Аналітичний звіт

за результатами громадського обговорення ОПП «Кібербезпека» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»

галузь знань – F Інформаційні технології

№ п/п	Складові ОПП	Пропозиції	Стейкхолдери	Результати обговорення	Обґрунтування
1	Складова ОПП «2.1. Перелік компонент ОПП»	В робочу програму з дисципліни «Тестування комп'ютерних систем на проникнення» ввести тему пов'язану з використанням агентів ШІ в тестуванні на проникнення	Володимир Драпак, директор комунального підприємства «Тернопільський інформаційно-аналітичний центр» Тернопільської обласної ради	Враховано	Введення теми, пов'язаної з використанням агентів ШІ в тестуванні на проникнення, є актуальним у зв'язку з активним розвитком автоматизованих інструментів аналізу вразливостей, генерації сценаріїв атак і підтримки прийняття рішень під час пентесту. Вивчення цієї теми дозволить здобувачам освіти зрозуміти можливості та обмеження ШІ-агентів, а також сформувати навички їх безпечного, етичного та контрольованого застосування у процесі оцінювання захищеності комп'ютерних систем.
2	Складова ОПП «2.1. Перелік компонент ОПП»	В робочу програму з дисципліни «Моніторинг та управління інформаційною безпекою» ввести зміни пов'язані із Законом України № 4336-IX від 27.03.2025 «Про	Микола Нетребяк, здобувач ОПП «Кібербезпека» другого (магістерського) рівня вищої освіти	Враховано	На виконання КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки

		внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури».			організації. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
3	Вибіркові компоненти	Ввести вибіркову дисципліну «Безпека генеративного штучного інтелекту»	Руслан Павлюк, здобувач ОПП «Кібербезпека» другого (магістерського) рівня вищої освіти	Враховано	Введення дисципліни «Безпека штучного інтелекту» є актуальним у зв'язку зі стрімким поширенням AI-систем у державному управлінні, бізнесі, освіті та критичній інфраструктурі. Використання штучного інтелекту створює нові ризики, пов'язані з витоком даних, маніпуляцією моделями, атаками на навчальні дані, prompt injection, несанкціонованим використанням генеративних моделей та порушенням принципів надійності й довіри до AI-рішень. Дисципліна спрямована на формування у здобувачів компетентностей щодо аналізу загроз AI-систем, оцінювання ризиків, захисту моделей, даних і інфраструктури, а також безпечного впровадження технологій штучного інтелекту відповідно до сучасних міжнародних підходів і стандартів.