



Силабус навчальної дисципліни
«Методи захисту інформації для забезпечення
адаптації інформаційно-телекомунікаційних систем
до зовнішніх впливів та живучості зв'язку»
Освітньо-наукова програма: «Телекомунікації та радіотехніка»
Спеціальність: 172 Телекомунікації та радіотехніка
Галузь знань: 17 Електроніка та телекомунікації

Рівень вищої освіти	Третій (освітньо-науковий)
Статус дисципліни	Навчальна дисципліна циклу дисциплін з оволодіння глибинними знаннями зі спеціальності
Курс	1 (перший)
Семестр	2 (другий)
Обсяг дисципліни, кредити ЄКТС/загальна кількість годин	3 кредити / 90 годин
Мова викладання	Українська
Що буде вивчатися (предмет навчання)	Навчальна дисципліна є дисципліною з оволодіння глибинними знаннями зі спеціальності 172 «Телекомунікації та радіотехніка» та спрямована на формування навичок щодо забезпечення інформаційної безпеки сучасних інформаційно-телекомунікаційних систем
Чому це цікаво/потрібно вивчати (мета)	Метою викладання дисципліни є детальне розкриття методів боротьби з кібер загрозами для сучасних інформаційно-телекомунікаційних систем, технологій підвищення живучості цих систем, методів аналізування систем перехоплення інформації в мережевому та безпроводному обладнанні, серверах та обладнанні робочих місць операторів інформаційно-телекомунікаційних систем.
Чому можна навчитися (результати навчання)	<p>ПРН 14. Концептуальні поглиблені знання методологічних і теоретичних основ побудови сучасних телекомунікаційних, інформаційних, радіотехнічних та електронних систем, зокрема для авіаційно-космічної галузі.</p> <p>ПРН 20. Профільовані знання й практичні навички з електроніки, електромагнетизму, оптики, квантової фізики для досліджень у сфері телекомунікацій та радіотехніки.</p> <p>ПРН 22. Знання у галузі інформаційної безпеки з аналізу різного роду загроз, зокрема в інформаційному просторі, уміння розробляти та досліджувати моделі загроз безпеки.</p> <p>ПРН 24. Знання про суб'єкти інформаційної безпеки та інформаційні аспекти кібербезпеки для удосконалення, розроблення та подальшого розвитку методів захисту інформаційно-телекомунікаційних мереж від загроз терористичної діяльності та гібридних війн, зокрема для відповідної складової авіаційної безпеки, уміння їх використовувати.</p> <p>ПРН 26. Уміння використовувати принципи функціонування систем і засобів криптографічного, стеганографічного та технічного захисту</p>

	<p>інформації для адаптації телекомунікаційних систем і мереж зв'язку до зовнішніх впливів, розроблення на цій основі методів підвищення живучості зв'язку.</p> <p>ПРН 27. Уміння відслідковувати тенденції та напрямки розвитку інформаційно-телекомунікаційних та радіотехнічних систем, а також суміжних і прикладних областей, зокрема пов'язаних з авіаційно-космічною галуззю.</p> <p>ПРН 31. Уміння підготувати самостійне розгорнуте дослідження (дисертацію), що пропонує розв'язання актуального наукового завдання в галузі телекомунікацій та/або радіотехніки або на межі кількох галузей, результати якого становлять оригінальний внесок у суму знань галузі телекомунікацій та/або радіотехніки та інших галузей.</p>
<p>Як можна користуватися набутими знаннями і уміннями (компетентності)</p>	<p>ФК 1. Здатність використовувати у науковій та науково-педагогічній діяльності концептуальні поглиблені знання методологічних і теоретичних основ побудови сучасних телекомунікаційних, інформаційних, радіотехнічних та електронних систем, зокрема для авіаційно-космічної галузі.</p> <p>ФК 7. Здатність використовувати професійно профільовані знання й практичні навички з електроніки, електромагнетизму, оптики, квантової фізики для досліджень у сфері телекомунікацій та радіотехніки.</p> <p>ФК 9. Здатність використовувати знання у галузі інформаційної безпеки для аналізу різного роду загроз, зокрема, в інформаційному просторі, а також вміння розробляти та досліджувати моделі загроз безпеки.</p> <p>ФК 11. Здатність використовувати знання про суб'єкти інформаційної безпеки та інформаційні аспекти кібербезпеки для удосконалення, розроблення та подальшого розвитку методів захисту інформаційно-телекомунікаційних мереж від загроз терористичної діяльності та гібридних війн, зокрема для відповідної складової авіаційної безпеки.</p> <p>ФК 13. Здатність використовувати принципи функціонування систем і засобів криптографічного, стеганографічного та технічного захисту інформації для адаптації телекомунікаційних систем і мереж зв'язку до зовнішніх впливів, розроблення на цій основі методів підвищення живучості зв'язку.</p> <p>ФК 14. Здатність відслідковувати тенденції та напрямки розвитку інформаційно-телекомунікаційних та радіотехнічних систем, а також суміжних і прикладних областей, зокрема пов'язаних з авіаційно-космічною галуззю..</p>
<p>Навчальна логістика</p>	<p>Зміст дисципліни: Моделі загроз в інформаційному просторі. Методи запровадження закладних пристроїв в мережеве обладнання. Системи протидії кіберзагрозам. Основні сучасні засоби захисту інформації в інформаційно-телекомунікаційних системах. Тенденції забезпечення інформаційної безпеки на авіаційному транспорті.</p> <p>Види занять: Лекційні та практичні.</p> <p>Методи навчання: робота в малих групах, проблемна дискусія, мозкова</p>

	атака, презентація, комп'ютерне моделювання.
Пререквізити	Базується на таких дисциплінах, як: «Системно-синергетичне моделювання об'єктів досліджень та математичні методи обробки даних в телекомунікаціях та радіотехніці» та «Методи забезпечення надійності та ефективності експлуатації сучасних телекомунікаційних та радіотехнічних систем».
Пореквізити	Є базою таких дисциплін як: «Оптимізація та синтез мережевих структур телекомунікацій», «Аналіз і синтез методів обробки інформації в системах CNS/ATM»
Інформаційне забезпечення з фонду та репозитарію НТБ НАУ	<p>1. Конахович Г.Ф., Прогонов Д.О., Пузиренко О.Ю. Компютерна стеганографічна обробка й аналіз мультимедійних даних: підручник. \ Київ: Центр учбової літератури, 2018.-558с.</p> <p>2. Кузнецов О.О. Захист інформації в інформаційних системах. – Х.: Вид. ХНЕУ, 2017.-512с.</p> <p>3. Konakhovich G., Symonychenko Y., Symonychenko A., Daradkeh Y.I. The research of realization of hidden channel for information transmission with the use of steganographic tools // CEUR Workshop Proceedings, 2020, Volume 2654, pp. 504-515.</p>
Локація та матеріально-технічне забезпечення	Корп. 3, ауд. 3/202, 3/203. Комп'ютери зі спеціалізованими програмами, проектор, екран
Семестровий контроль, екзаменаційна методика	Екзамен, тестування
Кафедра	Кафедра телекомунікаційних та радіоелектронних систем
Факультет	Факультет аеронавігації, електроніки та телекомунікацій
Викладач(і)	 <p>КОНАХОВИЧ ГЕОРГІЙ ФИЛИМОНОВИЧ Посада: професор кафедри ТКРС Науковий ступінь: доктор технічних наук Вчене звання: професор Профайл викладача: http://www.lib.nau.edu.ua/naukpraci/teacher.php?id=11048 Тел.: (068) 100-03-03 E-mail: heorhii.konakhovych@npp.nau.edu.ua Робоче місце: корп. 3, ауд. 3/202</p>
Оригінальність навчальної дисципліни	Авторський курс; оригінальні завдання до практичних робіт
Лінк на дисципліну	Після формування групи слухачів створюється кабінет в GoogleClassroom з необхідними матеріалами для навчання