

РЕЦЕНЗІЯ
на освітньо-професійну програму
«Професійна освіта. Управління інформаційною безпекою»
підготовки здобувачів другого (магістерського) рівня вищої освіти
за спеціальністю А5 Професійна освіта (за спеціалізаціями)
галузі знань А Освіта
Академії праці, соціальних відносин і туризму

Освітньо-професійна програма «Професійна освіта. Управління інформаційною безпекою» спрямована на підготовку магістрів, здатних поєднувати професійно-педагогічну діяльність із розв'язанням завдань управління безпекою цифрового освітнього середовища. Актуальність програми визначається залежністю освітніх процесів від мережевої інфраструктури, електронних платформ, хмарних сервісів та інформаційних ресурсів, надійне функціонування яких потребує обґрунтованих організаційних і технічних рішень.

Позитивно оцінюю концептуальне спрямування програми на взаємозв'язок між інформаційною безпекою та якістю професійної освіти. Захист інформації розглядається в контексті доступності навчальних матеріалів, конфіденційності даних здобувачів, достовірності результатів оцінювання та безперервності освітніх сервісів. Такий підхід дозволяє сформулювати розуміння безпеки як складової проєктування й управління освітнім середовищем.

Зміст програми поєднує методологічну, педагогічну, управлінську та технологічну підготовку. Освітні компоненти з цифрової дидактики й методик професійної освіти створюють основу для організації навчання, тоді як основи інформаційної безпеки, аналітика кіберінцидентів та управління цифровими освітніми проєктами конкретизують професійні завдання безпекового спрямування. Важливо, щоб технічні рішення відповідали освітнім потребам та можливостям їх педагогічного застосування.

З позицій підготовки у сфері мережевих та інтернет-технологій заслуговує на підтримку розширення вибіркової складової лабораторними практикумами з комп'ютерних мереж і мережевої кібербезпеки за технологіями Cisco. Робота з топологіями, адресацією, сегментацією, маршрутизацією та правилами доступу створює можливості для формування системного уявлення про те, як функціонує цифрова інфраструктура закладу освіти. Навчальна цінність таких завдань визначається здатністю здобувача пояснювати конфігурацію, перевіряти очікувані з'єднання й обмеження та документувати отриманий результат.

Доцільним є включення напрямів аналізу мережевого трафіку, моніторингу подій, адміністрування захищених сервісів, безпеки вебзастосунків, хмарних технологій та інтернету речей. У сукупності вони дозволяють розглядати освітню інформаційну систему через взаємодію її компонентів, залежностей і можливих відмов. При цьому лабораторна підготовка має супроводжуватися визначенням меж моделювання: результат у симуляторі потребує пояснення умов, за яких його можна перенести на реальну інфраструктуру.

Важливою перевагою програми є орієнтація на перевірювані професійні результати. Модель ризиків, матриця доступу, конфігурація навчальної мережі, протокол аналізу подій або план відновлення сервісу можуть бути об'єктивно оцінені за повнотою вихідних умов, коректністю рішення, відтворюваністю перевірки та обґрунтованістю висновків. Такий підхід сприяє розвитку інженерної культури мислення й відповідальності за запропоноване рішення.

Схвально оцінюю передбачене програмою критичне ставлення до результатів застосування штучного інтелекту. Для аналізу кіберінцидентів і підтримки управлінських

рішень суттєвими є якість даних, перевірка хибних спрацювань, пояснення обмежень моделі та збереження людського контролю. Включення цих питань до підготовки магістрів створює основу для відповідального використання аналітичних інструментів у професійній освіті.

Педагогічна й переддипломна практики, а також кваліфікаційна робота забезпечують послідовне застосування набутих знань. Здобувач має можливість перейти від розроблення навчального завдання до дослідження професійної проблеми, створення практичного продукту та захисту результатів цього дослідження. Для цієї програми особливо цінним є поєднання технічного прототипу з методичним забезпеченням його використання: інструкцією, сценарієм заняття, критеріями оцінювання та аналізом типових помилок.

Подальший розвиток програми доцільно пов'язувати з поглибленням комплексних лабораторних завдань, у яких здобувачі досліджуватимуть повний цикл функціонування освітнього сервісу: від визначення вимог і проєктування мережевої взаємодії до перевірки доступу, моніторингу, резервування та відновлення. Рекомендую посилювати увагу до функціональної стійкості, аналізу залежностей між сервісами та документування результатів випробувань. Корисним буде зіставлення альтернативних рішень за безпекою, доступністю, ресурсними витратами й педагогічною доцільністю, а також регулярне оновлення кейсів за результатами співпраці з академічними та професійними партнерами. Наведені пропозиції спрямовані на подальше посилення практичної та дослідницької складових програми.

Освітньо-професійна програма «Професійна освіта. Управління інформаційною безпекою» заслуговує на позитивну оцінку. Її зміст і структура створюють обґрунтовану основу для підготовки магістрів професійної освіти, здатних організовувати навчання та розв'язувати прикладні й дослідницькі завдання забезпечення безпеки цифрового освітнього середовища.

Рецензент:

завідувач кафедри мережевих та інтернет технологій
факультету інформаційних технологій

Київського національного університету імені Тараса Шевченка
доктор технічних наук, професор



Юрій КРАВЧЕНКО

22 жовтня 2026 р.

Заступник декана факультету інформаційних технологій з навчально-виховної роботи
Київського національного університету імені Тараса Шевченка

кандидат фізико-математичних наук, доцент



Наталія ТМЄНОВА