



**Силабус навчальної дисципліни
«АПАРАТНО-ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ
В БЕЗПЛОТНИХ АЕРОКОСМІЧНИХ КОМПЛЕКСАХ»**

**Спеціальність: 153 Мікро- та наносистемна техніка
Галузь знань: 15 Автоматизація та приладобудування**

Рівень вищої освіти	Бакалавр
Статус дисципліни	Навчальна дисципліна вибіркового компонента фахового переліку
Семестр	Весняний
Обсяг дисципліни, кредити ЄКТС/загальна кількість годин	3 кредити / 90 годин
Мова викладання	Українська, англійська
Що буде вивчатися (предмет навчання)	Конкретні апаратно-програмні засоби криптографічного захисту інформації, що використовуються в безпілотних аерокосмічних комплексах (БАК), у відповідності з їх класифікацією. А саме: системи потокового і блокового шифрування даних та захисту інформації з відкритим ключем, що будуються на основі сучасної мікро- та наноелектронної елементної бази, які необхідні для вирішення професійних завдань.
Чому це цікаво/потрібно вивчати (мета)	Головною метою викладання навчальної дисципліни «Апаратно-програмні засоби захист інформації в безпілотних аерокосмічних комплексах» є формування компетенцій, знань та умінь, необхідних для виконання професійних обов'язків фахівця з інформаційної та кібербезпеки в рамках об'єктів професійної діяльності за обраною спеціалізацією.
Чому можна навчитися (результати навчання)	По завершенні вивчення дисципліни студенти набувають знань у галузі теоретичної та практичної криптографії, а також з основних принципів побудови сучасних методів криптографічного захисту інформації (КЗІ) в каналах зв'язку з безпілотними аерокосмічними комплексами.
Як можна користуватися набутими знаннями і вміннями (компетентності)	Компетентнісний підхід навчальної дисципліни орієнтується на кінцевий результат освітнього процесу, спрямований на формування у майбутнього фахівця готовності ефективно використовувати набути знання для вирішення проблеми криптографічного захисту каналів передавання інформації до БАК від несанкціонованого доступу до їх життєво важливих компонентів.

Навчальна логістика	<p>Зміст дисципліни: Етапи розвитку криптографії, основні методи КЗІ та шифрування даних, математичні моделі та апаратно-програмні засоби потокового та блокового захисту інформації, методи асиметричної криптографії та криптографічні протоколи, основи квантової та постквантової криптографії.</p> <p>Види занять: Лекції, лабораторні, практичні, модульні контрольні роботи.</p> <p>Методи навчання: Навчально-дослідницькі на основі розповіді, дискусії, комп'ютерного моделювання та роботи онлайн.</p> <p>Форми навчання: Очна, дистанційна.</p>
Пререквізити	Загальні знання з програм вищої математики та фізики, поглиблене засвоєння основ модулярної арифметики, алгебраїчних структур полів Галуа, незвідних многочленів, вільне володіння комп'ютером.
Пореквізити	Оволодіння принципами побудови систем криптографічного захисту інформації в каналах зв'язку з БАК можуть бути використані під час написання бакалаврської та магістерської роботи, а також для подальшого удосконалення протягом трудової діяльності.
Інформаційне забезпечення з фонду та репозиторію НТБ НАУ	<p>http://er.nau.edu.ua/</p> <p>http://www.lib.nau.edu.ua/main/</p> <p>ntb@nau.edu.ua</p>
Локація та матеріально-технічне забезпечення	Навчальні заняття проводяться в спеціалізованій аудиторії, оснащеної комп'ютерною та проекційною технікою. Студенти забезпечуються електронними навчальними посібниками, лабораторним практикумом, пакетами прикладних програм та іншими навчально методичними засобами.
Семестровий контроль, екзаменаційна методика	<p>Контрольні заходи з навчальної дисципліни проводяться у формі:</p> <p>поточного контролю – визначення викладачем якості знань на підставі виконаних студентом робіт, в тому числі самостійних, тестів та інших завдань, з виставленням балів згідно із критеріями і шкалою оцінювання, затвердженими кафедрою;</p> <p>проміжного контролю – діагностика рівня опанування навчальним матеріалом в межах змістового модулю;</p> <p>підсумкового контролю (екзамен) – діагностика рівня опанування навчальним матеріалом в межах усієї навчальної дисципліни із оцінюванням результатів за національною шкалою і шкалою ECTS;</p> <p>Форма проведення екзамену визначається відповідним рішенням кафедри і може базуватися як на традиційній системі опитування за екзаменаційними білетами, так і на основі співбесіди.</p>
Кафедра	Електроніки, робототехніки і технологій моніторингу та Інтернету речей (ЕРМІТ)
Факультет	Аеронавігації, електроніки та телекомунікації (ФАЕТ)

Викладач	ПІБ Білецький Анатолій Якович Посада: Професор Вчений ступінь: Доктор техн. наук Профайл викладача: http://kafelec.nau.edu.ua Тел.: +38 (050) 312-23-38 E-mail: abelnau@nau.edu.ua , abelnau@ukr.net Робоче місце: НАУ, к. 3, ауд. 3-407
Оригінальність навчальної дисципліни	Значна частина алгоритмів криптографічного захисту інформації, що вивчаються в навчальній дисципліні, розроблена співробітниками та студентами кафедри ЕРМІТ на рівні, що не нище, або перевищують світові досягнення.
Лінк на дисципліну	http://kafelec.nau.edu.ua

Завідувач кафедри

Яновський Ф.Й.

Розробник

Білецький А.Я.