

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

ЗАТВЕРДЖУЮ



Ф-КАТАЛОГ
ВИБІРКОВИХ НАВЧАЛЬНИХ ДИСЦИПЛІН
ЦИКЛУ ПРОФЕСІЙНОЇ ПІДГОТОВКИ
для здобувачів ступеня доктора філософії за освітньою програмою
«Кібербезпека» за спеціальністю 125 Кібербезпека

УХВАЛЕНО:

Методичною радою
КПІ ім. Ігоря Сікорського
(протокол № 3 від «27» січня 2022 р.)

Вченою радою НН ФТІ
КПІ ім. Ігоря Сікорського
(протокол № 22 від « 28 » грудня 2021 р.)

Київ – 2022

Процедура вибору освітніх компонент відбувається згідно «Положення про реалізацію права на вільний вибір навчальних дисциплін здобувачами вищої освіти КПІ ім. Ігоря Сікорського»

https://osvita.kpi.ua/sites/default/files/downloads/Pologennia_vilnyi_vybir_2022.pdf

Силабуси усіх дисциплін та інша супровідна інформація розміщена на сайті кафедри:

<http://is.ipt.kpi.ua>

Дисципліни для вибору першокурсниками на другий рік навчання		
Необхідно обрати по одній дисципліні з наведених нижче для вивчення у кожному семестрі		
Третій (осінній) семестр		
<i>Дисципліна (5 кредитів, залік)</i>	<i>Кафедра</i>	<i>Стор.</i>
Моделі та методи оцінювання ризиків	ІБ	3
Моделі систем керування	ІБ	4
Сучасні методи обробки сигналів	ІБ	5
Четвертий (весняний) семестр		
<i>Дисципліна (5 кредитів, залік)</i>	<i>Кафедра</i>	<i>Стор.</i>
Сучасні технології кібербезпеки	ІБ	6
Математичні моделі кібербезпеки	ІБ	7
Кібернетичні моделі загроз, ризиків та контрдії інформаційної безпеки	ІБ	8
Інформаційна ентропія функціонального аналізу і квантова стеганографія	ІБ	9

Перелік позначень

Кафедри та факультети:

ІБ – кафедра інформаційної безпеки, ННФТІ

Дисципліна	Моделі та методи оцінювання ризиків		
Рівень ВО	Третій (підготовка докторів філософії)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, залік	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	Професор Даник Ю.Г.		
Вимоги до початку вивчення	1. Базові знання теорії ймовірностей, математичної статистики, теорії ризиків, теорії моделювання. 2. Вміння працювати з будь-якими програмними засобами з математичними функціями.		
Анотація дисципліни	<p>Ознакою сучасного суспільства є інтенсивний розвиток високих технологій та пов'язаних з цим загроз і ризиків. Поширеність та масовість виникнення ризиків в усіх сферах людської діяльності є стимулом пошуку способів їх пом'якшення або ж уникнення. Ризик – це також неминучий супутник будь-яких відкриттів, технологічних проривів, вдалих інноваційних та управлінських дій.</p> <p>У загальному випадку ризики аналізуються та досліджуються з певних позицій, частіше за все з діяльнісно-галузевих: в економіці, екології, політиці, науці, техніці, медицині, військовій галузі, підприємстві тощо. В цій ситуації на перший план виходить розгляд умов виникнення й розвинення ризикових ситуацій, механізмів та стадій формування ризику, знання типових моделей ризиків, що дозволяють формалізувати опис та дослідження ризиків незалежно від сфери їх існування, розгляду загальних аспектів яких присвячений цей курс.</p> <p>Мета дисципліни – формування у аспірантів знань щодо моделей, методів і засобів оцінювання ризиків та їх застосування в процесі проведення наукових досліджень, здатності діяти на основі вимог відповідних стандартів в галузі інформаційної і кібербезпеки та використовувати сучасні засоби управління ризиками в різних сферах діяльності.</p>		
Форма проведення занять	Лекції та практичні заняття		

Дисципліна	Моделі систем керування		
Рівень ВО	Третій (підготовка докторів філософії)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, залік	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	Доцент Смирнов С.А.		
Вимоги до початку вивчення	Для розуміння змісту курсу слухачам бажано попередньо володіти знаннями з наступних галузей: математичний аналіз, дискретний аналіз, лінійна алгебра, математичне моделювання, аналіз сигналів, теорія інформації, оптимальні рішення.		
Анотація дисципліни	<p>В курсі вивчаються основні закони, відповідні структури та алгоритми систем керування як класичними (аналоговими), так і сучасними (цифровими) об'єктами. Сучасний стан та перспективи розвитку кіберпростору людства багато в чому визначаються т. зв. вбудованими системами, які складають технічну базу Інтернету речей і, таким чином, забезпечують подальше його поширення та проникнення у всі сфери практичної діяльності. Системи керування, в свою чергу, є невід'ємною частиною вбудованих систем, які забезпечують імплементацію керуючих та інформаційних процесів у реальні технічні об'єкти, але також створюють нові вразливості та небезпеки внаслідок наявного мережевого доступу до них. Мета курсу полягає в оволодінні сучасними принципами та методами організації процесів керування у вбудованих системах з особливою увагою до відповідних небезпек та можливостей захисту.</p> <p>Моделі систем керування з врахуванням небезпек мережевого доступу мають значну цінність в сучасних умовах, бо вони є математичним фундаментом для організації захисту від проникнення з метою перехвату управління, що є однією з головних проблем саме кібербезпеки, актуальність якої лише зростає.</p>		
Форма проведення занять	Лекції та практичні заняття		

Дисципліна	Сучасні методи обробки сигналів		
Рівень ВО	Третій (підготовка філософії) докторів	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, залік	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	Доцент Прогонов Д.О.		
Вимоги до початку вивчення	<ul style="list-style-type: none"> • Знання основ спектрального аналізу одновимірних та багатовимірних сигналів; • Знання основ лінійної алгебри; • Знання основ теорії оптимізації (методи оптимізації функцій багатьох змінних, методи опуклої оптимізації); • Навички роботи з системами комп'ютерної математики та сучасними пакетами комп'ютерного моделювання на мові Python. 		
Анотація дисципліни	<p>Дисципліна присвячена огляду сучасних методів обробки багатовимірних сигналів, зокрема знешумлення, відновлення сигналів за частковими даними та розпізнавання слабких сигналів на фоні значних завад. Досліджуються новітні методи спектрального аналізу сигналів, наприклад SSA-аналіз, bandlet-аналіз, а також підходи до статистичного моделювання сигналів. Особлива увага приділяється методам компонентного аналізу, що дозволяють проводити реконструкцію сигналів в умовах обмеженості апіорних даних щодо виду та параметрів завад.</p> <p>За результатами вивчення курсу слухачі отримають навички обробки багатовимірних сигналів (знешумлення, відновлення за частковими даними) в сучасних системах комп'ютерної математики.</p>		
Форма проведення занять	Лекції та практичні заняття		

Дисципліна	Сучасні технології кібербезпеки		
Рівень ВО	Третій (підготовка філософії) докторів	Курс	Другий курс (четвертий семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, залік	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	Доцент Грайворонський М.В.		
Вимоги до початку вивчення	Щоб краще сприймати інформацію здобувачі освіти повинні мати диплом магістра за спеціальністю "Кібербезпека". Випускники магістратури інших спеціальностей для ефективного засвоєння курсу повинні добре володіти стандартними технологіями захисту інформації, такими як криптографічний захист, розмежування доступу, міжмережне екранування, віртуальні приватні мережі		
Анотація дисципліни	<p>Одним з найважливіших завдань кібербезпеки є своєчасне розпізнавання спроб атак для ефективної їм протидії. Сучасні технології кібербезпеки передбачають комбінування традиційних методів захисту інформації з проактивним захистом і штучним інтелектом. В курсі розглядаються різні методи збирання і оброблення інформації (зокрема, SIEM системи) для виявлення і класифікації аномалій. Практичні заняття проводяться на базі кібер-полігону кафедри з моделюванням атак та їх виявлення.</p> <p>Курс "Сучасні технології кібербезпеки" повністю забезпечений, як лекційними аудиторіями з сучасною технікою для проведення лекцій у формі презентацій, так і комп'ютерним класом (кібер-полігоном), який має необхідне програмне забезпечення.</p>		
Форма проведення занять	Лекції та практичні заняття		

Дисципліна	Математичні моделі кібербезпеки		
Рівень ВО	Третій (підготовка філософії) докторів	Курс	Другий курс (четвертий семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, залік	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	Доцент Смирнов С.А.		
Вимоги до початку вивчення	Для розуміння змісту курсу слухачам бажано попередньо володіти знаннями з наступних навчальних дисциплін: математичне моделювання, дискретний аналіз, теорія ймовірностей та статистика, оптимальні рішення.		
Анотація дисципліни	<p>В курсі вивчаються математичні моделі з акцентом на нові задачі кібербезпеки, пов'язані з поєднанням та спільним застосуванням сигнально-інформаційних, матеріально-енергетичних та керуючих процесів в сучасних складних системах, з врахуванням також особливої ролі суб'єкта керування та різноманітних аспектів складності. Навчальна дисципліни містить наступні розділи:</p> <ul style="list-style-type: none"> • Моделі складних систем, моделі невизначеності, методи подолання невизначеностей, структурний аспект складності, методи структурного аналізу, відповідні системні вразливості. • Наявність/відсутність рефлексії суб'єктів, моделі взаємодії рефлексивних суб'єктів, відповідні вразливості процесів прийняття рішень. • Мережевий доступ до систем керування, вразливості систем керування, загрози перехвату управління та відповідні моделі. <p>Мета курсу – навчити використовувати методи і прийоми моделювання складних сценаріїв кібербезпеки, аналізувати отримані моделі, визначати загрози та вразливості, пов'язані з їх структурою та наповненням, а також з варіантами доступності інформації про це.</p>		
Форма проведення занять	Лекції та практичні заняття		

Дисципліна	Кібернетичні моделі загроз, ризиків та контрдії інформаційної безпеки		
Рівень ВО	Третій (підготовка докторів філософії)	Курс	Другий курс (четвертий семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, залік	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	Доцент Луценко В.М.		
Вимоги до початку вивчення	<ul style="list-style-type: none"> • Знання вітчизняних та міжнародних нормативних документів в галузі інформаційної та кібернетичної безпеки; • Знання основ теорії ризиків; • Знання класифікації загроз в галузі інформаційної та кібернетичної безпеки, основних методик визначення та аналізу даних загроз. 		
Анотація дисципліни	<p>В Законі України "Про захист інформації в інформаційно-телекомунікаційних системах" зазначені вимоги до контрдій кіберзагрозам в "Статті 10. Повноваження державних органів у сфері захисту інформації в системах", а саме в розділі 7, де державні органи "здійснюють заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дають рекомендації з питань запобігання такій загрозі." Таким чином, засоби забезпечення інформаційної безпеки розглядаються законодавцем саме як засоби протидії кіберзлочинності.</p> <p>При формуванні моделей загроз, ризиків та контрдій в галузі інформаційної безпеки основним матеріалом є нормативно-правова база з інформаційної безпеки та ТЗІ в Україні та базові знання слухачів з питань: відомі підходи до класифікації загроз; докладні знання щодо змісту ДСТУ 3396 та підходів до його використання.</p>		
Форма проведення занять	Лекції та практичні заняття		

Дисципліна	Інформаційна ентропія функціонального аналізу і квантова стеганографія		
Рівень ВО	Третій (підготовка філософії) докторів	Курс	Другий курс (четвертий семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, залік	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	Професор Мачуський Є.А.		
Вимоги до початку вивчення	Дисципліна базується на знаннях основ квантової фізики, статистичного моделювання, теорії інформації, спектрального аналізу сигналів та вимагає навичок математичного моделювання та програмування.		
Анотація дисципліни	<p>Дисципліна розглядає та узагальнює принципи математичної та фізичної спорідненості інформаційної ентропії систем числення та функціонального аналізу з енергетичною ентропією у фізичних рівняннях руху матеріальних тіл та хвиль у різних середовищах і вказує нові напрямки пошуку у царині квантових метрик, квантових обчислень і квантової стеганографії.</p> <p>Метою навчальної дисципліни «Інформаційна ентропія функціонального аналізу і квантова стеганографія» є формування у студентів компетентностей із застосування новітніх методів функціонального аналізу та квантової стеганографії.</p>		
Форма проведення занять	Лекції та практичні заняття		