

**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

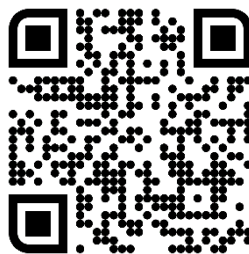
УДК 004.9

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/>



ПРОЄКТУВАННЯ ТА ДОСЛІДЖЕННЯ ЗАХИЩЕНОЇ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ У ВІРТУАЛЬНОМУ СЕРЕДОВИЩІ PNETLab

*студ. О.С. Єршов, Харківський національний університет
радіоелектроніки, м. Харків*

Продemonстровано процес створення інфокомунікаційної мережі з використанням протоколу резервування шлюзу за замовчуванням GLBP (Gateway Load Balancing Protocol). Проведено порівняльний аналіз основних механізмів захисту протоколу та обрано комплексний підхід, що передбачає застосування ACL та автентифікації MD5. Поєднання зазначених механізмів забезпечує захист GLBP на рівні контролю доступу до мережних пристроїв та автентифікації службових повідомлень, що дає змогу знизити ризик несанкціонованого втручання в роботу протоколу [1].

Для проведення дослідження використано віртуальне середовище PNETLab, яке підтримує моделювання мережної інфраструктури із застосуванням обладнання різних виробників, зокрема Cisco, MikroTik та Huawei. Використання віртуального середовища дозволило провести практичну перевірку обраних механізмів захисту без необхідності використання фізичного мережного обладнання [2].

У межах дослідження змодельовано функціонування мережі з протоколом GLBP та здійснено імітацію атаки шляхом підключення нелегітимного маршрутизатора з максимальним значенням пріоритету 255. Також розглянуто можливість отримання секретного ключа, необхідного для MD5-автентифікації. За результатами моделювання встановлено, що комплексне застосування ACL та MD5 ускладнює фальсифікацію службових повідомлень і знижує ризик отримання зловмисником контролю над передаванням трафіку через резервний шлюз. Отримані результати підтверджують доцільність використання комплексного захисту протоколу GLBP у мережах, де висуваються підвищені вимоги до надійності та безпеки маршрутизації.

Список літератури: 1. Mansour, M., Agomati, M., Alsaid, M. and Alasem, R. Performance analysis and functionality comparison of first hop redundancy protocol IPV6. *Procedia Computer Science*. 2022. Vol. 210. P. 19-27. DOI: <https://doi.org/10.1016/j.procs.2022.10.115>. 2. Grokipedia – PNETLab: вебсайт. URL: <https://grokipedia.com/page/PNETLab>.