



СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

ID 2335

Шифр, назва спеціальності та освітній рівень	123 Комп'ютерна інженерія (бакалавр)	Назва освітньої програми	Комп'ютерна інженерія (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"](#)

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: ЗК2. Здатність вчитися і оволодівати сучасними знаннями. ЗК3. Здатність застосовувати знання у практичних ситуаціях. ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК7. Вміння виявляти, ставити та вирішувати проблеми. Фахові: ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії. ФК4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки. ФК9. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи. ФК10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації. ФК13. Здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій.
Програмні результати навчання з ОП	ПР3. Знати новітні технології в галузі комп'ютерної інженерії. ПР6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей. ПР9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності. ПР11. Вміти здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії. ПР20. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення. ПР21. Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.
	Очна (денна) форма здобуття освіти:

Обсяг курсу	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 — 8 год.; лабораторні заняття — 8 год.; самостійна робота — 119 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: Захист звітів щодо виконання лабораторних робіт, тестування в системі електронного навчання Atutor 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: «Методології аудиту захищеності інформаційних комп'ютерних систем», «Безпека комп'ютерних мереж», «Веб-технології», «Прикладна криптологія», «Якість і тестування програмного забезпечення».
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	ЗФО
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	0,5
Лекція 11. Апаратно-програмні методи та засоби захисту інформації в ІКС.	2	0,5
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	0,5
Лекція 15. Управління інформаційною безпекою в ІКС.	2	0,5
Лекція 16. Проектування, введення в дію та супроводження захищених ІКС.	2	0,5
	РАЗОМ:	8
Лабораторний практикум (теми)	Годин	
	ОФЗО	ЗФО
Лабораторна робота № 1. Ізольований запуск програм у Windows. Пісочниця Windows.	4	1
Лабораторна робота № 2. Відновлення та знищення даних на електронних носіях.	4	1

Лабораторна робота № 3. Захист веб-додатків від SQL-ін'єкцій.	4	1
Лабораторна робота № 4. Налаштування параметрів безпеки Інтернет-браузерів.	4	1
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	8

ІНШІ ВИДИ РОБІТ

Теми, короткий зміст	1. Опрацювання лекційного матеріалу 2. Підготовка до лабораторних робіт 3. Підготовка та складання тестування: - модуль №1 - модуль №2
----------------------	--

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. Євсєєв, 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 ВНУ, 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; оцінювання результатів виконаних самостійних робіт; бесіди та обговорення проблемних питань; дискусії; індивідуальні консультації; залік. Можливий ректорський контроль.
Політика щодо консультування	Консультації при вивченні дисципліни проводяться згідно графіку 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 підсумкового контролю 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 лабораторні 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			
№ 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
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 КБ, протокол №1 від «29» серпня 2024 року.

ПОГОДЖЕНО

Гарант освітньої програми канд. техн. наук, старший викладач кафедри КС

Андрій ПАЛАМАР