Анотація навчальної дисципліни

Назва поля	Опис
Назва дисципліни	Цифрова криміналістика
Статус	Вільного вибору
Спеціальність	F5 Кібербезпека та захист інформації
Мова викладання	Українська
Кількість студентів, які можуть одночасно навчатися (мінімальна кількість)	15
Семестр, у якому викладається	7
Кількість: – кредитів ЄКТС – академічних годин (вказувати окремо лекції, лабораторні, практичні, самостійна робота студента)	кредити ЄКТС – 3 загальний обсяг годин – 90 годин аудиторних годин – 52 годин лекцій – 24 годин лабораторних – 24 годин практичних – 4 години самостійна робота – 38 годин
Форма підсумкового контролю	Диференційований залік
Викладач, що планується до викладання (окремо по навантаженнях)	Прокопенко Денис Петрович
Циклова комісія, що забезпечує викладання	Комп'ютерної інженерії, кібербезпеки та механіки
Попередні вимоги до вивчення дисципліни (якщо доречно)	Для успішного опанування дисципліни студент повинен мати базові знання та навички, отримані під час вивчення освітніх компонентів «Операційні системи та їх захист», «Програмування», «Захист комп'ютерних систем та мереж», «Моніторинг та тестування систем кібербезпеки», «Основи криптографічного захисту інформації». Студент повинен розуміти принципи функціонування операційних систем, файлових систем, мережевих протоколів та інформаційно-телекомунікаційних систем, володіти базовими навичками аналізу журналів подій, роботи з командним рядком та інструментами діагностики. Бажаними є

	знання основ кіберінцидентів, механізмів їх виникнення та методів реагування.
Перелік компетентностей, яких набуде студент після опанування дисципліни	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та розуміння професійної діяльності. ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК5. Здатність до пошуку, оброблення та аналізу інформації. ЗК8. Здатність працювати в команді. СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки. СК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах та забезпечення кібербезпеки. СК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. СК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики кібербезпеки. СК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою кібербезпеки. СК13. Здатність аргументувати вибір методів розв’язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати та захищати прийняті

	рішення.
Сфера реалізації компетентностей в майбутній професії	- проведення цифрових розслідувань інцидентів кібербезпеки з метою встановлення джерела, способу та наслідків несанкціонованого втручання; - виявлення, фіксація, збереження та аналіз цифрових доказів з комп'ютерних систем, мобільних пристроїв та мережевої інфраструктури; - аналіз журналів подій, мережевого трафіку та файлових систем для встановлення обставин кіберінцидентів; - участь у процедурах реагування на інциденти та відновлення штатного функціонування інформаційних систем; - підготовка експертних висновків і аналітичних звітів для внутрішніх служб безпеки, керівництва або правоохоронних органів; - робота у підрозділах інформаційної безпеки IT-компаній, фінансових установ, державних організацій та службах реагування на кіберінциденти.
Особливості навчання на курсі	Курс має практико-орієнтований характер і спрямований на формування навичок проведення цифрових розслідувань у сфері кібербезпеки. Навчання передбачає виконання лабораторних робіт із використанням спеціалізованих інструментів цифрової криміналістики для аналізу носіїв інформації, журналів подій, мережевого трафіку та інших цифрових артефактів. Особлива увага приділяється дотриманню процедур збереження цифрових доказів, забезпеченню їх цілісності, документуванню результатів досліджень та підготовці експертних висновків. Розглядаються правові та етичні аспекти діяльності фахівця з цифрової криміналістики. Навчальний процес включає моделювання

	типових сценаріїв кіберінцидентів, аналіз реалістичних кейсів та виконання індивідуальних практичних завдань, що відображають реальні умови професійної діяльності.
Стислий опис дисципліни	Дисципліна «Цифрова криміналістика (Digital Forensics)» орієнтована на формування знань і практичних навичок виявлення, фіксації, збереження та аналізу цифрових доказів у межах розслідування інцидентів кібербезпеки. Основна увага приділяється методам дослідження комп'ютерних систем, мобільних пристроїв, мережевого середовища та файлових систем із дотриманням встановлених процедур і вимог законодавства. Студенти набувають навичок аналізу журналів подій, мережевого трафіку, відновлення видалених даних, документування результатів розслідування та підготовки експертних висновків. Курс поєднує теоретичну підготовку з практичними завданнями, що моделюють реальні ситуації у сфері кібербезпеки та реагування на кіберінциденти.