СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«БЕЗПЕКА ІНТЕГРОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ»

№	Назва поля	Детальний контент, коментарі
1.	Назва факультету	Факультет інформаційних радіотехнологій та технічного захисту інформації (ІРТЗІ)
2.	Рівень вищої освіти	Другий (магістерський)
3.	Код і назва спеціальності	F6 Інформаційні системи і технології
4.	Тип і назва освітньої програми	ОПП «Архітектурне проєктування інформаційних систем»
5.	Код і назва дисципліни	ОК 10 Безпека інтегрованих інформаційних систем *(Security of integration information systems)*
6.	Кількість ЄКТС кредитів	3
7.	Структура дисципліни (розподіл за видами та годинами навчання)	ЛК – 16 год., ПЗ – 4 год., ЛБ – 8 год., конс. – 6 год., СР – 56 год. вид контролю: залік
8.	Графік (терміни) вивчення дисципліни	1-й рік, 1-й семестр
9.	Передумови для навчання за дисципліною	Раніше мають бути вивчені дисципліни: «Проектування інформаційних систем», «Теорія інформаційних систем»
10.	Анотація (зміст) дисципліни	Модулі дисципліни професійної та практичної підготовки: 1. Основні поняття національної безпеки. Система забезпечення національної безпеки в Україні. 2. Поняття інформаційної безпеки**.** Загрози інформаційній безпеці, фактори загроз інформаційній безпеці, забезпечення інформаційної безпеки, форми забезпечення інформаційної безпеки. 3. Міжнародні стандарти та рекомендації в галузі інформаційної безпеки. Основні положення стратегії кібербезпеки. Терміни та визначення. Загрози кібербезпеці. Національна система кібербезпеки, основні суб'єкти забезпечення кібербезпеки. 4. Предмет та об’єкт захисту у інформаційній безпеці. Інформаційно-телекомунікаційна система, комп'ютерна система, обчислювальна система, автоматизована система, політика безпеки, конфіденційність, цілісність, доступність, несприятливий вплив, загроза, атака, компрометація, уразливість системи, вади захисту. 5. Порушник, модель політики безпеки, модель загроз, модель порушника, захищена комп'ютерна система, комплекс засобів захисту, доступ, доступ до інформації, ідентифікація, автентифікація, авторизація. 6. Основні складові системи інформаційної безпеки. Політика в галузі інформатизації та інформаційної

		безпеки. Система державних органів, які створюють та впроваджують у життя політику інформаційної безпеки. 7. Класифікація інформації та інформаційних систем. Побудова і структура критеріїв захищеності інформації. Політики безпеки. 8. Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу. Порядок та умови доступу та обробки інформації за визначенням законодавством України. 9. Основі теоретичні положення захисту інформації в комп'ютерних системах. 10. Механізми захисту інформації від НСД. Основні типи політик безпеки. Ідентифікація та автентифікація. 11. Основні поняття криптографії. симетричні та асиметричні криптосистеми. 12. Передумови виникнення вразливостей у інтегрованих інформаційних системах. Шкідливе програмне забезпечення.
11.	Компетентності, знання, вміння, розуміння, якими оволодіє здобувач вищої освіти у процесі навчання	ЗК03. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності). ЗК04. Здатність розробляти проекти та управляти ними. ФК05. Здатність використовувати сучасні технології аналізу даних для оптимізації процесів в інформаційних системах. ФК07. Розробляти і реалізовувати інноваційні проекти у сфері ІСТ. ФК10. Здатність ефективно застосовувати архітектурні, структурні та об'єктно орієнтовані технології проєктування компонентів середовища інтегрованої інформаційної системи та прийняття проєктних рішень.
12.	Результати навчання здобувача вищої освіти	РН05. Визначати вимоги до ІСТ на основі аналізу бізнес-процесів та аналізу потреб зацікавлених сторін, розробляти технічні завдання. РН07. Здійснювати обґрунтований вибір проєктних рішень та проєктувати сервіс-орієнтовану інформаційну архітектуру підприємства (установи, організації тощо). РН09. Розробляти і використовувати сховища даних, здійснювати інтелектуальний аналіз даних для підтримки прийняття рішень. РН10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації.
13.	Система оцінювання відповідно до кожного завдання для складання заліку/екзамену	1. Виконати практичні роботи. 2. Відпрацювати та захистити лабораторні роботи. 3. Виконати тести. 4. Залік по курсу. Підсумкова рейтингова оцінка $O_{сем}$ розраховується як сума оцінок за різні види занять та контрольні заходи. 1. Максимальна рейтингова оцінка протягом семестру – 100 балів. Мінімальна – 60 балів.

14.	Якість освітнього процесу	Дотримання принципів академічної доброчесності (http://lib.nure.ua/plagiat). Оновлення робочої програми дисципліни відбувається на підставі сучасних практик та технологій, наукових досягнень, рекомендацій стейкхолдерів ОПП. Розробка робочої програми дисципліни – 2025 р.
15.	Методичне забезпечення	Комплекс навчально-методичного забезпечення навчальної дисципліни "Безпека інтегрованих інформаційних систем" для студентів другого (магістерського) рівня вищої освіти спеціальності 126 Інформаційні системи та технології, Освітньо-професійної програми "Архітектурне проєктування інформаційних систем" [Електронний ресурс] / ХНУРЕ; розроб. О.І. Цопа. – Харків, 2023. –352 с. https://catalogue.nure.ua/knmz/?subdivision=21&level=133&query=undefined
16.	Розробник силабусу (посада, ПІБ, ел. пошта)	Ганшин Д.Г. Ст. викладач кафедри РТІКС E-mail: dmytro.hanshyn@nure.ua