

Силабус навчальної дисципліни
«Методи побудови постквантових 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)	Методи побудови постквантових криптосистем
6.	Кількість ЄКТС кредитів	8 кредитів ЄКТС
7.	Структура дисципліни (розподіл за видами та годинами навчання)	Лекції – 48 годин, практичні заняття – 48 годин, консультації – 16 годин, самостійна робота – 128 годин, вид контролю: залік
8.	Графік (терміни) вивчення дисципліни	1-й рік, 2-й семестр
9.	Передумови для навчання за дисципліною	Наявність ступеня магістра (або освітньо-кваліфікаційного рівня спеціаліста)
10.	Анотація (зміст) дисципліни	Вибіркова дисципліна зі спеціальності, містить змістові модулі: 1. Основні поняття квантових обчислень. 2. Постквантові алгоритми та протоколи. 3. Постквантові криптосистеми на матричних групах.
11.	Компетентності, знання, вміння, розуміння, якими оволодіє здобувач в процесі навчання	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	Підсумковий модульний контроль з дисципліни передбачає залік. Оцінка з дисципліни складається з суми балів, отриманих здобувачем вищої освіти за виконання поточного контролю практичних занять протягом семестру за 100-бальною шкалою: $O_{\text{сем}} = \sum O_i$, де O_i – бали з i -го контрольного заходу поточного

		<p>контролю дисципліни; $O_{\text{сем}}$ – рейтингова оцінка з дисципліни в семестрі. Оцінювання навчальних досягнень здобувачів здійснюється: за національною шкалою (зараховано, не зараховано); 100-бальною шкалою та шкалою ЄКТС (А, В, С, D, E, FX, F). Шкала оцінювання: Зараховано: А (96-100), В (90-95), С (75-89), D (66-74), E(60-65). Не зараховано: FX (35-59), F (1-34)</p>
14.	Якість освітнього процесу	<p>Навчання з курсу передбачає: - відвідування аудиторних занять; - виконання та захист практичних завдань, рефератів тощо; - відпрацювання пропущених занять та незадовільних оцінок за графіком консультацій; - дотримання принципів академічної доброчесності (http://lib.nure.ua/plagiat). Оновлення робочої програми дисципліни – 2021 р.</p>
15.	Методичне забезпечення	<p>Комплекс навчально-методичного забезпечення навчальної дисципліни «Методи побудови постквантових криптосистем» підготовки докторів філософії спеціальності 125 Кібербезпека [Електронний ресурс] / ХНУРЕ; розроб. Г.З. Халімов, О.І. Цопа, О.В. Сєверінов. – Харків, 2021. – 294 с.</p>
16.	Розробник силабусу (посада, ПІБ, ел. пошта)	<p>доц. каф. БІТ к.т.н, доц.О.В. Сєверінов, E-mail: oleksandr.sievierinov@nure.ua</p>