	Силабус навчальної дисципліни Основи кібербезпеки Освітньо-професійна програма Автоматизація, комп`ютерно-інтегровані технології та робототехніка  Спеціальність 174 «Автоматизація, комп`ютерно-інтегровані технології та робототехніка» Галузь знань 17 Електроніка, автоматизація та електронні комунікації
Рівень освіти	Фахова передвища освіта
Освітньо-професійний/ освітній ступінь	Фаховий молодший бакалавр
Статус навчальної дисципліни	Нормативна
Семестр	7
Обсяг дисципліни (кредити ЄКТС/загальна кількість годин)	5 кредити ЄКТС / 150 годин
Мова викладання	Українська
Оригінальність навчальної дисципліни	Вивчення курсів Endpoint Security та Cyber Threat Management мережної академії Cisco
Мета навчальної дисципліни	Метою вивчення дисципліни є дослідження характеристик і тактик кіберзлочинців. Під час вивчення дисципліни здобувачі освіти заглиблюється в технології, продукти і процедури професіоналів боротьби з кіберзлочинністю. Данна дисципліна допоможе розвинути навички, необхідні для роботи в якості IT-фахівця.
Заплановані результати навчання	Інтегральні компетентності: ІК1. Здатність вирішувати типові спеціалізовані задачі в галузі автоматизації та комп'ютерно-інтегрованих технологій, або у процесі навчанні, що вимагає застосування положень і методів відповідних наук та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності; здійснювати контроль інших осіб у визначених ситуаціях. Загальні компетентності: ЗК1. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК4. Навички використання інформаційних і комунікаційних технологій. ЗК5. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК6. Здатність здійснювати безпечну діяльність. Спеціальні (фахові, предметні) компетентності: СК1. Здатність застосовувати базові знання математики в обсязі, необхідному для використання математичних методів у галузі автоматизації. СК3. Здатність застосовувати знання про основні принципи та методи вимірювання основних технологічних параметрів, необхідних для обслуговування систем автоматизації. СК5. Здатність оцінювати сучасний стан технічного та програмного забезпечення. СК7. Здатність застосовувати новітні технології в галузі автоматизації; використовувати комп'ютерно-інтегровані технології для збору даних та їх архівування; створювати бази даних параметрів процесу та їх візуалізації за допомогою засобів людино-машинного інтерфейсу. Результати навчання: РН16. Проводити інсталяцію та налаштування системного та прикладного програмного забезпечення, у тому числі програмних засобів захисту

	інформації з метою реалізації встановленної політики інформаційної безпеки.
Заплановані знання та вміння	Вміти: • здійснювати вибір, розробляти, розгортати, інтегрувати, діагностувати, адмініструвати та експлуатувати комп'ютерні системи та мережі, мережеві ресурси, сервіси та інфраструктуру організації; • ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їх компонентів шляхом використання аналітичних методів і методів моделювання; • використовувати сучасні інтегровані середовища, методи і технології розробки, впровадження, адміністрування комп'ютерних систем та мереж. Знати: • теоретичні положення, що лежать в основі функціонування апаратних та програмних засобів комп'ютерної інженерії; • основи мережного з'єднання і передавання даних; • IP-адресацію; • взаємодія між мережами; • взаємодія мережних застосунків; - основи мережної безпеки.
Навчальна логістика	Зміст навчальної дисципліни: Теми розділу 1. Кібербезпека: загрози, вразливості та атаки. Захист мереж. Атаки на базові функції. Загрози корпоративній діяльності. Бездротовий мережний зв'язок. Інфраструктура мережної безпеки. Безпека в операційній системі Windows. Безпека в операційній системі Linux. Захист системи та кінцевої точки. Принципи, методи та процеси кібербезпеки. Теми розділу 2. Управління та відповідність. Тестування безпеки мережі. Аналіз кіберзагроз. Оцінка вразливостей кінцевого пристрою. Управління ризиками та контроль безпеки. Цифрова експертиза, аналіз інцидентів і реагування. Види занять: лекції, лабораторні заняття. Методи навчання: – вербальні/словесні (пояснення, розповідь, бесіда); – лабораторні (лабораторні заняття); пояснювально-ілюстративний або інформаційно-рецептивний, який передбачає пред'явлення готової інформації викладачем та її засвоєння здобувачами фахової передвищої освіти.
Пререквізити	Даний предмет базується на знаннях, отриманих при вивченні предмету «Операційні системи та системне програмне забезпечення».
Постреквізити	Теоретичні знання і практичне вміння які отримані в процесі вивчення предмету є базою для навчальної та виробничої практик, а також кваліфікаційної роботи.
Рекомендовані навчально-методичні матеріали для вивчення навчальної дисципліни	Основна та допоміжна література 1. www.netacad.com, курс Endpoint Security. 2. Конспект викладача Гринченко О.С. 3. А. М. Десятко. Кібергігієна. Кібербезпека. Безпека держави. Матеріали наукових семінарів Київ, 2020 4. В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. Інформаційна та кібербезпека: соціотехнічний аспект. Київ ДУТ, 2015 5. Лісовська Ю.П. Кібербезпека: ризики та заходи. Видавничий дім «Кондор», 2019 6. О.Довгань. Кібербезпека в інформаційному суспільстві. Національна

	бібліотека України ім. В.І.Вернадського, 2024
Матеріально-технічне забезпечення	Програмне забезпечення Microsoft Word, Cisco Packet Tracer, Wireshark, VirtualBox
Семестровий контроль, критерії оцінювання	Форма семестрового контролю – екзамен. Контроль і оцінка результатів освоєння дисципліни здійснюється у процесі проведення лабораторних робіт та тестування. Оцінка «відмінно» виставляється за глибокі знання навчального матеріалу з дисципліни «Основи кібербезпеки», що міститься в основних і додаткових рекомендованих літературних джерелах, вміння чітко, лаконічно, логічно послідовно відповідати на поставлені питання, вміння застосовувати теоретичні положення при розв'язуванні практичних задач, узагальнювати опанований матеріал, самостійно користуватися джерелами інформації, приймати рішення; Оцінка «добре» виставляється за міцні знання навчального матеріалу, включаючи алгоритми, моделі, діаграми, аргументовані відповіді на поставлені питання, вміння застосовувати теоретичні положення при розв'язанні практичних задач, вміння аналізувати й систематизувати інформацію, використовувати загальновідомі докази із самостійною і правильною аргументацією; Оцінка «задовільно» виставляється за посередні знання навчального матеріалу, мало аргументовані відповіді, слабке застосування теоретичних положень при розв'язанні практичних задач; Оцінка «незадовільно» виставляється за незнання значної частини навчального матеріалу, суттєві помилки у відповідях на питання, невміння орієнтуватися при розв'язанні практичних задач, незнання основних фундаментальних положень. Дотримання академічної доброчесності здобувачами освіти передбачає: – самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей); дотримання норм законодавства про авторське право і суміжні права; надання достовірної інформації про результати власної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.
Циклова комісія	Комп'ютерних систем та мереж