Навчальна дисципліна

Методи і засоби криптозахисту

Галузі знань: *E 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)	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

<table>
<tr><td>Факультет</td><td colspan="3">Факультет радіоелектроніки, комп'ютерних систем та інфокомунікацій</td></tr>
<tr><td rowspan="5">Викладач</td><td rowspan="5">  </td><td>ПІБ</td><td>Пєвнєв
Володимир Яковлевич</td></tr>
<tr><td>Посада</td><td>професор</td></tr>
<tr><td>Вчене звання</td><td>доцент</td></tr>
<tr><td>Науковий ступінь</td><td>д.т.н.</td></tr>
<tr><td>e-mail</td><td>v.pevnev@csn.khai.edu</td></tr>
<tr><td>Посилання на електронні матеріали курсу</td><td colspan="3">https://mentor.khai.edu/course/view.php?id=1604</td></tr>
<tr><td>Посилання на силабус</td><td colspan="3"></td></tr>
</table>