НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

ЗАТВЕРДЖЕНО:

Методичною радою
КПІ ім. Ігоря Сікорського
(протокол № 5 від «06» 03 2025 р.)

Ф-КАТАЛОГ
ВИБІРКОВИХ НАВЧАЛЬНИХ ДИСЦИПЛІН
ЦИКЛУ ПРОФЕСІЙНОЇ ПІДГОТОВКИ

для здобувачів ступеня доктора філософії за освітньою програмою
«Кібербезпека» за спеціальністю 125 Кібербезпека та захист інформації

УХВАЛЕНО:

Вченою радою НН ФТІ
КПІ ім. Ігоря Сікорського
(протокол №1 від «27» січня 2025 р.)

Київ – 2025

Дисципліни вільного вибору студентів (вибіркові дисципліни), спрямовані на забезпечення загальних та фахових компетенцій за спеціальністю. Обсяг вибіркових навчальних дисциплін становить не менше 25% від загальної кількості кредитів ЄКТС. Вибір дисциплін регламентується «Положенням про реалізацію права на вільний вибір навчальних дисциплін здобувачами вищої освіти КПІ ім. Ігоря Сікорського» (https://osvita.kpi.ua/node/185).

Ф-Каталог містить анотований перелік вибіркових дисциплін, які, відповідно до освітньої програми, беруть участь у формуванні фахових компетентностей. Вибір дисциплін здійснюється у весняному семестрі, що передує навчальному року в системі «my.kpi.ua».

У разі неможливості формування навчальних груп для вивчення певної дисципліни студентам надається можливість здійснити повторний вибір, приєднавшись до вже сформованих навчальних груп (друга хвиля вибору). Результати вибору здобувачем навчальних дисциплін зазначаються в його індивідуальному навчальному плані в розділі «Обрані дисципліни» та засвідчуються його особистим підписом. Навчальні дисципліни, які внесені до індивідуального навчального плану здобувача, є обов'язковими для вивчення у відповідному семестрі.

Зверніть увагу: в анотаціях дисциплін Ф-каталогу вказуються викладачі, які попередньо плануються в якості лекторів відповідних дисциплін. Однак інколи можливі зміни, і лектор з обраної дисципліни не збігатиметься із зазначеним прізвищем!

Перелік позначень

Кафедри:

ММАД – кафедра математичного моделювання та аналізу даних
ММЗІ – кафедра математичних методів захисту інформації
ІБ – кафедра інформаційної безпеки
ПФ – кафедра прикладної фізики

Дисципліни для вибору першокурсниками на другий рік навчання		
Студенти першого курсу обирають одну дисципліну з наведеного нижче переліку для вивчення у третьому семестрі та одну для вивчення у четвертому		
Третій (осінній) семестр		
Дисципліна (1 слот, 6 кредитів, залік)	Кафедра	Стор.
Моделі та методи оцінювання ризиків	ІБ	4
Моделі систем керування	ІБ	5
Сучасні методи обробки сигналів	ІБ	6
Четвертий (весняний) семестр		
Дисципліни (1 слот, 6 кредитів, залік)	Кафедра	Стор.

Сучасні технології кібербезпеки	ІБ	8
Математичні моделі кібербезпеки	ІБ	9
Кібернетичні моделі загроз та ризиків, контрдії інформаційної безпеки	ІБ	10
Інформаційна ентропія функціонального аналізу і квантова стеганографія	ІБ	12

МОДЕЛІ ТА МЕТОДИ ОЦІНЮВАННЯ РИЗИКІВ (Професор Даник Ю.Г.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	3
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	150 годин (5 кредитів ECTS) (10 год. лекцій, 8 год. практичних, 132 год. СР)
Мова викладання	українська
Вимоги для початку вивчення дисципліни	1. Базові знання теорії ймовірностей, математичної статистики, теорії ризиків, теорії моделювання. 2. Вміння працювати з будь-якими програмними засобами з математичними функціями.
Що буде вивчатися	Ризики аналізуються та досліджуються з певних позицій, частіше за все з діяльнісно-галузевих: в економіці, екології, політиці, науці, техніці, медицині, військовій галузі, підприємництві 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.
Чому це цікаво/треба вивчати	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.
Чому можна навчитися	Формування моделей, розробка методів і засобів оцінювання ризиків та їх застосування в процесі проведення наукових досліджень.
Як можна користуватися набутими знаннями і вміннями	Оцінювати ризики на основі вимог відповідних стандартів в галузі інформаційної і кібербезпеки та використовувати сучасні засоби управління ризиками в різних сферах діяльності.
Інформаційне забезпечення дисципліни	Посилання на дистанційний ресурс на платформі “Сікорський” https://do.ipo.kpi.ua/course/view.php?id=3245
Вид семестрового контролю	залік

МОДЕЛІ СИСТЕМ КЕРУВАННЯ (Доцент Смирнов С.А.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	3
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ECTS (18 годин лекцій, 10 годин практик, 132 години СР)
Мова викладання	українська
Вимоги для початку вивчення дисципліни	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.
Що буде вивчатися	В курсі вивчаються основні закони, відповідні структури та алгоритми систем керування як класичними (аналоговими), так і сучасними (цифровими) об’єктами, а також їх гібриди.
Чому це цікаво/треба вивчати	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 мережевого доступу до них.
Чому можна навчитися	Мета курсу полягає в оволодінні сучасними принципами та методами організації процесів керування у вбудованих системах з особливою увагою до відповідних небезпек та можливостей захисту.
Як можна користуватися набутими знаннями і вміннями	Моделі систем керування з урахуванням небезпек мережевого доступу мають значну цінність в сучасних умовах, бо вони є базою для організації захисту від проникнення з метою перехвату управління, що є однією з головних проблем саме кібербезпеки, актуальність якої лише зростає.
Інформаційне забезпечення дисципліни	Посилання на дистанційний ресурс: Платформа “Сікорський”, курс “Моделі систем керування” https://classroom.google.com/c/NTE0NjIwNjg2NzMw?cjc=s4bvykb
Вид семестрового контролю	залік

СУЧАСНІ МЕТОДИ ОБРОБКИ СИГНАЛІВ (Доцент Прогонов Д.О.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	3
Курс, семестр	2 курс, У семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ECTS (18 годин лекцій, 10 годин практик, 132 години СР)
Мова викладання	українська
Вимоги для початку вивчення дисципліни	• Знання принципів спектрального аналізу сигналів (перетворення Фур'є, косинусне перетворення) та його застосування для обробки сигналів/даних • Знання методів для вирішення задач однокритеріальної оптимізації з обмеженнями (метод градієнтного спуску, метод спряжених градієнтів, метод Ньютона тощо) • Розуміння основ функціонального аналізу, зокрема лінійних операторів • Практичні навички роботи в системах комп'ютерної математики або навички використання програмних бібліотек (Python, C/C++) для обробки даних
Що буде вивчатися	• Вейвлет-перетворення одно- та багатовимірних сигналів • Спеціальні види вейвлет-перетворень (ріджлет/ширлет/бандлет перетворення тощо), та їх застосування для оцінки параметрів сигналів • Методи декомпозиції адитивної суміші сигналу та завад (метод головних компонентів, метод незалежних компонентів) • Методи оцінки статистичних, спектральних та структурних параметрів сигналів • Основи структурного аналізу сигналів
Чому це цікаво/треба вивчати	• Огляд сучасних методів виявлення, локалізації просторового/часового положення сигналів та визначення їх структури в умовах обмеженості даних щодо параметрів сигналів • Отримання навичок щодо вибору ефективних методів придушення впливу сильних адитивних/мультиплікативних завад
Чому можна навчитися	• Виявлення сигналів в умовах обмеженості апріорних даних щодо їх статистичних параметрів • Практичні навички використання методів структурного аналізу сигналів у сучасних системах

	комп’ютерної математики
Як можна користуватися набутими знаннями і вміннями	• Розширення доступних теоретичних та практичних інструментів для аналізу та обробки сигналів різної фізичної природи • Практичні навички застосування спеціалізованих методів структурного аналізу даних, виявлення прихованих закономірностей та особливостей структури сигналів
Інформаційне забезпечення дисципліни	• Murphy Kevin P. Machine Learning: A Probabilistic Perspective. – Adaptive Computation and Machine Learning series. – 1st edition. – The MIT Press, 2012. – 1104 p. – ISBN 978-0262018029. • Bishop Christopher M. Pattern Recognition and Machine Learning. – Information Science and Statistics series. – Springer, 2011. – 738 p. – ISBN 978-0387310732. • Mallat S. A Wavelet Tour of Signal Processing, Third Edition: The Sparse Way. – 3rd edition. – Academic Press, 2008. – 832 p. – ISBN 978-0123743701. • The transforms and applications handbook. – The electronic engineering handbook series. – 2nd edition, edited by Alexander D. Poularikas. – CRC Press and IEEE Press, 2000. – 1335 p. – ISBN 0-8493-8595-4.
Вид семестрового контролю	залік

СУЧАСНІ ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ (Доцент Коломицев М.В.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	3
Курс, семестр	2 курс, 4 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кред (150 годин) 10 лек., 8 прак., 132 години СР
Мова викладання	українська
Вимоги для початку вивчення дисципліни	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
Що буде вивчатися	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.
Чому це цікаво/треба вивчати	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.
Чому можна навчитися	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.
Як можна користуватися набутими знаннями і вміннями	На основі методів збирання і оброблення інформації (зокрема, SIEM систем) для виявлення і класифікації аномалій, забезпечувати своєчасне розпізнавання спроб атак для ефективної їм протидії.
Інформаційне забезпечення дисципліни	Посилання на дистанційний ресурс: Платформа “Сікорський”, https://do.ipo.kpi.ua/course/view.php?id=5597
Вид семестрового контролю	залік

МАТЕМАТИЧНІ МОДЕЛІ КІБЕРБЕЗПЕКИ (Доцент Смирнов С.А.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	3
Курс, семестр	2 курс, 4 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ECTS (18 годин лекцій, 10 годин практик, 132 години СР)
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Для розуміння змісту курсу слухачам бажано попередньо володіти знаннями з наступних навчальних дисциплін: математичне моделювання, дискретний аналіз, теорія ймовірностей та статистика, оптимальні рішення.
Що буде вивчатися	Навчальна дисципліни містить наступні розділи: 1) Моделі складних систем, моделі невизначеності, методи подолання невизначеностей, структурний аспект складності, методи структурного аналізу, відповідні системні вразливості. 2) Наявність або відсутність рефлексії суб'єктів, моделі взаємодії рефлексивних суб'єктів, відповідні вразливості процесів прийняття рішень. 3) Мережевий доступ до систем керування, вразливості систем керування, загрози перехвату управління та відповідні моделі.
Чому це цікаво/треба вивчати	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 урахуванням також особливої ролі суб'єкта керування та різноманітних аспектів складності.
Чому можна навчитися	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.
Як можна користуватися набутими знаннями і вміннями	Моделі кібербезпеки з урахуванням структурних та рефлексивних вразливостей, небезпек мережевого доступу мають значну цінність в сучасних умовах, бо вони є базою для організації захисту складних систем критичної інфраструктури, що є однією з головних проблем саме кібербезпеки, актуальність якої лише зростає.
Інформаційне забезпечення дисципліни	Посилання на дистанційний ресурс: Платформа "Сікорський", курс "Моделі систем керування" https://classroom.google.com/c/NTE0NjIwNjg2NzMw?cjc=s4bvykb
Вид семестрового контролю	залік

КІБЕРНЕТИЧНІ МОДЕЛІ ЗАГРОЗ ТА РИЗИКІВ, КОНТРДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (Доцент Луценко В.М.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	3
Курс, семестр	2 курс, 4 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ECTS (18 годин лекцій, 10 годин практик, 132 години СР)
Мова викладання	українська
Вимоги для початку вивчення дисципліни	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.
Що буде вивчатися	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. 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 3.7-001-99 і підходів до їх використання.
Чому це цікаво/треба вивчати	Тому, що кінцевою метою технології захисту інформації, як елементу Державної політики Держави, є створення проектів систем захисту та комплексних систем захисту. Без зазначених проектів використання і технічних засобів захисту і правових обмежень не має сенсу.
Чому можна навчитися	Проектувати системи захисту інформації об'єктів довільної складності і призначення. Створювати проекти інформаційного захисту за перспективними методиками.
Як можна користуватися набутими	Виконувати завдання в інтересах організації-замовника з створення проектів інформаційного захисту та захисту від

знаннями і вміннями	несанкціонованого доступу до носіїв інформації. Проектування регламенту використання виділених територій, тощо.
Інформаційне забезпечення дисципліни	Методи та засоби технічного захисту інформації. [Електронний ресурс] : навч. посіб. для здобувачів ступеня бакалавра за освітньою програмою «Системи технічного захисту інформації» спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: В. М. Луценко, Д. О. Прогонов. – Електронні текстові дані (1 файл: 37,65 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 306 с. – Назва з екрана URI (Уніфікований ідентифікатор ресурсу): https://ela.kpi.ua/handle/123456789/42397 КПІ. Розташовується у зібраннях: Підручники, навчальні посібники та практикуми (ФТЗЗІ)
Вид семестрового контролю	залік

ІНФОРМАЦІЙНА ЕНТРОПІЯ ФУНКЦІОНАЛЬНОГО АНАЛІЗУ І КВАНТОВА СТЕГАНОГРАФІЯ (Професор Мачуський Є.А.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	3
Курс, семестр	2 курс, 4 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ECTS (18 годин лекцій, 10 годин практик, 132 години СР)
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Дисципліна базується на знаннях основ квантової фізики, статистичного моделювання, теорії інформації, спектрального аналізу сигналів та вимагає навичок математичного моделювання та програмування.
Що буде вивчатися	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.
Чому це цікаво/треба вивчати	Поглиблення знань в галузі методів квантової обробки інформації.
Чому можна навчитися	формування компетентностей із застосування новітніх методів функціонального аналізу та квантової стеганографії
Як можна користуватися набутими знаннями і вміннями	Використовувати розглянуті методи для розширення переліку інструментів функціонального аналізу даних
Інформаційне забезпечення дисципліни	Радіотехніка: Енциклопедичний навчальний довідник: Навч. посібник / За ред. Ю.Л.Мазора, Є.А.Мачуського, В.І.Правди. - К.:Вища шк., 1999. –838 с.: іл.
Вид семестрового контролю	залік