

Силабус дисципліни

Назва дисципліни, обсяг у кредитах ЄКТС	Теорія проектування захищених комп'ютерних мереж; 7 кр.
Загальна інформація про викладача	Пахомова В.М., к.т.н., доцент кафедри «Електронні обчислювальні мережі», доцент, (056)373-15-89, viknikpakh@gmail.com
Семестр, у якому можливе (планується) вивчення дисципліни	2-й семестр для магістрів
Факультети, студентам яких пропонується вивчити дисципліну	Факультет «КТС», спеціальність «Кібербезпека»
Перелік компетентностей та відповідних результатів навчання, що забезпечує дисципліна	<p>Перелік компетентностей:</p> <ol style="list-style-type: none"> 1. Здатність до абстрактного мислення, аналізу та синтезу (загальна компетентність, ЗК1). 2. Здатність спілкуватися та користуватися інформаційними джерелами іноземною мовою (загальна компетентність, ЗК2). 3. Здатність використання інформаційних та комунікаційних технологій (загальна компетентність, ЗК3). 4. Здатність до пошуку, опрацювання та аналізу інформації з різних джерел (загальна компетентність, ЗК5). 5. Здатність до генерації нових ідей і варіантів розв'язування задач, до комбінування та експериментування, до оригінальності, конструктивності, економічності та простих рішень (загальна компетентність, ЗК6). 6. Здатність приймати обґрунтовані рішення (загальна компетентність, ЗК7). 7. Здатність застосовувати практичні методи, методологічні аспекти та комп'ютерну логіку при конструюванні, побудові та схемотехніці апаратних та програмних засобів захисту комп'ютерних систем та мереж, з врахуванням вимог техніки безпеки, охорони праці та протипожежної безпеки в професійній діяльності (професійна компетентність, ФК1). 8. Здатність до побудови ефективних алгоритмів формального прогнозу, моделей та методів змістовного прогнозування в методах захисту шляхом використання принципів функціонування та структури технічних засобів, математичних моделей, історії та логіки розвитку галузі у контексті відповідних величин, феноменів, моделей, методів функцій та структур технічних засобів, формальних та змістовних методів прогнозування функцій, структур, характеристик та параметрів комп'ютерних систем та мереж (професійна компетентність, ФК2). 9. Здатність проводити розробку і дослідження теоретичних та експериментальних моделей захисту об'єктів професійної діяльності (професійна компетентність, ФК3). 10. Здатність аналізувати, оптимізувати та моделювати складність архітектури комп'ютерної системи та мереж із застосуванням сучасних принципів побудови математичного, програмного, лінгвістичного, технічного та інформаційного забезпечення для захисту інформації (професійна компетентність, ФК5). 11. Здатність використовувати механізми штучного інтелекту для вирішення проблем забезпечення кібербезпеки, що складно формалізувати (професійна компетентність, ФК15). <p>Програмні результати навчання:</p> <ol style="list-style-type: none"> 1. Знати і розуміти наукові і математичні положення, що лежать в основі функціонування програмних і програмно-технічних засобів захисту інформації в комп'ютерних системах та мережах (ПРН1). 2. Знати професійно-орієнтовані дисципліни спеціальності (ПРН2). 3. Мати знання та навички щодо проведення експериментів, збору даних та моделювання загроз в комп'ютерних системах (ПРН3). 4. Уміння застосовувати знання і розуміння для розв'язку задач синтезу та аналізу захисних засобів в системах, які характерні обраній спеціальності (ПРН6). 5. Уміння використовувати сучасні комп'ютерні засоби системного, функціонального, конструктивного та технологічного проектування для створення сучасних захисних систем (ПРН7). 6. Уміння виконувати експериментальні дослідження та застосувати дослідницькі навички за професійною тематикою (ПРН8). 7. Уміння здійснювати збір, аналіз науково-технічної інформації, вітчизняного і зарубіжного досвіду з тематики дослідження (ПРН9). 8. Уміння використати набуті знання з спеціальності для знаходження нових, нешаблонних рішень і засобів їх здійснення при проведенні експериментальних досліджень для розв'язку поставлених задач (ПРН10).

	<p>9. Уміння опрацьовувати отримані результати, аналізувати та осмислювати їх, представляти результати роботи і обґрунтовувати запропоновані рішення на сучасному науково-технічному і професійному рівні (ПРН12).</p> <p>10. Уміння використати сучасні комп'ютерні засоби системного, функціонально-конструктивного та технологічного проектування програмних та апаратних засобів захисту інформації (ПРН14).</p> <p>11. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення (ПРН19).</p> <p>12. Відповідально ставитись до виконуваної роботи та досягати поставленої мети з дотриманням вимог професійної етики (ПРН20).</p>
Опис дисципліни	
Попередні умови, необхідні для вивчення дисципліни	Знання з вищої математики, комп'ютерних мереж, локальних мереж, систем штучного інтелекту, програмування
Максимальна кількість студентів, які можуть одночасно навчатися	Група 30-35 чоловік
Теми аудиторних занять та самостійної роботи	<p>32 год. лекцій, 16 год. практичних занять та 16 год. лабораторних робіт</p> <p>Основні теми лекцій:</p> <ul style="list-style-type: none"> • Імітаційне моделювання як основний метод проектування комп'ютерних мереж • Взаємодія імітаційного моделювання з теорією планування експерименту (ТПЕ) • Інтелектуальні методи мультиагентної оптимізації: мурашиний та ін. • Маршрутизація в комп'ютерній мережі на основі використання нейронної мережі • Прогнозування мережного трафіку з використанням нейромережної технології • Технологія виявлення мережних атак <p>Основні теми практичних занять:</p> <ul style="list-style-type: none"> • Дослідження протоколів маршрутизації на імітаційній моделі мережі в системі Ornet Modeler • Дослідження технології MPLS на імітаційній моделі мережі в системі Ornet Modeler • Організація експериментів на імітаційній моделі мережі з використанням ТПЕ <p>Основні теми лабораторних робіт:</p> <ul style="list-style-type: none"> • Вибір оптимального маршруту в комп'ютерній мережі засобами багатопарової нейронної мережі • Прогнозування мережного трафіку на основі використання нейронечіткої мережі • Визначення загроз в комп'ютерній мережі з використанням багатопарової нейронної мережі <p>Курсове проектування: Дослідження існуючої або проектування нової комп'ютерної мережі залізничного транспорту з використанням методів штучного інтелекту</p> <p>Самостійна робота:</p> <ul style="list-style-type: none"> • Нейронні мережі: мережа Хопфілда та ін. • Методи штучного інтелекту (що не розглядалися на заняттях)
Мова викладання	українська
Список основної та додаткової літератури	<p>Основна:</p> <ol style="list-style-type: none"> 1. Дистанційний курс з дисципліни «Теорія проектування захищених комп'ютерних мереж»; укладач доц. Пахомова В. М.; www.lider.diit.edu.ua 2. Пахомова В. М. Дослідження інформаційно-телекомунікаційної системи залізничного транспорту з використанням штучного інтелекту. Дніпро: Вид-во ПФ «Стандарт-Сервіс», 2018. 220 с. 3. Методичні поради до виконання лабораторних робіт з дисципліни «Теорія проектування комп'ютерних мереж»; укладач доц. Пахомова В. М. Дніпро: ДНУЗТ, 2019. 4. Методичні поради до виконання практичних робіт з дисципліни «Теорія проектування комп'ютерних мереж»; укладач доц. Пахомова В. М. Дніпро: ДНУЗТ, 2020. 5. Методичні поради до виконання курсового проєкту з дисципліни «Теорія проектування комп'ютерних мереж»; укладач доц. Пахомова В. М. Дніпро: ДНУЗТ, 2021. <p>Додаткова:</p> <ol style="list-style-type: none"> 6. Пахомова В. М. Можливості розвитку комп'ютерних мереж в автоматизованих системах залізничного транспорту. Дніпропетровськ: ДНУЗТ, 2015. 203 с. 7. Пахомова В. М. Дослідження характеристик локальної обчислювальної мережі методом імітаційного моделювання. Методичний посібник. Дніпропетровськ: ДІТ, 2000. 45 с. 8. Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі. Київ: Юніор, 2005. 396 с. 9. Глибовець М.М., Олецкий О.В. Штучний інтелект. Київ: Видавничий дім «КМ Академія», 2002. 336 с.