

**Силабус навчальної дисципліни**  
**«Математичні та комп'ютерні методи криптології»**

№	Назва поля	Детальний контент, коментарі
1.	Назва факультету	Інформаційно-аналітичних технологій та менеджменту
2.	Рівень вищої освіти	Другий (магістерський)
3.	Назва спеціальності	113 Прикладна математика
4.	Тип і назва освітньої програми	ОПП «Прикладна математика»
5.	Назва дисципліни	Математичні та комп'ютерні методи криптології
6.	Кількість ЄКТС кредитів	4
7.	Структура дисципліни (розподіл за видами та годинами навчання)	Лекції – 24 год., практичні заняття – 16 год., консультації – 8 год., самостійна робота – 72 год. Семестровий контроль – комбінований екзамен
8.	Графік (терміни) вивчення дисципліни	1-й рік навчання, 2-й семестр
9.	Передумови для навчання за дисципліною	Наявність ступеня бакалавра
10.	Анотація (зміст) дисципліни	Дисципліна професійної та практичної підготовки за освітньою програмою «Прикладна математика» (вибіркова). <i>Змістовий модуль 1. Вступ до криптології.</i> Тема 1. Основні поняття та задачі криптології. Тема 2. Історія криптології. Тема 3. Математичні основи криптології. <i>Змістовий модуль 2. Математичні та комп'ютерні методи криптології.</i> Тема 1. Симетричні системи шифрування. Тема 2. Асиметричні системи шифрування. Тема 3. Електронний цифровий підпис. Тема 4. Протоколи аутентифікації. Тема 5. Основи криптоаналізу.
11.	Компетентності, знання, вміння, розуміння, якими оволодіє здобувач в процесі навчання	ФК 5. Здатність обирати, застосовувати та модифікувати відомі математичні методи для розв'язання практичних задач моделювання об'єктів та процесів різної природи. ФК 6. Здатність розробляти алгоритми та наукомістке програмне забезпечення, створювати програмну документацію.
12.	Результати навчання здобувача	ПРН 6. Будувати ефективні щодо точності обчислень, стійкості, швидкодії та витрат системних ресурсів алгоритми для чисельного дослідження математичних моделей та розв'язання практичних задач. ПРН 7. Розробляти на основі структури математичної моделі та алгоритмів функціонування процесів, що моделюються, програмне забезпечення із застосуванням сучасних технологій програмування та систем комп'ютерної математики, аналізувати отримані результати на адекватність.
13.	Система оцінювання відповідно до кожного завдання для складання заліку/екзамену	1. Відпрацювати практичні заняття. 2. Пройти тестування. 3. Отримати за семестр не менше 60 балів.

		<p>4. Скласти комбінований екзамен.</p> <p>Оцінка за семестр <math>O_{\text{сем}} = (6-10) \times 8 \text{ пз} + (12-20) \times 1 \text{ тестування} = (60-100)</math> балів.</p> <p>Оцінка за комбінований екзамен <math>O_{\text{екз}} = (60-100)</math> балів.</p> <p>Підсумкова оцінка з дисципліни <math>O_{\text{п}} = 0,6 \cdot O_{\text{сем}} + 0,4 \cdot O_{\text{екз}}</math>.</p>
14.	Якість освітнього процесу	<p>Навчання з дисципліни передбачає:</p> <ul style="list-style-type: none"> <li>- відвідування аудиторних занять;</li> <li>- виконання практичних завдань, проходження тестування;</li> <li>- відпрацювання пропущених занять та незадовільних оцінок за графіком консультацій;</li> <li>- дотримання принципів академічної доброчесності (<a href="http://lib.nure.ua/plagiat">http://lib.nure.ua/plagiat</a>).</li> </ul> <p>Оновлення робочої програми дисципліни – 2023 р.</p>
15.	Методичне забезпечення	<p>Комплекс навчально-методичного забезпечення навчальної дисципліни «Математичні та комп'ютерні методи криптології» підготовки здобувачів другого (магістерського) рівня вищої освіти спеціальності 113 Прикладна математика за освітньою програмою «Прикладна математика» [Електронний ресурс] / ХНУРЕ; розроб. Н.В. Гибкіна. Харків, 2023.</p>
16.	Розробник силабусу (посада, ПІБ, ел. пошта)	<p>Доцент кафедри прикладної математики, канд. техн. наук, доц. Гибкіна Надія Валентинівна <a href="mailto:nadiia.gybkina@nure.ua">nadiia.gybkina@nure.ua</a></p>