СИЛАБУС
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕХНОЛОГІЇ РОЗРОБКИ ЗАХИЩЕНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ID 4670

Шифр, назва спеціальності та освітній рівень	126 Інформаційні системи та технології (магістр)	Назва освітньої програми	Інформаційні системи та технології (2023)
Тип програми	Освітньо-професійна	Мова викладання	Українська
Факультет	Факультет комп'ютерно-інформаційних систем і програмної інженерії (ФІС)	Кафедра	Каф. комп'ютерних наук (КН)

Викладач/викладачі

Козак Руслан Орестович, канд. техн. наук, доцент, доцент, профіль на порталі "Науковці ТНТУ"

Загальна інформація про дисципліну

Мета курсу	Формування професійної компетентності майбутніх фахівців зі спеціальності Інформаційні системи та технології, достатньої для розробки захищеного програмного забезпечення. Завданням дисципліни є сформувати здатність обирати та застосовувати методи та засоби захисту програмного забезпечення на усіх стадіях життєвого циклу програмної системи В даній дисципліні розглядаються такі питання: життєвий цикл програмного забезпечення, вимоги безпеки до програмних систем, проектування програмних продуктів згідно із стандартами безпеки, створення безпечного коду, тестування безпеки програмного забезпечення, заходи із забезпечення безпеки програм на стадії розгортання та підтримки.
Формат курсу	Дисципліна передбачає проведення лекційних, лабораторних занять та консультацій. Для кращого розуміння та засвоєння викладеного матеріалу дисципліна має супровід у вигляді електронного курсу Тернопільський національний технічний університет ім. І. Пулюя (https://dl.tntu.edu.ua). Електронні навчальні курси мають лекційний матеріал, лабораторні роботи та систему тестування.
Компетентності ОП	ЗК05. Здатність оцінювати та забезпечувати якість виконуваних робіт. СК01. Здатність розробляти та застосувати ІСТ, необхідні для розв'язання стратегічних і поточних задач СК03. Здатність проектувати інформаційні системи з урахуванням особливостей їх призначення, неповної/недостатньої інформації та суперечливих вимог. СК05. Здатність використовувати сучасні технології аналізу даних для оптимізації процесів в інформаційних системах. СК06. Здатність управляти інформаційними ризиками на основі концепції інформаційної безпеки.
Програмні результати навчання з ОП	РН03 Приймати ефективні рішення з проблем розвитку інформаційної інфраструктури, створення і застосування ІСТ. РН10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації.
Обсяг курсу	**Очна (денна) форма здобуття освіти:** Кількість кредитів ECTS — 4,5; лекції — 30 год.; лабораторні заняття — 20 год.; самостійна робота — 85 год.;
Ознаки курсу	Рік навчання — 6; семестр — 11; Обов'язкова (для здобувачів інших ОП може бути вибірковою) дисципліна; кількість модулів — 2;
Форма контролю	Поточний контроль: Підсумковий контроль: екзамен
Компетентності та дисципліни, що є передумовою для вивчення	Студенти повинні володіти знаннями з дискретної математики, програмування, основ теорії інформації, розробки програмного забезпечення, комп'ютерних мереж. Вітаються знання з основ інформаційної безпеки, тестування програмного забезпечення.

Матеріально-технічне та/ або інформаційне забезпечення	Обладнання: персональні комп’ютери з доступом до інтернет, операційна система Microsoft Windows, Linux. Програмне забезпечення: Kali Linux, Oracle Virtual Box, VMware Workstation Burp Suite, bWAPP.

СТРУКТУРА КУРСУ

Теми занять, короткий зміст

Лекційний курс	Годин ОФЗО	ЗФЗО
1. Життєвий цикл програмного забезпечення (SDLC). Основні поняття та принципи інформаційної безпеки.	4	
2. Принципи побудови програмних систем. Принципи побудови безпечного програмного забезпечення.	4	
3. Компоненти життєвого циклу програмного забезпечення. Моделі розробки програмних систем.	2	
4. Атаки на програмне забезпечення: Buffer overflow, Cache poisoning.	2	
5. OWASP - Open Web Application Security Project.	4	
6. Вимоги інформаційної безпеки. Класифікація даних. Технології захисту програмного забезпечення.	4	
7. Атаки на програмне забезпечення: SYN Flooding attack, TCP Session Hijacking.	2	
8. Тестування безпеки програмного забезпечення.	2	
9. Механізми автентифікації та авторизації. Інфраструктура відкритих ключів	4	
10. Атаки на програмне забезпечення: Cross-site scripting (XSS), Cross-site request forgery (CSRF)	2	
РАЗОМ:	30	

Лабораторний практикум (теми)	Годин ОФЗО	ЗФЗО
1. Injection, Injection flaws, SQL, NoSQL, OS, LDAP	2	
2. Broken Authentication	2	
3. Sensitive Data Exposure	2	
4. XML External Entities (XXE)	2	
5. Broken Access Control	2	
6. Security Misconfiguration	2	
7. Cross-Site Scripting XSS	2	
8. Insecure Deserialization	2	
9. Using Components with Known Vulnerabilities	2	
10. Insufficient Logging & Monitoring	2	

РАЗОМ: 20

Курсова робота/проєкт

Мета виконання курсового проєкту	- поглиблення знань студентів з актуальних проблем захисту інформації в інформаційно-комунікаційних системах; - систематизація здобутих знань з навчальної дисципліни; - застосування здобутих знань та вмінь для вирішення практичних завдань; - розвиток умінь самостійного критичного опрацювання літературних джерел та міжнародних стандартів безпеки; - формування дослідницьких умінь студентів; - стимулювання студентів до самостійного наукового пошуку; - розвиток уміння аналізувати сучасний досвід та узагальнювати власні спостереження; - формування вміння практичної реалізації результатів дослідження проблеми в самостійно виконаних розробках.
Завдання курсового проєкту	Варіанти завдань на курсовий проєкт: 1. Розробка програмного забезпечення для: a. автоматизованого пошуку вразливостей в <назва системи> b. виявлення аномалій в мережевому трафіку c. для оцінювання ризиків інформаційної безпеки підприємства <назва підприємства> 2. Дослідження вразливостей інформаційних систем <назва сайту, програмного забезпечення>: a. на основі методології методології OWASP (або інша) b. методи усунення вразливостей c. з використанням динамічного та статичного аналізу коду 3. Дослідженням методів та засобів розробки захищеного програмного забезпечення на етапі: a. аналізу вимог b. проектування c. кодування d. розгортання та підтримки e. тестування 4. Аналіз стандартів та підходів до розробки захищеного програмного забезпечення: (зробити порівняльний аналіз різних комбінацій стандартів)
Структура курсового проєкту	Титульний лист; завдання на курсовий проєкт; анотація; зміст; перелік умовних позначень; вступ; основна частина; висновки; список використаних джерел; додатки.
Обсяг курсового проєкту	Рекомендований обсяг - 30-40 сторінок.
Етапи виконання	Вибір та затвердження теми курсового проєкту; критичний аналіз нормативно-правової бази, спеціальної літератури з проблем, що розглядаються, пошук додаткових джерел інформації; складання плану курсового проєкту; узагальнення та аналіз накопиченого матеріалу, обробка даних, обґрунтування пропозицій; написання тексту і оформлення курсового проєкту; захист курсового проєкту згідно з встановленим графіком.
Оцінювання курсового проєкту	Зміст курсового проєкту – 75 балів, захист курсового проєкту – 25 балів.

Форма контролю	Захист курсового проєкту передбачає: - стислу доповідь (5 хв.) магістранта, в якій необхідно відокремити мету, об’єкт, предмет дослідження та коротко висвітлити зміст одержаних результатів дослідження. Зробити акцент на висновках та рекомендаціях. Бажано, щоб доповідь магістранта під час захисту супроводжувалась презентацією результатів, підготовленою за допомогою засобів «Microsoft PowerPoint»; - співбесіду і відповіді на запитання наукового керівника та членів комісії. Курсовий проєкт та її захист оцінюється відповідно до вимог кредитно-модульної системи.
Технічне й програмне забезпечення	Технічні засоби для демонстрування результатів виконання курсового проєкту (ноутбук, проектор). Пакет програмних продуктів Microsoft Office.

ІНШІ ВИДИ РОБІТ

Теми, короткий зміст	

Інформаційні джерела для вивчення курсу

Рекомендована література

1. Gary McGraw. Software Security: Building Security In, 2006.
2. Gerardus Blokdyk. Software Security Vulnerability A Complete Guide, 2020.
3. Security in Software Engineering Notebook, Professional Notebook, Office Writing Notebook, Daily Notes & Action Items Notebook, 140 pages, 2021.
4. Adam Shostack. Threat Modeling: Designing for Security, 2014
5. Ірина Бородкіна, Георгій Бородкин. Інженерія програмного забезпечення. Посібник для студентів вищих навчальних закладів. – 2018. – 204 с.

Інформаційні ресурси

1. Електронні навчальні курси ТНТУ імені І. Пулюя: http://dl.tntu.edu.ua
2. OWASP Top Ten: https://owasp.org/www-project-top-ten/
3. An application cyber-attack: https://owasp.org/www-community/attacks/
4. CVE Program: https://cve.mitre.org/

Політики курсу

Політика контролю	Використовуються такі засоби оцінювання та методи демонстрування результатів навчання: поточне опитування; тестування; презентації результатів виконаних завдань; оцінювання результатів виконаних лабораторних робіт; бесіди та обговорення проблемних питань, дискусії; індивідуальні консультації; екзамен.
Політика щодо консультування	Консультації при вивченні дисципліни проводяться згідно затвердженого на кафедрі КБ. Консультування передбачено як очно ,так і з використанням ресурсів електронного навчального курсу у середовищі електронного навчання університету.
Політика щодо перескладання	Студент має право на повторне складання модульного контролю з метою підвищення рейтингу протягом тижня після складання модульного контролю за графіком. Перескладання екзамену відбувається в терміни, визначені графіком освітнього процесу. Здобувач ВО має право на зарахування результатів навчання здобутих у неформальній чи інформальній освіті.
Політика щодо академічної доброчесності	При складанні усіх видів контролю у середовищі електронного навчання завжди активується система розпізнавання особи, що складає контроль. Усі практичні роботи у ЕНК перевіряються вбудованою системою Антиплагіат. При складанні усіх форм контролю забороняється списування, у тому числі з використанням сучасних інформаційних технологій.
Політика щодо відвідування	Відвідування занять є обов'язковим компонентом освітнього процесу. За наявності поважних причин (наприклад, хвороба, особливі потреби, відрядження, сімейні обставини, участь у програмах академічної мобільності тощо) навчання може здійснюватися за індивідуальним графіком, погодженим з деканом факультету.

СИСТЕМА ОЦІНЮВАННЯ

Розподіл балів, які отримують студенти за курс

Модуль 1			Модуль 2			Підсумковий контроль		Разом з дисципліни
Аудиторна та самостійна робота			Аудиторна та самостійна робота			Теоретичний курс	Практичне завдання	100
Теоретичний курс (тестування)	Лабораторна робота		Теоретичний курс (тестування)	Лабораторна робота				
15	25		10	25		25	0	
№ лекції	Види робіт	К-ть балів	№ лекції	Види робіт	К-ть балів			
Тема 1	Лабораторна робота №1	5	Тема 6	Лабораторна робота №6	5			
Тема 2	Лабораторна робота №2	5	Тема 7	Лабораторна робота №7	5			
Тема 3	Лабораторна робота №3	5	Тема 8	Лабораторна робота №8	5			
Тема 4	Лабораторна робота №4	5	Тема 9	Лабораторна робота №9	5			
Тема 5	Лабораторна робота №5	5	Тема 10	Лабораторна робота №10	5			

Розподіл балів, які отримують студенти за виконання та захист КП

Модуль 1		Підсумковий контроль	Разом за КП
Виконання розділу 1		Захист КП	100
75		25	
Види робіт	К-ть балів		
Ступінь обґрунтування обраної ідеї захисту	20		
Правильність оформлення	15		
Оригінальність і самостійність вирішення поставленого завдання	30		
Обсяг і якість курсового проєкту	10		

Розподіл оцінок

Сума балів за навчальну діяльність	Шкала ECTS	Оцінка за національною шкалою
90-100	A	Відмінно
82-89	B	Добре
75-81	C	Добре
67-74	D	Задовільно
60-66	E	Задовільно
35-59	FX	Незадовільно з можливістю повторного складання
1-34	F	Незадовільно з обов’язковим повторним вивченням дисципліни

Затверджено рішенням кафедри КН, протокол №1 від «30» серпня 2023 року.