Опис освітнього компонента вільного вибору

Освітній компонент	Вибіркова дисципліна 5 «Кібергігієна»
Рівень ВО	перший (бакалаврський)
Назва спеціальності/освітньо-професійної програми	262 Правоохоронна діяльність / Правоохоронна діяльність
Форма навчання	денна і заочна
Курс, семестр, протяжність	2 курс, 4 семестр, один семестр
Семестровий контроль	залік
Обсяг годин (усього: з них лекції/практичні)	120 год, з них: дфн – лекц. – 24 год, практ. – 32 год зфн – лекц. – 6 год, практ. – 10 год
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Кримінального права і процесу
Автор ОК	**Гусак Андрій Петрович,** к.ю.н., доцент, доцент кафедри кримінального права і процесу **Бендовський Григорій Валерійович,** завідувач криміналістичної лабораторії
Короткий опис	
Вимоги до початку вивчення	Базові знання та навички користування цифровими продуктами
Що буде вивчатися	Цей курс покликаний озброїти здобувачів освіти необхідними знаннями та навичками для підтримання безпечного та надійного цифрового середовища. У сучасному світі кібербезпека має першочергове значення, а кібергігієна відіграє ключову роль у захисті конфіденційної інформації та запобіганні кіберзагрозам. Цей курс знайомить здобувачів освіти з основними передовими практиками кібергігієни, які є важливими для окремих осіб та організацій, щоб захистити себе від різних кіберризиків.
Чому це цікаво/треба вивчати	Розуміння основ кібергігієни: здобувачі освіти отримають всебічне розуміння концепцій кібергігієни, включаючи важливість підтримки сильної позиції кібербезпеки, наслідки нехтування базовими заходами безпеки та роль кібергігієни у запобіганні кіберінцидентам. Ідентифікація загроз кібербезпеки: здобувачі освіти дізнаються про різні загрози кібербезпеки та вектори атак, такі як шкідливе програмне забезпечення, фішинг, соціальна інженерія, програми-вимагачі тощо. Впровадження надійного управління паролями:

	здобувачі освіти дізнаються про важливість використання надійних паролів і навчаться створювати, керувати та безпечно зберігати паролі, щоб мінімізувати ризик несанкціонованого доступу до своїх облікових записів і систем. Практика безпечного перегляду веб-сторінок та користування електронною поштою: Будуть розглянуті найкращі практики безпечного користування Інтернетом та електронною поштою, які допоможуть визначити потенційно небезпечні веб-сайти, вкладення та посилання, а також розпізнати поширені спроби фішингу. Захист особистої інформації: здобувачі освіти навчяться захищати свою особисту інформацію в Інтернеті та зрозуміють важливість відповідального обміну даними для зменшення ризику крадіжки особистих даних та порушення конфіденційності. Розуміння ризиків соціальних мереж: Курс розглядає потенційні ризики, пов'язані з використанням соціальних мереж, включаючи надмірне поширення інформації та налаштування конфіденційності, що дозволить слухачам безпечніше керувати своєю присутністю в Інтернеті.
Чому можна навчитися (результати навчання)	РН 3. Збирати необхідну інформацію з різних джерел, аналізувати і оцінювати її. РН 4. Формулювати і перевіряти гіпотези, аргументувати висновки. РН 8. Здійснювати пошук інформації у доступних джерелах для повного та всебічного встановлення необхідних обставин. РН 10. Виокремлювати юридично значущі факти і формувати обґрунтовані правові висновки. РН 11. Знати і розуміти сучасні правові доктрини, цінності та принципи функціонування національної правової системи.
Як можна користуватися набутими знаннями й уміннями (компетентності)	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності. ЗК 4. Здатність використовувати інформаційні та телекомунікаційні технології. СК 4. Здатність до критичного та системного аналізу правових явищ і застосування набутих

	знань та навичок у професійній діяльності. СК 9. Здатність ефективно застосовувати сучасні техніку і технології захисту людини, матеріальних цінностей і суспільних відносин від проявів криміногенної обстановки та обґрунтовувати вибір засобів та систем захисту людини і суспільних відносин. СК 14. Здатність до використання технічних приладів та спеціальних засобів, інформаційно-пошукових систем та баз даних СК 18. Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об’єктів критичної інфраструктури. СК 20. Здатність вживати заходів з метою запобігання, виявлення та припинення адміністративних і кримінальних правопорушень, заходів, спрямованих на усунення загроз життю та здоров’ю фізичних осіб та публічній безпеці.