СИЛАБУС
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ID 2335

Шифр, назва спеціальності та освітній рівень	126 Інформаційні системи та технології (бакалавр)	Назва освітньої програми	Інформаційні системи та технології (2024)
Тип програми	Освітньо-професійна	Мова викладання	Українська
Факультет	Факультет комп'ютерно-інформаційних систем і програмної інженерії (ФІС)	Кафедра	Каф. кібербезпеки (КБ)

Викладач/викладачі

Максимчук Олександр Олександрович, асистент кафедри кібербезпеки, профіль на порталі "Науковці ТНТУ"

Муж Валерій Вікторович, канд. юрид. наук, доцент кафедри кібербезпеки, профіль на порталі "Науковці ТНТУ"

Загальна інформація про дисципліну

Мета курсу	Метою викладання навчальної дисципліни «Захист інформації в інформаційно-комунікаційних системах» є формування у студентів теоретичних знань та практичних навичок щодо оцінки можливих небезпек, ступеня захищеності та ризику втрат інформації в інформаційно-комунікаційних системах (ІКС), уміння вирішувати задачі аналізу середовищ функціонування програмних та програмно-апаратних комплексів в ІКС, формування політики безпеки інформації в ІКС, застосовувати нормативно-правові, організаційні та технічні процедури підготовки до впровадження комплексних систем захисту інформації.
Формат курсу	Дисципліна передбачає проведення лекційних, лабораторних занять та консультацій. Для кращого розуміння та засвоєння викладеного матеріалу дисципліна має супровід у вигляді електронного навчального курсу в системі A-Tutor (https://dl.tntu.edu.ua, ID: 2335). Електронний навчальний курс має лекційний матеріал, лабораторні роботи, питання підсумкового контролю та систему оцінювання.
Компетентності ОП	Загальні компетентності: КЗ01. Здатність до абстрактного мислення, аналізу та синтезу. КЗ02. Здатність застосовувати знання у практичних ситуаціях. КЗ03. Здатність до розуміння предметної області та професійної діяльності. КЗ04. Здатність спілкуватися іноземною мовою. КЗ05. Здатність вчитися і оволодівати сучасними знаннями. КЗ08. Здатність оцінювати та забезпечувати якість виконуваних робіт. Фахові компетентності: КС01. Здатність аналізувати об’єкт проєктування або функціонування та його предметну область. КС02. Здатність застосовувати стандарти в області інформаційних систем та технологій при розробці функціональних профілів, побудові та інтеграції систем, продуктів, сервісів і елементів інфраструктури організації. КС04. Здатність проєктувати, розробляти та використовувати засоби реалізації інформаційних систем, технологій та інфокомунікацій (методичні, інформаційні, алгоритмічні, технічні, програмні та інші). КС06. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов’язків. КС10. Здатність вибору, проєктування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.
	ПР03. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології

Програмні результати навчання з ОП	розроблення алгоритмів і комп’ютерних програм мовами високого рівня із застосуванням об’єктно-орієнтованого програмування для розв’язання задач проєктування і використання інформаційних систем та технологій. ПР05. Аргументувати вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій. ПР06. Демонструвати знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп’ютерних систем та середовищ з метою їх запровадження у професійній діяльності. ПР09. Здійснювати системний аналіз архітектури підприємства та його ІТ інфраструктури, проводити розроблення та вдосконалення її елементної бази і структури.
Обсяг курсу	**Очна (денна) форма здобуття освіти:** Кількість кредитів ECTS — 4; лекції — 32 год.; лабораторні заняття — 32 год.; самостійна робота — 56 год.; **Заочна форма здобуття освіти:** Кількість кредитів ECTS — 4; лекції — 6 год.; лабораторні заняття — 6 год.; самостійна робота — 108 год.;
Ознаки курсу	Рік навчання — 4; семестр — 7; Обов’язкова (для здобувачів інших ОП може бути вибірковою) дисципліна; кількість модулів — 2;
Форма контролю	Поточний контроль: тестові завдання Підсумковий контроль: залік
Компетентності та дисципліни, що є передумовою для вивчення	Ефективність засвоєння змісту дисципліни «Захист інформації в інформаційно-комунікаційних системах» значно підвищиться, якщо студент попередньо опанував матеріали таких дисциплін як: «Технології створення програмних продуктів», «Операційні системи», «Комп'ютерні мережі», «Організація баз даних», «Об'єктно-орієнтоване програмування».
Матеріально-технічне та/або інформаційне забезпечення	1. Лекційна аудиторія. 2. Стаціонарний мультимедійний проектор. 3. Екран для мультимедійних презентацій. 4. Комп’ютери ПК Intel Core i3-4150 3,50 GHz / RAM 16,0 Gb / Lan / Windows 10 x64 (2018) - 8 шт.

5. Комп’ютери ПК AMD A4-6300 3,70 GHz / RAM 4,0 Gb / Lan / Windows 10 x64 (2018) - 8 шт.
6. Ноутбук HP250G5.

СТРУКТУРА КУРСУ

Теми занять, короткий зміст

Лекційний курс	Годин ОФЗО	Годин ЗФЗО
Лекція 1. Правові та організаційні засади захисту інформації в інформаційних системах.	2	0,5
Лекція 2. Основні загрози безпеці інформації в інформаційно-комунікаційних системах.	2	0,5
Лекція 3. Концепція побудови інформаційної безпеки.	2	0,5
Лекція 4. Засоби антивірусного захисту інформації.	2	0,5
Лекція 5. Системи контролю та керування доступом.	2	0,5
Лекція 6. Захист інформації на рівні операційної системи.	2	0,5
Лекція 7. Захист інформації в комп'ютерних мережах.	2	0,5
Лекція 8. Захист інформації в базах даних.	2	0,5
Лекція 9. Програмні методи та засоби захисту інформації в ІКС.	2	0,5
Лекція 10. Технічний захист інформації в ІКС.	2	0
Лекція 11. Апаратно-програмні методи та засоби захисту інформації в ІКС.	2	0
Лекція 12. Безпека програмного забезпечення, методологія безпечного програмування.	2	0,5
Лекція 13. Криптографічні методи захисту інформації.	2	0,5
Лекція 14. Стеганографічні методи захисту інформації.	2	0
Лекція 15. Управління інформаційною безпекою в ІКС.	2	0
Лекція 16. Проектування, введення в дію та супроводження захищених ІКС.	2	0,5
РАЗОМ:	32	6

Лабораторний практикум (теми)	Годин ОФЗО	ЗФЗО
Лабораторна робота № 1. Ізольований запуск програм у Windows. Пісочниця Windows.	4	0.5
Лабораторна робота № 2. Відновлення та знищення даних на електронних носіях.	4	0.5
Лабораторна робота № 3. Захист веб-додатків від SQL-ін’єкцій.	4	0.5
Лабораторна робота № 4. Налаштування параметрів безпеки Інтернет-браузерів.	4	0.5
Лабораторна робота № 5. Захист інформації в архівах.	4	1
Лабораторна робота № 6. Захист інформації на електронних носіях.	4	1
Лабораторна робота № 7. Робота з електронними цифровими підписами.	4	1
Лабораторна робота № 8. Аналіз ефективності парольного захисту PDF документів.	4	1
РАЗОМ:	32	6

ІНШІ ВИДИ РОБІТ

Теми, короткий зміст	1. Опрацювання лекційного матеріалу. 2. Підготовка до лабораторних робіт. 3. Опрацювання окремих розділів програми, які не виносяться на лекції. 4. Підготовка до модульних контролів та заліку.

Інформаційні джерела для вивчення курсу

Навчально-методичні матеріали:

1. Козак Р.О., Хомишин В.Г., Максимчук О.О. Захист інформації в інформаційно-комунікаційних системах [електронний ресурс] // Інституційний репозиторій ATutor (код дисципліни ID 2335): офіційний сайт Тернопільського національного технічного університету імені Івана Пулюя – Тернопіль, 2014. – Режим доступу: https://dl.tntu.edu.ua/index.php .
2. Козак Р.О., Хомишин В.Г., Максимчук О.О. Конспект лекцій з дисципліни "Захист інформації в інформаційно-комунікаційних системах" для студентів денної та заочної форм навчання спеціальностей 122 "Комп'ютерні науки", 123 "Комп'ютерна інженерія" та 125 "Кібербезпека та захист інформації". Тернопіль: ТНТУ. 2023. – Режим доступу: https://dl.tntu.edu.ua/index.php.
3. Козак Р.О., Хомишин В.Г., Максимчук О.О. Методичні вказівки для виконання лабораторних робіт з дисципліни "Захист інформації в інформаційно-комунікаційних системах" для студентів денної та заочної форм навчання спеціальностей 122 "Комп'ютерні науки", 123 "Комп'ютерна інженерія" та 125 "Кібербезпека та захист інформації". Тернопіль: ТНТУ. 2023. – Режим доступу: https://dl.tntu.edu.ua/index.php.
4. Козак Р.О., Хомишин В.Г., Максимчук О.О. Методичні вказівки для виконання самостійної роботи з дисципліни "Захист інформації в інформаційно-комунікаційних системах" для студентів денної та заочної форм навчання спеціальностей 122 "Комп'ютерні науки", 123 "Комп'ютерна інженерія" та 125 "Кібербезпека та захист інформації". Тернопіль: ТНТУ. 2023. – Режим доступу: https://dl.tntu.edu.ua/index.php.

Рекомендована література:

1. Новітні технології захисту інформації: підручник / М.Г. Луцький , В.О. Хорошко, Ю.Є. Хохлачова та ін. – Київ: НАУ, 2023. – 310 с.
2. Бобало Ю.Я. Інформаційна безпека: навч. посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник та ін. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
3. Остроухов В.В. Інформаційна безпека. Підручник / В.В. Остроухов, М.М. Присяжнюк, О.І. Фармагей, М.М. Чеховська та ін.; під ред. В.В. Остроухова – К.: Видавництво «Ліра-К», 2021. – 412 с.
4. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Львів: «Новий Світ – 2000», 2020. – 678 с.
5. Сагун А.В. Основи криптографічного та стеганографічного захисту інформації : навч. посіб. для студентів спец. 125 – «Кібербезпека», 12 «Інформаційні технології» всіх форм навчання. Ч. 1 : Криптографічний захист інформації / А.В. Сагун, О.М. Кулініч, В.В. Хайдуров. – Київ: НУБіП України, 2023. – 303 с.
6. Сагун А.В. Основи криптографічного та стеганографічного захисту інформації : навч. посіб. для студентів спец. 125 – «Кібербезпека», 12 «Інформаційні технології» всіх форм навчання. Ч. 2 : Стеганографічний захист інформації / А.В. Сагун, О.М. Кулініч, В.В. Хайдуров. – Київ: НУБіП України, 2023. – 144 с.
7. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.
8. Технічний захист інформації: Навч. посіб. в 2 ч. Ч. 1: Основи технічного захисту інформації / В.М. Богуш, В.Д. Бровко, О.С. Кобус, В.Д. Козюра. – К.: Видавництво «Ліра-К», 2022. – 286 с.
9. Програмне забезпечення систем захисту інформації: підручник / Н.М. Блавацька, В.Д. Козюра, В.О. Хорошко. – К.: Вид. ДУПКТ, 2011. – 330 с.
10. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В.М. Богуш, В.В. Богуш, В.Д. Бровко, В.П. Настрадін; під. ред. В. М. Богуша. – К.: Видавництво «Ліра-К», 2020. – 554 с.

Політики курсу

Політика контролю	Використовуються такі засоби оцінювання та методи демонстрування результатів навчання: поточне опитування; тестування; виконання індивідуальних завдань та презентацій; оцінювання результатів виконаних самостійних робіт; бесіди та обговорення проблемних питань; дискусії; індивідуальні консультації; екзамен. Можливий ректорський контроль.
Політика щодо консультування	Консультації при вивченні дисципліни проводяться згідно затвердженого на кафедрі . 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			Одна третя від суми балів, набраних здобувачем впродовж семестру	100
Теоретичний курс (тестування)	Лабораторна робота		Теоретичний курс (тестування)	Лабораторна робота			
20	17		20	18		25	
№ лекції	Види робіт	К-ть балів	№ лекції	Види робіт	К-ть балів		
Тема 1	Лабораторна робота № 1	4	Тема 9	Лабораторна робота № 5	4		
Тема 2			Тема 10				
Тема 3	Лабораторна робота № 2	4	Тема 11	Лабораторна робота № 6	5		
Тема 4			Тема 12				
Тема 5	Лабораторна робота № 3	5	Тема 13	Лабораторна робота № 7	5		
Тема 6			Тема 14				
Тема 7	Лабораторна робота № 4	4	Тема 15	Лабораторна робота № 8	4		
Тема 8			Тема 16				

Розподіл оцінок		
Сума балів за навчальну діяльність	**Шкала ECTS**	**Оцінка за національною шкалою, залік**
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 з можливістю повторного складання
1-34	F	Не зараховано з обов’язковим повторним вивченням дисципліни

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