




## Методи і засоби криптозахисту

Галузі знань: *Е Природничі науки, математика та статистика, F Інформаційні технології, G Інженерія, виробництво та будівництво, J Транспорт та послуги*

Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	вибіркова (Математично-технічний блок на вибір)
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)	<p>В результаті навчання студент знатиме:</p> <ul style="list-style-type: none"><li>– базові положення (концепції) теорії чисел;</li><li>– знати методи побудови та перевірки чисел на простоту;</li><li>– вміти знаходити найбільший спільний дільник;</li><li>– вміти знаходити прямі та оборотні числа;</li><li>– володіти алгоритмами факторизації та дискретного логарифмування;</li></ul> <p><b>матиме компетентності:</b></p> <ul style="list-style-type: none"><li>– здатність ефективно використовувати основні математичні відомості, які стануть у нагоді при опануванні криптографічних алгоритмів;</li><li>– здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.</li></ul> <p><b>Особливості курсу:</b></p> <ul style="list-style-type: none"><li>– практична спрямованість і кейс-орієнтований підхід при викладанні;</li><li>– надає комплекс знань, практичних навичок і компетентностей, достатніх для подальшого самостійного вивчення і застосування для практичної діяльності;</li><li>– побудований з урахуванням досвіду провідних університетів (зокрема, Massachusetts Institute of Technology) і потреб провідних ІТ-компаній (зокрема, EPAM, NIX Solutions), а також стандартів і методичних матеріалів NIST (National Institute of Standards and Technology, USA);</li><li>– розроблений і викладається фахівцем, який має досвід у галузі криптографії, кібербезпеки та реалізації систем безпеки інформаційних і комунікаційних систем.</li></ul> <p>Розробник курсу має багаторічний досвід викладання високотехнологічних курсів з захисту інформації, криптографії, безпеки інформаційних і комунікаційних систем. Автор більш 200 публікацій і винаходів</p>
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

<b>Факультет</b>	Факультет радіоелектроніки, комп'ютерних систем та інфокомунікацій		
<b>Викладач</b>		ПІБ	<b>Абакумов Артем Ігорович</b>
		Посада	асистент
		Вчене звання	
		Науковий ступінь	
		e-mail	<a href="mailto:a.i.abakumov@csn.khai.edu">a.i.abakumov@csn.khai.edu</a>
<b>Посилання на електронні матеріали курсу</b>	<a href="https://mentor.khai.edu/course/view.php?id=1604">https://mentor.khai.edu/course/view.php?id=1604</a>		
<b>Посилання на силабус</b>			