



**Силабус навчальної дисципліни  
«НОВІТНІ ТЕХНОЛОГІЇ ПОБУДОВИ СИСТЕМ  
КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЇ»**

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

<b>Рівень вищої освіти</b>	Бакалавр
<b>Статус дисципліни</b>	Навчальна дисципліна вибіркового компонента фахового переліку
<b>Семестр</b>	Весняний
<b>Обсяг дисципліни, кредити ЄКТС/загальна кількість годин</b>	3 кредити / 90 годин
<b>Мова викладання</b>	Українська, англійська
<b>Що буде вивчатися (предмет навчання)</b>	Конкретні типи алгоритмів шифрування та криптографічних перетворень, 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 алгебраїчної теорії шифрування цифрової інформації, теорії еліптичної, квантової та постквантової криптографії, мікро- та наноелектронної елементної бази, які необхідні для вирішення професійних завдань.
<b>Чому це цікаво/потрібно вивчати (мета)</b>	Головною метою викладання навчальної дисципліни «Новітні технології побудови систем комплексного захисту інформації» 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.
<b>Чому можна навчитися (результати навчання)</b>	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.
<b>Як можна користуватися набутими знаннями і вміннями (компетентності)</b>	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.

<b>Навчальна логістика</b>	<p><b>Зміст дисципліни:</b> 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><b>Види занять:</b> Лекції, лабораторні, практичні, модульні контрольні роботи.</p> <p><b>Методи навчання:</b> Навчально-дослідницькі на основі розповіді, дискусії, комп'ютерного моделювання та роботи онлайн.</p> <p><b>Форми навчання:</b> Очна, дистанційна.</p>
<b>Пререквізити</b>	<p>Загальні знання з програм вищої математики та фізики, поглиблене засвоєння основ модулярної арифметики, алгебраїчних структур полів Галуа, незвідних многочленів, вільне володіння комп'ютером.</p>
<b>Пореквізити</b>	<p>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.</p>
<b>Інформаційне забезпечення з фонду та репозиторію НТБ НАУ</b>	<p><a href="http://er.nau.edu.ua/">http://er.nau.edu.ua/</a>  <a href="http://www.lib.nau.edu.ua/main/">http://www.lib.nau.edu.ua/main/</a>  <a href="mailto:ntb@nau.edu.ua">ntb@nau.edu.ua</a></p>
<b>Локація та матеріально-технічне забезпечення</b>	<p>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.</p>
<b>Семестровий контроль, екзаменаційна методика</b>	<p>Контрольні заходи з навчальної дисципліни проводяться у формі:</p> <p><b>поточного контролю</b> – 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><b>проміжного контролю</b> – діагностика рівня опанування навчальним матеріалом в межах змістового модулю;</p> <p><b>підсумкового контролю</b> (екзамен) – діагностика рівня опанування навчальним матеріалом в межах усієї навчальної дисципліни із оцінюванням результатів за національною шкалою і шкалою ECTS;</p> <p><b>Форма проведення екзамену</b> визначається відповідним рішенням кафедри і може базуватися як на традиційній системі опитування за екзаменаційними білетами, так і на основі співбесіди.</p>
<b>Кафедра</b>	<p>Електроніки, робототехніки і технологій моніторингу та Інтернету речей (ЕРМІТ)</p>
<b>Факультет</b>	<p>Аеронавігації, електроніки та телекомунікації (ФАЕТ)</p>

<b>Викладач</b>	<b>ПІБ</b> Білецький Анатолій Якович <b>Посада:</b> Професор <b>Вчений ступінь:</b> Доктор техн. наук <b>Профайл викладача:</b> <a href="http://kafelec.nau.edu.ua">http://kafelec.nau.edu.ua</a> <b>Тел.:</b> +38 (050) 312-23-38 <b>E-mail:</b> <a href="mailto:abelnau@nau.edu.ua">abelnau@nau.edu.ua</a> , <a href="mailto:abelnau@ukr.net">abelnau@ukr.net</a> <b>Робоче місце:</b> НАУ, к. 3, ауд. 3-407
<b>Оригінальність навчальної дисципліни</b>	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.
<b>Лінк на дисципліну</b>	<a href="http://kafelec.nau.edu.ua">http://kafelec.nau.edu.ua</a>

Завідувач кафедри

Яновський Ф.Й.

Розробник

Білецький А.Я.