| | |
|---|---|
| | **Силабус навчальної дисципліни**<br>**«Безпека розробки та підтримки додатків»**<br><br>**Галузь знань: 12 «Інформаційні технології»**<br>**Спеціальності: 122 «Комп'ютерні науки»**<br><br>**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 "Безпека розробки та підтримки додатків" вивчають широкий спектр тем, спрямованих на забезпечення безпеки програмних додатків на кожному етапі їхнього життєвого циклу. Це включає розуміння загроз безпеці, аналіз потенційних ризиків, вивчення стратегій захисту від кібератак, встановлення заходів безпеки, кодування з урахуванням вразливостей, тестування на проникнення, а також виявлення та усунення вад безпеки. Студенти ознайомляються з актуальними стандартами безпеки, методами шифрування даних, механізмами аутентифікації та авторизації, а також з основами кібербезпеки для забезпечення стійкості додатків до потенційних атак та вразливостей. Крім теоретичного матеріалу, цей курс спрямований на практичні вправи, які дозволяють студентам застосовувати отримані знання для створення безпечних програмних продуктів та виявлення потенційних проблем безпеки. |
| **Чому це цікаво / необхідно вивчити (мета)** доступом | Розуміння безпеки розробки та підтримки додатків стає надзвичайно важливим у світі, де цифрові технології використовуються широко та неперервно. Цей курс допомагає студентам освоїти ключові аспекти захисту програмних продуктів від потенційних кіберзагроз. У сучасному цифровому ландшафті безпека є не лише пріоритетом, а й необхідністю. Знання, отримані під час цього курсу, дають можливість розробникам та фахівцям з IT безпечно створювати та підтримувати програми, уникати потенційних вразливостей та захищати користувачів від можливих кіберзагроз, забезпечуючи надійність та конфіденційність відповідно до сучасних стандартів безпеки. Отримання цих навичок відкриває двері до кар'єрних можливостей у сфері розробки програмного забезпечення та кібербезпеки, що робить цей курс дуже важливим для майбутніх фахівців в галузі IT. |

| | |
|---|---|
| **Чому можна навчитись (компетентності)** | Інтегральна компетентність<br>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.<br>Загальні компетентності:<br>ЗК5. Знання та розуміння предметної області та розуміння професійної діяльності.<br>ЗК8. Здатність вчитися і оволодівати сучасними знаннями.<br>Спеціальні (фахові, предметні) компетентності:<br>СК2. Здатність використовувати теоретичні та фундаментальні знання в галузі комп'ютерних наук та інформаційних технологій для вирішення різноманітних проблем.<br>СК5. Здатність застосовувати принципи і методи побудови та використання мережевих технологій.<br>СК6. Здатність застосовувати методи та засоби захисту програмного забезпечення та даних від несанкціонованого доступу в умовах супроводження та експлуатації програмних систем і комплексів<br>СК8. Здатність застосовувати сучасні методи, технології та інструментальні засоби проєктування й створення програмних систем та їх супроводження<br>Результати навчання:<br>РН07. Застосовувати основні механізми та методи безпеки мереж і програмних систем. |
| **Як можна користуватись набутими знаннями і вміннями (результати навчання)** | Отримані під час цього курсу знання та навички з безпеки розробки програмних додатків відкривають різноманітні перспективи для практичного застосування. Вони дають можливість працювати у сферах розробки програмного забезпечення, аудиту безпеки, кібербезпеки та консультування з питань захисту даних. Ці знання дозволяють виявляти та усувати потенційні вразливості в програмах, розробляти безпечні програмні рішення та застосовувати найкращі практики в сфері кібербезпеки. Вони також можуть бути застосовані у власних проектах, дозволяючи забезпечити високий рівень захисту та конфіденційності в інформаційному середовищі. Такі знання стають невід'ємною складовою будь-якої сучасної ІТ-кар'єри, відкриваючи можливості для професійного зростання та розвитку в галузі інформаційної безпеки. |
| **Пререквізити** | «Основи телекомунікацій та комп'ютерні мережі» |
| **Постреквізити** | «Технологія захисту інформації», |
| **Навчальна логістика** | Основи кібербезпеки.Загрози кібербезпеці та основні принципи захисту в інформаційному середовищі.<br>Аудит безпеки.Методи та інструменти для виявлення вразливостей та оцінки ризиків безпеки програмних систем.<br>Створення безпечного коду. Безпека в процесі програмування, виявлення та усунення вразливостей, впровадження найкращих практик безпеки коду.<br>Захист даних. Шифрування, методи аутентифікації та авторизації, захист конфіденційної інформації.<br>Стратегії виявлення та реагування на кібератаки. Реагування на інциденти, методи виявлення та захист від кіберзагроз.<br>Управління безпекою програмних продуктів.Розробка та підтримка безпечних програмних додатків, управління безпекою в життєвому циклі програм. |

| | |
|---|---|
| **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.<br>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»).<br>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.<br>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.<br>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.<br>***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.<br>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.<br>***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).<br>***Дистанційна*** – сучасні платформи та онлайн-сервіси дистанційного навчання. |
| **Семестровий контроль** | *залік* |
| **Циклова комісія** | інформаційних технологій |