Навчальна дисципліна

Методи і засоби криптозахисту

Галузі знань: *10 Природничі науки, 11 Математика та статистика, 12 Інформаційні технології, 13 Механічна інженерія, 14 Електрична інженерія, 16 Хімічна інженерія та біоінженерія, 17 Електроніка, автоматизація та електронні комунікації, 19 Архітектура та будівництво, 27 Транспорт*

Рівень вищої освіти	*перший (бакалаврський)*
Статус дисципліни	*вибіркова*
Обсяг дисципліни	150 годин/ 5 кредитів ЄКТС
Мова викладання	*українська*
Що буде вивчатися (предмет вивчення)	Засвоєння базових знань, знань, навичок та вмінь, необхідних для опанування методології, основних напрямів, методів і алгоритмів захисту інформації в комп'ютерних системах та мережах
Чому це цікаво/треба вивчати (мета)	Вивчення базових теоретичних засад, які мають стати в нагоді при вивченні принципів побудови криптографічних алгоритмів забезпечення захисту інформації
Як можна користуватися набутими знаннями і уміннями (компетентності)	В результаті навчання студент знатиме: – базові положення (концепції) теорії чисел; – знати методи побудови та перевірки чисел на простоту; – вміти знаходити найбільший спільний дільник: – вміти знаходити прямі та оборотні числа; – володіти алгоритмами факторизації та дискретного логарифмування; **матиме компетентності**: – здатність ефективно використовувати основні математичні відомості, які стануть у нагоді при опануванні криптографічних алгоритмів; – здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки. **Особливості курсу**: – практична спрямованість і кейс-орієнтований підхід при викладанні; – надає комплекс знань, практичних навичок і компетентностей, достатніх для подальшого самостійного вивчення і застосування для практичної діяльності; – побудований з урахуванням досвіду провідних університетів (зокрема, Massachusetts Institute of Technology) і потреб провідних IT-компаній (зокрема, EPAM, NIX Solutions), а також стандартів і методичних матеріалів NIST (National Institute of Standards and Technology, USA); – розроблений і викладається фахівцем, який має досвід у галузі криптографії, кібербезпеки та реалізації систем безпеки інформаційних і комунікаційних систем. Розробник курсу має багаторічний досвід викладання високотехнологічних курсів з захисту інформації, криптографії, безпеки інформаційних і комунікаційних систем. Автор більш 200 публікацій і винаходів
Пререквізити	Вища математика
Кореквізити	Прикладна криптологія
Організація навчання	Види занять: лекції, практичні заняття. Форми здобуття освіти: денна. Форми контролю: модульний контроль, іспит
Кафедра	Кафедра комп'ютерних систем, мереж і кібербезпеки № 503

Факультет	Факультет радіоелектроніки, комп'ютерних систем та інфокомунікацій		
Викладач		ПІБ	**Пєвнєв Володимир Яковлевич**
		Посада	професор
		Вчене звання	доцент
		Науковий ступінь	д.т.н.
		e-mail	v.pevnev@csn.khai.edu
Посилання на електронні матеріали курсу	https://mentor.khai.edu/course/view.php?id=1604		
Посилання на робочу програму (силабус)			