	Силабус навчальної дисципліни **«Основи кібербезпеки»** **(назва навчальної дисципліни)** **Освітньо-професійної програми: Інженерія програмного забезпечення** **(назва освітньо-професійної програми)** **Спеціальність: 121 «Інженерія програмного забезпечення»** **(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	6
Обсяг дисципліни (кредити ЄКТС/загальна кількість годин)	4 кредити ЄКТС / 120 годин
Мова викладання	Українська
Оригінальність навчальної дисципліни	Вивчення кусу мережної Академії Cisco, 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 отримуємо наступні програмні результати:** ● РН 16. Впроваджувати та обслуговувати комп’ютерні мережі різного виду та призначення. ● РН 17 Проводити інсталяцію та налаштування системного та прикладного

	програмного забезпечення, у тому числі програмних засобів захисту інформації з метою реалізації встановленої політики інформаційної безпеки **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. **Види занять:** лекції, лабораторні заняття. **Методи навчання:** - вербальні/словесні (пояснення, розповідь, бесіда); - практичні (практичні заняття); - пояснювально-ілюстративний або інформаційно-рецептивний, який передбачає пред'явлення готової інформації викладачем та її засвоєння здобувачами фахової передвищої освіти.
Пререквізити	Безпека програм та даних
Постреквізити	
Рекомендовані навчально-методичні матеріали для вивчення навчальної дисципліни	1. www.netacad.com, курс Cybersecurity Essentials. 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, 2020
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