



Опис навчальної дисципліни

Теорія і методи сучасної криптології

Спеціальності: 122 Комп'ютерні науки; 123 Комп'ютерна інженерія;
125 Кібербезпека

Рівень вищої освіти	Третій (освітньо-науковий)		
Статус дисципліни	Вибіркова		
Обсяг дисципліни	150 годин/ 5 кредити ЄКТС		
Мова викладання	українська		
Анотація	Дисципліна «Теорія і методи сучасної криптології» будується на знаннях, які добути при вивченні курсів «Основи криптології», «Прикладна криптологія», «Методи побудови та аналізу криптосистем», які вивчалися на бакалаврському та магістерському рівнях. При вивченні даного курсу основна увага приділяється малоресурсної криптографії, яка дозволяє значно зменшити часові витрати при проведенні операцій шифрування та дешифрування, але криптостійкість системи практично не зменшується. Другою частиною курсу є сучасні підходи до проблеми криптоаналізу, подальший розвиток якого значно впливає на визначення шляхів розвитку криптологічних систем. Значна увага приділяється питанням захисту інформації при використанні сучасних технологій обробці та збереженню інформації – хмарним технологіям. Розробник дисципліни має 20-річний досвід роботи у сфері інформаційної безпеки, виконавець наукових проєктів		
Пререквізити	Базові знання з криптології, обробка та аналіз результатів наукових досліджень з використанням ІТ		
Кафедра	Комп'ютерних систем, мереж і кібербезпеки		
Факультет	Радіoeлектроніки, комп'ютерних систем та інфокомунікацій		
Викладач		ПІБ	Пєвнєв Володимир Яковлевич
		Посада	Доцент
		Вчене звання	Кандидат технічних наук
		Науковий ступінь	Доцент
		e-mail	v.pevnev@csn.khai.edu
		Персональна сторінка	
Посилання на електронні матеріали курсу	Курс у розробці		
Посилання на робочу програму (силабус)	https://khai.edu/assets/files/robochi-programi/125/aspiranti/silabus_aspirant_125_teoriya-i-metodi-suchasnoi-kriptologii_vk2.pdf		