Силабус навчальної дисципліни
«АУДИТ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»

Спеціальність: 125 Кібербезпека
Галузь знань: 12 Інформаційні технології

Рівень вищої освіти	Доктор філософії
Статус дисципліни	Навчальна дисципліна вибіркового компонента фахового переліку
Курс	2 (другий)
Семестр	4 (четвертий)
Обсяг дисципліни, кредити ЄКТС/загальна кількість годин	5 кредитів/150 годин
Мова викладання	Українська
Що буде вивчатися (предмет навчання)	Дана навчальна дисципліна є теоретичною та практичною основою сукупності знань та вмінь, що формують профіль фахівця в галузі безпеки інформаційних технологій. Місце даної дисципліни є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області кібербезпеки. Використання методів фундаментальних наук для розв'язання загально інженерних, професійних та наукових задач; Генерація нових ідей і варіантів розв'язання задач в галузі кібербезпеки; Застосування сучасних процедур аудиту кібербезпеки об'єктів критичної інфраструктури для створення системи захисту критичної інфраструктури; Проведення аналізу можливих загроз та потенційних негативних наслідків, а також запобігання та попередження виникнення таких загроз для критичної інфраструктури; Розробка та використання засобів, що можуть використовуватись для аудиту кібербезпеки об'єктів критичної інфраструктури.
Чому це цікаво/потрібно вивчати (мета)	Метою дисципліни є вивчення та застосування сучасних процедур аудиту кібербезпеки об'єктів критичної інфраструктури для ефективного забезпечення захисту критичної інфраструктури держави.
Чому можна навчитися (результати навчання)	ПРН4. Здатність та уміння використовувати математичний апарат (теорії нечітких множин, математичної статистики, теорії імовірності тощо) для освоєння теоретичних основ, моделювання даних, практичного використання (обробки експериментальних даних), розробки нових та удосконалення існуючих методів, засобів та систем у сфері інформаційної та кібербезпеки. ПРН5. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем аналізу і оцінювання ризиків інформаційної та/або кібербезпеки при побудові комплексних систем захисту інформації, систем управління інформаційною безпекою, аудит стану кібербезпеки. ПРН6. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем аналізу і оцінювання негативних наслідків (шкоди) державі, суспільству, приватній чи юридичній особі у разі витоку державних інформаційних ресурсів, інформації з обмеженим доступом. ПРН7. Здатність проводити дослідження, розвиток та удосконалення

	сучасних нейромережевих моделей, методів, засобів та систем виявлення нових загроз, мережевих кібератак, шкідливого програмного забезпечення, аналізу і оцінювання параметрів стану забезпечення активного захисту та кібербезпеки інформаційних (автоматизованих), інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури. ПРН8. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем виявлення вторгнень, визначати їх базові характеристики, а також обґрунтовано обирати та застосовувати в практичній роботі при побудові систем кібербезпеки. ПРН9. Здатність продемонструвати знання та розуміння застосування методів, моделей та засобів ідентифікації аномальних станів для побудови систем виявлення вторгнень заснованих на теорії нечітких множин. ПРН10. Вміти аналізувати, обґрунтовувати вибір та застосовувати методи фундаментальної та прикладної математики задля розв'язання задач аналізу, проектування і розробки елементів інтелектуальних систем кібербезпеки. ПРН11. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем кібербезпеки в умовах неповної визначеності.
Як можна користуватися набутими знаннями і вміннями (компетентності)	ФК3. Здатність та уміння проводити дослідження теоретичних, науково-технічних і технологічних проблем, пов'язаних із організацією, створенням методів та засобів забезпечення захисту інформації та/або кібербезпеки при її зберіганні, обробці й передачі з використанням сучасних математичних методів, інформаційних технологій та технічних засобів. ФК4. Здатність та уміння проводити дослідження проблеми забезпечення інформаційної безпеки національних інтересів України, вивчати і обґрунтовувати форми та методи захисту людини, суспільства й держави від зовнішніх і внутрішніх загроз в інформаційній сфері, а також шляхи підвищення ефективності функціонування інформаційних систем держави в сучасних умовах. ФК5. Уміння застосовувати та розробляти сучасні технології, системи, технічні засоби, методи та моделі, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій, освітній та професійній діяльності; ФК7. Здатність та уміння проводити дослідження проблеми забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів, інформаційні ресурси різних класів на об'єктах інформаційної діяльності та критичної інфраструктури, системи управління, на основі технології, методів, моделей та засобів у сфері інформаційної безпеки та/або кібербезпеки (пропозиція на основі стандарту магістра 125 «Кібербезпека»).
Навчальна логістика	**Зміст дисципліни:** Віднесення об'єктів до критичної інфраструктури. Категорії критичності об'єктів інфраструктури. Критерії віднесення об'єктів до критичної інфраструктури. Реєстр об'єктів критичної інфраструктури. Паспортизація об'єктів критичної інфраструктури. Процедури аудиту кібербезпеки об'єктів критичної інфраструктури. Розробка та використання засобів, що можуть використовуватись для аудиту кібербезпеки об'єктів критичної інфраструктури. **Види занять:** лекції, практичні **Методи навчання:** навчальна дискусія, онлайн **Форми навчання:** очна, заочна, дистанційна

Пререквізити	Теоретичною базою вивчення дисципліни є попередні навчальні дисципліни: «Правове, економічне та інформаційне забезпечення наукових досліджень», «Методологія наукових досліджень у сфері кібербезпеки», «Наукові розробки та дослідження у сфері інформаційної безпеки та кібербезпеки (у т.ч. наукової школи «Кібербезпеки» НАУ)», «Теоретико-множинне моделювання даних для вирішення задач кібербезпеки/захисту інформації», «Англійська мова наукового спрямування».
Пореквізити	Результати навчання даного курсу можуть бути використані під час написання кандидатської дисертації.
Інформаційне забезпечення з фонду та репозитарію НТБ НАУ	**Начальна та наукова література:** 1 Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.. 2. Л. Щербак, С. Гнатюк, В. Сидоренко, О. Шаховал, «Метод визначення рівня важливості об'єктів критичної інформаційної інфраструктури в галузі цивільної авіації», Безпека інформації, Том 23, №1, с. 27- 38, 2017. 3. В. Сидоренко, А. Положенцев, С. Гнатюк, «Метод оцінювання рівня кібербезпеки галузі критичної інформаційної інфраструктури держави», Вісник інженерної академії України, Вип. 42, с. 81- 89, 2017.
Локація та матеріально-технічне забезпечення	Аудиторія теоретичного навчання, проектор
Семестровий контроль, екзаменаційна методика	Залік, тестування
Кафедра	Безпеки інформаційних технологій
Факультет	Кібербезпеки, комп'ютерної та програмної інженерії
Викладач(і)	 **Сидоренко Вікторія Миколаївна** **Посада:** доцент **Вчене звання:** доцент **Науковий ступінь:** кандидат технічних наук **Профайл викладача:** http://bit.nau.edu.ua/sklad/918 **Тел.:** +38(044) 406-70-22 **E-mail:** v.sydorenko@ukr.net **Робоче місце: 11.422**
Оригінальність навчальної дисципліни	Авторський курс, викладання українською мовою
Лінк на дисципліну	