

Силабус навчальної дисципліни  
**«Математичні методи побудови сучасних криптосистем»**

№	Назва поля	Детальний контент, коментарі
1.	Назва	Факультет комп'ютерної інженерії та управління
2.	Рівень вищої освіти	Третій (освітньо-науковий) рівень вищої освіти
3.	Код і назва спеціальності	125 Кібербезпека
4.	Тип і назва освітньої програми	ОНП «Кібербезпека»
5.	Код і назва дисципліни (інформація з ЦІСТ)	Математичні методи побудови сучасних криптосистем
6.	Кількість ЄКТС кредитів	4 кредити ЄКТС
7.	Структура дисципліни (розподіл за видами та годинами навчання)	Лекції – 24 годин, практичні заняття – 24 годин, консультації – 8 годин, самостійна робота – 64 годин, вид контролю: залік
8.	Графік (терміни) вивчення дисципліни	1-й рік, 1-й семестр
9.	Передумови для навчання за дисципліною	Наявність ступеня магістра (або освітньо-кваліфікаційного рівня спеціаліста)
10.	Анотація (зміст) дисципліни	Обов'язкова дисципліна зі спеціальності. Мета вивчення дисципліни: отримання студентами необхідних знань щодо: математичних методів аналізу існуючих криптографічних примітивів; математичних методів синтезу та аналізу перспективних доказовостійких криптографічних перетворень, в тому числі для застосування в перехідний та постквантовий періоди; побудови моделей безпеки в умовах застосування методів класичного та квантового криптоаналізу. Змістові модулі: 1. Постквантовостійкі криптосистеми. Аналіз і вимоги. 2. Побудова і застосування сучасних криптосистем.
11.	Компетентності, знання, вміння, розуміння, якими оволодіє здобувач в процесі навчання	Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання і можуть бути опубліковані у провідних наукових виданнях . Здатність використовувати сучасні досягнення науки, передові технології та математичні методи для розв'язування задач забезпечення інформаційної та кібербезпеки. Здатність аналізувати, використовувати, оцінювати ефективність та розробляти методи і засоби криптографічного та технічного захисту для забезпечення інформаційної та кібербезпеки в умовах сучасних загроз та викликів.
12.	Результати навчання здобувача	Уміти застосовувати, удосконалювати та розробляти нові математичні моделі та методи забезпечення інформаційної та кібербезпеки, а також виконувати їх експериментальну перевірку з використанням сучасних інформаційних технологій. Застосовувати знання і розуміння фізико-

		математичних методів побудови систем захисту при проведенні досліджень, розробці нових методів й засобів забезпечення інформаційної та кібербезпеки, спираючись на сучасні досягнення світової науки.
13.	Система оцінювання відповідно до кожного завдання для складання заліку/екзамену	<p>Підсумковий модульний контроль з дисципліни передбачає залік.</p> <p>Оцінка з дисципліни складається з суми балів, отриманих здобувачем вищої освіти за виконання поточного контролю практичних занять протягом семестру за 100-бальною шкалою: <math>O_{\text{сем}} = \sum O_i</math>,</p> <p>де <math>O_i</math> – бали з <math>i</math>-го контрольного заходу поточного контролю дисципліни;</p> <p><math>O_{\text{сем}}</math> – рейтингова оцінка з дисципліни в семестрі.</p> <p>Оцінювання навчальних досягнень здобувачів здійснюється:</p> <p>за національною шкалою (зараховано, не зараховано);</p> <p>100-бальною шкалою та шкалою ЄКТС (А, В, С, D, E, FX, F).</p> <p>Шкала оцінювання:</p> <p>Зараховано: А (96-100), В (90-95), С (75-89), D (66-74), E(60-65).</p> <p>Не зараховано: FX (35-59), F (1-34).</p>
14.	Якість освітнього процесу	<p>Навчання з курсу передбачає:</p> <ul style="list-style-type: none"> <li>- відвідування аудиторних занять;</li> <li>- виконання та захист практичних завдань, рефератів тощо;</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 – 2021 р.</p>
15.	Методичне забезпечення	Комплекс навчально-методичного забезпечення навчальної дисципліни «Математичні методи побудови сучасних криптосистем» підготовки докторів філософії спеціальності 125 Кібербезпека [Електронний ресурс] / ХНУРЕ; розроб. І.Д. Горбенко, Г.З. Халімов. – Харків, 2021. – 212 с.
16.	Розробник силабусу (посада, ПІБ, ел. пошта)	<p>зав. каф. БІТ</p> <p>д-р техн. наук, проф.</p> <p>Г.З. Халімов,</p> <p>E-mail: <a href="mailto:hennadii.khalimov@nure.ua">hennadii.khalimov@nure.ua</a></p>