

Код та назва дисципліни українською мовою/ Назва дисципліни англійською мовою	2у-10-42 Кібербезпека в освітньому просторі / Cybersecurity in the educational space
Рекомендується для галузі знань (<i>спеціальності, освітньої програми</i>)	Для всіх спеціальностей
Кафедра (<i>зазначати повну назву кафедри</i>)	Кібербезпеки і комп'ютерно-інтегрованих технологій
П.І.П. НПП (<i>за можливості</i>)	
Рівень ВО	Другий (магістерський)
КУРС, семестр (<i>в якому буде викладатись</i>)	
Мова викладання	українська
Пререквізити (<i>передумови вивчення дисципліни</i>)	відсутні
Чому це цікаво/треба вивчати	Побудова ефективної системи інформаційної безпеки та керування рівнем захищеності інформаційних ресурсів є необхідною умовою не тільки для підприємств, бізнесу, а також є необхідністю для освітнього простору
Перелік тем з дисципліни	Тема 1. Вступ до кібербезпеки в освіті. Поняття кібербезпеки в контексті освітнього середовища. Особливості цифрового простору закладів освіти. Типові загрози та вразливості в освітніх системах Тема 2. Персональні дані та їх захист. Законодавчі аспекти захисту персональної інформації. Робота з конфіденційними даними студентів та викладачів. Політика конфіденційності в навчальних платформах Тема 3. Безпека в цифровому навчальному середовищі Захист акаунтів, паролів, облікових записів. Основи кібергігієни для студентів і викладачів. Загрози при використанні електронних журналів, LMS, хмарних сервісів. Тема 4. Протидія соціальній інженерії та фішингу в освітньому просторі Методи впливу на користувача з метою отримання доступу. Типові приклади атак на студентів і працівників ЗВО. Алгоритми реагування та навчання користувачів Тема 5. Кіберінциденти в освітній сфері: аналіз та реагування Класифікація інцидентів у навчальних закладах. План дій у разі витоку інформації або атак. Впровадження політик інформаційної безпеки Тема 6. Етичні аспекти кібербезпеки в освіті Академічна доброчесність та цифрова етика. Використання ШІ, плагіат, порушення авторського права. Відповідальність за порушення цифрової безпеки Тема 7. Кібербезпека дистанційного та

	змішаного навчання Ризики, пов'язані з відеоконференціями та онлайн-оцінюванням. Технічні рішення для захисту віртуальних аудиторій Поведінкові та технічні рекомендації для безпечного навчання.
Як можна користуватися набутими знаннями і уміннями (<i>компетентність</i>)	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки
Очікувані результати навчання	1. Здатність аналізувати загрози кібербезпеці в освітньому середовищі та обґрунтовувати вибір відповідних методів захисту інформації. 2. Здатність застосовувати основні принципи кібергігієни, технічні та організаційні засоби для захисту персональних даних і цифрових ресурсів в освітньому процесі. 3. Здатність виявляти, оцінювати та реагувати на кіберінциденти в навчальних платформах та інформаційно-комунікаційних системах закладів освіти.
Інформаційне забезпечення	Конспект лекцій, методичні вказівки щодо практичних занять
Види навчальних занять (<i>лекції, практичні, семінарські, лабораторні заняття тощо</i>)	Лекції і практичні заняття
Вид семестрового контролю	диференційований залік
Максимальна кількість здобувачів на семестр/ Мінімальна кількість здобувачів (<i>тільки для мовних, творчих дисциплін, за необхідності</i>)	Без обмежень