

Силабус навчальної дисципліни

№	Назва поля	Детальний контент, коментарі
1.	Назва факультету	Факультет інформаційних радіотехнологій та медіаінженерії
2.	Рівень вищої освіти	Бакалаврський
3.	Код і назва спеціальності	Міждисциплінарна ОП за спеціальностями G5/F5 (Електроніка, електронні комунікації, приладобудування та радіотехніка / Кібербезпека та захист інформації)
4.	Тип і назва освітньої програми	ОПП «Радіоінженерія інформаційної безпеки» ОПП «Інформаційні радіотехнології»
5.	Код і назва дисципліни (інформація з ЦІСТ)	СИСТЕМИ ЕЛЕКТРОННОЇ ІДЕНТИФІКАЦІЇ
6.	Кількість ЄКТС кредитів	4
7.	Структура дисципліни (розподіл за видами та годинами навчання)	24г. – 12лк, 8г. – 4пз, 16г. – 4лб, 8г. – 4конс, 64 г. – самостійна робота, вид контролю: залік
8.	Графік (терміни) вивчення дисципліни	4-й рік, 8-й семестр
9.	Передумови для навчання за дисципліною	Раніше мають бути вивчені дисципліни «Фізика» (розділ «Електрика»), «Сигнали та процеси», «Поля і хвилі в системах ТЗІ», «Інформаційно-комунікаційні системи», «Методи та засоби захисту інформації»
10.	Анотація (зміст) дисципліни	<p>Вибіркова дисципліна професійної та практичної підготовки. Мета дисципліни: ознайомлення з основними типами сучасних систем електронної ідентифікації. Основний акцент зроблено на принципах побудови, характеристиках та особливостях використання систем радіочастотної (RFID) ідентифікації та смарт карт, які активно використовуються в системах безпеки, транспортній логістиці, зберіганні тощо.</p> <p>Дисципліна містить наступні змістові модулі:</p> <ol style="list-style-type: none"> 1. Технології автоматичної ідентифікації (штрих-коди, біометрія, смарт-карти, радіочастотна ідентифікація). 2. Базові принципи систем радіочастотної ідентифікації (класифікація, характеристики). 3. RFID системи: зчитувачі та транспондери, особливості передавання даних (кодування даних та антиколізійні процедури). 4. Системи електронної ідентифікації на поверхневих акустичних хвилях. 5. Смарт-карти: архітектура, функціонування та життєвий цикл. 6. Базові технології захисту даних у системах радіочастотної ідентифікації: сервіси аутентифікації; методи та алгоритми шифрування; хешування та управління крипто-ключами.
11.	Компетентності, знання, вміння, розуміння, якими	За результатом вивчення дисципліни здобувачі повинні:

	<p>оволодіє здобувач вищої освіти в процесі навчання</p>	<ul style="list-style-type: none"> - Знати та розуміти предметну область і професійну діяльність (ЗК 2). - Мати здатність вчитися і оволодівати сучасними знаннями (ЗК 5) в області систем електронної ідентифікації. - Знати сучасні методології та підходи у побудові систем електронної ідентифікації, підсистем вхідного контролю в системах фізичного захисту об'єктів; - Вміти здійснювати комп'ютерне моделювання пристроїв, систем і процесів з використанням універсальних пакетів прикладних програм. - Бути здатними до проведення оцінки технічних засобів електронної ідентифікації, знати принципи їх роботи, методи захисту інформації в таких системах. <p>Також здобувачі повинні мати:</p> <p>СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та систем захисту інформації.</p> <p>СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.</p> <p>СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.</p>
12.	<p>Результати навчання здобувача вищої освіти</p>	<p>За результатом вивчення дисципліни здобувач повинен (перелік сформованих компетентностей):</p> <p>РН 5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.</p> <p>РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.</p> <p>РН 7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.</p> <p>РН 8. Застосовувати знання й розуміння</p>

		<p>математики та фізики в професійній діяльності, формулювати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональні методи вирішення.</p> <p>PH 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.</p> <p>PH 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.</p> <p>PH 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.</p> <ul style="list-style-type: none"> – мати спроможність здійснювати пошук інформації в різних джерелах для розв'язання задач пов'язаних з проєктуванням ефективних систем захисту (систем електронної ідентифікації); – мати спроможність застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації систем та пристроїв електронної ідентифікації для вирішення технічних задач побудови сучасних безпекових систем;
13.	Система оцінювання відповідно до кожного завдання для складання заліку/екзамену	<ol style="list-style-type: none"> 1. Відпрацювати та захистити лабораторні роботи. 2. Виконати практичних заняття. 3. Отримати за семестр не менш ніж 30 балів. 4. Скласти семестровий тест-залік. <p>Оцінка за семестр $O_{\text{сем}} : (0 \dots 10) \times 4 \text{ лб} + (0 \dots 5) \times 4 \text{ пз} + (0 - 40) \times 1 \text{ тест} = (60 - 100) \text{ балів}$</p>
5.	Якість освітнього процесу	<p>Оновлення робочої програми дисципліни – 2025 р.</p> <p>Політика дисципліни: дотримання принципів академічної доброчесності (http://lib.nure.ua/plagiat); надання індивідуальних завдань для ПЗ і ЛБ; можливість відпрацювання пропущених занять та доопрацювання завдань, поданих невчасно, у визначений викладачем термін.</p> <p>Практичні та лабораторні заняття забезпечено сучасним ліцензованим програмним засобом AWR Desin Environment та іншим спеціалізованим програмним забезпеченням.</p>
6.	Методичне забезпечення	<ol style="list-style-type: none"> 1. Комплекс навчально-методичного забезпечення навчальної дисципліни "Системи електронної ідентифікації" підготовки бакалаврів спеціальності G5 (172) «Електроніка, електронні комунікації, приладобудування та радіотехніка» та F5 (125)

		«Кібербезпека та захист інформації», освітні програми «Інформаційні радіотехнології» та «Радіоінженерія інформаційної безпеки» [Електронний ресурс] / ХНУРЕ ; розроб. Д.С. Гавва. – Харків, 2025. – 146 с. http://catalogue.nure.ua/knmz .
7.	Розробник силябусу (посада, ПБ, ел. пошта)	Д.С. Гавва, зав. каф. ІРТЗІ, к.т.н., доцент E-mail: dmytro.gavva@nure.ua