєрволи — стійкі, безпечні, підтримують специфічні OT-протоколи, оптимальні для критичних систем з низькою толерантністю до збоїв.

В таблиці 3.4 наведено порівння UTM та спеціалізованих брандмауерів котрі працюють виключно у OT мережі.

Таблиця 3.4 - Порівняння UTM та Спеціалізованих OT-фаєрволів

Характеристика	Багатофункціональний пристрій (UTM)	Спеціалізований OT-фаєрвол
1	2	3
Цільове призначення	Загальний захист IT-мереж	Розроблений спеціально для АСУТП
Підтримка протоколів	IT-протоколи (TCP/IP, HTTP тощо)	Глибока підтримка OT-протоколів (Modbus, DNP3, OPC)
Складність	Вища, широкий функціонал	Простий, оптимізований під OT-потреби
Політики безпеки	Базовані на додатках і користувачах	Правила на рівні протоколу, вайтлистинг

Кінець таблиці 3.4

1	2	3
Оновлення / патчі	Часті	Рідші (для збереження стабільності OT-систем)
Інтеграція з IT-засобами	Повна інтеграція	Потребує адаптації для з’єднання з IT
Призначене середовище	Дата-центри, офісні мережі	Промислові об’єкти, підстанції, віддалені майданчики
Толерантність до затримок	Вища	Мінімальні затримки, детермінована передача даних

В таблиці 3.5 наведено рекомендації щодо імплементації різних типів фаерволів.

Таблиця 3.5 – Рекомендація застосування різних типів фаерволів

Сценарій використання	Рекомендоване рішення
1	2
Загальна корпоративна мережа	NGFW (наприклад, Palo Alto, Fortinet, Cisco FTD)
Зона конвергенції IT/OT з високими ризиками	NGFW з підтримкою OT-протоколів або гібридне рішення
Чутлива до збоїв мережа АСУТП із застарілими PLC	Спеціалізований OT-фаєрвол (Tofino, FortiGate Rugged, Hirschmann)
Віддалені виробничі або енергетичні об’єкти	Комбінація NGFW + OT-фаєрвол з пріоритетом стабільності

3.3 Порівняльний аналіз та пропозиція рекомендацій брандмауерів котрі спеціалізуються на захисті цифрового периметру та брандмауерах для фільтрації трафіку

Забезпечення безпеки цифрового периметру є одним із ключових елементів побудови комплексної системи захисту OT-мереж. Оскільки промислові системи працюють із критично важливими технологічними процесами, будь-яке порушення їхньої роботи може призвести до масштабних інцидентів, включаючи зупинку виробництва, втрату даних або фізичні пошкодження обладнання. Саме тому важливим завданням є формування чітко окресленого та контрольованого периметру доступу.

Цифровий периметр — це сукупність технічних засобів, політик і механізмів, які обмежують та контролюють взаємодію зовнішніх та внутрішніх сегментів мережі. На відміну від традиційних IT-мереж, у промислових системах периметр вимагає жорсткішого сегментування та мінімальної кількості точок доступу.

Основні компоненти цифрового периметру:

- Мережеве сегментування — розмежування IT, DMZ та OT-зони з чіткими правилами взаємодії між ними;
- Контроль доступу — використання принципів мінімального привілею (PoLP) та багаторівневої аутентифікації;
- Моніторинг периметра — застосування IDS/IPS-систем, контроль вхідних та вихідних потоків трафіку, аналіз аномалій;
- Використання брандмауерів різних типів — NGFW, OT-фаєрволів, UTM рішень.

Завдяки такій архітектурі значно зменшується ймовірність несанкціонованих підключень, зловмисних дій або неочікуваної взаємодії між компонентами мережі [16].

В таблиці 3.6 наведено порівняння брандмауерів за критерієм призначення.

Таблиця 3.6 – Порівняльна таблиця брандмауерів за критерієм призначення

Критерій	Захист цифрового периметру	Фільтрація трафіку
1	2	3
Призначення	Контроль доступу до OT-мережі ззовні	Аналіз і контроль внутрішнього трафіку OT
Тип захисту	Превентивний (запобігання доступу)	Детекційний/превентивний (виявлення та блокування загроз)
Контроль над протоколами OT	Обмежений	Глибокий (з DPI та підтримкою OT-протоколів: Modbus, DNP3 тощо)
Виявлення внутрішніх атак	Ні	Так

Кінець таблиці 3.6

1	2	3
Впровадження	Простіше: брандмауери, DMZ, VPN	Складніше: IDS/IPS, DPI, аналіз аномалій
Необхідність знань OT-протоколів	Низька	Висока
Вартість	Зазвичай нижча	Зазвичай вища
Першочерговість у впровадженні	Початковий крок	Наступний рівень захисту
Вимоги IEC 62443	Необхідний (Network Segmentation, Secure Remote Access)	Рекомендовано (Anomaly Detection, System Integrity Monitoring)

Фільтрація трафіку займає центральне місце у системі захисту промислових мереж. Вона передбачає контроль, перевірку та класифікацію мережевих пакетів з метою недопущення небажаної або шкідливої активності.

Ключові рівні фільтрації трафіку:

- Фільтрація на рівні мережевих адрес та портів (L3–L4)

Включає перевірку IP-адрес, портів, типів протоколів. Це традиційний рівень фільтрації, який дозволяє забезпечити базовий контроль мережі;

- Глибока інспекція пакетів (DPI)

NGFW аналізує структуру пакетів на рівні їхнього вмісту, що дає можливість визначати специфічні команди OT-протоколів, блокувати аномальні або небезпечні запити (наприклад, Modbus Write Multiple Registers);

- Контроль додатків та користувачів (L7)

Забезпечує гранулярний доступ не лише на основі IP-адрес, а й з урахуванням конкретних сервісів, додатків та поведінки користувачів;

- Фільтрація OT-протоколів.

Додатково фільтрація може включати SSL/TLS-декрипцію, виявлення аномалій та інтеграцію з системами аналізу шкідливого ПЗ.

В таблиці 3.7 наведено рекомендації застосовні з метою захисту цифрового периметру.

Таблиця 3.7 – Рекомендація сучасних рішень для захисту цифрового периметру (Network Segmentation, Access Control)

Виробник / Продукт	Опис
Fortinet (FortiGate + FortiSwitch)	Брандмауери з підтримкою сегментації, VPN, DMZ, інтеграції з NAC
Cisco (Secure Firewall, ISE)	Контроль доступу, сегментація за допомогою ISE (Identity Services Engine)
Palo Alto Networks (NGFW)	Контроль доступу до OT-зон, підтримка App-ID та Protocol-ID
Rhebo (OT Monitoring + FW)	Комбіноване рішення з базовим контролем периметру та аналізом трафіку
Juniper Networks (SRX)	VPN, NAT, класичний фаєрвол, логічна сегментація для OT-підмереж

Роль фільтрації у забезпеченні стійкості OT-середовищ

Фільтрація трафіку для OT-систем є не лише засобом кіберзахисту, але й важливим інструментом забезпечення стабільності та передбачуваності виробничих процесів [23].

Вона мінімізує:

- ризик несанкціонованих змін конфігурації контролерів;
- можливість запуску небезпечних команд у PLC;
- негативний вплив IT-трафіку на промислову мережу;
- поширення шкідливого ПЗ через неконтрольовані канали.

Особливо критичною є фільтрація у випадках використання застарілих або неоновлюваних PLC, які можуть не мати вбудованих механізмів захисту.

В таблиці 3.8 наведено рекомендації застосовні з метою фільтрації трафіку.

Таблиця 3.8 – Рекомендація сучасних рішень для фільтрації трафіку (DPI, Anomaly Detection, IDS/IPS)

Виробник / Продукт	Опис
1	2
Nozomi Networks (Guardian)	Глибока інспекція OT-протоколів, виявлення аномалій, побудова мережевих карт

Кінець таблиці 3.8

1	2
Claroty (xDome, Medigate)	DPI, моніторинг активів, захист медичних та OT-мереж
Dragos Platform	Повноцінна OT SOC-платформа з аналітикою та контекстною детекцією загроз
Cisco Cyber Vision	Моніторинг OT-трафіку, інтеграція з Cisco-брандмауерами
Radiflow (iSID, iSAP)	DPI, аналіз потоків, активний/пасивний моніторинг OT
FortiGate + FortiAnalyzer	DPI у поєднанні з SIEM-аналітикою (менш глибокий аналіз порівняно з Claroty/Dragos)

Nozomi Networks Guardian забезпечує глибоку інспекцію OT-протоколів, автоматично будує карту мережі та виявляє аномалії у технологічному трафіку.

Claroty, зі своїми платформами xDome та Medigate, орієнтований на детальний моніторинг активів і DPI, включно з медичними та промисловими системами.

Dragos Platform — це фактично повноцінна SOC-платформа для OT, яка поєднує аналітику, контекстну обробку подій і розширені модулі детекції загроз.

Cisco Cyber Vision інтегрується з екосистемою Cisco і дозволяє відстежувати OT-трафік безпосередньо у мережевій інфраструктурі підприємства.

Radiflow з продуктами iSID та iSAP пропонує DPI, аналіз потоків та гнучкий активний або пасивний моніторинг діяльності в OT-мережах.

І нарешті, FortiGate разом із FortiAnalyzer надають DPI у поєднанні з SIEM-аналітикою, хоча глибина аналізу зазвичай нижча, ніж у спеціалізованих рішень, таких як Dragos чи Claroty.

Рекомендація комбінованих рішень (периметр та трафік):

- Palo Alto + Nozomi;
- Fortinet OT Security Bundle;
- Cisco ISE + Cyber Vision + SecureX;
- Claroty + Microsoft Defender for IoT.

Представлені у таблицях дані дозволяють класифікувати брандмауери за способом їх реалізації (апаратні, програмні, хмарні), а також за функціональними можливостями (традиційні FW, NGFW, UTM та спеціалізовані OT-брандмауери). Такий поділ є фундаментальним для формування стратегії сегментації мережі та визначення точок контролю, оскільки кожен тип брандмауера виконує власну роль у загальній архітектурі захисту [22,1].

Порівняльний аналіз показує, що традиційні фаєрволи забезпечують лише базову фільтрацію трафіку та контроль портів і протоколів. Це робить їх ефективними у простих периметрових сценаріях, але недостатніми для сучасних багаторівневих середовищ, де застосунки, користувачі та протоколи взаємодіють значно складніше. У свою чергу, NGFW інтегрують DPI, поведінковий аналіз, роботу з шифрованим трафіком, механізми IDS/IPS та підтримку промислових протоколів, що розширює їх застосування в ICS-середовищі.

UTM-рішення, хоч і поєднують у собі широкий набір функцій (від антивіруса до VPN), найкраще підходять для малих та середніх підприємств. Вони створюють єдину точку управління, але через універсальний підхід не завжди забезпечують необхідну продуктивність та гнучкість у складних промислових мережах [27].

Особливе місце займають OT-брандмауери, спрямовані на глибокий аналіз специфічних протоколів (Modbus, DNP3, IEC 104 та ін.). Саме вони дозволяють контролювати й блокувати потенційно небезпечні команди, що можуть безпосередньо вплинути на роботу PLC, приводів, сенсорів або SCADA-систем. У контексті промислової безпеки це робить їх незамінними засобами, які доповнюють, а іноді й повністю перекривають можливості традиційних або NGFW у сегменті OT.

Використання графічної схеми та наведених таблиць дозволяє сформувати цілісний погляд на еволюцію брандмауерів та їхню роль у системах ICS. Кожна таблиця в даному підрозділі не лише демонструє функціональні

відмінності, але й підкреслює логіку розподілу засобів захисту за рівнями моделі Purdue, вказуючи на необхідність поєднання кількох типів брандмауерів для створення ефективної багаторівневої стратегії кіберзахисту.

Таким чином, аналіз підтверджує, що сучасні промислові мережі потребують не одного універсального рішення, а ретельно підібраного комплексу засобів контролю трафіку, де кожен тип брандмауера відіграє конкретну роль. Це дозволяє забезпечити не лише периметрову безпеку, а й захист критичних технологічних процесів, мінімізувати ризики інцидентів та підтримувати безперервність виробничих операцій [16].

3.4 Захист промислового трафіку з використанням VPN

Забезпечення конфіденційності та цілісності даних є критично важливим аспектом безпеки промислових систем, особливо у випадках, коли інформація передається між віддаленими сегментами мережі або виходить за межі локального технологічного контуру. У такому контексті технології VPN (Virtual Private Network) стають одним із ключових інструментів захисту промислового трафіку, забезпечуючи криптографічний захист даних, аутентифікацію учасників зв’язку та ізоляцію логічних каналів зв’язку.

Використання VPN у промислових мережах має свою специфіку, оскільки трафік ICS відрізняється низькою толерантністю до затримок, чутливістю до втрати пакетів та необхідністю підтримки безперервної роботи технологічного обладнання. Тому застосування VPN у таких середовищах вимагає детального аналізу його впливу на продуктивність каналів зв’язку та особливостей взаємодії із контролерами (PLC), шлюзами, SCADA-системами та іншими компонентами OT-інфраструктури [12].

У промислових мережах застосовуються три основні типи VPN, кожен з яких виконує окремі завдання:

- Site-to-site VPN — забезпечує захищений зв’язок між двома або більше промисловими майданчиками, часто використовується для об’єднання

виробничих ліній, підстанцій або диспетчерських центрів. Переваги: стабільність, централізоване управління, низький ризик несанкціонованого доступу. Недоліки: складність масштабування та залежність від продуктивності каналів зв’язку;

- Remote-access VPN — застосовується для безпечного доступу технічного персоналу або підрядників до систем контролю, коли фізична присутність на об’єкті неможлива. Переваги: гнучкість, можливість швидкого розгортання. Недоліки: підвищені вимоги до аутентифікації та контролю дій користувача;
- Industrial VPN — спеціалізовані рішення, розроблені для роботи з OT протоколами та обладнанням (наприклад, Moxa, HMS, Siemens SINEMA RC). Переваги: оптимізація під низькі затримки, підтримка специфічних промислових протоколів, централізований контроль доступу до PLC. Недоліки: вища вартість та обмежена інтеграція зі звичайними IT-системами.

У промислових мережах застосування VPN повинно забезпечувати такі механізми:

- Шифрування трафіку — забезпечує захист переданих даних від перехоплення та несанкціонованого аналізу;
- Аутентифікація користувачів та пристроїв — унеможливлює підключення сторонніх пристроїв до технологічної мережі;
- Цілісність переданих даних — захист від модифікації команд, що передаються до контролерів;
- Сегментація доступу — обмежує доступ до окремих PLC, HMI або сегментів SCADA-системи;
- Журналювання й моніторинг — дозволяє відстежувати активність користувачів і вчасно виявляти аномалії.

Забезпечення цих функцій є необхідною умовою для побудови безпечного каналу зв’язку між компонентами системи, особливо у випадку управління критично важливими технологічними процесами.

Використання VPN у системах OT має певні обмеження, які необхідно враховувати:

- Затримки, спричинені шифруванням, можуть негативно впливати на протоколи реального часу (наприклад, PROFINET або EtherCAT);
- Проблеми сумісності з промисловими протоколами, які зазвичай не були спроєктовані з урахуванням тунелювання;
- Необхідність відмовостійкості, оскільки обрив VPN-каналу може призвести до втрати керування обладнанням;
- Ризики компрометації через неправильну конфігурацію, як-от слабкі ключі або відсутність багатофакторної аутентифікації.

У зв’язку з цим промислові VPN часто впроваджуються у поєднанні з сегментацією за моделлю Purdue, брандмауерами NGFW та спеціалізованими OT-брандмауерами.

Застосування VPN у промислових мережах надає низку ключових переваг:

- захист конфіденційності технологічних даних (телеметрія, команди управління);
- можливість безпечного віддаленого доступу до обладнання;
- ізоляція від загроз, що надходять з зовнішніх мереж;
- мінімізація ризику MITM-атак та перехоплення промислового трафіку;
- створення контролюваних каналів зв’язку між підприємствами, підрядниками та сервісними центрами виробників обладнання.

Ці властивості роблять VPN одним із ключових інструментів захисту промислових мереж у сучасних умовах [9].

3.5 Порівняльний аналіз VPN та SD-WAN у промислових мережах

У промислових мережах забезпечення захищеної та стабільної передачі даних є критично важливою умовою безпеки та безперервності технологічних процесів. Традиційно для створення захищених каналів зв’язку

використовувалися VPN, які забезпечували шифрування, аутентифікацію та логічну ізоляцію трафіку. Однак із розвитком промислової автоматизації, зростанням кількості розподілених об’єктів, використанням хмарних сервісів та появою потреби у централізованому управлінні мережею, все більше підприємств переходять до застосування SD-WAN (Software-Defined Wide Area Network).

SD-WAN, на відміну від класичних VPN, не лише створює захищені канали, а й дозволяє динамічно маршрутизувати трафік, оптимізувати пропускну здатність, підтримувати відмовостійкість та інтегруватися з хмарними сервісами. Це робить технологію перспективною для складних промислових інфраструктур, де традиційні VPN інколи виявляються недостатньо гнучкими.

Традиційні VPN працюють за принципом створення зашифрованого тунелю між двома точками (site-to-site або remote-access). У цьому випадку весь трафік проходить через заздалегідь визначений маршрут, що ускладнює масштабування та може призводити до збільшення затримок. У свою чергу, SD-WAN забезпечує інтелектуальне управління мережею, дозволяючи автоматично вибирати найкращий маршрут залежно від навантаження, стану ліній зв’язку та критичності трафіку.

На відміну від VPN, SD-WAN здатна:

- здійснювати пріоритизацію OT-трафіку (наприклад, Modbus, DNP3, IEC 104);
- розподіляти навантаження між кількома каналами (MPLS, LTE, 5G, інтернет);
- автоматично перемикатися при відмові каналу без втрати зв’язку з PLC або SCADA;
- забезпечувати централізовану політику безпеки і управління для десятків або сотень майданчиків.

Тому SD-WAN вважається більш адаптивним підходом для промислових підприємств, які мають велику кількість віддалених об’єктів (підстанції, свердловини, насосні станції, виробничі майданчики) [13,2].

В таблиці 3.9 наведено порівняння технологій VPN та SD-WAN, котра може допомогти визначитися з технологічною потребою впровадження рішень для покращення рівня інформаційної безпеки.

Таблиця 3.9 – Порівняння VPN та SD-WAN у промислових мережах

Критерій	VPN	SD-WAN
1	2	3
Принцип роботи	Створення зашифрованих тунелів між вузлами	Динамічне маршрутизування і віртуалізація WAN
Гнучкість маршрутизації	Фіксована, маршрути задаються вручну	Автоматична оптимізація маршруту
Управління трафіком	Обмежені можливості	Пріоритизація OT-трафіку, QoS, балансування
Відмовостійкість	Залежить від одного каналу або тунелю	Автоматичне перемикання між каналами (LTE/5G/MPLS/Інтернет)
Масштабованість	Складна конфігурація при збільшенні кількості вузлів	Централізоване керування для великої кількості об’єктів
Інтеграція з хмарою	Обмежена	Повна інтеграція з SaaS/Cloud сервісами
Безпека	Шифрування, аутентифікація, базові політики	Вбудовані NGFW-функції, IDS/IPS, сегментація
Продуктивність у промислових мережах	Може створювати затримки	Оптимізація каналів для критичного OT-трафіку
Вартість впровадження	Низька або середня	Зазвичай вища, але ефективніша при великій кількості вузлів
Найкраще застосування	Безпечний доступ або з’єднання між двома майданчиками	Складні розподілені промислові системи з високими вимогами до доступності

SD-WAN надає додаткові можливості, які особливо важливі в OT-середовищах:

- розмежування IT та OT трафіку в одному каналі;
- підтримка ізоляції критичного трафіку відповідно до Purdue-моделі;
- можливість інтеграції з промисловими брандмауерами та SIEM системами;
- мінімізація часу простою за рахунок самовідновлення каналів;
- можливість створення політик доступу для підрядників та сервісних

організацій.

Ці функції дозволяють забезпечити стабільний зв’язок з віддаленими PLC, RTU, HMI або об’єктами телеметрії навіть за умов низької якості зв’язку або використання змішаних каналів.

Переваги SD-WAN над традиційним VPN у контексті OT:

- Підтримка *real-time* протоколів за рахунок мінімізації джитерів і втрат пакетів;
- Можливість створення політик маршрутизації з урахуванням критичності технологічних процесів;
- Швидке масштабування у системах з десятками або сотнями промислових вузлів;
- Централізоване (cloud-based) управління всією інфраструктурою WAN;
- Вбудовані засоби аналізу трафіку та безпеки, що дозволяє мінімізувати використання додаткових пристроїв.

3.6 SASE-архітектура у контексті захисту промислових мереж

Сучасні промислові підприємства все частіше застосовують хмарні рішення, віддалений доступ, мобільні робочі станції та розподілені виробничі майданчики. У результаті традиційні периметрові моделі безпеки, засновані на статичних брандмауерах і VPN, стають недостатніми для забезпечення комплексного захисту OT-інфраструктури. Це стимулювало появу нової концепції — SASE (Secure Access Service Edge), яка поєднує функції мережевої інфраструктури та безпеки в єдину хмарно орієнтовану архітектуру [21].

В таблиці 3.10 проілюстровано основні компоненти SASE-архітектури та призначення цих компонентів.

Таблиця 3.10 – Основні компоненти SASE та їх призначення

Компонент	Призначення
1	2
SD-WAN	Оптимізація маршрутизації трафіку між філіями, хмарними сервісами та дата-центрами

Кінець таблиці 3.10

1	2
CASB (Cloud Access Security Broker)	Контроль доступу до хмарних застосунків та моніторинг їх використання
SWG (Secure Web Gateway)	Фільтрація веб-трафіку, блокування шкідливих ресурсів і запобігання веб-атакам
ZTNA (Zero Trust Network Access)	Забезпечення доступу до застосунків на основі ідентичності користувача та політик Zero Trust
FWaaS (Firewall as a Service)	Хмарний фаєрвол з централізованим керуванням і єдиною політикою безпеки
DLP (Data Loss Prevention)	Захист від витоку конфіденційної інформації та контроль переміщення даних

SASE об’єднує механізми SD-WAN та засоби кібербезпеки у межах хмарної платформи, забезпечуючи контроль доступу, маршрутизацію, інспекцію трафіку й захист у рамках однієї консолі. Такий підхід є особливо актуальним для сучасних ICS/OT-мереж, де важливим є не лише шифрування даних, а й постійний моніторинг, адаптивне застосування політик безпеки та мінімізація ризиків проникнення у технологічні сегменти.

Архітектура SASE складається з декількох взаємопов’язаних технологічних блоків, кожен з яких виконує окрему функцію у захисті трафіку та контролі доступу:

- SD-WAN: забезпечує інтелектуальне керування трафіком та оптимізацію WAN-каналів. У контексті OT дозволяє підтримувати стабільний зв’язок з розподіленими промисловими об’єктами, такими як підстанції, сенсорні вузли або SCADA-центри.
- Secure Web Gateway (SWG): фільтрує вихідний та вхідний веб-трафік, забезпечує контроль доступу до веб-ресурсів і захист від шкідливого контенту. У промислових мережах SWG допомагає мінімізувати ризики зараження інженерних робочих станцій.
- Cloud Access Security Broker (CASB): контролює доступ до хмарних сервісів, моніторить ризикову активність та забезпечує відповідність політикам безпеки. Для ICS/OT цей компонент важливий у випадках використання хмарних платформ для обміну телеметрією чи керування обладнанням.

- Zero Trust Network Access (ZTNA): реалізує принцип нульової довіри, де кожне підключення до системи перевіряється та авторизується. У технологічних мережах це дозволяє уникнути неконтрольованого доступу до PLC, HMI або серверів управління.

- Firewall-as-a-Service (FWaaS): хмарний аналог традиційних брандмауерів, який дозволяє централізовано застосовувати політики безпеки. Забезпечує інспекцію трафіку незалежно від географічного розташування обладнання або користувача [25].

У промислових системах SASE забезпечує низку критично важливих можливостей:

- Уніфіковане управління безпекою — одна платформа керує доступом, політиками та моніторингом у масштабах усієї OT-мережі;
- Гнучкість і масштабованість — легко інтегрується з розподіленими об’єктами (енергетичні станції, нафтогазові платформи, заводські цехи);
- Підтримка Zero Trust — мінімізація ризику lateral movement у разі компрометації вузла;
- Оптимізація доступу до хмарних сервісів — особливо важливо для підприємств, що використовують хмарні SCADA, аналітичні платформи або віддалене технічне обслуговування;
- Зниження витрат на локальне обладнання — оскільки основні функції переносяться у хмару;
- Безперервний моніторинг загроз — завдяки інтеграції з Threat Intelligence платформами та системами поведінкового аналізу.

Попри значні переваги, інтеграція SASE у середовище OT може мати певні обмеження:

- Необхідність високої якості зв’язку — хмарна модель вимагає стабільних каналів із низькими затримками;
- Ризики залежності від провайдера — критично важливі процеси не можуть повністю покладатися на зовнішній сервіс без резервних механізмів;
- Потенційні конфлікти з реальногочасовими протоколами — деякі ICS

протоколи можуть бути чутливими до маршрутизаційних затримок;

- Необхідність ретельної сегментації мережі — SASE не замінює Purdue модель, а працює у поєднанні з нею;
- Підготовка персоналу — перехід до хмарних моделей потребує нових навичок керування та моніторингу.

Це особливо актуально для організацій із розподіленими офісами, віддаленими працівниками або перехідною до хмари інфраструктурою [14,5].

На таблиці 3.11 зображено власні рекомендації програмних рішень виробників технологій захисту інформації, щодо впровадження SASE – хмарного рішення, котрий поєднує глобальні мережі (WAN) та служби мережевої безпеки в єдину уніфіковану платформу.

Таблиця 3.11 – Рекомендації рішень SASE - архітектури

Виробник	Продукт (SASE-рішення)
1	2
Cisco	Cisco+ Secure Connect
Zscaler	Zscaler Internet Access / Zscaler Private Access
Palo Alto Networks	Prisma Access
Fortinet	FortiSASE
Cloudflare	Cloudflare One
Netskope	Netskope SASE

SASE = Мережа + Безпека + Хмара + Zero Trust в одному.

Cisco пропонує рішення Cisco+ Secure Connect, яке інтегрує мережеві та безпекові функції для масштабної корпоративної інфраструктури.

Zscaler представлений продуктами Zscaler Internet Access та Zscaler Private Access — це одні з найпоширеніших у світі SASE-платформ, орієнтованих на веб-захист і безпечний доступ до внутрішніх сервісів.

Palo Alto Networks забезпечує SASE через Prisma Access, яке включає NGFW-функції, ZTNA, URL-фільтрацію та захист застосунків у хмарі.

Fortinet пропонує FortiSASE, що поєднує SD-WAN, хмарний фаєрвол і механізми Zero Trust у спільному середовищі.

Cloudflare надає Cloudflare One, яке фокусується на швидкому доступі, DDoS-захисті та Zero Trust-підході до керування доступами.

І нарешті, Netskope із платформою Netskope SASE робить акцент на захисті даних, CASB-функціях і хмарному аналізі загроз.

На таблиці 3.12 пропонуються рекомендації використання SD-WAN, SASE та засобів захисту ОТ

Таблиця 3.12 – Рекомендації щодо використання SD-WAN, SASE та засобів захисту ОТ

Питання	Відповідь
1	2
Чи використовувати SD-WAN?	Тільки у випадках, коли це не створює ризиків для критичних ОТ-додатків та враховує специфіку промислових протоколів.
Чи використовувати SASE?	Доцільно у гібридних середовищах ОТ/ІТ, де є потреба в доступі до хмари, централізованому контролі та інтеграції з ІТ-системами.
Що краще для чистого ОТ?	Сегментовані мережі, промислові фаєрволи, DPI, системи виявлення аномалій — інструменти, що працюють на рівні ICS/SCADA.

У розділі проведено оцінку сучасних засобів мережевої безпеки, що застосовуються для захисту передавання даних у промислових ОТ-мережах. Порівняння класичних та новітніх брандмауерів показало, що NGFW, UTM та спеціалізовані ОТ-фаєрволи значно перевершують традиційні рішення завдяки DPI, інтеграції з IDS/IPS та підтримці промислових протоколів. Дослідження використання VPN засвідчило їхню ефективність для захисту каналів зв’язку, однак у промислових системах їх слід застосовувати обережно через ризик приховування аномалій. Аналіз VPN і SD-WAN продемонстрував, що SD-WAN доцільний у гібридних середовищах, тоді як для критичних ICS оптимальними залишаються сегментація й детерміновані канали. Розгляд архітектури SASE підтвердив її перспективність для масштабних підприємств, але впровадження у чистому ОТ вимагає адаптації та поетапного переходу.

Загалом комплексний підхід, що поєднує сегментацію, спеціалізовані фаєрволи, DPI, VPN та елементи SASE/SD-WAN у некритичних зонах, забезпечує найвищий рівень безпеки передачі даних у промислових мережах [23].

ВИСНОВКИ

В ході проведення дослідження, результати аналітичних робіт показують, що вибір брандмауера для забезпечення безпеки OT-мереж залежить від конкретних умов експлуатації, вимог до стабільності та типу трафіку, який необхідно контролювати. Традиційні рішення, такі як UTM чи класичні IT-фаєрволи, широко застосовуються у корпоративних мережах, проте вони не завжди враховують специфіку промислових протоколів та обмеження реального часу, характерні для АСУТП.

Брандмауери нового покоління (NGFW) значно розширюють можливості контролю, забезпечуючи глибоку інспекцію трафіку, інтеграцію з системами запобігання вторгненням та підтримку сучасних механізмів розвідки загроз. Це робить їх оптимальним вибором для зон конвергенції IT/OT, де необхідно поєднати високу безпеку з гнучкістю управління доступом.

У середовищах, де пріоритетом є надійність, детермінованість та підтримка специфічних OT-протоколів, ключову роль відіграють спеціалізовані OT-брандмауери. Вони дозволяють мінімізувати затримки, забезпечити сумісність із застарілими PLC та впроваджувати політики безпеки на рівні промислових протоколів, що особливо важливо для критичної інфраструктури.

Оптимальною стратегією стає комбіноване використання NGFW та OT-фаєрволів, що дозволяє поєднати широкий спектр захисних можливостей NGFW із стабільністю та точністю контролю, характерною для OT-рішень. Такий підхід забезпечує багаторівневий захист, враховує особливості різних сегментів мережі та формує стійку архітектуру безпеки для сучасних промислових систем.

У межах роботи було комплексно розглянуто сучасні технології мережевої безпеки, що застосовуються для захисту як традиційних IT-середовищ, так і промислових мереж ICS/SCADA. Проведений аналіз дозволяє сформувати цілісне уявлення про те, які інструменти є найбільш ефективними в

різних сценаріях, як вони доповнюють один одного та які обмеження варто враховувати при їх впровадженні.

Порівняння класичних брандмауерів із їх сучасними поколіннями показало, що традиційні FW залишаються актуальними для базового периметрового захисту, проте значною мірою поступаються можливостями NGFW. Нова генерація фаєрволів включає глибокий аналіз пакетів, інтеграцію з IDS/IPS, підтримку SSL/TLS-інспекції, механізми аналізу вмісту та загроз, що є критичними у сучасних умовах. Ще потужнішими є UTM-системи й спеціалізовані OT-брандмауери, які враховують специфіку промислових протоколів, особливості технологічних процесів та суворі вимоги до безперебійності виробництва.

Особливу увагу приділено захисту промислового трафіку за допомогою VPN. Було встановлено, що класичні механізми створення тунелів (IPsec, SSL-VPN) надають достатній рівень захищеності під час передавання даних між сегментами мережі, віддаленими майданчиками або сервісними підрозділами. Водночас VPN у чистому вигляді не розв’язує проблему контролю доступу за контекстом, а у промислових мережах може створювати додаткові ризики через прихованість трафіку та потенційне маскування аномалій. Ці обставини вимагають строгого застосування принципів сегментації та моніторингу.

Порівняльний аналіз VPN та SD-WAN засвідчив, що SD-WAN доцільний для гнучкого управління маршрутизацією, покращення доступу до хмари та оптимізації зв’язності між майданчиками. Однак у промислових середовищах його застосування має бути обмеженим і ретельно адаптованим до вимог OT, оскільки агресивна оптимізація трафіку або динамічна маршрутизація можуть негативно впливати на протоколи реального часу. У свою чергу VPN залишається більш стабільним і прогнозованим рішенням для ICS, але гірше масштабується у розподілених або хмарно-орієнтованих сценаріях.

Окремим напрямом аналізу стала архітектура SASE, яка поєднує SD-WAN та хмарні безпекові сервіси (FWaaS, ZTNA, CASB, SWG, DLP). Дослідження показало, що SASE є перспективною моделлю для великих

підприємств із розгалуженою інфраструктурою, особливо у випадку гібридного OT/IT-середовища. Такі рішення надають централізований контроль, масштабованість та гнучкість, знижують залежність від локального обладнання та підвищують видимість мережевих процесів. Водночас повноцінне впровадження SASE у критичну OT-мережу потребує обережності через жорсткі вимоги до латентності, стабільності каналів та локального контролю.

Підсумовуючи викладене, можна зазначити, що:

- У промислових мережах найефективнішою залишається модель багаторівневого захисту, яка поєднує сегментацію, спеціалізовані OT-брандмауери, DPI та системи виявлення аномалій;
- VPN доцільно використовувати для захищеного доступу та міжсегментної взаємодії, проте тільки за умов забезпечення видимості трафіку та ізоляції технологічних потоків від загальних корпоративних каналів;
- SD-WAN варто застосовувати у невиробничих або мало критичних зонах, а також у ситуаціях, коли необхідно інтегрувати промислові майданчики з хмарною інфраструктурою без шкоди для детермінованості зв’язку;
- SASE є стратегічним напрямом розвитку індустріальних мереж, але для критичних систем потребує поетапного впровадження та адаптації під вимоги OT.

Таким чином, результати роботи підтверджують, що вибір інструментів кібербезпеки для ICS повинен ґрунтуватися на балансі між функціональністю, надійністю та сумісністю з технологічним процесом. Різні технології не виключають, а доповнюють одна одну, формуючи комплексну систему захисту, здатну ефективно протидіяти сучасним загрозам та забезпечувати стабільність роботи промислових об’єктів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. IEC 62443. Industrial communication networks – Network and system security. – International Electrotechnical Commission, 2018.

2. NIST SP 800-207. Zero Trust Architecture. – National Institute of Standards and Technology. Gaithersburg, 2020.

3. NIST SP 800-82. Guide to Industrial Control Systems (ICS) Security. – National Institute of Standards and Technology. Gaithersburg, 2015. – 247 p.

4. NIST SP 800-53. Security and Privacy Controls for Federal Information Systems and Organizations. – NIST, 2020.

5. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.

6. ISA/IEC standards for Automation Security. – International Society of Automation, 2019.

7. Ackerman P. Industrial Cybersecurity: Efficiently secure critical infrastructure systems. – Birmingham: Packt Publishing, 2017. – 455 p.

8. Knapp E. D., Langill J. Industrial Network Security. – 2nd ed. – Waltham: Syngress, 2014. – 460 p.

9. Byres E., Lowe J. Industrial Cybersecurity for SCADA, DCS, PLC & RTU. – New York: Momentum Press, 2020. – 315 p.

10. Ginter A. Secure Operations Technology (OT Security). – Waterfall Security Solutions, 2019.

11. Stouffer K., Falco J., Scarfone V. Guide to Industrial Control Systems Security. – NIST, 2015. – 247 p.

12. Weiss J. Protecting Industrial Control Systems from Electronic Threats. – New York: Momentum Press, 2010. – 240 p.

13. Knowles W., Prince D., Hutchison D. A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection. – 2015. – Vol. 9. – 80 P.

14. Sumit K., Harsh V. Cybersecurity of OT networks: A tutorial and overview Institute for Software Integrated Systems, Vanderbilt University. – 2025. – 25 p.

15. How to Design Security for OT Network Environments [Електронний ресурс]. - Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/ebook/eb-how-to-design-security-for-ot-network-environments.pdf (Дата звернення 25.09.2025).

16. Recommended Cybersecurity Practices for Industrial Control Systems. [Електронний ресурс]. - Режим доступу: https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf (Дата звернення 25.09.2025).

17. Humayed A., Luo F., Sitnikova E., Watters P. Cyber-physical systems security: A survey. Future Generation Computer Systems. – 2017. – Vol. 68. – P. cyber–security–ICS.

18. Cheminod M., Durante L., Valenzano A. Review of Security Issues in Industrial Networks. IEEE Transactions on Industrial Informatics. – 2013. – Vol. 9(1). – P. 277–293.

19. SANS Institute Unveils Critical Infrastructure Strategy Guide for 2024: A Call to Action for Securing ICS/OT Environments [Електронний ресурс]. - Режим доступу: https://thehackernews.com/2025/09/sans-institute-unveils-critical.html (Дата звернення 27.09.2025).

20. OT Cybersecurity Quick Start Guide for IT Professionals. [Електронний ресурс]. - Режим доступу: https://hub.dragos.com/guide/ot-cs-quick-start-guide (Дата звернення 27.09.2025).

21. Cybersecurity Best Practices for Industrial Control Systems [Електронний ресурс]. - Режим доступу: https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems_508.pdf (Дата звернення 29.09.2025).

22. A Solution Guide to Operational Technology Cybersecurity. [Електронний ресурс]. - Режим доступу:

https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-solution-guide-to-ot-cybersecurity.pdf (Дата звернення 29.09.2025).

23. Industrial Security 3.1. [Електронний ресурс]. - Режим доступу: https://www.cisco.com/c/dam/en/us/td/docs/Technology/Industrial-Security-3-1-DG.pdf (Дата звернення 01.09.2025).

24. AlienVault USM Appliance & Features. [Електронний ресурс]. - Режим доступу: https://www.esecurityplanet.com/products/alienvault-usm (Дата звернення 02.09.2024).

25. USM Appliance™ User Guide. [Електронний ресурс]. - Режим доступу: https://cybersecurity.att.com/documentation/resources/pdf/usm-appliance-user-guide.pdf (Дата звернення 02.09.2025).

26. Critical Software. Cyber Security for Industrial Control Systems – Assessing and Building Secure Systems [Електронний ресурс]. – White Paper, 2017. – Режим доступу: https://criticalsoftware.com/multimedia/critical/de/B8mmfH_jy-CSW_-_White_Paper_-_Cyber_Security_for_ICS.pdf (Дата звернення 04.09.2025).

27. Yokogawa Electric Corporation. The First Step in Securing your OT Environment [Електронний ресурс]. – White Paper WP-S-20220713-02, Jul. 2022. – Режим доступу: https://web-material3.yokogawa.com/2/29743/files/WP-S-20220713-02_Whitepaper_The-First-Step-in-Securing-your-OT-Environment_Upate072022%20_1_.pdf (Дата звернення 06.09.2025).

28. Allianz für Cyber Sicherheit / BSI. Industrial Control System Security – Top 10 Threats and Measures [Електронний ресурс]. – 2022. – Режим доступу: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.pdf?__blob=publicationFile&v=6 (Дата звернення 06.09.2024).

29. Canadian Centre for Cyber Security. Security Considerations for Industrial Control Systems [Електронний ресурс]. – ITSAP.00.050, Jul. 2021. – Режим доступу:

https://www.cyber.gc.ca/sites/default/files/cyber/2021-07/ITSAP.00.050-Security-considerations-for-industrial-control-systems_e.pdf (Дата звернення 07.09.2025).

ДОДАТОК А

ПРЕЗЕНТАЦІЯ

Рисунок А.1 – Титульний слайд

Рисунок А.2 – Слайд 1

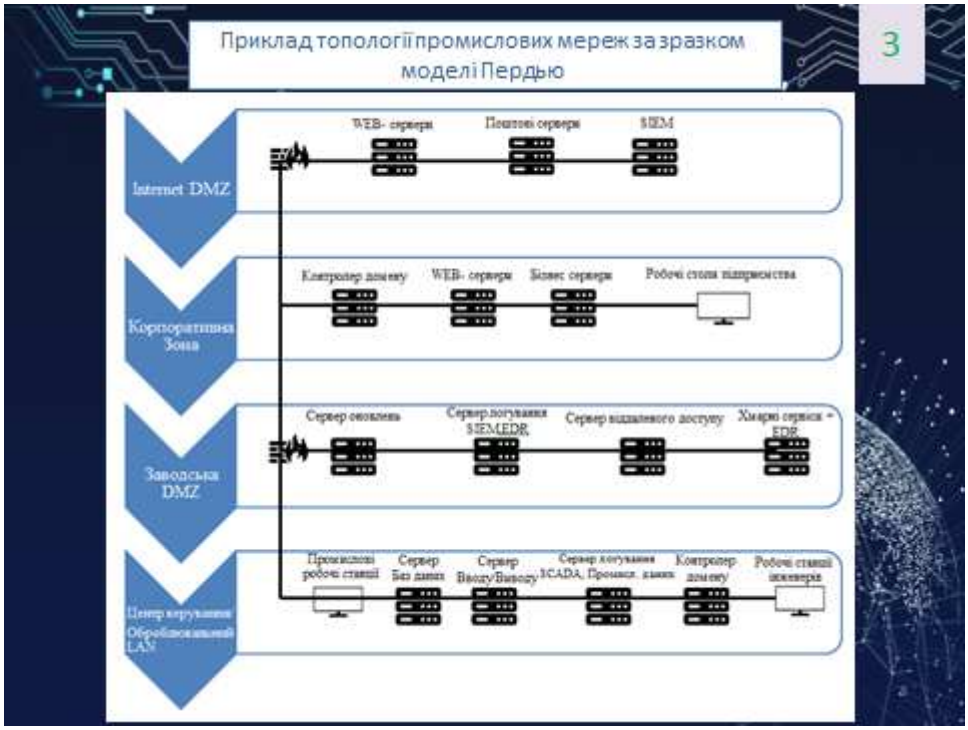

Рисунок А.3 – Слайд 2

Рисунок А.4 – Слайд 3

Рисунок А.5 – Слайд 4

Рисунок А.6 – Слайд 5

Рисунок А.7 – Слайд 6

Рисунок А.8 – Слайд 7

Рисунок А.9 – Слайд 8

Рисунок А.10 – Слайд 9

Рисунок А.11 – Слайд 10

Рисунок А.12 – Слайд 11

Рисунок А.13 – Слайд 12

Рисунок А.14 – Слайд 13

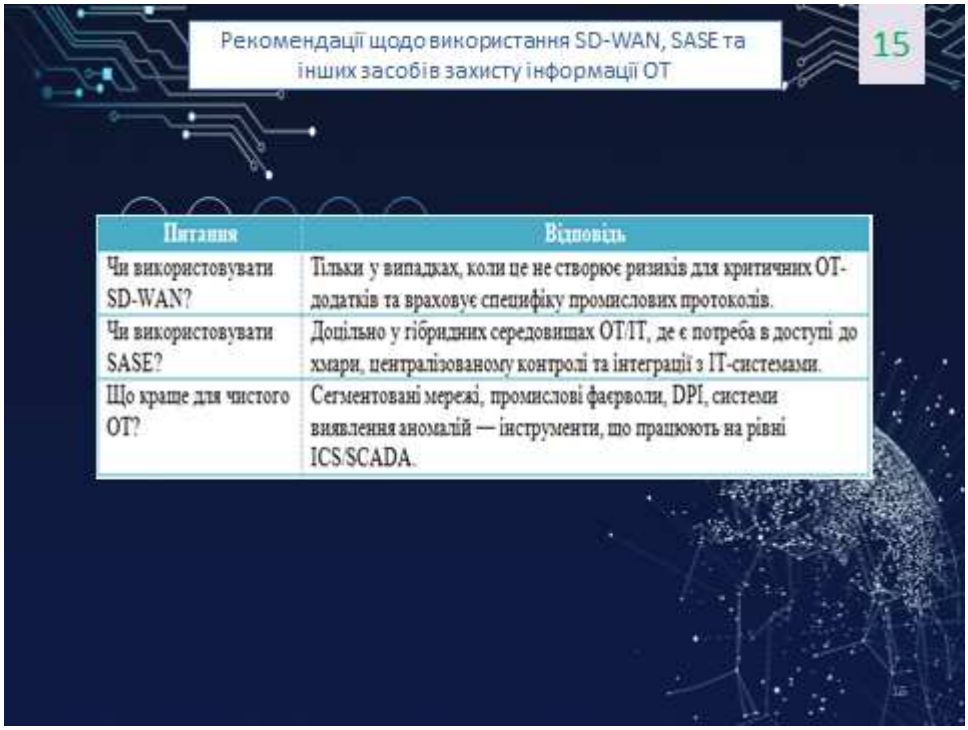

Рисунок А.15 – Слайд 14

Рисунок А.16 – Слайд 15

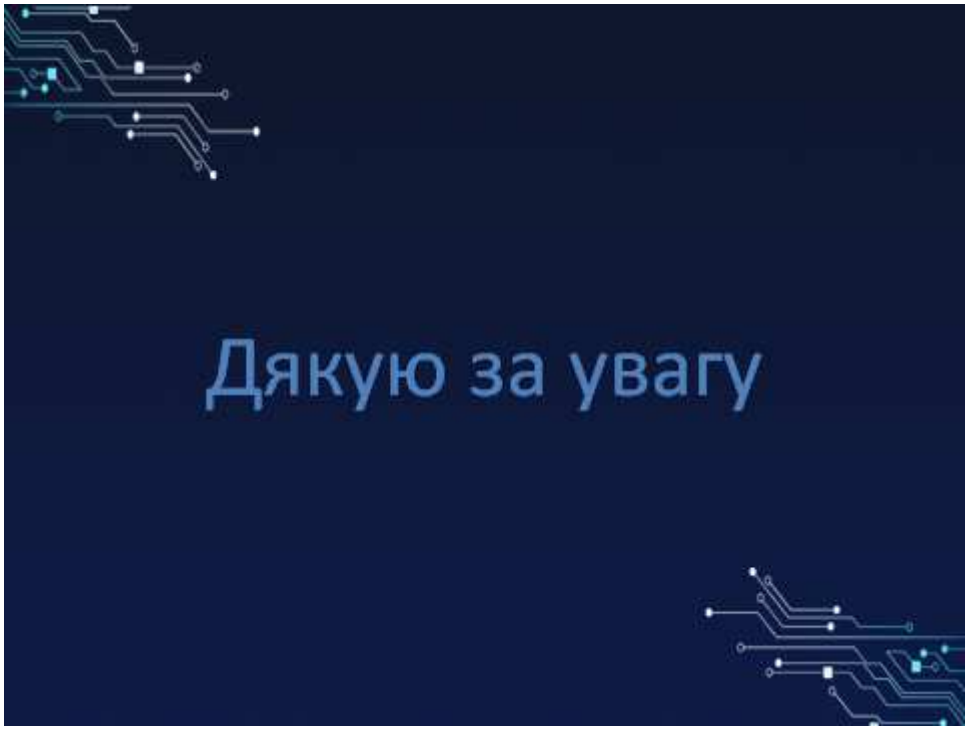

Рисунок А.17 – Слайд 16