Силабус навчальної дисципліни
«Основи кібербезпеки»
(назва навчальної дисципліни)
Освітньо-професійної програми: Комп'ютерна інженерія
(назва освітньо-професійної програми)
Спеціальність: 123 «Комп'ютерна інженерія»
(код та назва спеціальності)
Галузь знань: 12 «Інформаційні технології»
(шифр та назва галузі знань)

Рівень освіти	Фахова передвища освіта/вища освіта
Освітньо-професійний/ освітній ступінь	Фаховий молодший бакалавр/бакалавр
Статус навчальної дисципліни	Нормативна/вибіркова
Семестр	I
Обсяг дисципліни (кредити ЄКТС/загальна кількість годин)	3 кредитів ЄКТС / 90 годин
Мова викладання	Українська
Оригінальність навчальної дисципліни	Вивчення кусів Мережної Академії Cisco, Introduction to Cybersecurity та Cybersecurity Essentials
Мета навчальної дисципліни	Метою вивчення дисципліни є дослідження характеристик і тактик кіберзлочинців. Під час вивчення дисципліни курсанти 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	В процесі навчання студенти охоплюють основні знання і навички у всіх областях безпеки в кіберпросторі - інформаційна безпека, системна безпека, мережна безпека, мобільна безпека, фізична безпека, етика і закони, пов'язані технології, використання технологій захисту і пом'якшення у захисті бізнесу.
Заплановані знання та вміння	**В результаті вивчення дисципліни студент повинен керуватися загальними та спеціальними компетентностями:** • СК15. Здатність розрізняти типові загрози, атаки, проблеми захисту даних, поняття ідентифікації, методів аутентифікації, авторизації, основні типи засобів контролю цілісності даних, технології реагування на інциденти. **Та мати наступні програмні результати:** • РН 17. Налаштовувати локальну та групову політики безпеки комп'ютерних систем • РН 18 налаштовувати базову безпеку на маршрутизаторах та застосовувати знання з кібербезпеки в практичній діяльності **Вміти:** • описати характеристики злочинців і героїв в сфері кібербезпеки;

	• описати, які принципи конфіденційності, цілісності і доступності, пов'язані з станом даних і контрзаходами щодо кібербезпеки; • описати тактику, методи та процедури, які використовуються кіберзлочинцями; • описати, які технології, продукти і процедури використовуються для захисту конфіденційності та для забезпечення цілісності і високої доступності; • пояснити, як професіонали кібербезпеки використовують технології, процеси та процедури для захисту всіх компонентів мережі; • пояснити мету законів, пов'язаних з кібербезпекою. **Знати:** • характеристики злочинців і героїв в сфері кібербезпеки; • принципи конфіденційності, цілісності і доступності, пов'язані з станом даних і контрзаходами щодо кібербезпеки; • тактику, методи та процедури, які використовуються кіберзлочинцями; • технології, продукти і процедури які використовуються для захисту конфіденційності та для забезпечення цілісності і високої доступності; • як професіонали з кібербезпеки використовують технології, процеси та процедури для захисту всіх компонентів мережі; • мету законів, пов'язаних з кібербезпекою.
Навчальна логістика	**Зміст дисципліни:** **Розділ 1. Вступ до кібербезпеки** Теми розділу 1. Потреба у кібербезпеці. Атаки, поняття та методи. Захист даних і конфіденційність. Захист організації. Правові та етичні питання кібербезпеки, освіта і кар'єра. **Розділ 2. Основи кібербезпеки** Теми розділу 2. Світ експертів і злочинців. Куб кібербезпеки. Кібербезпека - загрози, вразливості та атаки. Мистецтво захисту таємниць. Мистецтво забезпечення цілісності. Концепція п'яти дев'яток. Захист домену кібербезпеки. Як стати спеціалістом з кібербезпеки.
Пререквізити	Захист інформації у комп'ютерних системах.
Постреквізити	Навчальна практика. Виробнича (технологічна) практика. Технічне обслуговування та діагностика ЕОМ та периферійні пристрої. Бездротові мережі та їх захист.
Рекомендовані навчально-методичні матеріали для вивчення навчальної дисципліни	1. www.netacad.com, курс Introduction to Cybersecurity та Cybersecurity Essentials 2. Конспект викладача Гринченко О.С. 3. Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов / Отв. ред. М.Б. Касенова; сост. О.В. Демидов и М.Б. Касенова. – М.: Статут, 2013. – с.] 4. Монаппа К.А. Анализ вредоносных программ / пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2019. – 452 с.: ил. 5. Эдриан Прутяну Как стать хакером: Сборник практических сценариев, позволяющих понять, как рассуждает злоумышленник / пер. с англ. Д. А. Беликова – М.: ДМК Пресс, 2020. –380 с.: ил.

	6. Камский В.А. Защита личной информации в интернете, смартфоне и компьютере. — СПб.: Наука и Техника, 2017. — 272 с., ил. 7. Масалков А.С. Особенности киберпреступлений в России: инструменты нападения и защиты информации. – М.: ДМК Пресс, 2018. – 226 с.: ил.
Матеріально-технічне забезпечення	Програмне забезпечення Cisco Packet Tracer, Oracle VM VirtualBox. Образ Linux Ubuntu_CyberEss
Семестровий контроль, критерії оцінювання	Форма семестрового контролю – залік. Контроль і оцінка результатів освоєння дисципліни здійснюється у процесі проведення лабораторних робіт, тестування та проведення комплексної контрольної роботи. 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/ кафедра	Комп'ютерних систем та мереж