

**ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
ЗАКЛАДУ ВІЩОЇ ОСВІТИ «ВІДКРИТИЙ МІЖНАРОДНИЙ УНІВЕРСИТЕТ
РОЗВИТКУ ЛЮДИНИ «УКРАЇНА»
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ ФАХОВИЙ КОЛЕДЖ**

ЗАТВЕРДЖУЮ
Директор Центральноукраїнського
фахового коледжу
Ірина ТКАЧЕНКО
«19» травня 2026 р.

**ПРОТОКОЛ
відвідування відкритого заняття**

Викладач Лукина Катерина Федорівна

Циклова комісія Економіки та журналістики

Форма навчання денна, спеціальність Журналістика, Фінанси, банківська справа,
страхування та фондовий ринок

Курс 1, група ФН-25-1 фмб.se-kd, ЖР-25-1 фмб.se-kd

Навчальна дисципліна Інформатика

Вид заняття практичне

Тема заняття Системи аналізу вмісту поштового і веб-трафіку (електронна пошта і
HTTP). Політики безпеки, сценарії і варіанти застосування і реагування. Віртуальні
приватні мережі (VPN). Загрози, пов'язані з використанням VPN.

Дата 19.05.2026 р. Початок заняття 13.10 Аудиторія 108

Короткий аналіз відкритого заняття

Відкрите практичне заняття проведено на високому науково-теоретичному,
технічному та методичному рівнях із дотриманням вимог компетентнісного підходу,
актуального для сучасної інженерно-технічної освіти в галузі ІТ. Зміст заняття повністю
відповідає робочій програмі навчальної дисципліни та відображає сучасні тренди індустрії
кібербезпеки.

Викладач продемонстрував глибоку науково-технічну компетентність,
представивши архітектуру захисту корпоративного мережевого периметра як інтегровану
екосистему. В основу заняття було покладено детальний аналіз функціонування шлюзів
безпеки електронної пошти (SEG) та вебшлюзів (SWG), механізмів глибокого аналізу
пакетів (DPI) для протоколів HTTP/HTTPS і SMTP/IMAP, а також криптографічних засад
побудови віртуальних приватних мереж (VPN). Особливу наукову цінність мало вивчення
сучасних вразливостей і векторів атак на інфраструктуру віддаленого доступу, що
відповідає актуальним вимогам NIST та OWASP.

Структура заняття відзначалася логічною послідовністю, раціональним розподілом
часу та чітким когнітивним переходом від концептуального розбору політик безпеки до
виконання інженерно-технічних завдань у симуляційному або реальному середовищі.

У ході заняття було ефективно застосовано комплекс інтерактивних, лабораторно-
аналітичних та праксеологічних методів навчання:

- Метод аналізу мережевого трафіку (Packet Analysis): здобувачі за допомогою інструментів аналізу (зокрема, Wireshark) досліджували дампи поштового (SMTP) та веб-трафіку (HTTP), виявляючи аномалії, індикатори компрометації (IoC) та спроби експлуатації вразливостей.
- Моделювання політик безпеки та сценаріїв реагування: розробка й конфігурування правил контентної та сигнатурної фільтрації для виявлення фішингу, витоку конфіденційних даних (DLP) та завантаження шкідливого ПЗ.

- Аналіз ризиків і тестування захищеності VPN: практичне дослідження архітектур криптографічних тунелів (IPsec, OpenVPN, WireGuard), аналіз загроз «людина посередині» (MITM), витоку DNS/IPv6 та експлуатації застарілих протоколів шифрування.

З метою інтенсифікації освітнього процесу викладач залучив сучасні інформаційно-комунікаційні технології (ІКТ) та інфраструктуру віртуалізованих лабораторій. Практична робота виконувалася в ізолюваному середовищі (на базі віртуальних машин або хмарних платформ), що дозволило студентам безпечно взаємодіяти із макетами мережеских загроз. Для візуалізації топології мереж та процесів інкапсуляції трафіку використано сучасне програмне забезпечення для моделювання (наприклад, GNS3 / Cisco Packet Tracer). Вхідний контроль знань криптографічних примітивів проведено за допомогою інтерактивного тестування.

Заняття сприяло формуванню та закріпленню базових спеціальних компетентностей у сфері кібербезпеки:

- Професійно-технічна компетентність: здатність налаштовувати, адмініструвати та модернізувати технічні засоби контролю поштового і веб-трафіку, розгортати захищені канали зв'язку.
- Аналітичне та критичне мислення: вміння виявляти приховані загрози при використанні VPN-технологій (наприклад, уразливості нульового дня у VPN-шлюзах, ризики несанкціонованого доступу через скомпрометовані кінцеві точки).
- Здатність до інцидент-менеджменту: навички швидкого формування сценаріїв реагування (блокування IP/доменів, ізоляція сегментів мережі) на виявлені факти аномальної активності.

На занятті домінувала суб'єкт-суб'єктна модель взаємодії, релевантна концепції DevOps/SecOps-команд (педагогіка партнерства). Викладач професійно виконував роль архітектора з інформаційної безпеки (SOC Lead) та фасилітатора, спрямовуючи хід інженерного пошуку студентів. Здобувачі вищої освіти продемонстрували високу технічну грамотність, вільне оперування спеціальним понятійно-категоріальним апаратом, розвинені навички командної роботи (Blue Teaming) під час локалізації змодельованих кібератак.

Проведене відкрите практичне заняття повністю досягло своєї дидактичної та праксеологічної мети. Заняття продемонструвало високу методичну ефективність завдяки успішній інтеграції складного інженерного інструментарію кіберзахисту з актуальними сценаріями відбиття реальних мережеских загроз. Досвід використання віртуалізованих лабораторних стендів для аналізу трафіку та тестування VPN рекомендується до вивчення та впровадження у практику педагогічного складу споріднених спеціальностей.

Висновки

1. Загальна констатація навчального та науково-методичного рівня заняття:

Практичне заняття проведене з дотримання усіх критеріїв

2. Рівень проведення заняття: «високий», «достатній», «низький» (потрібне підкреслити або доповнити) високий

Пропозиції щодо вдосконалення рівнів проведення відкритого заняття:

професійного _____

наукового _____

методичного _____

організаційного вміння зняти напруження і втом в аудиторії.

Відкрите заняття відкрито: посада, ІПН, підпис:

1. директор Людмила ТКАЧЕНКО

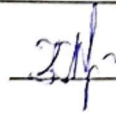
2. голова циклової комісії Наталя МИЛЬНІЧЕНКО

3. викладач  Олена КРАВЧЕНКО
4. викладач  Вікторія ЛЕСІВА

Думка лектора:

З висновками згоден (не згоден – обґрунтувати): _____

З відгуком ознайомлений: «19» травня 2026 року



підпис

Результати відвідування відкритого заняття обговорені на засіданні циклової комісії Економіки та журналістики Протокол № 11 від «19» червня 2026 р.

Голова циклової комісії економіки та журналістики



Наталя МИЛЬНИЧЕНКО