

Силабус навчальної дисципліни
«Новітні технології забезпечення кібербезпеки в інфокомунікаціях»

№	Назва поля	Детальний контент, коментарі
1.	Назва факультету	Факультет інфокомунікацій
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)	Новітні технології забезпечення кібербезпеки в інфокомунікаціях
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 години, самостійна робота – 128 годин. Семестровий контроль – залік
8.	Графік (терміни) вивчення дисципліни	1-й рік навчання, 2-й семестр
9.	Передумови для навчання за дисципліною	Наявність ступеня магістра (або освітньо-кваліфікаційного рівня спеціаліста)
10.	Анотація (зміст) дисципліни	Дисципліна зі спеціальності (вибіркова) Змістові модулі: 1. Сучасні підходи до аналізу захищеності систем в інфокомунікаційних системах. 2. Методи аналізу даних кіберзагроз та захисту інфокомунікаційних систем
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 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	Планувати і виконувати експериментальні та/або теоретичні дослідження з використанням сучасних інструментів, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми. 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>Для оцінювання роботи аспіранта протягом семестру підсумкова рейтингова оцінка розраховується як сума оцінок, які аспірант набрав протягом семестру, виконуючи всі види контролю, передбачені робочою програмою:</p> <ul style="list-style-type: none"> – 2 тести, кожний з яких оцінюється від 12 до 20 балів; – 2 індивідуальні завдання, кожний з яких оцінюється від 12 до 20 балів; – реферат, який оцінюється від 12 до 20 балів.
14.	Якість освітнього процесу	<p>Навчання з курсу передбачає:</p> <ul style="list-style-type: none"> - 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). <p>Оновлення робочої програми дисципліни – 2021 р.</p>
15.	Методичне забезпечення	<p>Комплекс навчально-методичного забезпечення навчальної дисципліни «Новітні технології забезпечення кібербезпеки в інфокомунікаціях» [Електронний ресурс] / ХНУРЕ; розроб. Т.А.Радівілова – Харків, 2021.</p>
16.	Розробник силабусу (посада, ПІБ, ел. пошта)	<p>проф. каф. ІКІ ім. В.В.Поповського д.т.н. доц. Т.А. Радівілова, E-mail: tamara.radivilova@nure.ua</p>