	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)	4 кредити ЄКТС / 120 годин
Мова викладання	Українська
Оригінальність навчальної дисципліни	Вивчення курсу Endpoint Security 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	РН16. Спілкуватись усно та письмово з професійних питань українською та іноземною мовою.
Заплановані знання та вміння	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. ЗК1. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ЗК4. Здатність застосовувати знання у практичних ситуаціях. ЗК5. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК6. Здатність спілкуватися іноземною мовою. 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 забезпечувати захист інформації в комп’ютерних системах та мережах з метою реалізації встановленої політики інформаційної 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. Операційна система

	Windows. Конфігурація та моніторинг безпеки Windows. Огляд Linux. Базове адміністрування Linux. Захист системи та кінцевої точки. Принципи, методи та процеси кібербезпеки. 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 «Апаратне та програмне забезпечення ПК (IT Essentials)», «Операційні системи та системне програмне забезпечення» та навчальної практики «Операційні системи»
Постреквізити	Теоретичні знання і практичне вміння які отримані в процесі вивчення предмету є базою для вивчення предмету «Комп'ютерні системи та мережі «CCNAv7: Introduction to Networks», навчальної та виробничої практик, а також кваліфікаційної роботи.
Рекомендовані навчально-методичні матеріали для вивчення навчальної дисципліни	Основна та допоміжна література Основна література: 1. www.netacad.com, курс Endpoint Security. 2. О.Довгань. Кібербезпека в інформаційному суспільстві. Національна бібліотека України ім. В.І.Вернадського, 2024 3. Сілін Є.С., Кадубовський О.А. Основи кібербезпеки: навчальний посібник. Дніпро, 2023. – 200 с. 4. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2024.– №3 (березень) . – 339 с. Допоміжна література: 5. А. М. Десятко. Кібергігієна. Кібербезпека. Безпека держави. Матеріали наукових семінарів Київ, 2020 6. В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. Інформаційна та кібербезпека: соціотехнічний аспект. Київ ДУТ, 2015 7. Лісовська Ю.П. Кібербезпека: ризики та заходи. Видавничий дім «Кондор», 2019
Матеріально-технічне забезпечення	Програмне забезпечення Microsoft Word, Cisco Packet Tracer, Wireshark, VirtualBox
Семестровий контроль, критерії оцінювання	Форма семестрового контролю – залік. Контроль і оцінка результатів освоєння дисципліни здійснюється у процесі проведення лабораторних робіт та тестування. Критерії оцінювання з дисципліни «Основи кібербезпеки»: • «Відмінно»: Здобувач демонструє глибокі та всебічні знання матеріалу. Вільно орієнтується в сучасних кіберзагрозах та методах соціальної інженерії. Професійно володіє інструментами моніторингу й захисту ОС Windows та Linux: впевнено працює в CLI та PowerShell, аналізує системні процеси, реєстри та журнали подій. Здатний самостійно проводити аудит мережевої безпеки (сканування портів, аналіз DNS-трафіку), налаштовувати політики доступу та механізми шифрування.

	Відповіді аргументовані, з елементами творчого підходу до вирішення прикладних задач. • «Добре»: Здобувач виявляє міцні знання теоретичного матеріалу, знає основні типи вразливостей та атак. Впевнено виконує практичні завдання із захисту кінцевих вузлів, налаштовує базові функції безпеки в ОС Windows та Linux, використовує сканери вразливостей. Орієнтується в синтаксисі Linux Shell та PowerShell, проте може припускатися некритичних помилок у складних скриптах чи аналізі журналів, які здатний виправити самостійно. Вміння узагальнювати інформацію знаходиться на високому рівні. • «Задовільно»: Здобувач володіє базовими поняттями (класифікація ШПЗ, принципи парольного захисту), але практичні навички застосовує переважно за алгоритмом чи шаблоном. Здатний виконувати прості операції в терміналі (навігація, базові права доступу) та запускати антивірусний моніторинг. Виникають труднощі з інтерпретацією результатів мережевого сканування та аналізом трафіку без сторонньої допомоги. Відповіді на теоретичні питання мають поверхневий характер. «Незадовільно»: Здобувач не володіє значною частиною навчального матеріалу, не орієнтується в типах загроз. Відсутні навички роботи з командним рядком, віртуальними машинами та принципами розмежування прав доступу. Здобувач не здатний виконати практичні/лабораторні роботи навіть за наявності методичних вказівок.
Циклова комісія	Комп‘ютерних систем та мереж