	Силабус навчальної дисципліни **«Захист інфраструктури веб додатку»** **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	5
Обсяг дисципліни, кредити ЄКТС / загальна кількість годин	4 кредитів /120 год.
Мова викладання	**українська**
Що буде вивчатися (предмет навчання)	У курсі "Захист інфраструктури веб-додатків" розглядаються ключові аспекти забезпечення безпеки та захисту веб-додатків від потенційних кіберзагроз. Студенти отримують знання про основні вразливості, що можуть виникати в веб-додатках та методи їх запобігання. Це включає аналіз можливих атак, таких як SQL-ін'єкції, перехоплення сесій, XSS або CSRF, та розробку стратегій захисту від них. Основна увага приділяється розробці та використанню заходів безпеки на різних рівнях: від налагодження правильних конфігурацій серверів до використання шифрування та механізмів аутентифікації. Студентам надаються практичні вміння для тестування на проникнення, виявлення потенційних слабких місць та розробки стратегій усунення вразливостей, що робить цей курс надзвичайно корисним для розробників та адміністраторів, які працюють з веб-додатками.
Чому це цікаво / необхідно вивчити (мета) доступом	Вивчення захисту інфраструктури веб-додатків стає надзвичайно цікавим у зв'язку зі зростанням цифрового середовища та поширенням онлайн-платформ. Цей курс дозволяє студентам розуміти потенційні загрози, з якими може стикнутися будь-який веб-додаток, і вчить ефективно захищати їх від цих загроз. Це надзвичайно актуально, оскільки безпека веб-додатків стає пріоритетом у сфері інформаційної безпеки. Студенти, які опановують цей курс, здатні розробляти ефективні стратегії захисту, виявляти вразливості та миттєво реагувати на потенційні кіберзагрози. Це дозволяє їм стати цінними фахівцями в галузі кібербезпеки та забезпечує широкі можливості у сфері розробки веб-додатків та інформаційних технологій.

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: ЗК5. Знання та розуміння предметної області та розуміння професійної діяльності. ЗК8. Здатність вчитися і оволодівати сучасними знаннями. Спеціальні (фахові, предметні) компетентності: СК2. Здатність використовувати теоретичні та фундаментальні знання в галузі комп'ютерних наук та інформаційних технологій для вирішення різноманітних проблем. СК6. Здатність застосовувати методи та засоби захисту програмного забезпечення та даних від несанкціонованого доступу в умовах супроводження та експлуатації програмних систем і комплексів Результати навчання: РН07. Застосовувати основні механізми та методи безпеки мереж і програмних систем.
Як можна користуватись набутими знаннями і вміннями (результати навчання)	Набуті знання та вміння у захисті інфраструктури веб-додатків стають цінним активом у сфері інформаційної безпеки. Ці компетенції можна використовувати для розробки та вдосконалення безпечних веб-продуктів, а також для аудиту та виявлення потенційних вразливостей у вже існуючих системах. Знання про ризики та загрози кібербезпеки дозволяють ефективно впроваджувати заходи захисту, працювати зі стандартами безпеки та впроваджувати стратегії для запобігання можливим атакам. Це відкриває можливості для розвитку кар'єри у сферах кібербезпеки, аудиту безпеки, консультування або роботи в IT-компаніях, де захист веб-додатків є пріоритетом. Такі знання дозволяють стати ключовим гравцем у галузі інформаційної безпеки та відкривають двері до різноманітних можливостей для використання цих навичок у практичній роботі.
Пререквізити	«Основи телекомунікацій та комп'ютерні мережі»
Постреквізити	«Технологія захисту інформації»
Навчальна логістика	Огляд загроз та вразливостей веб-додатків Принципи безпеки веб-додатків Управління ідентифікацією та автентифікацією Захист від кросс-сайтових атак (XSS) Управління сесіями та захист від крадіжок сесій SQL-ін'єкції та їх запобігання Захист від атак на внедрення коду (Code Injection) Шифрування та безпека зв'язку Тестування на проникнення веб-додатків Управління безпекою веб-додатків: патчі, вразливості та аудит

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