ОПИС ВИБІРКОВОГО ОСВІТНЬОГО КОМПОНЕНТА

Назва освітнього компонента	Безпека комп’ютерних систем
Факультет	Природничо-математичної та технологічної освіти
Кафедра	Професійної освіти та технологій за профілями
ПІБ НПП або ПП, науковий ступінь, вчене звання (за наявності)	Гедзик Андрій Андрійович – доктор філософії, старший викладач
Рівень (рівні) вищої освіти	Перший (бакалаврський)
Загальний обсяг освітнього компонента	4 кредити ЄКТС / 120 годин
Семестр (семестри) вивчення	8 семестр
Форма підсумкового контролю	Залік
Мова викладання	Українська
Форми здобуття освіти та розподіл годин	Денна: лекції – 20; практичні/семінарські/лабораторні – 20; самостійна робота – 80. Заочна: лекції – 8; практичні/семінарські/лабораторні – 8; самостійна робота – 104.
Коротка анотація та мета	Дисципліна присвячена вивченню базових принципів безпечної роботи з комп'ютерною технікою та в мережах. Курс охоплює практичні аспекти захисту персональних та робочих даних, безпечного налаштування спільного доступу до файлів та базової протидії поширеним комп'ютерним вірусам і шахрайству в інтернеті. Мета: Опанування принципів інформаційної безпеки та кібергігієни, необхідних для надійного захисту робочих даних, безпечного налаштування локальних комп'ютерних мереж, розмежування прав доступу до ресурсів та роботи із захищеним електронним документообігом.
Компетентності та/або результати навчання, що формуються або поглиблюються	Здатність здійснювати базове конфігурування операційних систем з урахуванням вимог інформаційної безпеки (налаштування політик парольного захисту, управління локальними обліковими записами та їхніми привілеями). Уміння організовувати захищену мережеву взаємодію на рівні локальних мереж, керувати політиками доступу та розмежуванням прав користувачів до спільних інформаційних ресурсів. Здатність застосовувати сервіси електронної довіри та засоби криптографічного захисту інформації для надійної автентифікації користувачів, підписання документів та захисту електронного документообігу. Уміння ідентифікувати актуальні кіберзагрози (соціальна інженерія, фішинг, шкідливе програмне забезпечення) та застосовувати штатні і спеціалізовані програмні засоби захисту (антивірусні комплекси, брандмауери) для протидії їм. Здатність розробляти та реалізовувати заходи із забезпечення цілісності та доступності даних, включаючи організацію надійного зберігання,

	резервного копіювання та відновлення критично важливої інформації.
Пререквізити / рекомендований рівень підготовки	Успішне засвоєння базових тем з навчальних дисциплін «Інформатика та інформаційно-комунікаційні технології» та «Програмне забезпечення» (або їх аналогів, що формують загальну цифрову грамотність). Володіння практичними навичками роботи з персональним комп'ютером на рівні впевненого користувача (розуміння структури файлової системи, вміння керувати файлами та папками). Базовий досвід роботи в середовищі сучасних графічних операційних систем (вміння здійснювати базові налаштування ОС, встановлювати та запускати стандартне програмне забезпечення). Загальне розуміння принципів пошуку інформації в мережі Інтернет, роботи з веб-браузерами та електронною поштою.
Мінімальна та максимальна чисельність групи	