

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІНІСТЕРСТВО ВИЩОЇ ОСВІТИ, НАУКИ ТА ІННОВАЦІЙ
РЕСПУБЛІКИ УЗБЕКИСТАН
МІНІСТЕРСТВО НАУКИ ТА ОСВІТИ АЗЕРБАЙДЖАНСЬКОЇ
РЕСПУБЛІКИ
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"**

**ПРОБЛЕМИ
ІНФОРМАТИКИ ТА МОДЕЛЮВАННЯ
(ПІМ-2026)**

**ТЕЗИ ДВАДЦЯТЬ ШОСТОЇ МІЖНАРОДНОЇ
НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ
(25 – 28 вересня 2026 року)**

Харків

2026

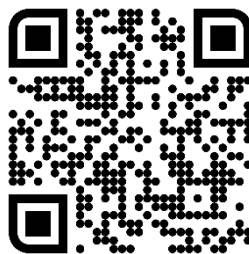
УДК 004.9

Проблеми інформатики та моделювання (ПІМ-2026). Тези двадцять шостої міжнародної науково-технічної конференції. – Харків: НТУ "ХПІ", 2026. – 202 с.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ:

- Міністерство освіти і науки України;
- Національна Академія наук України;
- Національний технічний університет "ХПІ", Харків;
- Національний університет "Одеська політехніка", Одеса;
- Інститут проблем моделювання в енергетиці імені Г.Є. Пухова НАНУ, Київ;
- Харківський національний університет радіоелектроніки, Харків;
- Донбаська державна машинобудівна академія, Краматорськ;
- Ташкентський інститут інженерів іригації і механізації сільського господарства, Ташкент, Узбекистан;
- Азербайджанський державний університет нафти і промисловості, Баку, Азербайджан;
- Грузинський технічний університет, Тбілісі, Грузія.

Електронна адреса сайту конференції: <https://web.kpi.kharkov.ua/pim/>



АНАЛІЗ ВРАЗЛИВОСТЕЙ ТА ЗАХИСТ КОМПЛЕКСУ МОНІТОРИНГУ ЕЛЕКТРОСПОЖИВАННЯ

*магістр Р.Г. Холод, Харківський національний університет
радіоелектроніки, м. Харків*

Під час експлуатації промислових систем моніторингу важливим завданням є зниження ризиків несанкціонованого доступу, модифікації даних і порушення доступності обладнання [1]. Отже, було проаналізовано вразливості окремих компонентів програмно-апаратного комплексу моніторингу електроспоживання та визначено відповідні заходи захисту. Для Modbus TCP/IP було враховано відсутність у класичній реалізації протоколу вбудованих механізмів автентифікації, що створює ризик несанкціонованого доступу до пристроїв і зміни даних. Для його зниження запропоновано сегментацію мережі, використання міжмережних екранів і списків контролю доступу. Для безпроводового сегмента Wi-Fi/AirMAX розглянуто можливість перехоплення або підміни мережного трафіку. Запропоновано застосування надійної автентифікації, обмеження віддаленого адміністрування та фільтрацію за MAC-адресами. Для бази даних MySQL визначено ризики втрати або модифікації архівних даних, для зменшення яких рекомендовано розмежування прав доступу та регулярне резервне копіювання. Захист сервера збору і візуалізації даних запропоновано забезпечувати оновленням операційної системи, антивірусним захистом, налаштуванням міжмережного екрана та використанням UPS. Окремо розглянуто ризик компрометації облікових записів користувачів, для якого передбачено застосування складних паролів і контроль доступу. Також рекомендовано змінювати стандартні облікові записи мережного обладнання та обмежувати доступ до сервісів, які не використовуються під час роботи комплексу.

Додатково рекомендовано ведення журналів подій та моніторинг мережних підключень для виявлення несанкціонованої активності. Застосування запропонованих заходів дозволяє сформулювати багаторівневий захист мережної, серверної та програмної складових комплексу. Це сприяє зниженню ризиків порушення конфіденційності, цілісності та доступності даних про електроспоживання.

Список літератури: 1. Sikora A. Industrial IoT- and OT-Networks: Recent Trends in Real-Time and Secure Communication / A. Sikora // 2025 60th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST), Ohrid, North Macedonia, 2025. P. 1-5. DOI: <https://doi.org/10.1109/ICEST66328.2025.11098300>.