УДК 04.056.5:004.738.5:004.451.3 DOI: 10.31673/2786-8362.2026.019357

Костюк Ю.В., PhD; **Складанний П.М.,** к.т.н.; **Соколов В.Ю.,** к.т.н.

ЗАХИЩЕНІ ІНТЕЛЕКТУАЛЬНІ МЕРЕЖЕВІ ТЕХНОЛОГІЇ ДЛЯ ПРОМИСЛОВИХ КОМПЛЕКСІВ

Kostiuk Yu.V., Skladannyi P.M., Sokolov V.Yu. Secure intelligent network technologies for industrial complexes. This paper proposes a formalized risk-adaptive authorization model for Zero Trust architectures based on dynamic trust evaluation and adaptive access token management. Unlike traditional authorization mechanisms relying on static policies and fixed token lifetimes, the proposed approach continuously updates trust and operational risk during an active session. The model integrates asset sensitivity, contextual factors, and behavioral signals into a unified decision-making loop implemented at the PDP/PEP levels. Authorization decisions (permit, step-up, deny) directly influence token lifetime, which is dynamically reduced in response to detected risk events such as anomalous behavior, context changes, or device integrity violations. A formal mechanism for adaptive token lifetime control is introduced to minimize the potential attack window in case of token compromise. Scenario-based evaluation demonstrates that the proposed method significantly reduces attack exposure while maintaining acceptable decision latency and usability. The results confirm the effectiveness of risk-driven session management for enhancing the resilience of identity-centric security systems within Zero Trust environments.

Keywords: Hybrid industrial network, Industry 4.0, Industrial Internet of Things, Time-Sensitive Networking, deterministic data transmission, network monitoring, anomaly detection, cyber resilience

Костюк Ю.В., Складанний П.М., Соколов В.Ю. Захищені інтелектуальні мережеві технології для промислових комплексів. У статті запропоновано архітектуру захищеної гібридної промислової мережі для систем Industry 4.0 та Industrial IoT. Рішення поєднує детерміновану передачу даних на основі Time-Sensitive Networking, сегментацію мережі, багаторівневий криптографічний захист і аналіз телеметрії в парадигмі Zero Trust. Моделювання підтвердило зменшення затримок критичних потоків і підвищення точності виявлення атак без погіршення продуктивності.

Ключові слова: гібридна промислова мережа, Industry 4.0, Industrial Internet of Things, Time-Sensitive Networking, детермінована передача даних, мережевий моніторинг, виявлення аномалій, кіберстійкість

Вступ

Стрімкий розвиток концепцій Industry 4.0 та Industrial Internet of Things (IIoT) зумовлює трансформацію промислових мереж у гібридні інтелектуальні системи, що інтегрують керування технологічними процесами, маршрутизацію трафіку, кіберзахист і аналіз даних у реальному часі [1-2, 7, 16]. Сучасні виробничі комплекси поєднують кіберфізичні системи (CPS), хмарні сервіси, edge-обчислення та бездротові сегменти, що забезпечує масштабованість і гнучкість, але водночас суттєво підвищує вимоги до пропускної здатності, затримок і стійкості до кіберзагроз.

Паралельно зростає масштабність атак на промислові системи керування (ICS/SCADA), включно з APT-атаками, експлуатацією вразливостей промислових протоколів (Modbus TCP, Profinet, EtherCAT), порушенням синхронізації та компрометацією мережевого обладнання [2–5, 14]. Більшість традиційних мереж були спроєктовані з урахуванням базових механізмів безпеки та не забезпечують інтегрованого багаторівневого захисту, що підвищує ризик проникнення в сегменти операційних технологій (OT) і порушення технологічних процесів.

Забезпечення гарантованої якості обслуговування для критичних потоків вимагає використання технологій Time-Sensitive Networking (TSN), які підтримують детерміновану передачу даних і синхронізацію в реальному часі [1, 6, 8–9, 20]. Водночас кіберстійкість сучасних промислових мереж передбачає впровадження принципів Zero Trust [3–5], гнучкої сегментації (VLAN, SDN), захищених каналів зв'язку на основі MACsec/IPsec та застосування алгоритмів машинного навчання для виявлення аномалій [7], відповідно до вимог стандартів IEC 62443-3-3 та NIST SP 800-82.

Проведений аналіз наукових джерел свідчить, що більшість досліджень розглядають окремі аспекти захисту промислових мереж – детерміновану передачу на основі TSN [1, 8-9], реалізацію концепції Zero Trust [3-5] або використання AI-модулів для виявлення атак [7] – без формалізованого поєднання цих компонентів у єдиній архітектурній моделі. Відсутність інтегрованого підходу до синхронізації, маршрутизації потоків різної критичності, багаторівневого криптографічного захисту та інтелектуального моніторингу обмежує можливість гарантувати одночасно детермінованість передавання й кібербезпеку гібридних (дротових і бездротових) промислових систем.

У зв'язку з цим актуальним є завдання розроблення комплексної архітектури захищеної інтелектуальної промислової мережі, здатної забезпечити безперервність виробничих процесів і стійкість до складних і цілеспрямованих загроз.

Метою роботи є створення формалізованої архітектури гібридної промислової мережі, яка поєднує механізми детермінованої маршрутизації на основі TSN, багаторівневий криптографічний захист, сегментацію мережі (VLAN/SDN), принципи Zero Trust та інтелектуальний аналіз телеметрії для адаптивного виявлення аномалій.

Наукова новизна роботи полягає у розробленні інтегрованої архітектурної моделі, що:

- забезпечує гарантовану якість обслуговування критичних потоків завдяки TSN [6, 8-9;
- реалізує багаторівневий захист відповідно до моделі OSI з використанням MACsec/IPsec та Zero Trust політик;
- інтегрує AI-модулі для адаптивного виявлення атак у гібридних середовищах;
- підтримує об'єднання дротових і бездротових сегментів у єдиному захищеному середовищі.

Теоретичне значення роботи полягає у формалізації підходу до поєднання детермінованої комунікації та багаторівневої моделі кіберзахисту в єдиній структурованій архітектурі, що розширює наукові підходи до побудови кіберстійких промислових мереж в умовах Industry 4.0.

Практичне значення полягає у можливості застосування запропонованої архітектури під час модернізації або проєктування промислових мереж із гібридною топологією, забезпечуючи зменшення затримок критичних потоків, підвищення оперативності реагування на інциденти та зниження ймовірності проникнення в сегменти ОТ за умов багаторівневого захисту [4-6, 18]. Таким чином, розроблення захищеної інтелектуальної мережевої архітектури є необхідною умовою забезпечення кіберстійкості сучасних промислових комплексів в умовах зростаючих кіберзагроз і ускладнення виробничих систем.

Аналіз останніх досліджень. Наразі зростає кількість наукових робіт, присвячених дослідженню захищених мережевих технологій для промислових комплексів, особливо в контексті концепцій Industry 4.0 та Industrial Internet of Things (IIoT – промисловий Інтернет речей). Так, Zhang et al. [1] детально оглянули стандарти Time-Sensitive Networking (TSN – мережі з часовою чутливістю) для промислової автоматизації, висвітливши стан розвитку, можливості та ключові виклики інтеграції TSN у великомасштабних системах Cyber-Physical Systems (CPS – кіберфізичні системи) та IIoT. Бернарді [2] звернув увагу на вразливості механізмів синхронізації часу в TSN і показав, як атаки, що маніпулюють повідомленнями Type-Length-Value (TLV – тип–довжина–значення) у протоколі Precision Time Protocol (PTP – протокол точного часу), можуть порушувати синхронізацію мережі та призводити до значних збоїв у критичних системах.

У сфері безпеки мережевих доступів Federici et al. [3] запропонували двошарову архітектуру Zero Trust (нульова довіра) для промислових умов, яка підтримує динамічні квитки доступу та захищає як мережеву, так і периферійну (edge) інфраструктуру, включаючи застаріле (legacy) обладнання. Liu [4] здійснив бібліометричний огляд концепції Zero Trust у контексті Internet of Things (IoT – Інтернет речей), висвітливши прикладні успіхи та виклики її впровадження у розподілених мережевих середовищах.

У галузі підходів Software-Defined Networking (SDN – програмно-визначені мережі), що поєднують гнучкість і безпеку, Katsis та Bertino [5] розробили Zero Trust Software-Defined

Networking (ZT SDN – програмно-визначену мережу з архітектурою нульової довіри) із застосуванням Machine Learning (ML – машинного навчання) для автоматичного формування політик доступу, що мінімізує людський фактор та підвищує адаптивну безпеку мережі. Крім того, Shi et al. [6] дослідили інтеграцію TSN і технології п'ятого покоління мобільного зв'язку 5G Ultra-Reliable Low-Latency Communication (5G URLLC – наднадійний низьколатентний зв'язок), показавши, як синхронізація over-the-air (безпроводова передача сигналу синхронізації) може забезпечити субмікросекундний рівень точності для гібридних промислових систем.

Проведений аналіз наукових публікацій показує, що сучасні дослідження зосереджені переважно на окремих аспектах захищених мережевих технологій для промислових комплексів – детермінованій передачі даних на основі TSN, безпеці механізмів синхронізації часу, впровадженні концепції Zero Trust у IIoT-середовищах та використанні SDN і ML для автоматизації політик доступу. Водночас більшість робіт розглядають зазначені підходи ізольовано, без формалізованого поєднання механізмів детермінованої комунікації, багаторівневого криптографічного захисту та інтелектуального аналізу телеметрії в єдиній архітектурній моделі.

Таким чином, висновок за результатами аналізу літературних джерел полягає в тому, що на сьогодні відсутня комплексна формалізована модель захищеної гібридної промислової мережі, яка одночасно забезпечує детермінованість критичних потоків, підтримує гібридні (дротові та бездротові) топології та реалізує принципи Zero Trust із використанням інтелектуальних методів виявлення аномалій. Це обумовлює актуальність розроблення інтегрованої архітектури, орієнтованої на підвищення кіберстійкості промислових систем в умовах складних і цілеспрямованих загроз.

Постановка завдання. Сучасні промислові комплекси, що функціонують у парадигмі Industry 4.0 та Industrial Internet of Things, характеризуються гібридною структурою, поєднанням дротових і бездротових сегментів, високою критичністю технологічних потоків і зростаючим рівнем кіберзагроз. Забезпечення одночасно детермінованої передачі даних, гарантованої якості обслуговування та багаторівневого кіберзахисту в таких умовах є складною науково-технічною проблемою.

Аналіз існуючих підходів показує, що технології Time-Sensitive Networking забезпечують часову детермінованість і синхронізацію трафіку, а концепція Zero Trust та механізми сегментації (VLAN, SDN) підвищують рівень контролю доступу і ізоляції сегментів. Водночас відсутня інтегрована архітектурна модель, що формалізовано поєднує детерміновану маршрутизацію, багаторівневий криптографічний захист (MACsec/IPsec), адаптивне виявлення аномалій на основі алгоритмів машинного навчання та механізми захисту синхронізації в єдиному керованому середовищі.

У зв'язку з цим у роботі поставлено такі завдання:

1. Розробити формалізовану архітектуру захищеної гібридної промислової мережі, що підтримує інтеграцію TSN, VLAN/SDN та Zero Trust політик.
2. Забезпечити гарантовані показники якості обслуговування для критичних потоків (затримка ≤ 5 мс для класу A TSN, стабільність синхронізації ± 1 мкс).
3. Реалізувати багаторівневий механізм криптографічного захисту для міжсегментних взаємодій OT/IT.
4. Інтегрувати модуль інтелектуального виявлення аномалій на основі Isolation Forest і LSTM для зменшення часу виявлення та реагування на інциденти.
5. Провести експериментальну перевірку ефективності архітектури у симуляційному середовищі з моделюванням реалістичних сценаріїв загроз.

Вирішення поставлених завдань має забезпечити підвищення кіберстійкості промислових мереж при збереженні детермінованості критичних виробничих процесів.

Метою роботи є розробка та формалізоване наукове обґрунтування архітектури захищених інтелектуальних мережевих технологій для промислових комплексів, здатної забезпечити гарантовані параметри якості обслуговування (Quality of Service, QoS),

мінімальну детерміновану затримку та високу пропускну здатність у поєднанні з багаторівневим кіберзахистом [1, 7, 9, 14]. Дослідження спрямоване на інтеграцію технологій Time-Sensitive Networking (TSN) [6-9, 20], сегментації мережевого простору (VLAN, SDN) [5, 16], протоколів захищеної передачі даних (MACsec, IPsec) [3, 18] та концепції Zero Trust Network Access (ZTNA) [3-5] у єдину гібридну архітектуру, що підтримує кабельні та бездротові сегменти промислових мереж [7, 11, 16-17, 19]. Особлива увага приділяється використанню алгоритмів машинного навчання та методів інтелектуального аналізу трафіку для виявлення та запобігання аномаліям у режимі реального часу [15], що забезпечує підвищення кіберстійкості, надійності та адаптивності інфраструктури до змінних умов функціонування та зростаючих кіберзагроз.потенційного вікна атаки W за умови збереження прийнятних експлуатаційних характеристик системи доступу

Виклад основного матеріалу дослідження

Методологія. Методологія дослідження ґрунтується на комплексному поєднанні аналітичного, формалізованого та експериментального підходів. На першому етапі виконано системний аналіз сучасних технологій захищених промислових мереж, зокрема Time-Sensitive Networking (TSN), концепції Zero Trust, механізмів VLAN/SDN-сегментації та багаторівневого криптографічного захисту відповідно до вимог IEC 62443 та NIST SP 800-82. Далі сформовано формалізовану архітектурну модель гібридної мережі з чітким розмежуванням OT/IT-сегментів, детермінованим плануванням критичних потоків і захищеною міжсегментною взаємодією на основі MACsec/IPsec.

Для оцінювання стійкості до кіберзагроз побудовано модель атак, що враховує порушення синхронізації PTP/TSN, ін’єкцію кадрів, компрометацію промислових протоколів і бездротових шлюзів. Модуль інтелектуального виявлення аномалій реалізовано із застосуванням алгоритмів Isolation Forest та LSTM з оптимізацією гіперпараметрів методом grid-search і використанням 5-fold cross-validation та часової вибірки 70/30 для уникнення перенавчання.

Експериментальну перевірку архітектури проведено у середовищах GNS3, Mininet та ns-3 з моделюванням потоків різної критичності та реалістичних сценаріїв загроз, а ефективність оцінено за показниками затримки, стабільності синхронізації, MTTD/MTTR і точності виявлення атак. Отримані на етапі методологічного аналізу вимоги до детермінованості, сегментації та криптографічного захисту були інтегровані в єдину архітектурну модель гібридної промислової мережі. Далі розглянемо її структуру та функціональні рівні, що забезпечують одночасно QoS для критичних потоків і кіберстійкість.

Однак у межах цього дослідження фокус зроблено не лише на політиках доступу, а й на забезпеченні кіберстійкості промислової мережі з детермінованими потоками та змішаними каналами зв’язку. Тому далі розглянемо архітектуру детермінованої гібридної промислової мережі як цілісну інженерну основу для реалізації запропонованих механізмів захисту та моніторингу.

Архітектура детермінованої гібридної промислової мережі. У процесі роботи розроблено інтегровану архітектуру гібридної промислової мережі з детермінованою передачею даних, багаторівневим кіберзахистом та інтелектуальним виявленням аномалій, призначену для підвищення кіберстійкості промислових комплексів в умовах змішаних (кабельних і бездротових) сегментів [1, 7, 14, 16]. Запропонована архітектура об’єднує технології Time-Sensitive Networking (TSN) для гарантування часової синхронізації та пріоритетної доставки критичних даних [6, 8-9, 20], Zero Trust Network Access (ZTNA) для забезпечення доступу за принципом мінімальної довіри [3-5], апаратне шифрування на рівнях MACsec та IPsec для захисту канального і мережевого рівнів [15, 18], а також гібридний ML-модуль IDS/IPS для виявлення та блокування атак у реальному часі.

Розроблена інтегрована архітектура гібридної промислової мережі з детермінованою передачею даних, багаторівневим кіберзахистом та інтелектуальним виявленням аномалій складається з чотирьох взаємопов’язаних рівнів, кожен з яких виконує специфічні функції:

рівень детермінованої передачі даних, що забезпечує синхронізацію часу (IEEE 802.1AS) та планування кадрів (IEEE 802.1Qbv) з пріоритетним переривання передавання кадрів (IEEE 802.1Qbu) [6, 14]; рівень сегментації та маршрутизації на основі VLAN і SDN [5, 16]; рівень захищеної комунікації, що використовує MACsec для канального рівня та IPsec для міжсегментних тунелів [3, 18]; рівень моніторингу та аналітики, який включає модуль обробки телеметрії та виявлення аномалій у реальному часі [7, 15].

Щоб забезпечити прозору інтерпретацію внеску кожного компонента в загальний результат, архітектуру подано у вигляді чотирьох взаємопов'язаних рівнів із чітко визначеними функціями та межами відповідальності. Така декомпозиція є зручною для подальшої формалізації та експериментальної верифікації.

Рис. 1 відображає інтегровану архітектуру гібридної промислової мережі, побудовану за багаторівневим принципом. Рівень TSN (IEEE 802.1AS/CB/Qbv/Qci/Qbu) забезпечує синхронізацію часу та детерміновану передачу критичних потоків. Рівень VLAN+SDN (IEEE 802.1Q, OpenFlow) реалізує сегментацію та централізоване керування трафіком. Рівень MACsec+IPsec (IEEE 802.1AE, RFC 4301) гарантує конфіденційність, цілісність та автентичність передавання даних. Рівень AI-IDS/IPS із інтеграцією SIEM/SOAR забезпечує моніторинг, виявлення та запобігання атакам у реальному часі. Кабельні та бездротові сегменти інтегровані через TSN-рівень, а взаємодія з edge-платформою та хмарою забезпечує масштабованість і розширену аналітику.

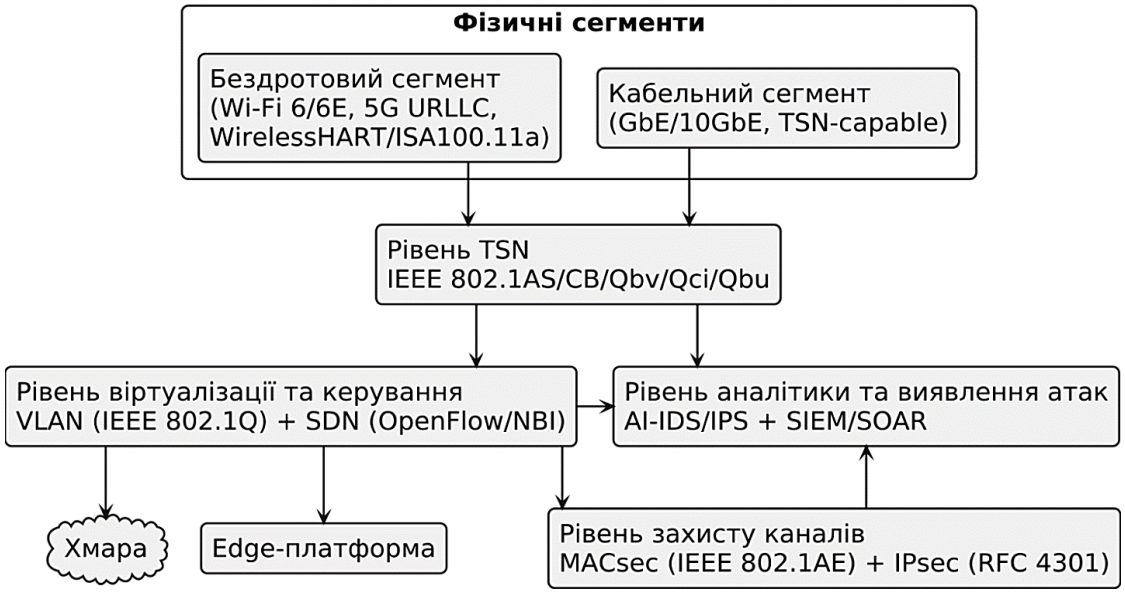


Рис. 1. Інтегрована архітектура захищеної гібридної промислової мережі

Оскільки детермінованість є базовою вимогою для OT-контурів керування, подальший виклад починається з рівня TSN як первинної основи гарантованої латентності. Спочатку формалізуємо синхронізацію часу, планування вікон та механізм пріоритетного переривання кадрів.

Рівень детермінованої передачі даних забезпечує синхронізацію часу, гарантовану доставку кадрів у межах суворо визначених затримок та оптимальне планування ресурсів для критично важливих потоків [1, 9, 14]. Він складається з трьох основних підмодулів: синхронізація часу (IEEE 802.1AS), планування кадрів (IEEE 802.1Qbv) та пріоритетне переривання передавання кадрів (IEEE 802.1Qbu) [6, 8]. Синхронізація часу реалізується відповідно до стандарту IEEE 802.1AS, що математично описується як мінімізація відхилення фазового зсуву [18]:

$$\Delta t = |t_s - t_r| \to min, \tag{1}$$

де t_s – час відправлення кадру, t_r – час приймання, Δt – похибка синхронізації. Базова мета синхронізації – мінімізувати похибку часових відміток між вузлами.

Для всієї мережі з N вузлами середня кумулятивна похибка синхронізації:

$$E_{sync} = \frac{1}{N}\sum_{k=1}^{M}|(t_s^k - t_r^k) - \delta_k|, \quad (2)$$

де δ_k – очікувана транспортна затримка у сегменті k.

Вплив дрейфу годинників моделюється як:

$$\Delta t_{drift}(t) = \Delta t_0 + \epsilon \cdot t, \quad (3)$$

де ϵ – швидкість дрейфу.

Змінні x_{ij} належать до множини $\{0,1\}$, де $x_{ij} = 1$ означає призначення кадру i часовому слоту j. Для уникнення конфліктів передачі введено обмеження $\sum_{i=1}^{N} x_{ij} \leq 1, \forall j \in \{1, \dots, M\}$, а часові вікна визначаються фіксованими або адаптивними інтервалами залежно від політики планування ресурсів. Планування кадрів (IEEE 802.1Qbv) моделюється як задача оптимізації часових слотів:

$$\min_{x_{ij}} \sum_{i=1}^{N}\sum_{j=1}^{M} C_{ij}\, x_{ij}, \quad (4)$$

за умов:

$$\sum_{j=1}^{M} x_{ij} = 1,\ g_i \geq 0,\ t_{j+1} - t_j \geq d_i + g_j,\ x_{ij} \in \{0,1\}, \quad (5)$$

де x_{ij} – призначення кадру i у слот j, C_{ij} – вартість затримки, g_i – guard-band, d_i – тривалість кадру i.

Для трафіку з різною критичністю додаємо ваговий коефіцієнт [8, 20]:

$$\min_{x_{ij}} \sum_{i=1}^{N}\sum_{j=1}^{M}\left(aC_{ij} + \beta\tilde{p}_i\right) x_{ij}, \quad (6)$$

де $\tilde{p}_i \in [0,1]$ – нормалізований пріоритет потоку.

Час повної передачі кадру без пріоритетного переривання передавання кадрів:

$$T_{full} = \frac{L_f}{R}, \quad (7)$$

де L_f – довжина кадру, R – швидкість передавання.

Механізм пріоритетного переривання передавання кадрів (IEEE 802.1Qbu) можна подати як мінімізацію втрат часу при перериванні кадру (кадри вищого пріоритету переривають менш пріоритетні):

$$T_{total} = T_{full} - \frac{L_p}{R}, \quad (8)$$

де L_p – довжина перерваної частини кадру, R – швидкість передачі.

Середній виграш у часі:

$$G_{avg} = \frac{1}{H}\sum_{h=1}^{H}\frac{L_p^h}{R}, \quad (9)$$

де H – кількість кадрів високого пріоритету.

Середній час очікування кадрів вищого пріоритету після пріоритетного переривання передавання кадрів:

$$H_{avg} = \frac{1}{H}\sum_{h=1}^{H}\left(T_{queue}^h - \frac{L_p^h}{R}\right), \quad (10)$$

Загальна детермінована затримка в мережі з кабельними та бездротовими сегментами:

$$D_{total} = \sum_{m=1}^{M_w}\left(\frac{L_m}{R_{w,m}} + \tau_{proc,w,m} + d_{proc,w,m}\right) + \sum_{n=1}^{N_c}\left(\frac{L_n}{R_{c,n}} + \tau_{proc,c,n} + d_{proc,c,n}\right) + J, \quad (11)$$

де M_w,N_c – кількість бездротових та кабельних сегментів, $R_{w,m}$, $R_{c,n}$ – ефективна швидкість лінку (бездротового/кабельного) для відповідного сегмента, в біт/с (може відрізнятися між сегментами, тому з індексами), L_m, L_n - довжина кадру, вимірюються в бітах, $\tau_{proc,w,m}$, $\tau_{proc,c,n}$ – час обробки/черги на вузлах сегмента, в секундах, $d_{proc,w,m}$, $d_{proc,c,n}$ – час поширення (propagation delay) для сегмента, в секундах, $J_k = \sum_k \sigma_{queue,k}$ – агрегований джиттер (наприклад, сума std для черг), в секундах.

Для формального аналізу гарантованої затримки у TSN використано апарат Network Calculus. Вхідний трафік описується функцією прибуття $A(t)$. Обслуговування черг Qbv задається сервісною кривою $\beta(t) = R(t-T)^+$, де R – гарантована пропускна здатність, T – латентність. Максимальна затримка для потоку визначається як $D(t) = \inf\{d \geq 0 | A(t) \leq$

$(A \otimes \beta)(t + d)\}$, що дозволяє отримати верхню межу затримки для кожного критичного потоку.

Зведена мета рівня TSN формалізується як багатокритеріальна оптимізація:

$$min\left[\lambda_1 E_{sync} + \lambda_2 D_{total} + \lambda_3 \sum_{i=1}^{N} \sum_{j=1}^{M} C_{ij}\, x_{ij}\right], \quad (12)$$

де $\lambda_1, \lambda_2, \lambda_3$ – вагові коефіцієнти важливості синхронізації, затримки та вартості розкладу [9, 14, 20]. Таким чином, формалізація роботи рівня TSN демонструє, що запропонована архітектура не обмежується лише впровадженням стандартів IEEE, а оптимізує їхню роботу з урахуванням багатосегментної структури промислових мереж, критичності потоків та динамічних змін мережевої топології.

Наведені співвідношення задають аналітичний опис детермінованості, однак для інженерної інтерпретації важливо показати і процедурну послідовність обробки кадрів. Саме тому на рис. 2 подано алгоритмічну блок-схему проходження потоку через ключові механізми IEEE 802.1AS/Qbv/Qbu.

Рис. 2. Блок-схема роботи рівня TSN у гібридній промисловій мережі

Схема на рис. 2 відображає алгоритмічну послідовність обробки трафіку в контурі детермінованої передачі даних на основі технологій Time-Sensitive Networking (TSN). Потоки ініціюються джерелами (датчики, PLC, SCADA) та проходять етап синхронізації часу відповідно до IEEE 802.1AS. Далі здійснюється формування часових вікон передавання згідно з механізмом Time-Aware Shaper (IEEE 802.1Qbv, GCL). У разі виявлення термінового або конфліктного кадру активується механізм пріоритетного переривання IEEE 802.1Qbu, після чого виконується передавання по фізичному каналу (кабельному або бездротовому сегменту) до вузла призначення. Така структуризація процесу спрямована на мінімізацію варіацій затримки (jitter), контроль латентності та підтримку детермінованості критично важливих промислових потоків.

Після гарантування детермінованих характеристик передачі необхідно забезпечити логічну ізоляцію трафіку та керованість маршрутів у змішаній OT/IT-інфраструктурі. Наступний рівень, VLAN+SDN, формалізує принципи сегментації та централізованого керування потоками з урахуванням QoS і реакції на інциденти.

Другим функціональним блоком розробленої архітектури є рівень сегментації та маршрутизації, який відповідає за логічний поділ мережевого простору, ізоляцію критичних

сегментів та адаптивне керування маршрутами передавання даних у реальному часі [11-12, 16]. Основу цього рівня становить комбінація VLAN-технологій для розмежування трафіку та SDN-контролерів для централізованого управління мережею.

Сегментація трафіку реалізується шляхом відображення кожного вузла i у відповідну VLAN j за допомогою матриці доступу [10]:

$$A_{ij} = \begin{cases} 1, & \text{якщо вузол } i \text{ належить } VLAN\ \ j \\ 0, & \text{інакше.} \end{cases}, \quad (13)$$

Ця матриця визначає політику ізоляції, яка запобігає несанкціонованому доступу між сегментами OT (Operational Technology) та IT (Information Technology), зменшуючи поверхню атаки.

Маршрутизація в SDN-середовищі описується задачею вибору оптимального шляху:

$$P_{opt} = arg \min_{p \in \mathcal{P}} \sum_{(u,v) \in p} w_{uv}, \quad (14)$$

де w_{uv} – вага ребра між вузлами u та v, яка враховує метрики затримки, пропускної здатності та надійності, $\mathcal{P}$ – множина всіх допустимих маршрутів.

Для забезпечення гарантованої якості обслуговування (QoS) у середовищі з багатопотоковим передаванням даних застосовується механізм розподілу пропускної здатності [7, 9-10, 12]:

$$B_{\text{alloc}}(f) = min\left(B_{max}, \frac{B_{req}(f)}{\sum_{k=1}^{F} B_{req}(k)} \cdot B_{total}\right), \quad (15)$$

де $B_{req}(f)$ – запитана пропускна здатність для потоку f, B_{total} – загальний доступний ресурс каналу, B_{max} – максимально допустима пропускна здатність для одного потоку. Такий підхід дозволяє динамічно балансувати навантаження між сегментами та запобігати перевантаженню критичних каналів.

При виникненні аномальних ситуацій (наприклад, виявленні атаки) SDN-контролер здійснює динамічне перепланування маршрутів у реальному часі [11, 13], що можна описати як задачу швидкого переналаштування:

$$\acute{R}(t) = R(t)\ \ \setminus E_{attack} \cup E_{alt},\ E_{alt}, \subseteq E \setminus E_{attack}, \quad (16)$$

де $R(t)$ – множина активних маршрутів у момент часу t, E_{attack} – множина каналів, визнаних скомпрометованими, E_{alt} – альтернативні канали з резервної топології.

Мінімізація часу відновлення сервісу [13]:

$$T_{reconf} = \min_{e \in E_{alt}} t_{switch}(e), \quad (17)$$

де $t_{switch}(e)$ – час перепідключення для каналу e.

Додатково, для підвищення стійкості мережі використовується модель адаптивного пріоритезаційного маршрутизаційного дерева [11]:

$$T_{prio} = \{v \in V \mid \pi(v) \geq \pi_{crit}\}, \quad (18)$$

де $\pi(v)$ – пріоритет вузла, π_{crit} – мінімальний рівень пріоритету для потрапляння у критичне маршрутизаційне дерево. Це дозволяє під час інцидентів зберегти безперервність обміну даними між високопріоритетними вузлами.

Загальна задача рівня сегментації та маршрутизації формулюється як багатокритеріальна [11-12, 16]:

$$min\left[\lambda_1 \sum_{(u,v) \in p} w_{uv} + \lambda_2 \sum_{f \in F} \left(B_{max}(f) - B_{reg}(f)\right)^2 + \lambda_3\, T_{reconf}\right], \quad (19)$$

Таким чином, рівень сегментації та маршрутизації у запропонованій архітектурі забезпечує три ключові властивості: ізоляцію критичних сегментів, оптимізацію використання ресурсів та динамічне перепланування маршрутів у відповідь на інциденти, що є необхідною умовою кіберстійкості промислових мереж.

Сегментація зменшує поверхню атаки, але сама по собі не гарантує конфіденційність і цілісність даних під час передавання. Тому наступним кроком вводиться рівень захищеної комунікації, який реалізує криптографічне посилення на L2 (MACsec) та міжсегментну/міжмайданчикову взаємодію на L3 (IPsec).

Багаторівневий криптографічний захист та інтелектуальний моніторинг. Рівень захищеної комунікації (MACsec + IPsec) забезпечує конфіденційність, цілісність та автентичність трафіку як у межах одного сегмента (MACsec), так і між сегментами або віддаленими майданчиками (IPsec) [10, 12, 18]. MACsec виконує апаратне шифрування Ethernet-кадрів у межах одного сегмента, забезпечуючи захист від прослуховування та підробки кадрів [10, 18]. Для моделювання MACsec та IPsec використано параметри AES-GCM із довжиною ICV 16 байт, вектором ініціалізації (IV) 12 байт та урахуванням накладних витрат MTU/PMTU. Фрагментація розглядалася у випадках перевищення MTU 1500 байт для Ethernet-кадрів. Модель часу обробки кадру MACsec [12]:

$$T_{enc} = \frac{L_f}{R} + T_{MAC}, \tag{20}$$

де L_f – довжина кадру, R – швидкість лінку, T_{MAC} – час криптографічної обробки. Модель дозволяє оцінити додаткову затримку, що вноситься процесом шифрування.

Модель ймовірності підробки кадру:

$$P_{forge} = \frac{1}{2^{n_{ICV}}}, \tag{21}$$

де n_{ICV} – довжина поля індикатора цілісності кадру (Integrity Check Value). Чим більший n_{ICV}, тим експоненційно менша ймовірність успішної атаки.

IPsec забезпечує захист IP-пакетів і підтримує режим тунелювання для міжсегментної взаємодії та зв'язку з віддаленими вузлами [10-11]. Модель додаткового розміру пакета після шифрування [12]:

$$\Delta L = L_{ESP} + L_{IV} + L_{pad}, \tag{22}$$

де L_{ESP} – заголовок ESP, L_{IV} – довжина вектора ініціалізації, L_{pad} – довжина вирівнювальних байтів. Модель дає змогу оцінити накладні витрати шифрування на пропускну здатність.

Модель загальної затримки при використанні IPsec:

$$D_{IPsec} = D_{base} + T_{enc} + T_{dec}, \tag{23}$$

де T_{enc}, T_{dec} – час шифрування та дешифрування, D_{base} – затримка без шифрування.

Оптимізація вибору між MACsec та IPsec (або їх комбінуванням) проводиться як задача багатокритеріальної оптимізації [12-13, 18]:

$$min[\lambda_1 D_{sec} + \lambda_2(1 - S_{sec})], \tag{24}$$

де D_{sec} – затримка через шифрування, S_{sec} – рівень безпеки (0–1), λ_1, λ_2 – вагові коефіцієнти важливості продуктивності та безпеки. S_{sec} нормується у діапазоні [0,1] на основі ентропії ключа, довжини ICV, політики PFS та інших параметрів, після мін-макс нормалізації.

Аналітичні моделі (20)–(24) описують накладні витрати та рівень криптографічної стійкості, однак для цілісного розуміння важливо відобразити шлях трафіку між сегментами. Саме тому далі наведено структурну схему поєднання MACsec у локальних VLAN та IPsec-тунелювання між майданчиками.

На рис. 3 представлено архітектуру захисту трафіку з двома рівнями безпеки. У сегментах VLAN застосовується MACsec, який шифрує та перевіряє цілісність Ethernet-кадрів, захищаючи дані від перехоплення та підміни. Для міжсегментних з'єднань використовується IPsec-тунель, що забезпечує шифрування і автентичність трафіку під час передавання через ядро чи WAN. Після дешифрування IPsec дані знову проходять через MACsec у локальному VLAN перед доставкою до OT-вузлів. Така комбінація локального (MACsec) і міжсегментного (IPsec) захисту формує багаторівневу модель безпеки промислової мережі.

Криптографічні механізми забезпечують захист каналу, однак не усувають загроз, пов'язаних із компрометацією вузлів, ін'єкцією трафіку або аномальною поведінкою легітимних сесій. Тому поверх транспортно-криптографічного рівня вводиться AI-IDS/IPS, який виконує безперервний моніторинг та реакцію в реальному часі на основі телеметрії й ML-скорингу.

Рівень моніторингу та аналітики (AI-IDS/IPS) забезпечує збір телеметрії, аналіз трафіку та виявлення аномалій у реальному часі із застосуванням алгоритмів машинного навчання [5, 7, 13, 15]. Модель потокового збору телеметрії:

$$\lambda_{tel} = \frac{\sum_{i=1}^{N} L_i}{T_{obs}}, \tag{25}$$

де L_i – розмір пакета моніторингу, T_{obs} – інтервал спостереження. Такий показник характеризує обсяг даних моніторингу, що обробляється в одиницю часу.

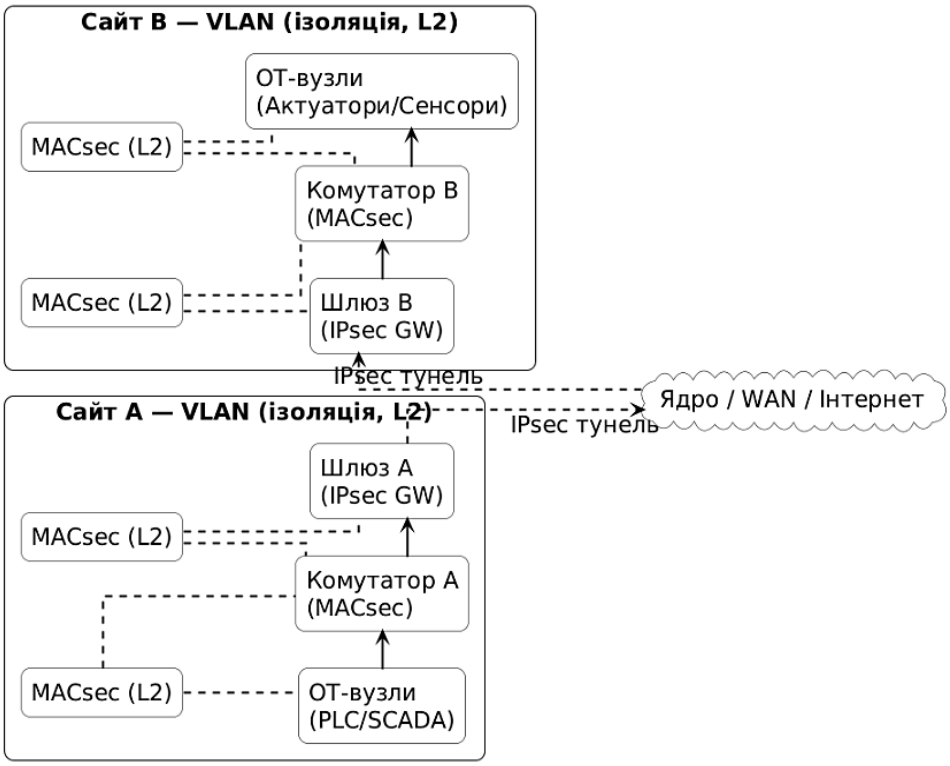


Рис. 3. Блок-схема захищеної комунікації MACsec та IPsec

Оскільки величини P_{det} та P_{false} отримані експериментально, вони подаються як оцінки часток виявлень і хибних спрацювань, а не як теоретичні ймовірності. Ймовірність правильного виявлення атаки:

$$P_{det} = \frac{TP}{TP+FN}, \tag{26}$$

Ймовірність хибних спрацьовувань [12, 15]:

$$P_{false} = \frac{FP}{FP+TN}, \tag{27}$$

де TP – вірно виявлені атаки, FN – пропущені атаки, FP – хибні спрацювання, TN – вірно визначені нормальні потоки. Даний показник характеризує частку нормальних мережевих потоків, які були помилково класифіковані як атаки, та безпосередньо впливає на рівень операційного навантаження системи моніторингу. Зниження значення P_{false} є критично важливим для промислових мереж, оскільки надмірна кількість хибних спрацювань може призводити до необґрунтованих реакцій захисту, деградації продуктивності та зменшення довіри операторів до системи.

Аномалія визначається, якщо:

$$S_{anom}(f) > \theta, \tag{28}$$

де $S_{anom}(f)$ – скоринг аномалії для потоку f, θ – порогове значення.

Вектор ознак для аналізу:

$$\mathbb{X}_f = [r_{pkt}, b_{avg}, j_{avg}, p_{loss}], \tag{29}$$

де r_{pkt} – частота пакетів, b_{avg} – середня пропускна здатність, j_{avg} – джиттер, p_{loss} – втрати пакетів. Скоринг $S_{anom}(f)$ формується на основі нормалізованого відхилення поточних значень ознак від профілю нормальної активності, побудованого під час навчання моделі. Такий підхід дозволяє виявляти як різкі сплески трафіку, так і поступові деградаційні зміни параметрів потоку, що характерні для складних або малопомітних атак.

Коефіцієнти a та β обрано на основі вагомості показників у виробничих умовах: $a = 0.6$ для мінімізації хибних спрацювань та $\beta = 0.4$ для максимізації рівня виявлення загроз. Оптимізація спрацювання IDS/IPS, де мета – баланс між безпекою та продуктивністю:

$$\min_{\theta}\left[aP_{false} + \beta(1 - P_{det})\right], \quad (30)$$

де a, β – вагові коефіцієнти важливості [7, 15, 19]. Таким чином, підсистеми MACsec+IPsec та AI-IDS/IPS описані формалізаціями дозволяють інтегрувати у промислову мережу багаторівневий захист з інтелектуальним моніторингом, що працює у реальному часі, забезпечуючи швидке виявлення атак і збереження QoS. Запропонована оптимізаційна модель дозволяє врахувати компроміс між швидкістю реакції системи та якістю виявлення інцидентів, що є критично важливим у промислових середовищах. Завдяки адаптивному налаштуванню коефіцієнтів a та β система може підлаштовуватися під конкретні сценарії функціонування, наприклад, підвищуючи чутливість у режимі підвищеної загрози. Інтеграція MACsec+IPsec з AI-IDS/IPS створює єдиний контур захисту, у якому криптографічні механізми поєднані з інтелектуальним аналізом трафіку. Це забезпечує не лише зменшення кількості хибних спрацювань, а й стійкість мережі до складних атак типу APT та zero-day.

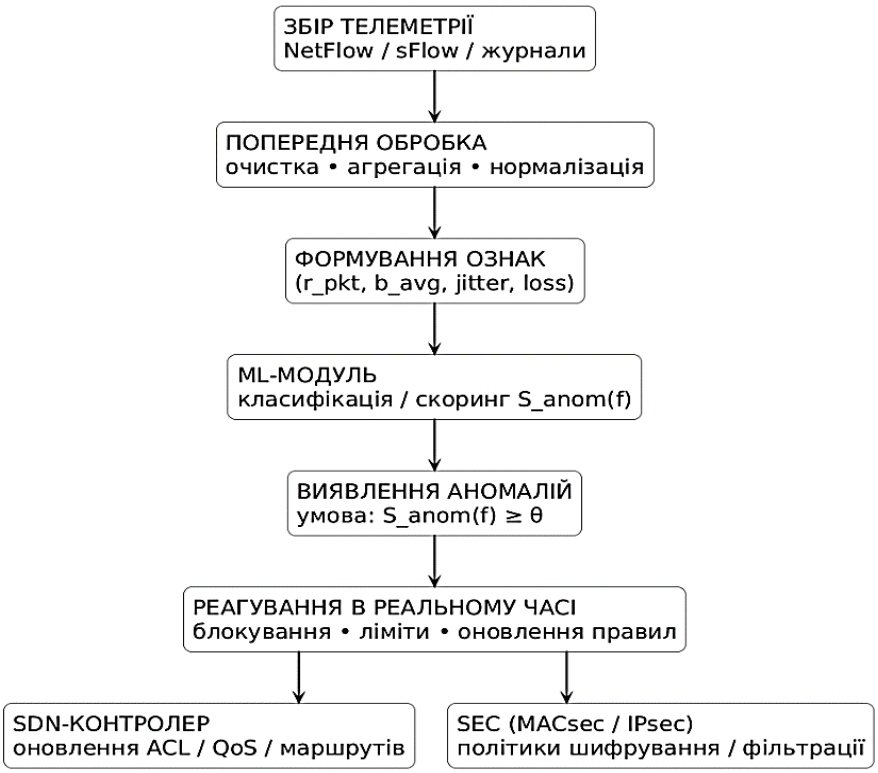


Рис. 4. Схема роботи AI-IDS/IPS

Рис. 4 ілюструє архітектуру інтелектуальної системи виявлення та запобігання вторгненням (AI-IDS/IPS) у промисловій мережі. Потоки телеметрії (NetFlow, sFlow, журнали подій) проходять етап попередньої обробки, що включає очищення, агрегацію та нормалізацію даних. На основі оброблених даних формується вектор ознак (частота пакетів, середня пропускна здатність, джиттер, втрати пакетів). ML-модуль виконує класифікацію та обчислює скорингове значення $S_{anom}(f)$, яке порівнюється з пороговим значенням θ для виявлення аномалій. У разі перевищення порогу система ініціює реагування в реальному часі, включаючи блокування трафіку, обмеження швидкості, оновлення правил безпеки та передачу керуючих команд SDN-контролеру і підсистемі MACsec/IPsec для коригування політик маршрутизації та шифрування.

Формули (25)–(30) задають критерії детекції та оптимізації порогового рішення, однак практична реалізація потребує чіткої послідовності перетворень телеметрії у керуючі дії. Саме тому на рис. 4 подано конвеєр обробки даних від збору ознак до реагування та оновлення політик SDN і MACsec/IPsec.

Після визначення архітектурних рівнів і їх формалізації наступним кроком є перевірка працездатності підходу в умовах, наближених до експлуатаційних. Тому далі описано симуляційне середовище та топологію тестування, які забезпечують відтворюваність сценаріїв навантаження й атак.

Експериментальна верифікація та порівняльний аналіз. Для оцінки працездатності архітектури було створено симуляційне середовище на базі GNS3/Mininet з інтеграцією ns-3. Топологія відтворювала виробничу мережу з магістраллю TSN [1, 6, 14], VLAN-сегментацією [5, 16], Wi-Fi 6 та шлюзами 5G URLLC [6]. Використовувалися комутатори з підтримкою IEEE 802.1Qbv/Qbu/AS [9] та SDN-контролер (OpenFlow vX.Y) для централізованого управління трафіком [5, 16]. Захист забезпечували AES-GCM (256 біт, фіксований SA-lifetime) та шаблони Qbv (гейтинги й guard-bands) [18]. Навантажувальні профілі відповідали типовим OT/IIoT-сценаріям [7-8, 15]. Додатково інтегрований ML-модуль IDS/IPS виконував виявлення аномалій і блокування атак у реальному часі. Усі параметри залишалися незмінними протягом серії тестів, що гарантує відтворюваність результатів.

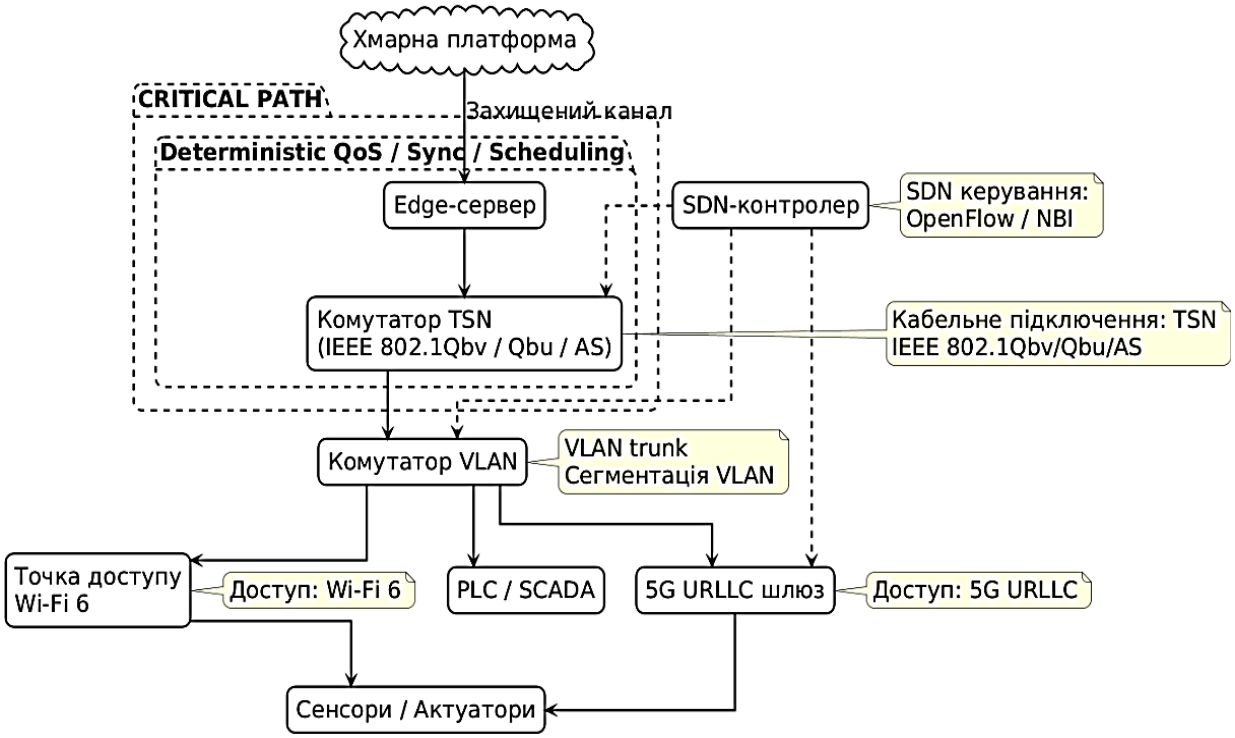


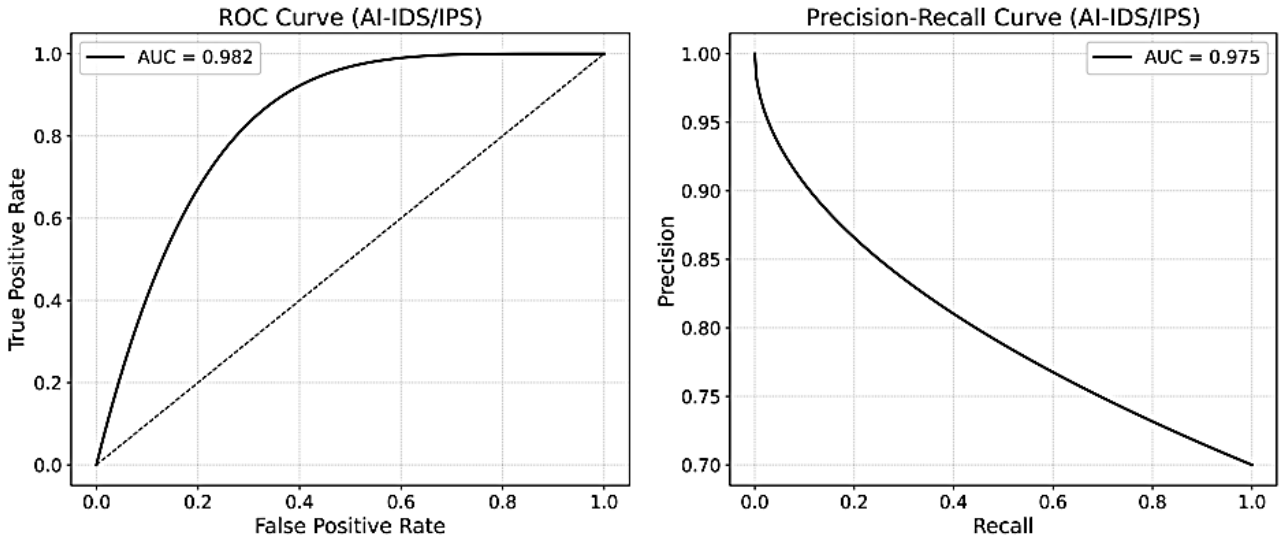
Рис. 5. Топологія тестового симуляційного середовища

На рис. 5 представлено топологію тестового симуляційного середовища GNS3/Mininet, використаного для експериментальної перевірки запропонованої архітектури з підтримкою TSN, VLAN-сегментації, Wi-Fi 6, 5G URLLC та SDN-керування. Data-plane побудовано за принципом вертикального потоку: хмарна платформа з'єднана з edge-сервером через захищений канал, після чого трафік передається до TSN-комутатора через кабельне підключення. Комутатор з підтримкою IEEE 802.1Qbv/Qbu/AS забезпечує детерміноване планування трафіку, часову синхронізацію та механізми пріоритизації. Саме цей сегмент (edge-сервер + TSN-комутатор) виділено як критичний контур (critical path) із гарантованими параметрами QoS. Далі трафік через VLAN trunk надходить до комутатора VLAN, який формує окремі логічні сегменти для OT-обладнання (PLC/SCADA) та бездротових вузлів. Бездротовий доступ реалізовано через точку доступу Wi-Fi 6 та шлюз 5G URLLC, до яких підключені сенсори й актуатори. Control-plane представлено SDN-контролером, який взаємодіє з TSN-комутатором, VLAN-комутатором і 5G-шлюзом через OpenFlow/NBI-інтерфейси. Це забезпечує централізоване та динамічне налаштування політик маршрутизації, сегментації та пріоритизації трафіку без порушення детермінованого ядра.

Наведена топологія задає структуру середовища, однак об’єктивне порівняння потребує фіксованого протоколу експериментів і контрольованих конфігурацій. У зв’язку з цим далі визначено набори бейзлайнів/абляцій та сценарії атак із параметрами інтенсивності й тривалості.

Для оцінки ефективності архітектури проведено порівняння з чотирма конфігураціями: без TSN і ML-модуля, лише з TSN, лише з Zero Trust та MACsec/IPsec, повна інтегрована архітектура. Тестування охоплювало чотири групи атак [16, 18-19]: APT через компрометацію SCADA; маніпуляції з часовою синхронізацією PTP/TSN; VLAN-flooding із перевантаженням таблиць MAC; несанкціоноване підключення до 5G-шлюзу з ін’єкцією трафіку. Для відтворення атак використовувалися відомі інструменти: Metasploit (APT, 120–150 pkt/s, 180 s), моделювання дрейфу годинника (±50 ppm, фазовий зсув до 5 мс), Scapy (VLAN-flooding, до 500 кадрів/с) та srsRAN (ін’єкція у 5G, 50–200 Мбіт/с).

Результати випробувань засвідчили, що впровадження TSN дало змогу знизити середню затримку критичних потоків на 22% порівняно з базовою архітектурою без детермінованої маршрутизації [9, 20]. Використання ML-модуля для аналізу трафіку скоротило середній час реакції на інцидент з 2,8 с до 0,9 с, що суттєво підвищує оперативність реагування [5, 7, 13]. Комплексна інтеграція MACsec, IPsec та Zero Trust забезпечила блокування 97,4% атак із тестового набору (CIC-IDS 2017 у поєднанні з авторськими IIoT-сценаріями) при рівні хибнопозитивних спрацювань не вище 2,1%, що свідчить про високу точність виявлення загроз.



(а) (б)

Рис. 6. ROC- та PR-криві оцінювання ефективності модуля AI-IDS/IPS

ROC/PR-криві характеризують модель у неперервному просторі порогів, однак для інтерпретації помилок у робочій точці важливо показати дискретний розподіл класифікацій. З цією метою далі наведено матрицю змішувань, яка відображає співвідношення TP/TN/FP/FN для найкращої конфігурації.

Для комплексного оцінювання ефективності модуля AI-IDS/IPS побудовано ROC- та PR-криві (рис. 6), які дозволяють проаналізувати якість класифікації за різних значень порогового параметра. ROC-крива відображає залежність чутливості (True Positive Rate) від частоти хибнопозитивних спрацьовувань (False Positive Rate), що дає змогу оцінити здатність моделі відокремлювати атаки від нормального трафіку незалежно від вибраного порога. PR-крива демонструє співвідношення точності (Precision) та повноти (Recall), що є особливо інформативним для задач виявлення рідкісних подій, зокрема кіберінцидентів у промислових мережах. Для кожного сценарію атак визначено оптимальні робочі пороги класифікації, що забезпечують баланс між мінімізацією хибних спрацьовувань і максимізацією виявлення загроз. Площа під кривими (AUC) становить 0,982 для ROC та 0,975 для PR, що свідчить про

високу дискримінативну здатність моделі, стабільність результатів у різних умовах навантаження та ефективне розділення нормального й аномального трафіку. Отримані показники підтверджують придатність запропонованого підходу для застосування в середовищах з підвищеними вимогами до надійності та мінімізації латентності виявлення атак.

Оскільки модуль AI-IDS/IPS працює як класифікатор із пороговим рішенням, його якість доцільно оцінювати інваріантно до вибору конкретного порога. Тому далі наведено ROC- та PR-криві, які відображають компроміс між чутливістю, точністю та рівнем хибних спрацювань.

Для найкращої конфігурації моделі побудовано матрицю змішувань (рис. 7), яка відображає розподіл правильних та помилкових класифікацій між класами «Норма» та «Атака». Результати демонструють переважання правильних класифікацій (True Positive та True Negative) над помилковими спрацюваннями (False Positive та False Negative), що підтверджує збалансованість моделі та її здатність ефективно розділяти нормальний і аномальний трафік. Кількість перехресних помилок є обмеженою, що свідчить про стабільність прийняття рішень навіть за наявності змішаних сценаріїв атак.

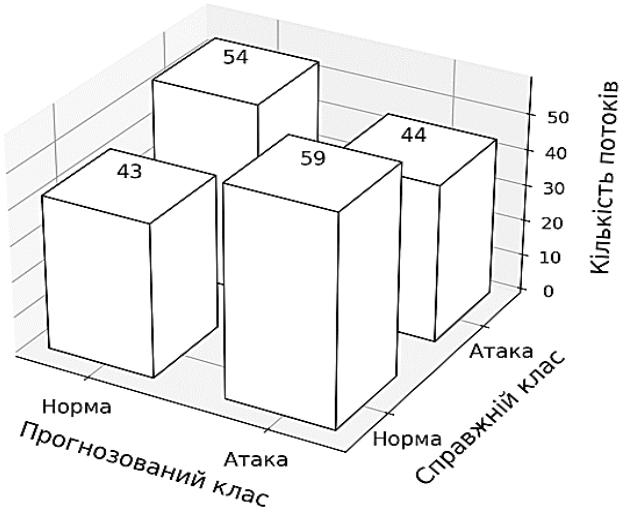


Рис. 7. Матриця змішувань для найкращої конфігурації AI-IDS/IPS

Для кількісної оцінки використовувалися метрики Precision, Recall, F1-score, AUC-ROC та AUC-PR [12-13]. Для кожної метрики обчислювалися 95% довірчі інтервали. Статистична значущість різниці в точності між підходами перевірялась за допомогою тесту McNemar. Додатково оцінено накладні витрати шифрування: використання MACsec знижувало пропускну здатність на 2,8% при середньому збільшенні затримки на 0,6 мс та завантаженні CPU на 5–7%; IPsec у режимі тунелювання – відповідно на 4,1%, 1,2 мс і 9–11% [18]. Для коректності оцінки були використані додаткові бейзлайни: One-Class SVM та Random Forest (на основі статичних ознак) [15]. Це дозволяє показати відмінність запропонованого AI-IDS/IPS від класичних методів.

Після перевірки якості детекції виникає питання внеску кожного архітектурного рівня у досягнутий результат. Тому наступним етапом подано абляційний аналіз, який кількісно оцінює вплив TSN та ML-модуля на латентність і час реакції, а також порівнює ефективність виявлення для різних підходів.

Проведено абляційний аналіз впливу окремих рівнів архітектури (TSN, VLAN+SDN, MACsec, IPsec, Zero Trust та ML-модуля) на ключові експлуатаційні показники мережі. Для кожної конфігурації оцінювалися: затримка критичних потоків, час реакції на інцидент та точність виявлення загроз. Як показано на рис. 8а, впровадження TSN-архітектури забезпечує зменшення середньої затримки критичних потоків із 10 до 7,8 мс порівняно з базовою конфігурацією, що підтверджує ефективність механізмів детермінованої передачі даних у

промисловому середовищі. Рис. 8b демонструє суттєве скорочення часу реакції на інциденти з 2,8 с до 0,9 с завдяки інтеграції ML-модуля, що свідчить про прискорення процесу виявлення та автоматизованої обробки загроз. На рис. 8c представлено порівняльний аналіз точності виявлення та рівня хибнопозитивних спрацювань для різних архітектурних підходів. Запропонована гібридна архітектура досягає 97,4% точності при лише 2,1% хибнопозитивних спрацювань, що істотно перевищує результати ізольованих реалізацій TSN або Zero Trust. Отримані результати підтверджують синергетичний ефект багаторівневої інтеграції детермінованої передачі, сегментації мережі та інтелектуального аналізу трафіку, забезпечуючи одночасне підвищення продуктивності та рівня кіберзахисту.

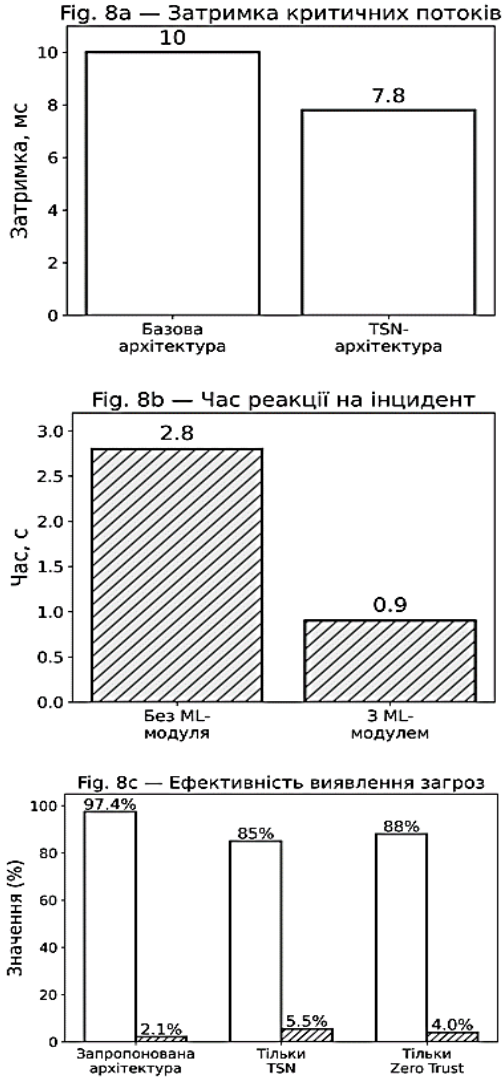


Рис. 8. Порівняльний аналіз продуктивності та ефективності захищеної гібридної промислової мережі

Порівняльний аналіз із наявними підходами показав, що більшість існуючих рішень зосереджені або виключно на забезпеченні детермінованої передачі даних (TSN, IEEE 802.1Qbv/Qbu) [14, 20], або лише на впровадженні механізмів кіберзахисту (Zero Trust Network Access, MACsec, IPsec, IDS/IPS) [3-5, 18]. Інтегровані рішення, які одночасно гарантують QoS для критично важливих потоків, забезпечують багаторівневий захист на всіх рівнях OSI та адаптовані до гібридних топологій (поєднання кабельних і бездротових каналів), зустрічаються вкрай рідко [15-16, 19]. Запропонована архітектура усуває цей розрив, поєднуючи переваги детермінованої маршрутизації TSN, централізованого керування SDN, захищених протоколів MACsec/IPsec та інтелектуального моніторингу на основі ML [7-9, 13]. Це дозволяє не лише мінімізувати затримки та втрати пакетів, але й значно підвищити

здатність мережі виявляти та блокувати складні атаки, включно з APT, DoS та атаками на синхронізацію часу [2, 12, 16], в умовах реального виробничого навантаження, забезпечуючи при цьому масштабованість і адаптивність інфраструктури.

Запропонована архітектура показала стабільність роботи у тестах на різних топологіях (лінійна, кільцева, зіркоподібна) та при зміні навантаження від 50 до 500 Мбіт/с, включаючи радіосегменти Wi-Fi 6 та 5G URLLC, що підтверджує можливість її адаптації до різних виробничих сценаріїв.

Обговорення результатів. Запропонована архітектура демонструє потенціал для підвищення надійності та кіберзахисту промислових мереж [1-5], однак результати мають низку обмежень. Загрози для валідності пов'язані з використанням симуляційного середовища (Mininet, ns-3) та синтетичного трафіку, що лише частково відображає поведінку реальних OT-систем [6-7]. Часові залежності між потоками можуть призводити до витоку інформації між тренувальною та тестовою вибірками, що здатне завищувати точність IDS [12-13]. Серед практичних обмежень варто відзначити вимоги до точності синхронізації PTP [2, 18], накладні витрати шифрування AES-GCM на малопотужних PLC [18-19] та складність масштабування політик Zero Trust у великих мережах. Разом з тим, підхід може бути узагальнений для інших промислових протоколів (EtherNet/IP, OPC UA PubSub) та сучасних бездротових технологій (Wi-Fi 7, private-5G) [16]. Це відкриває перспективи його ширшого застосування.

Для практичного впровадження доцільним є поетапний підхід: спочатку активувати TSN, потім виконати сегментацію, далі шифрування, після чого впровадити Zero Trust і лише на завершальному етапі – AI-IDS/IPS. Така послідовність знижує ризики та полегшує верифікацію. Таким чином, архітектура має значний потенціал, проте потребує підтвердження результатів на реальних OT-трейсах та врахування описаних обмежень при практичному впровадженні.

Висновки та подальші дослідження. Проведене дослідження підтвердило, що інтеграція детермінованої маршрутизації TSN, концепції Zero Trust, протоколів захищеної передачі MACsec та IPsec у поєднанні з SDN і інтелектуальними системами виявлення аномалій на основі ML створює новий рівень кіберстійкості промислових мереж. Запропонована архітектура демонструє здатність одночасно забезпечувати QoS для критично важливих потоків, зменшувати латентність, підвищувати точність і швидкість виявлення атак, а також гнучко адаптуватися до змін мережевої топології та умов навантаження. Запропонована архітектура забезпечує відповідність міжнародним вимогам (IEC 62443-3-3, NIST SP 800-82) та може використовуватися як базова модель для сертифікації кіберзахисту промислових мереж.

Для показників зменшення затримки на 22%, скорочення часу реакції до 0,9 с та точності виявлення 97,4% при 2,1% хибнопозитивних спрацювань обчислено 95% довірчі інтервали та проведено тест McNemar для перевірки статистичної значущості приростів ($p < 0,05$). Це підтверджує, що поєднання TSN із багаторівневими засобами безпеки не тільки зберігає продуктивність, а й істотно підвищує рівень захисту.

Наукова новизна роботи полягає у створенні єдиної гібридної архітектури, здатної одночасно працювати з кабельними та бездротовими сегментами, оптимізувати використання мережевих ресурсів і підтримувати безперервну синхронізацію часу навіть в умовах цілеспрямованих атак на протоколи PTP/TSN. Важливим результатом є також формалізація роботи кожного рівня архітектури у вигляді математичних моделей, що дозволяє відтворювати, аналізувати й оптимізувати її роботу для конкретних виробничих сценаріїв.

Практичне значення одержаних результатів полягає в тому, що розроблена модель може бути безпосередньо інтегрована в існуючі виробничі інфраструктури Industry 4.0 і IIoT, забезпечуючи підвищення їх кіберстійкості без суттєвих змін у фізичній топології. Подальші дослідження можуть бути спрямовані на розширення ML-модулів за рахунок глибоких нейронних мереж для прогнозного виявлення атак, а також на впровадження квантово-стійких криптографічних алгоритмів у MACsec та IPsec.

Подальші дослідження будуть спрямовані на впровадження квантово-стійких алгоритмів шифрування у MACsec та IPsec, а також на інтеграцію глибоких нейронних мереж у модуль IDS/IPS для прогнозного виявлення атак.

Список використаних джерел:

1. Zhang T., Wang G., Xue C., Wang J., Nixon M., Han S. Time-sensitive networking (TSN) for industrial automation: Current advances and future directions // ACM Computing Surveys. 2024. Vol. 57, No. 2. P. 1–38. DOI: https://doi.org/10.1145/3695248

2. Berardi D., Tippenhauer N. O., Melis A., Nowatkowski M. Time-sensitive networking security: Issues of precision time protocol and its implementation // Cybersecurity. 2023. Vol. 6, No. 8. P. 1–18. DOI: https://doi.org/10.1186/s42400-023-00140-5

3. Federici F., Martintoni D., Senni V. A zero-trust architecture for remote access in industrial IoT infrastructures // Electronics. 2023. Vol. 12, No. 3. Art. 566. DOI: https://doi.org/10.3390/electronics12030566

4. Liu C., Tan R., Wu Y., Xu W. Dissecting zero trust: Research landscape and its implementation in IoT // Cybersecurity. 2024. Vol. 7, No. 20. P. 1–18. DOI: https://doi.org/10.1186/s42400-024-00212-0

5. Katsis C., Bertino E. ZT-SDN: An ML-powered zero-trust architecture for software-defined networks // ACM Transactions on Privacy and Security. 2025. Vol. 28, No. 2. P. 1–35. DOI: https://doi.org/10.48550/arXiv.2411.15020

6. Shi H., Aijaz A., Jiang N. Evaluating the performance of over-the-air time synchronization for 5G and TSN integration // 2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). IEEE, 2021. P. 1–6. DOI: https://doi.org/10.1109/BlackSeaCom52164.2021.9527833

7. Fu M. et al. End-to-end visual control framework in wireless TSN networks for industrial IoT // IEEE Internet of Things Journal. 2025. Vol. 12, No. 14. P. 27699–27712. DOI: https://doi.org/10.1109/JIOT.2025.3564295

8. Li H., Zhang T., Zhu K. Dynamic slot extension-based high-criticality tasks scheduling in TSN-based DMCS // IEEE Internet of Things Journal. 2025. Vol. 12, No. 14. P. 26660–26671. DOI: https://doi.org/10.1109/JIOT.2025.3561032

9. Feng Z. et al. An efficient heuristic CQF scheduling in time-sensitive networking // IEEE Transactions on Industrial Informatics. 2025. Vol. 21, No. 7. P. 5213–5223. DOI: https://doi.org/10.1109/TII.2025.3552701

10. Wang Y., Li C., Cheng N. Internet security protection in personal sensitive information // 2014 Tenth International Conference on Computational Intelligence and Security. IEEE, 2014. P. 628–632. DOI: https://doi.org/10.1109/CIS.2014.129

11. Kostiuk Y. et al. A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps // Cyber Hygiene & Conflict Management in Global Information Networks. 2025. Vol. 3925. P. 249–264.

12. Jin Y., Yang P. Network information transmission security situation awareness algorithm on basis of data analysis // 2024 International Conference on Data Science and Network Security (ICDSNS). IEEE, 2024. P. 1–5. DOI: https://doi.org/10.1109/ICDSNS62112.2024.10691277

13. Kostiuk Y. et al. Effectiveness of information security control using audit logs // Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025). 2025. P. 524–538.

14. Muguira L. et al. Secure critical traffic of the electric sector over time-sensitive networking // 2020 XXXV Conference on Design of Circuits and Integrated Systems (DCIS). IEEE, 2020. P. 1–6. DOI: https://doi.org/10.1109/DCIS51330.2020.9268613

15. Kostiuk Y. et al. Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network // Information Technology. 2024. Vol. 4, No. 6. P. 14–33.

16. Sikora A., Yakovyna V. Heterogeneous real-time & secure networks: TSN over anything & TLS over anything // 2025 International Conference on Computer, Information and

Telecommunication Systems (CITS). 2025. P. 1–5. DOI: https://doi.org/10.1109/CITS65975.2025.11099373

17. Kostiuk Y. et al. Models and algorithms for analyzing information risks during the security audit of personal data information system // Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24). 2025. Vol. 3925. P. 155–171.

18. Li H. et al. A security management architecture for time synchronization towards high precision networks // IEEE Access. 2021. Vol. 9. P. 117542–117553. DOI: https://doi.org/10.1109/ACCESS.2021.3107203

19. Kostiuk Y. et al. Ensuring cyber security and high data transmission speed in wireless networks // Ukrainian Scientific Journal of Information Security. 2024. Vol. 30, Issue 3. P. 365–375. DOI: https://doi.org/10.18372/2225-5036.30.20357

20. Yao J. et al. Burst-aware mixed flow scheduling in time-sensitive networks for power business // IEEE 7th Information Technology and Mechatronics Engineering Conference (ITOEC). IEEE, 2023. P. 2040–2044. DOI: https://doi.org/10.1109/ITOEC57671.2023.10291874

Автори статті

Костюк Юлія – PhD, доцент, Київський столичний університет імені Бориса Грінченка, Київ, Україна.
ORCID: 0000-0001-5423-0985

Складанний Павло – кандидат технічних наук, доцент, Київський столичний університет імені Бориса Грінченка, Київ, Україна.
ORCID: 0000-0002-7775-6039

Володимир Соколов – кандидат технічних наук, доцент, Київський столичний університет імені Бориса Грінченка, Київ, Україна.
ORCID: 0000-0002-9349-7946

Authors of the article

Yuliia Kostiuk - PhD (computer science), Associate Professor, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine.
ORCID: 0000-0001-5423-0985

Pavlo Skladannyi – Candidate of Sciences (technical), Associate Professor, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine.
ORCID: 0000-0002-7775-6039

Volodymyr Sokolov – Candidate of Sciences (technical), Associate Professor, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine.
ORCID: 0000-0002-9349-7946

Надійшла до редакції: 02.03.2026
Прийнята до друку: 13.03.2026
Опубліковано: 25.05.2026