СИЛАБУС
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ID 4968

Шифр, назва спеціальності та освітній рівень	122 Комп’ютерні науки (бакалавр)	Назва освітньої програми	Комп’ютерні науки (2021) Computer science (2021)
Тип програми	Освітньо-професійна	Мова викладання	Українська
Факультет	Факультет комп'ютерно-інформаційних систем і програмної інженерії (ФІС)	Кафедра	Каф. кібербезпеки (КБ)

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 Комп'ютерні науки, 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	Загальні: ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК2. Здатність застосовувати знання у практичних ситуаціях. ЗК6. Здатність вчитися і оволодівати сучасними знаннями. ЗК7. Здатність до пошуку, оброблення й аналізу інформації з різних джерел. ЗК8. Здатність генерувати нові ідеї (креативність). ЗК11. Здатність приймати обґрунтовані рішення. Фахові: СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури.
Програмні результати навчання з ОП	ПР15. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних.
Обсяг курсу	**Очна (денна) форма здобуття освіти:** Кількість кредитів ECTS — 4,5; лекції — 32 год.; лабораторні заняття — 32 год.; самостійна робота — 71 год.; **Заочна форма здобуття освіти:**

	Кількість кредитів ECTS — 4,5; лекції — 6 год.; лабораторні заняття — 6 год.; самостійна робота — 123 год.;
Ознаки курсу	Рік навчання — 4; семестр — 7; Вибіркова дисципліна; кількість модулів — 2;
Форма контролю	Поточний контроль: захист лабораторних робіт Підсумковий контроль: залік
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	Годин ЗФЗО
1. Життєвий цикл програмного забезпечення (SDLC). Основні поняття та принципи інформаційної безпеки.	2	1
2. Принципи побудови програмних систем. Принципи побудови безпечного програмного забезпечення.	4	1
3. Компоненти життєвого циклу програмного забезпечення. Моделі розробки програмних систем.	4	0.5
4. Атаки на програмне забезпечення: Buffer overflow, Cache poisoning.	2	0.5
5. OWASP - Open Web Application Security Project.	4	0.5
6. Вимоги інформаційної безпеки. Класифікація даних. Технології захисту програмного забезпечення.	4	0.5
7. Атаки на програмне забезпечення: SYN Flooding attack, TCP Session Hijacking.	2	0.5
8. Тестування безпеки програмного забезпечення.	4	0.5
9. Механізми автентифікації та авторизації. Інфраструктура відкритих ключів	4	0.5
10. Атаки на програмне забезпечення: Cross-site scripting (XSS), Cross-site request forgery (CSRF)	2	0.5
РАЗОМ:	32	6

Лабораторний практикум (теми)	Годин ОФЗО	Годин ЗФЗО
1. Shellcode Development	2	0.5
2. Buffer Overflow Vulnerability	4	0.5
3. Return-to-libc Attack	2	0.5
4. SQL Injection Attack	2	0.5
5. Format-String Vulnerability	2	0.5

	6. Race_Condition Vulnerability	4	0.5
	7. TCP/IP Attack	4	0.5
	8. The Mitnick Attack	4	0.5
	9. Cross-Site Request Forgery Attack	4	1
	10. Cross-Site Scripting Attack	4	1
	РАЗОМ:	32	6

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; залік.
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 (захисту лабораторної роботи) з метою підвищення рейтингу протягом тижня після складання модульного контролю (захисту лабораторної роботи) за графіком. Перескладання екзамену (заліку) 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			Одна третя від суми балів, набраних здобувачем впродовж семестру	100
Теоретичний курс (тестування)	Лабораторна робота		Теоретичний курс (тестування)	Лабораторна робота			
10	30		10	25		25	
№ лекції	Види робіт	К-ть балів	№ лекції	Види робіт	К-ть балів		
Тема 1	Лабораторна робота №1	6	Тема 6	Лабораторна робота №6	5		
Тема 2	Лабораторна робота №2	6	Тема 7	Лабораторна робота №7	5		
Тема 3	Лабораторна робота №3	6	Тема 8	Лабораторна робота №8	5		
Тема 4	Лабораторна робота №4	6	Тема 9	Лабораторна робота №9	5		
Тема 5	Лабораторна робота №5	6	Тема 10	Лабораторна робота №10	5		

Розподіл оцінок		
Сума балів за навчальну діяльність	**Шкала ECTS**	**Оцінка за національною шкалою**
90-100	A	Зараховано
82-89	B	Зараховано
75-81	C	Зараховано
67-74	D	Зараховано
60-66	E	Зараховано
35-59	FX	Не зараховано
1-34	F	Не зараховано

Затверджено рішенням кафедри КБ, протокол №1 від «29» серпня 2024 року.

ПОГОДЖЕНО

Гарант освітньої програми канд. техн. наук, доцент кафедри КН

Леся ДМИТРОЦА