	Силабус навчальної дисципліни **«Менеджмент командної розробки систем захисту»** **Галузь знань: 12 «Інформаційні технології»** **Спеціальності: 122 «Комп'ютерні науки»** **Освітні програми: «Обслуговування програмних систем та комплексів»**
Статус дисципліни	Навчальна дисципліна є *вибірковою*
Курс	3
Семестр	6
Обсяг дисципліни, кредити ЄКТС / загальна кількість годин	3 кредитів /90 год.
Мова викладання	**українська**
Що буде вивчатися (предмет навчання)	Дисципліна "Менеджмент командної розробки систем захисту" спрямована на вивчення стратегій, методів та інструментів управління процесом розробки та впровадження захисних систем та технологій. Студенти освоюють принципи командної роботи в контексті проектів зі збереження та захисту інформації, де акцент здійснюється на плануванні, організації та контролі за виконанням завдань в рамках команди. Вивчаються методи управління ризиками в області кібербезпеки, а також принципи побудови ефективних комунікаційних стратегій між учасниками проекту. Курс розглядає сучасні стандарти індустрії з захисту інформації та надає інструменти для ефективного планування та реалізації заходів з кібербезпеки в умовах командної розробки. Також звертає увагу на важливість етичних та юридичних аспектів у сфері захисту даних та принципи створення безпечних інформаційних систем.
Чому це цікаво / необхідно вивчити (мета)	Вивчення дисципліни "Менеджмент командної розробки систем захисту" має ключове значення в сучасному цифровому середовищі. Ця область відкриває розуміння не лише технічних аспектів створення захисних систем, але й важливість співпраці та ефективного керування командами для успішної розробки та впровадження кібербезпечних рішень. Вивчення цього курсу дає можливість освоїти стратегії та методи управління проектами у сфері кібербезпеки, вирішувати складні завдання у командному середовищі та ефективно координувати роботу забезпечення безпеки даних. Це надає унікальні навички, важливі для розвитку кар'єри в сфері інформаційної безпеки, дозволяючи стати ключовим фахівцем у сфері захисту від кіберзагроз та управління проектами з цього напрямку.

Чому можна навчитись (компетентності)	Інтегральна компетентність Здатність вирішувати типові спеціалізовані задачі в галузі інформаційних технологій або у процесі навчання, що вимагає застосування положень і методів комп'ютерних наук та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності; здійснювати контроль інших осіб у визначених ситуаціях Загальні компетентності: ЗК2. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя ЗК5. Знання та розуміння предметної області та розуміння професійної діяльності ЗК8. Здатність вчитися і оволодівати сучасними знаннями СК2. Здатність використовувати теоретичні та фундаментальні знання в галузі комп'ютерних наук та інформаційних технологій для вирішення різноманітних проблем; СК9. Здатність застосовувати знання сучасних методів і технологій створення та супроводження розподілених систем. Результати навчання: РН01. Аналізувати явища і події соціально-політичного, культурного, духовного середовища для формування світогляду людини та встановлювати зв'язок між ними
Як можна користуватись набутими знаннями і вміннями (результати навчання)	Набуті знання та вміння з дисципліни "Менеджмент командної розробки систем захисту" виявляються надзвичайно корисними в сучасному цифровому ландшафті. Ці компетенції дозволяють керувати складними проектами у сфері кібербезпеки, встановлювати ефективний процес комунікації та співпраці в командах, а також управляти ризиками та вирішувати виклики в області захисту даних. Вони можуть бути використані у різних сферах, від IT-компаній до фінансових установ та урядових органів, де кібербезпека стає дедалі більш важливою. Ці навички стають основою для розвитку кар'єри в області інформаційної безпеки, консалтингу чи управління проектами, де знання процесів командної роботи та експертиза у сфері кіберзахисту стають ключовими факторами успіху.
Постреквізити	«Переддипломни практика», «Технологія захисту інформації»
Навчальна логістика	Основи командної роботи та управління проектами в області кібербезпеки. Стратегії планування та виконання захисту інформації. Методи визначення та оцінки ризиків у кібербезпеці. Комунікаційні моделі в командному середовищі захисту даних. Управління проектами з реалізації заходів кібербезпеки в організаціях. Аналіз вразливостей та стратегії захисту від кібератак. Керування ефективністю та моніторинг проектів в сфері кібербезпеки. Правові аспекти та етика в області кіберзахисту та інформаційної безпеки. Управління змінами та впровадження інновацій в системи захисту. Створення та вдосконалення стратегій реагування на кіберзагрози та кіберінциденти.

Політика навчальної дисципліни, оцінювання результатів навчання та академічна доброчесність	***Політика щодо відвідування та проведення занять***. Під час лекцій, практичних та лабораторних занять використовуються різноманітні інтерактивні технології навчання, які допомагають не тільки засвоїти теми курсу, а й розвинути навички критичного мислення, уміння працювати з інформацією, презентувати результати власних досліджень. Передбачається обов'язкова присутність студента на кожному занятті, тому що для отримання ефекту занурення у проблематику дисципліни необхідне групове обговорення певних завдань та шляхи їх вирішення («мозковий штурм»). Слід відзначити, що через відсутність студента на занятті можна втратити логіку опанування теоретичного та практичного матеріалу, якою пов'язані всі теми курсу. Як правило, викладач попереджає це на вступній лекції, на який відбувається знайомство зі структурно-логічною схемою курсу. У випадку, якщо була поважна причина відсутності студента на занятті, необхідно відвідати консультацію та з викладачем обговорити проблемні питання теми або низки тем через розбір «скрізних» питань, виконати практичні завдання. Під час вивчення курсу можна використовувати як рекомендовану літературу, так й різні інформаційні ресурси. Викладач контролює якість інформації, яку використовують здобувачі під час виконання завдань, вчить їх працювати з науковою інформацією, формує навички відрізняти якісну інформацію від неякісної. Мобільні пристрої під час проведення занять дозволяється використовувати лише для навчальних та наукових цілей. ***Політика щодо академічної доброчесності***. Політика щодо академічної доброчесності побудована на основі Положення про академічну доброчесність в ВСП «ФКЗІ ДУІТЗ». Усі види письмових робіт повинні бути написані здобувачами самостійно та мати високий рівень оригінальності. До заліку допускаються здобувачі, які виконали індивідуальне завдання. Здобувач, який не з'явився на залік або не був допущений на момент його проведення, має право повторно його пройти у визначені викладачем терміни під час консультацій/ відпрацювань. ***Загальна оцінка з дисципліни*** – максимум 100 балів. У випадку отримання менше 60 балів, здобувач обов'язково здійснює перескладання для ліквідації академічної заборгованості.
Локація та	***Навчальна аудиторія*** (дошка, проектор, ноутбук, інше

матеріально-технічне забезпечення	обладнання). ***Дистанційна*** – сучасні платформи та онлайн-сервіси дистанційного навчання.
Семестровий контроль	*залік*
Циклова комісія	інформаційних технологій