

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

ЗАТВЕРДЖЕНО:

Методичною радою
КПІ ім. Ігоря Сікорського
(протокол № 8 від 20.06.2024 р.)

Ф-КАТАЛОГ

ВИБІРКОВИХ НАВЧАЛЬНИХ ДИСЦИПЛІН

ЦИКЛУ ПРОФЕСІЙНОЇ ПІДГОТОВКИ

для здобувачів ступеня магістра за освітньо-науковою програмою
«Математичні методи моделювання, розпізнавання образів та комп'ютерного зору»
за спеціальністю 113 Прикладна математика

УХВАЛЕНО:

Вченою радою НН ФТІ
КПІ ім. Ігоря Сікорського
(протокол №3 від «26» лютого 2024 р.)

Дисципліни вільного вибору студентів (вибіркові дисципліни), спрямовані на забезпечення загальних та фахових компетенцій за спеціальністю. Обсяг вибірових 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 вибірових дисциплін, які, відповідно до освітньої програми, беруть участь у формуванні фахових компетентностей. За два роки навчання на першому та другому курсах другого (магістерського) рівня вищої освіти здобувач має обрати з нього 7 дисциплін загалом. Вибір дисциплін здійснюється в першому семестрі на другий семестр та у другому на третій 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!

До складу вибірових дисциплін входять освітні компоненти сертифікатної програми «Моделі аналізу даних для комп'ютерного зору». Ці дисципліни, які помічені *, можна обирати окремо, а можна подати заяву на сертифікатну програму та при здачі відповідних заліків отримати сертифікат КПІ ім. Ігоря Сікорського за підписом проректора.

Дисципліни, що помічені ** можуть обиратись лише магістрами, які навчаються за програмою дуальної освіти з Samsung R&D Institute Ukraine.

Силабуси усіх дисциплін та інша супровідна інформація розміщена на сайті кафедри: https://mmda.ipt.kpi.ua/change_master/

Здійснення вибору студентами навчальних дисциплін зі сформованого Ф-Каталогу відбувається за графіком в спеціалізованій інформаційній системі «my.kpi.ua» (контролюється кураторами груп з метою забезпечення участі всіх студентів у процедурі вибору дисциплін та коректності вибору).

Для вибору дисциплін необхідно зробити наступне:

- Зареєструватись на сайті <https://my.kpi.ua/>

- У меню «Профіль» => «Прив'язка даних» знайти своє прізвище, ввести свою дату народження і прив'язати (зберегти) дані. Ви отримаєте доступ до кабінету студента і до вибору дисциплін. Далі необхідно здійснити технічно вибір дисциплін.

Не допускається зміна обраних дисциплін після початку навчального семестру, в якому вони викладаються.

Дисципліни для вибору на перший рік навчання

Магістри першого курсу обирають **дві** екзаменаційні дисципліни та **три** залікові дисципліни з наведеного переліку для вивчення у **другому** семестрі

Другий (весняний) семестр, екзаменаційні дисципліни

<i>Дисципліна (5 кредитів, екзамен)</i>	<i>Кафедра</i>	<i>Стор.</i>
*Методи аналізу великих гетерогенних даних	ММАД	5
*Методи глибокого навчання на різномірних даних	ММАД	6
Технологія блокчейн та розподілені системи	ММЗІ	7
Теорія і методи соціальної інженерії в кібербезпеці	ІБ	8

<i>Другий (весняний) семестр, залікові дисципліни</i>		
<i>Дисципліна (4 кредити, залік)</i>	<i>Кафедра</i>	<i>Стор.</i>
*Інформаційні технології аналізу великих гетерогенних даних	ММАД	10
Моделювання екологічних процесів та систем	ММАД	11
Моделі та рішення в умовах невизначеності	ММАД	12
Ймовірнісні моделі в задачах розпізнавання образів	ММЗІ	13
Математичні основи квантових обчислень	ММЗІ	14
Інфраструктури відкритих ключів	ММЗІ	15
Проектування розподілених систем	ІБ	16
Аналіз бінарних вразливостей	ІБ	17
** Технології штучного інтелекту у системах інформаційної безпеки 1	ІБ	18
** Технології захисту персональних даних 1	ІБ	19

Дисципліни для вибору на другий рік навчання

Магістри першого курсу обирають **дві** залікові дисципліни з наведеного переліку для вивчення у **третьому** семестрі

<i>Дисципліна (4 кредити, залік)</i>	<i>Кафедра</i>	<i>Стор.</i>
Методи обробки та розпізнавання даних	ММАД	21
Структурні методи розпізнавання образів	ММАД	22
Наближені обчислення у математичному моделюванні	ММАД	24
Моделі цінності інформації та ефективність інформаційного захисту	ММЗІ	26
Квантові обчислення та квантова криптографія	ММЗІ	28
Методи реалізації криптографічних механізмів	ММЗІ	29
Безпека кіберфізичних систем	ІБ	30
** Технології штучного інтелекту у системах інформаційної безпеки 2	ІБ	31
** Технології захисту персональних даних 2	ІБ	33

* Складові сертифікатної програми «Моделі та методи інтелектуального аналізу гетерогенних даних»

** Тільки для магістрів, які навчаються за програмою дуальної освіти з Samsung R&D Institute Ukraine

Перелік позначень

Кафедри:

ММАД – кафедра математичного моделювання та аналізу даних

ММЗІ – кафедра математичних методів захисту інформації

ІБ – кафедра інформаційної безпеки

**ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ
ПЕРШОГО КУРСУ НАВЧАННЯ
(ЕКЗАМЕНАЦІЙНІ ДИСЦИПЛІНИ)**

МЕТОДИ АНАЛІЗУ ВЕЛИКИХ ГЕТЕРОГЕННИХ ДАНИХ

Сертифікатна програма	Моделі та методи інтелектуального аналізу гетерогенних даних
Лектор	Доцент Колотій А.В.
Кафедра, яка забезпечує викладання	Математичного моделювання та аналізу даних
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (5 кредитів ЄКТС) 150 год Лекційних занять: 36 год Лабораторних занять: 18 год Самостійна робота студентів: 96 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Для вивчення дисципліни студент має бути знайомий з основами баз даних, бажано знати елементи SQL, структури даних, основи мови Python та вміти працювати в терміналі Linux (bash), проте досвід проектування алгоритмів або участі в олімпіадах необов'язковий. Бажано розуміти принципи побудови та функціонування програмних систем, володіти навичками підготовки та аналізу даних, бути знайомим з методами штучного інтелекту.
Що буде вивчатися	Технології розподіленої обробки даних, які можуть бути масштабовані для великих датасетів. Воркфлоу, які лежать в основі сучасних Data Warehouse.
Чому це цікаво/треба вивчати	Курс показує сучасні реалії підготовки та обробки великих різномірних даних в розподілених системах
Чому можна навчитися	Розуміння основ роботи з інфраструктурою Apache Hadoop / Apache Spark. Створення воркфлоу для керування потоками даних в Data Warehouse.
Як можна користуватися набутими знаннями і уміннями	Для вирішення задач розподіленої обробки великих обсягів даних
Інформаційне забезпечення дисципліни	Силабус, Google Classroom з матеріалами
Вид семестрового контролю	Екзамен

МЕТОДИ ГЛИБОКОГО НАВЧАННЯ НА РІЗНОРІДНИХ ДАНИХ

Сертифікатна програма	Моделі та методи інтелектуального аналізу гетерогенних даних
Лектор	Асистент Яворський О.А.
Кафедра, яка забезпечує викладання	Математичного моделювання та аналізу даних
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (5 кредитів ЄКТС) 150 год Лекційних занять: 18 год Лабораторних занять: 36 год Самостійна робота студентів: 96 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Навички програмування на мові Python, знання з теорії ймовірності та математичної статистики, базові знання з машинного навчання, базові навички програмування на мові C++, базові знання з теорії оптимізації
Що буде вивчатися	<ul style="list-style-type: none"> - Основні архітектури глибинних мереж - Методи fine-tuning (покращення) моделей - Методи дистиляції знань - Проблеми побудови RAG систем - Фізично-обґрунтовані архітектури - Проблеми оцінки якості та ефективності моделей - Методи інженерії даних (feature engineering) - Мультимодальні архітектури - Вступ до роботи з CUDA
Чому це цікаво/треба вивчати	Дисципліна дозволить студентам краще ознайомитися з актуальними проблемами в глибинному навчанні, та оволодіти навиками, які необхідні для роботи з специфічними завданнями, а також такими, що вимагаються на спеціалізованих підприємствах
Чому можна навчитися	<ul style="list-style-type: none"> - Методи fine-tuning (покращення) моделей - Методи дистиляції знань та feature engineering - Навички побудови RAG систем - Методи прискореного аналізу даних на основі cuML та дотичних бібліотек - Будувати tracing/tracking системи для моделей
Як можна користуватися набутими знаннями і уміннями	<ul style="list-style-type: none"> - Навчання моделей - Оцінка моделей - Побудова застосунків, що базуються на глибинних даних - Оптимізація існуючих моделей та застосунків
Інформаційне забезпечення дисципліни	Силабус, онлайн курси, курс в google classroom
Вид семестрового контролю	Екзамен

ТЕХНОЛОГІЯ БЛОКЧЕЙН ТА РОЗПОДІЛЕНІ СИСТЕМИ

Лектор	Професор Кудін А.М.
Кафедра, яка забезпечує викладання	Математичних методів захисту інформації
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (5 кредитів ЄКТС) 150 год Лекційних занять: 36 год Лабораторних занять: 18 год Самостійна робота студентів: 96 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Пройдені курси: «Алгебра та геометрія», «Дискретна математика», «Програмування», «Математичне моделювання». Бажано пройти «Теорія складності»
Що буде вивчатися	Постановки задач забезпечення безпеки сучасного кіберпростору суттєво відрізняється від традиційних задач забезпечення безпеки інформації. Одна з основних відмінностей сучасного кіберпростору – можливість самоуправління, в тому числі – за рахунок децентралізованих керуючих систем. Відомо, що структури даних та процеси, які використовуються в системах відповідають їх принципам функціонування, саме тому блокчейн-технології широко використовуються в сучасному кіберпросторі. Зберігання та обробка даних за допомогою блокчейн технології є одним з різновидів розподіленої обробки даних, основним механізмом захисту яких є криптографічні механізми захисту. Отже предметом вивчення дисципліни є криптографічні технології захисту блокчейнів та децентралізованих додатків.
Чому це цікаво/треба вивчати	Спеціаліст у галузі Інформаційних технологій, який до того ж знайомий з блокчейн-технологіями та криптологією, завжди збере для себе найкращі пропозиції на сучасному ринку праці. До того ж децентралізовані інформаційні системи в майбутньому будуть широко використовуватись практично в усіх галузях промисловості, тому розуміння принципів їх побудови розширює коло потенціальних пропозицій на ринку праці.
Чому можна навчитися	Сучасним методам та прийомам побудови систем криптографічного захисту інформації для блокчейн-систем та систем децентралізованих додатків Прослухавши курс, ви будете знати: <ul style="list-style-type: none"> • особливості блокчейну як об'єкту захисту інформації; • основних криптографічних механізмів та про-

	<p>токолах, які використовуються в блокчейнах;</p> <ul style="list-style-type: none"> • аналізу стійкості та ефективності за обраними критеріями протоколів узгоджень; • проектування та розробки системи криптографічного захисту блокчейн технологій.
Як можна користуватися набутими знаннями і уміннями	<p>Отримані знання можна використовувати для</p> <ul style="list-style-type: none"> • проведення криптографічного аналізу основних характеристик протоколів узгодження блокчейну; • розгортання програмної платформи та окремих інструментів розробки блокчейнів; • розробки системи смарт-контрактів; • проведення оцінки стійкості до криптоаналізу криптографічних систем, реалізованих за технологією децентралізованих додатків.
Інформаційне забезпечення дисципліни	Силабус, дистанційний курс
Вид семестрового контролю	Екзамен

ТЕОРІЯ ТА МЕТОДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В КІБЕРБЕЗПЕЦІ

Лектор	Доцент Стьопочкіна І.В.
Кафедра, яка забезпечує викладання	Інформаційної безпеки
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	<p>Загальна кількість: (5 кредитів ЄКТС) 150 год</p> <p>Лекційних занять: 36 год</p> <p>Практичних занять: 18 год</p> <p>Самостійна робота студентів: 96 год</p>
Мова викладання	Українська
Вимоги для початку вивчення дисципліни	Загальні знання з інформаційних технологій
Що буде вивчатися	Теоретичні основи та практичні техніки атак соціальної інженерії в кібербезпеці, методи захисту від атак соціальної інженерії, відповідне програмне забезпечення.
Чому це цікаво/треба вивчати	Атаки на основі соціальної інженерії складно піддаються виявленню технічними засобами, і є дуже поширеним та багатогранним явищем. Великий відсоток таких атак є успішним.
Чому можна навчитися	Технікам соціальної інженерії (для задач offensive security, тестування на проникнення), опанувати засоби та методи протидії.
Як можна користуватися набутими знаннями та вміннями	Набуті знання можна використовувати в професійній сфері, для наукової роботи та в повсякденному житті.
Інформаційне забезпечення дисципліни	Силабус, дистанційний курс на Сікорському з матеріалами
Вид семестрового контролю	Екзамен

**ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ
ПЕРШОГО КУРСУ НАВЧАННЯ**

(ЗАЛКОВІ ДИСЦИПЛІНИ)

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ АНАЛІЗУ ВЕЛИКИХ ГЕТЕРОГЕННИХ ДАНИХ

Сертифікатна програма	Моделі та методи інтелектуального аналізу гетерогенних даних
Лектор	Професор Шелестов А.Ю.
Кафедра, яка забезпечує викладання	Математичного моделювання та аналізу даних
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 36 год Практичних занять: 18 год Самостійна робота студентів: 66 год
Мова викладання	Українська
Вимоги для початку вивчення дисципліни	Студент має бути знайомий з основами програмування, бажано на Python, структурами даних, проте досвід проектування алгоритмів необов'язковий. Бажано також розуміти загальні принципи побудови та функціонування програмних систем.
Що буде вивчатися	Технології аналізу великих різнорідних даних
Чому це цікаво/треба вивчати	Дані великого обсягу наразі аналізуються та обробляються великою кількістю систем. Виділяються хмари, озера даних та ін.
Чому можна навчитися	Володінню методами та засобами аналізу великих гетерогенних даних
Як можна користуватися набутими знаннями та вміннями	Дисципліна "Інформаційні технології аналізу великих гетерогенних даних" присвячена вивченню сучасних засобів аналізу гетерогенних даних та основних інформаційних технологій для роботи з даними великого об'єму з різних джерел. В межах даної навчальної дисципліни розглядаються сучасні інформаційні технології та програмне забезпечення для обробки гетерогенних даних, підходи до обміну та представлення гетерогенної інформації.
Інформаційне забезпечення дисципліни	Силабус, монографія, навчальний посібник
Вид семестрового контролю	Залік

МОДЕЛЮВАННЯ ЕКОЛОГІЧНИХ ПРОЦЕСІВ ТА СИСТЕМ

Лектор	Професор Ковалець І.В.
Кафедра, яка забезпечує викладання	Математичного моделювання та аналізу даних
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 18 год Практичних занять: 18 год Лабораторних занять: 18 год Самостійна робота студентів: 66 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Слухачі мають володіти базовими знаннями з математичного аналізу, диференційних рівнянь, програмування (Python або C)
Що буде вивчатися	У першій частині курсу вивчаються моделі транспорту речовин у довкіллі. Розглядаються механізми та методи чисельного моделювання: - адвективно-дифузійного транспорту; - турбулентної дисперсії та осадження; У другій частині курсу розглядаються моделі динаміки популяцій та екосистем: - Моделювання фізико-хімічних трансформацій в екосистемах; - Моделі динаміки популяцій; - Моделювання екосистем на прикладі моделей якості води.
Чому це цікаво/треба вивчати	Існування людства можливе тільки у його взаємодії з природними екосистемами; наслідки цього необхідно намагатись передбачати, зокрема, за допомогою математичного моделювання.
Чому можна навчитися	- термінології в області моделей екологічних систем; - розумінню видів моделей екологічних систем та основ їх побудови. - базових знань та навичок з моделювання транспорту речовин у довкіллі; - базових знань та навичок з моделювання динаміки популяцій; - базових знань та навичок з моделювання фізико-хімічних трансформацій в екосистемах на прикладі моделей якості води.
Як можна користуватися набутими знаннями і уміннями	Методи математичного моделювання можна застосовувати для оцінювання екологічних наслідків антропогенного впливу.
Інформаційне забезпечення дисципліни	Лекції у формі презентацій, умови лабораторних робіт з вказівками до виконання, літературні джерела, завантажені у папці курсу на Google Drive
Вид семестрового контролю	Залік

МОДЕЛІ ТА РІШЕННЯ В УМОВАХ НЕВИЗНАЧЕНОСТІ

Лектор	Доцент Терещенко І.М.
Кафедра, яка забезпечує викладання	Математичного моделювання та аналізу даних
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 36 год Практичних занять: 18 год Самостійна робота студентів: 66 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Для опанування матеріалом курсу студентам достатньо мати базові знання з таких навчальних дисциплін як дискретний аналіз та теорія ймовірності
Що буде вивчатися	В курсі вивчаються процеси прийняття рішень в умовах невизначеності, недостовірності даних, неповноти даних тощо та існуючі підходи до вирішення подібного роду проблем для осіб, що приймають рішення
Чому це цікаво/треба вивчати	В сучасних умовах достатньо часто виникають ситуації, коли необхідно зробити вибір або здійснити вплив на певні процеси і при цьому не завжди в момент прийняття рішень може бути наявною вся необхідна інформація
Чому можна навчитися	Студенти можуть опанувати прийоми моделювання та відповідні методи для прийняття рішень в умовах невизначеності, вміти аналізувати як отримані моделі так і розуміти природу змодельованих явищ
Як можна користуватися набутими знаннями і вміннями	Отримані знання дозволяють аналізувати та моделювати доволі широкий спектр сучасних проблем, визначати критичні моменти та загрози, розуміти природу прийняття рішень
Інформаційне забезпечення дисципліни	Силабус
Вид семестрового контролю	Залік

ЙМОВІРНІСНІ МОДЕЛІ В ЗАДАЧАХ РОЗПІЗНАВАННЯ ОБРАЗІВ

Лектор	Старший викладач Рябов Г.В.
Кафедра, яка забезпечує викладання	Математичних методів захисту інформації
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 36 год Самостійна робота студентів: 84 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Пройдені курси “Теорія ймовірностей”, “Математична статистика”, “Випадкові процеси”, “Статистичні методи розпізнавання”
Що буде вивчатися	В курсі дисципліни вивчаються сучасні результати теорії ймовірностей та теорії випадкових процесів, які дозволяють ефективно оцінювати якість алгоритмів розпізнавання: нерівності концентрації, складність множин, гіббсовські розподіли.
Чому це цікаво/треба вивчати	Дослідження статистичних моделей, які виникають в задачах розпізнавання образів, спираються на сучасні фундаментальні результати теорії ймовірностей, які не входять в програму стандартного курсу. Під час вивчення даного курсу студенти оволодіють методами дослідження розподілів випадкових елементів в функціональних просторах, зокрема методами оцінки параметрів гіббсовських розподілів, ознайомляться із застосуваннями ймовірнісних методів в задачах розпізнавання та машинного навчання.
Чому можна навчитися	Дисципліна присвячена окремим напрямкам та методам теорії ймовірностей та теорії випадкових процесів, які використовуються в аналізі алгоритмів розпізнавання. Перша частина курсу присвячена специфічним нерівностям концентрації, які дозволяють ефективно оцінювати зв'язок між емпіричним та теоретичним ризиком алгоритмів розпізнавання. Друга частина присвячена оцінці параметрів гіббсовських полів, які є однією з основних моделей в сучасних задачах розпізнавання.
Як можна користуватися набутими знаннями і уміннями	Набуті знання та навички дозволять аналізувати алгоритми розпізнавання та машинного навчання.
Інформаційне забезпечення дисципліни	Силабус, монографії та статті, дистанційний курс Google Classroom
Вид семестрового контролю	Залік

МАТЕМАТИЧНІ ОСНОВИ КВАНТОВИХ ОБЧИСЛЕНЬ

Лектор	Старший викладач Фесенко А.В.
Кафедра, яка забезпечує викладання	Математичних методів захисту інформації
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 36 год Практичних занять: 18 год Самостійна робота студентів: 66 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Опановані знання з лінійної алгебри, дискретної математики та теорії імовірностей.
Що буде вивчатися	Основні теми, які розглядаються у курсі: 1) бра-кет нотація Дірака; 2) основні постулати квантової моделі обчислень; 3) модель квантових схем; 4) одно та багатокубітні перетворення; 5) найпростіші квантові алгоритми; 6) квантова модель Тюрінга.
Чому це цікаво/треба вивчати	Навчальна дисципліна «Математичні основи квантових обчислень» присвячена ознайомленню студентів з формальною математичною моделлю квантових обчислень. Основною метою дисципліни є формування у студентів глибокого розуміння математичної формалізації квантової моделі обчислень.
Чому можна навчитися	Основним квантовим алгоритмам та перетворенням, математичній формалізації квантових обчислень, що дозволить будувати більш складні квантові алгоритми для прикладних математичних задач.
Як можна користуватися набутими знаннями і уміннями	Набуті знання та навички дозволять будувати та аналізувати квантові алгоритми та квантові схеми.
Інформаційне забезпечення дисципліни	Силабус
Вид семестрового контролю	Залік

ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

Лектор	Доцент Яковлев С.В.
Кафедра, яка забезпечує викладання	Математичних методів захисту інформації
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 36 год Самостійна робота студентів: 84 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Пройдений курс «Криптографія» або знання основних положень симетричної та асиметричної криптографії (поняття ключа, шифру, цифрового підпису, основних сучасних алгоритмів шифрування та цифрового підпису)
Що буде вивчатися	Основні теми, які розглядаються у курсі: 0) електронні довірчі послуги, класифікація електронних підписів та їх функціональність; механізми eIDAS; 1) життєвий цикл криптографічних ключів, організація керування життєвим циклом ключів, різні варіанти будови інфраструктур відкритих ключів, Центри сертифікації ключів; 2) мова ASN.1, стандарти кодування BER, CER, DER; 3) формат сертифікатів відкритих ключів X.509v3; 4) перевірка статусу сертифікатів, атрибути сертифікати, списки відкликаних сертифікатів, протокол OCSP; 5) протоколи керування сертифікатами (PKCS10, CMC, CMP); 6) формати криптографічних повідомлень (CMS), підписані повідомлення, часові штампелі; розширені формати підписаних повідомлень (CAdES); 7) формати захищених повідомлень.
Чому це цікаво/треба вивчати	Навчальна дисципліна «Інфраструктури відкритих ключів» знайомить студентів з принципами, методами та механізмами організації систем керування ключами та захищеного документообігу. Такі системи зараз надзвичайно поширені через невідому та невблаганну діджиталізацію послуг та сервісів, впровадження якої вимагає відповідних механізмів безпеки (зокрема, захисту персональних даних)
Чому можна навчитися	Після опанування курсу студенти знатимуть основні принципи роботи центрів сертифікації ключів, організації життєвого циклу ключів, форматів основних структур даних, які використовуються у механізмах захисту систем захищеного документообігу
Як можна користуватися набутими знаннями і уміннями	Одержані знання та навички дозволяють користуватись на практиці системами, які використовують кваліфікований електронний підпис, та системами захищеного

	документообороту, самостійно розробляти, проектувати, впроваджувати та інтегрувати системи криптографічного захисту з урахуванням нормативно-правових аспектів, пов'язаних із використанням цифрових підписів.
Інформаційне забезпечення дисципліни	Силабус
Вид семестрового контролю	Залік

ПРОЕКТУВАННЯ РОЗПОДІЛЕНИХ СИСТЕМ

Лектор	Доцент Родіонов А.М.
Кафедра, яка забезпечує викладання	Інформаційної безпеки
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 36 год Лабораторних занять: 18 год Самостійна робота студентів: 66 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Знання архітектури та принципів розробки ПЗ, бази даних, мережева взаємодія та протоколи прикладного рівня. Знання будь-якої мови програмування та створення за її допомогою Web-застосунків
Що буде вивчатися	<ul style="list-style-type: none"> - виклики що виникають при побудові розподілених систем - взаємодія між частинами розподіленої системи - вимоги до архітектури та поведінки розподілених застосунків - мікросервісна архітектура як приклад розподіленої системи - паттерни мікросервісної архітектури
Чому це цікаво/треба вивчати	Розподілені системи та мікросервісна архітектура є наразі єдиним підходом до побудови сучасних застосунків здатних витримувати велику кількість користувачів, бути масштабованими, відмовостійкими та високодоступними
Чому можна навчитися	Паттернам мікросервісної архітектури та принципам побудови розподілених систем
Як можна користуватися набутими знаннями і вміннями	Застосовувати під час розробки розподілених застосунків та застосунків з мікросервісною архітектурою
Інформаційне забезпечення дисципліни	Силабус, записи онлайн-курсів, презентаційні матеріали
Вид семестрового контролю	Залік

АНАЛІЗ БІНАРНИХ ВРАЗЛИВОСТЕЙ

Лектор	Доцент Ільїн М.І.
Кафедра, яка забезпечує викладання	Інформаційної безпеки
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 18 год Лабораторних занять: 36 год Самостійна робота студентів: 66 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Спеціальних знань не вимагається
Що буде вивчатися	Вивчаються сучасні технології захисту від експлуатації бінарних вразливостей, та їх обмеження. Досліджуються методи автоматизованого пошуку (різновиди фазингу), та генерації експлоїтів.
Чому це цікаво / треба вивчати	Засоби експлуатації бінарних вразливостей безпосередньо використовуються в атаках на інформаційні системи, дають можливість захоплення керування та закріплення. Навички аналізу і розробки досліджуваних компонентів є суттєвою складовою професійної компетентності спеціалістів технічного захисту, кіберрозвідки та кібердії.
Чому можна навчитися	Методам пошуку, аналізу та експлуатації вразливостей системного та прикладного програмного забезпечення для ОС Windows, Linux, прошивок вбудованих систем (мережеве обладнання, IoT) для платформ Intel x86/x86_64, ARM/AArch64, MIPS.
Як можна користуватися набутими знаннями і уміннями	Знання і уміння використовуються при захисті інформаційних систем від застосування шкідливого програмного забезпечення на етапах доставки, а також при проведенні активних наступальних дій в рамках діяльності сил безпеки та оборони.
Інформаційне забезпечення дисципліни	Матеріали лекцій, лабораторних робіт, додаткова інформація до курсу доступні у telegram групі @kpi_bv.
Вид семестрового контролю	Залік

**ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ
У СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 1**

Лектор	Доцент Прогонов Д.О.
Кафедра, яка забезпечує викладання	Інформаційної безпеки
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Тільки для магістрів, які навчаються за програмою дуальної освіти з Samsung R&D Institute Ukraine
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 0 год Лабораторних занять: 0 год Самостійна робота студентів: 120 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Прослухані курси «Математичний аналіз», «Програмування» Рекомендовані знання: <ul style="list-style-type: none"> - Основ спектрального аналізу сигналів - Сучасних систем комп'ютерної математики (MATLAB, MathCAD) та пакетів для моделювання на мові програмування Python - Принципів обробки мультимедійних даних (стиснення, фільтрація від завад, підвищення якості)
Що буде вивчатися	Метою навчальної дисципліни є формування у студентів компетентностей з автоматизації процесів аналізу, класифікації та обробки інформації з обмеженим доступом в умовах опрацювання значних об'ємів даних. Предметом дисципліни є методи статистичного аналізу та статистичного моделювання числових даних.
Чому це цікаво/треба вивчати	Оволодіння знаннями і навичками даної дисципліни озброює студента поглибленими компетенціями в сучасних інформаційних технологіях
Чому можна навчитися	Поглиблення розуміння принципів роботи, області застосування та обмежень сучасних статистичних моделей даних. Підвищення точності роботи статистичних моделей в умовах зашумленості та/або даних.
Як можна користуватися набутими знаннями і уміннями	Отримані знання та вміння можуть бути використаними для вирішення практичних завдань, пов'язаних із застосуванням методів теорії розпізнавання образів для обробки різнорідних типів даних.
Інформаційне забезпечення дисципліни	Силабус
Вид семестрового контролю	Залік

ТЕХНОЛОГІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ 1

Лектор	Доцент Прогонов Д.О.
Кафедра, яка забезпечує викладання	Інформаційної безпеки
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Тільки для магістрів, які навчаються за програмою дуальної освіти з Samsung R&D Institute Ukraine
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 0 год Лабораторних занять: 0 год Самостійна робота студентів: 120 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Прослухані курси «Математичний аналіз», «Програмування» Рекомендовані знання: <ul style="list-style-type: none"> - Основ спектрального аналізу сигналів - Сучасних систем комп'ютерної математики (MATLAB, MathCAD) та пакетів для моделювання на мові програмування Python - Принципів обробки мультимедійних даних (стиснення, фільтрація від завад, підвищення якості)
Що буде вивчатися	Метою навчальної дисципліни є формування у студентів компетентностей з проведення порівняльного аналізу сучасних пристроїв, систем та комплексів захисту інформації за наявною у відкритому доступі інформацією, роботи з науковою літературою для визначення альтернативних (конкуруючих) рішень та/або методів вирішення задач обробки та захисту інформації. Предметом дисципліни є методи аналізу систем.
Чому це цікаво/треба вивчати	Поглиблення розуміння методів імітаційного моделювання складних систем.
Чому можна навчитися	Знання методів декомпозиції та порівняльного аналізу складних систем; Знання методів проведення імітаційного моделювання елементів та систем обробки даних; Вміння проведення наукового пошуку альтернативних (конкуруючих) рішень та/або методів вирішення задач обробки та захисту інформації; Навички практичної роботи з сучасними системами комп'ютерно математики для проведення імітаційного моделювання (MATLAB Simulink, LabVIEW, Wolfram System Modeler, Modelica).
Як можна користуватися набутими знаннями і уміннями	Підвищення точності імітаційного моделювання фізичних процесів та явищ.
Інформаційне забезпечення дисципліни	Силабус
Вид семестрового контролю	Залік

**ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ
ДРУГОГО КУРСУ НАВЧАННЯ**

МЕТОДИ ОБРОБКИ ТА РОЗПІЗНАВАННЯ ДАНИХ

Лектор	Доцент Юзефович В.В.
Кафедра, яка забезпечує викладання	Математичного моделювання та аналізу даних
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 36 год Лабораторних занять: 18 год Самостійна робота студентів: 66 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Пройдені курси «Статистичні методи розпізнавання», «Моделі та рішення в умовах невизначеності»
Що буде вивчатися	<ol style="list-style-type: none"> 1. Методи формалізації даних та показники їх якості, задача та методи підвищення якості даних. 2. Методи згладжування даних. 3. Методи прогнозування (прогнозні моделі) даних. 4. Методи агрегування (комплексування, інтеграції, групування (кластеризації)) даних. 5. Методи розпізнавання об'єктів (явищ, процесів, подій). 6. Методи обробки зображень. 7. Методи формування еталонних зображень для кореляційно-екстремальних систем навігації керованих об'єктів.
Чому це цікаво/треба вивчати	Широкий клас сучасних технічних систем здійснюють обробку різномірної інформації з метою забезпечення різних інформаційних потреб користувачів або вирішення інших, суто технічних задач. Вміння обробляти інформацію, починаючи від її формалізації, підвищення якості, прогнозування, і закінчуючи формуванням узагальнених інформаційних об'єктів та їх розпізнаванням сприятиме підвищенню ефективності роботи майбутнього фахівця як у науковій сфері, так і будь-якій іншій галузі, де обробка інформації складає основу діяльності.
Чому можна навчитися	В результаті вивчення дисципліни студенти навчаться: <ul style="list-style-type: none"> - формалізувати різномірні дані; - застосовувати методи підвищення поточної якості ряду даних, що надходять від одного, чи декількох джерел; - будувати прогнозні моделі, на основі методів, що добре піддаються автоматизації; - використовувати різні методи формування узагальнених даних; - застосовувати нечіткі операції обробки да-

	них; - застосовувати нечітке інтегрування, у тому числі при вирішенні задачі розпізнавання (класифікації, виявлення, ідентифікації) об'єктів, подій, явищ, процесів; - використовувати методи обробки зображень для виявлення інформативних ознак та вирішення задачі кореляційно-екстремальної навігації керованих об'єктів.
Як можна користуватися набутими знаннями і уміннями	Набуті знання та уміння можуть бути безпосередньо застосовані при вирішенні задач формування та використання інформаційного ресурсу технічних та соціо-технічних систем, а також в процесі розробки сучасних кореляційно-екстремальних систем автономної навігації керованих об'єктів.
Інформаційне забезпечення дисципліни	Силабус, презентаційні матеріали.
Вид семестрового контролю	Залік

СТРУКТУРНІ МЕТОДИ РОЗПІЗНАВАННЯ ОБРАЗІВ

Лектор	Доцент Хайдуров В.В.
Кафедра, яка забезпечує викладання	Математичного моделювання та аналізу даних
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 36 год Лабораторних занять: 18 год Самостійна робота студентів: 66 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Рекомендовані знання з дисциплін: «Теорія ймовірностей», «Математична статистика», «Математичний аналіз», «Алгебра та геометрія», «Методи обчислень», рекомендовано пройти курси «Методи машинного навчання» та «Комп'ютерна графіка».
Що буде вивчатися	У курсі розглядаються: різні методи ідентифікації образів на основі структуризації даних, а також з використанням статистичного підходу та машинного навчання, аналізу зображень з відповідними образами; формування нових зображень на основі математичного апарату вбудовування одного образу в інший, пошук обличчя на зображення з використанням машинного навчання, знаходження структурних елементів об'єктів на основі методів машинного навчання, методи й технології трекінгу об'єктів у відеопотоці даних.

Чому це цікаво/треба вивчати	Об'єкти на зображеннях зазвичай мають заздалегідь відому форму або правила взаємного розташування, які в сукупності формують структуру зображення. Прикладом таких правил є зображення, що знімає відеореєстратор. На основі відео потоку виконується аналіз рухомих об'єктів, вилучається відповідна інформація, аналізується і вноситься у відповідну базу. Наприклад, відеореєстратор зафіксував автомобіль, який перевищив порогову швидкість. Відеореєстратор отримав фото даного автомобіля, знаходить на ньому відповідні номерні знаки авто та передає у базу з метою виписування штрафу власнику даного автомобіля. На практиці розпізнавання образів виконується не лише на зображенні, а й у будь-якому текстовому, числовому, символному наборі даних різного походження.
Чому можна навчитися	На основі отриманих практичних навичок студент зможе будувати ефективні моделі навчання для пошуку різних візуальних структурних елементів (образів), а також здобуде навички оптимізації програмного коду при створенні модулів для розпізнавання образів загалом, які можуть бути інтегровані в глобальні системи розпізнавання образів загалом, у тому числі й структурних образів.
Як можна користуватися набутими знаннями і уміннями	У галузі комп'ютерної графіки продовжуються активні дослідження та розробки нових методів та технологій, наприклад, у галузі реалістичного рендерингу, комп'ютерного зору. Основні навички з комп'ютерної графіки можна застосовувати у медицині (візуалізація медичних даних), моделюванні й візуалізації даних тощо. Сучасна комп'ютерна графіка та її прикладні методи швидко розвиваються та знаходять різні застосування залежно від інноваційних технічних завдань.
Інформаційне забезпечення дисципліни	Дистанційний курс в Classroom
Вид семестрового контролю	Залік

НАБЛИЖЕНІ ОБЧИСЛЕННЯ У МАТЕМАТИЧНОМУ МОДЕЛЮВАННІ

Лектор	Доцент Хайдуров В.В.
Кафедра, яка забезпечує викладання	Математичного моделювання та аналізу даних
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 36 год Лабораторних занять: 18 год Самостійна робота студентів: 66 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Для успішного засвоєння даної дисципліни студентам необхідно пройти повний магістерський курс «Побудова математичних моделей в природознавстві», а також пройти бакалаврські курси «Математичний аналіз», «Диференціальні рівняння», «Програмування», «Методи обчислень» та «Алгоритми та структури даних».
Що буде вивчатися	У ході вивчення курсу будуть розглянуті: - прикладні моделі технічних процесів, які зводяться до диференціальних рівнянь в частинних похідних та їх систем; - основні кінцево-різницеві методи побудови різницевих схем (явних та неявних) для диференціальних рівнянь в частинних похідних різного типу (еліптичного, гіперболічного та параболічного); - методи побудови кінцево-різницевих схем підвищеної точності для різних типів диференціальних рівнянь в частинних похідних; – для дискретних аналогів математичних моделей рівнянь в частинних похідних будуть вивчені основні техніки оптимального зберігання і розв'язання систем звичайних рівнянь великої розмірності; - чисельно-аналітичні методи знаходження наближених розв'язків крайових задач диференціальних рівнянь; - метод кінцевих елементів (з методами побудови триангуляції досліджуваної області) та інші методи знаходження наближених розв'язків диференціальних рівнянь в частинних похідних та їх систем; - прикладне програмне забезпечення моделювання процесів з використанням кінцевих елементів.
Чому це цікаво / треба вивчати	Наближені методи відіграють ключову роль у математичному моделюванні сучасних процесів

	<p>у різних галузях науки та техніки. Сучасні процеси часто описуються складними математичними моделями, для яких знаходження аналітичних розв'язків практично неможливо. Наближені методи надають ефективні засоби для вирішення систем рівнянь та апроксимації складних функцій, що дозволяє отримувати чисельні (наближені) розв'язки. У фізиці, хімії, біології та інших науках наближені методи використовуються для моделювання складних фізичних явищ. Це може включати розрахунки електромагнітних полів, теплопередачу, динаміку рідин і газів, а також квантові явища. В інженерних областях наближені методи широко застосовуються для аналізу та проектування різних систем, таких як структури, машини, електронні пристрої та інші. Ці методи допомагають оптимізувати дизайн, враховувати різні впливи та передбачати поведінку систем. Для вивчення змін клімату та їхнього впливу на навколишнє середовище активно використовуються лише наближені методи. Моделювання клімату включає складні рівняння, що описують динаміку атмосфери, океану та інших компонентів земної системи.</p>
Чому можна навчитися	<p>На основі отриманих практичних навичок студент може вирішувати різні наукові й прикладні завдання, які описуються математичними моделями диференціальних рівнянь та їх систем, будувати ефективні різницеві схеми, розробляти програмний код для знаходження відповідного наближеного розв'язку поставленої перед ним задачі, а також застосувати сучасні прикладні програмні забезпечення для розв'язання подібних задач.</p>
Як можна користуватися набутими знаннями і вміннями	<p>Отримані навички студент може використовувати у моделюванні різних процесів для розвитку науки й техніки, зокрема студент зможе вирішувати прикладні завдання, які передбачають моделювання розподілу температури у матеріалах з метою проектування систем опалення та охолодження. Отримані навички також ефективно можна застосовувати в оптимізації процесів теплової обробки матеріалів, проектуванні теплорозсіювальних систем в електроніці, дослідженні теплових процесів в енергетичних установках тощо.</p>
Інформаційне забезпечення дисципліни	Дистанційний курс в Classroom
Вид семестрового контролю	Залік

**МОДЕЛІ ЦІННОСТІ ІНФОРМАЦІЇ
ТА ЕФЕКТИВНІСТЬ ІНФОРМАЦІЙНОГО ЗАХИСТУ**

Лектор	Професор Савчук М.М.
Кафедра, яка забезпечує викладання	Математичних методів захисту інформації
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 18 год Практичних занять: 18 год Самостійна робота студентів: 84 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Пройдені курси «Дискретна математика», «Теорія імовірностей», «Математична статистика»; студенти повинні мати базові знання та представлення з алгебри, комбінаторики, теорії інформації та криптографії.
Що буде вивчатися	У навчальній дисципліні «Моделі цінності інформації та ефективність інформаційного захисту» розглядаються теоретичні поняття інформації, математичних моделей цінності інформації, різних способів означення та вимірювання цінності інформації, дезінформації, а також аспекти практичного застосування цих питань до проблем оцінювання стійкості криптографічних примітивів та механізмів захисту інформації. Основні теми, які будуть розглядатись: 1) різні підходи до визначення цінності інформації; 2) інформаційно-аналітична система передачі інформації в умовах невизначеності; означення цінності інформації в повідомленні, умовна і безумовна цінність інформації; закон збереження інформації; 3) цінність інформації та відстані між повідомленнями, метрики на множині повідомлень; поняття від'ємної інформації (дезінформації), різні випадки дезінформації; 4) досконало секретна (цілком таємна) крипто-система за Шенноном; транзитивні, досконалі, S-досконалі шифри, їх властивості; спряжено-транзитивні шифри і їх співвідношення з досконалими та S-досконалими шифрами; (S,P)-досконалі шифри; ієрархія різних класів досконалих шифрів; 5) Практична стійкість та імітостійкість шифрів з урахуванням цінності інформації і її старіння. Вплив спотворень у каналі зв'язку на цінність отриманої шифрованої інформації. 6) Узагальнена модель цінності інформації в системі передачі інформації в умовах невизна-

	ченості. Стратегії користувача і спостерігача в узагальненій моделі цінності інформації. Оцінки стійкості криптосистем в узагальненій моделі цінності інформації, розширення поняття досконалих шифрів.
Чому це цікаво/треба вивчати	У курсі розглядаються теоретичні поняття інформації, цінності інформації, різних способів означення та вимірювання цінності інформації, поняття дезінформації з точки зору цінності інформації, а також аспекти практичного застосування цих питань до проблем оцінювання стійкості криптографічних примітивів та розширення поняття цілком таємних систем за Шенноном. Вивчені підходи, методи, математичні моделі, алгоритми дають новий погляд на кількісні оцінки інформації, ризику, обмін повідомленнями в умовах невизначеності, розширення поняття криптографічної стійкості систем.
Чому можна навчитися	Можна навчитися глибинному розумінню сучасних проблем та напрямків в сфері захисту інформаційних технологій і криптографічного захисту інформації, зокрема, підходів щодо оцінювання цінності інформації, яка міститься у повідомленнях та її використання у алгебраїчних та статистичних методах криптоаналізу. Навчитися використовувати різні підходи до оцінювання ризиків безпеки, враховувати цінність інформації в системах інформаційної безпеки, розпізнавати дезінформацію, аналізувати стратегії і можливі сценарії в так званих іграх в дезінформацію.
Як можна користуватися набутими знаннями і вміннями	Набуті знання і вміння дозволять: а) знати та розуміти сучасні підходи щодо визначення інформації, дезінформації та методів оцінювання цінності інформації та ризиків; б) вміти застосовувати моделі цінності інформації для побудови і дослідження систем передачі та захисту інформації з урахуванням інформаційної невизначеності; в) вміти вибирати і використовувати різні поняття стійкості для оцінки ефективності інформаційних систем і надійності захисту інформації; г) застосовувати моделі кількісної оцінки цінності інформації для аналізу телекомутаційних інформаційних систем в умовах невизначеності та можливої дезінформації.
Інформаційне забезпечення дисципліни	Силабус
Вид семестрового контролю	Залік

КВАНТОВІ ОБЧИСЛЕННЯ ТА КВАНТОВА КРИПТОГРАФІЯ

Лектор	Ст. викл. Фесенко А.В.
Кафедра, яка забезпечує викладання	Математичного моделювання та аналізу даних
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 36 год Практичних занять: 18 год Самостійна робота студентів: 66 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Для засвоєння матеріалу курсу «Квантові обчислення та квантова криптографія» є необхідними знання лінійної алгебри та дискретної математики.
Що буде вивчатися	Основні теми, які розглядаються у курсі: 1) формальна модель квантових обчислень; 2) сучасні ефективні квантові алгоритми та їхня реалізація; 3) квантові протоколи; 4) елементи квантового криптоаналізу.
Чому це цікаво/треба вивчати	Навчальна дисципліна «Квантові обчислення та квантова криптографія» присвячена новітньому напрямку досліджень і охоплює сучасні результати, отримані у квантовій моделі обчислень, та їхній вплив на криптографічні механізми захисту інформації. Основною метою дисципліни є ознайомлення студентів з новітніми результатами квантової моделі обчислень, наявними квантовими алгоритмами та протоколами; формування у студентів навичок використання методів квантових обчислень, зокрема, при дослідженні криптографічних примітивів. Для досягнення мети передбачається опрацювання розрахункових та аналітичних задач, які ілюструють та розширюють лекційний матеріал, та реалізацію базових алгоритмів квантових обчислень на доступних квантових комп'ютерах та їхніх моделях
Чому можна навчитися	Наявним новітнім результатам квантової моделі обчислень; особливостям побудови квантових алгоритмів та протоколів, а також наявним можливостям їхньої реалізації.
Як можна користуватися набутими знаннями і уміннями	Набуті знання та навички дозволять аналізувати квантові алгоритми та протоколи, а також опанувати навички програмування квантових алгоритмів.
Інформаційне забезпечення дисципліни	Силабус
Вид семестрового контролю	Залік

МЕТОДИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ

Лектор	Професор Кудін А.М.
Кафедра, яка забезпечує викладання	Математичних методів захисту інформації
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 36 год Лабораторних занять: 18 год Самостійна робота студентів: 66 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Пройдені курси: Алгебра та геометрія Дискретна математика Програмування Теорія складності Математичне моделювання
Що буде вивчатися	Математичні моделі криптографічних перетворень, алгоритмів, протоколів, криптосистем та засобів криптографічного захисту інформації. Методи реалізації криптографічних алгоритмів та систем. Мета вивчення дисципліни є ознайомлення студентів з сучасними моделями, що застосовуються в криптології та їх практичною реалізацією, надання інформації про алгоритми реалізації криптосистем.
Чому це цікаво/треба вивчати	Перехід людства до інформаційного суспільства супроводжується революційними змінами в усіх сферах громадської діяльності, а насамперед – в технології захисту інформаційних ресурсів. Ці зміни поширюються і на всі науки, що досліджують проблеми захисту інформації від навмисних та ненавмисних загроз, в тому числі – криптології. Так в останні роки з'явилися численні роботи (зокрема Голдрейха, Гольдвассер та інших), в яких досліджується основи криптології, формулюються специфічні саме для криптології методи досліджень – тобто проходить процес ставлення криптології як самостійної науки, а не тільки як розділу прикладної математики. Іншою рисою останнього часу є створення поняття „відкритої криптографії” і поширення криптографічних методів для захисту інформації в недержавних і „відкритих” автоматизованих системах. Ці фактори приводять до актуалізації проблеми адекватної реалізації базових криптографічних примітивів та протоколів, адекватності створених теоретичних моделей криптології реальним ситуаціям, що виникають при їх застосуванні, вміння

	практичного застосування методів криптології.
Чому можна навчитися	Адекватно оцінювати стійкість реальних крипто-систем, основних алгоритмів їх реалізації, а також установлення взаємозв'язку між теоретичними моделями та реалізаціями криптографічних механізмів в автоматизованих системах.
Як можна користуватися набутими знаннями і уміннями	Отримані знання можна використовувати для <ul style="list-style-type: none"> • отримання практичних навичок оцінки стійкості криптографічних алгоритмів та криптосистем • програмної та програмно-апаратної реалізації криптосистем.
Інформаційне забезпечення дисципліни	Силабус, дистанційний курс
Вид семестрового контролю	Залік

БЕЗПЕКА КІБЕРФІЗИЧНИХ СИСТЕМ

Лектор	Доцент Смирнов С.А.
Кафедра, яка забезпечує викладання	Інформаційної безпеки
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Без обмежень
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 36 год Лабораторних занять: 18 год Самостійна робота студентів: 66 год
Мова викладання	Українська
Вимоги для початку вивчення дисципліни	Для розуміння змісту курсу студентам достатньо мати базові знання з наступних навчальних дисциплін: математичний аналіз, лінійна алгебра, загальна фізика, математичне моделювання.
Що буде вивчатися	Навчальна дисципліна орієнтована на оволодіння сучасними кібернетичними та фізичними принципами побудови, функціонування та забезпечення широкого спектру кіберфізичних систем.
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. Кіберфізичні системи, в свою чергу, є науково-технологічною базою вбудованих систем, яка підтримує імплементацію керуючих та інформаційних процесів у реальні фізичні системи але породжує нові вразливості та загрози.
Чому можна навчитися	Знання: основних принципів організації інформаційних процесів, зв'язку між сигнально-інформаційною та матеріально-енергетичною складовою реальних процесів та явищ; зв'язку

	<p>між інформацією, прийняттям рішень та їх реалізацією (управлінням); класифікації загроз для систем управління та методів їх аналізу, виявлення та попередження; видів синхронізації, управління синхронізацією та управління хаосом;</p> <p><i>Уміння:</i> вільно володіти і оперувати основними поняттями систем управління у фізичному контексті; вміти визначати цілі управління та засоби їх досягнення, характеристики систем управління (стійкість, вразливість, керованість, спостережуваність); будувати алгоритми управління на основі градієнтних методів та методу швидкісного градієнту; перевіряти алгоритми керування на вразливості та небезпеки.</p>
Як можна користуватися набутими знаннями та вміннями	Курс дозволяє вільно орієнтуватися на якісному і кількісному рівні в основних фізичних принципах, умовах, можливостях, обмеженнях та загрозах, пов'язаних з обробкою та використанням інформації в кіберфізичних системах; виробити навички практичного використання засвоєних знань, методів і підходів у подальшому навчанні та професійній діяльності.
Інформаційне забезпечення дисципліни	Силабус, дистанційний ресурс на платформі "Сікорський"
Вид семестрового контролю	Залік

ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 2

Лектор	Доцент Прогонов Д.О.
Кафедра, яка забезпечує викладання	Інформаційної безпеки
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Тільки для магістрів, які навчаються за програмою дуальної освіти з Samsung R&D Institute Ukraine
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 0 год Лабораторних занять: 0 год Самостійна робота студентів: 120 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Прослухані курси «Математичний аналіз», «Програмування». Рекомендовані знання: Основ спектрального аналізу сигналів Сучасних систем комп'ютерної математики (MATLAB, MathCAD) та пакетів для моделювання на мові програмування Python

	Принципів обробки мультимедійних даних (стиснення, фільтрація від завад, підвищення якості)
Що буде вивчатися	Метою навчальної дисципліни є формування у студентів компетентностей з розробки математичних моделей динамічних систем для вирішення задачі визначення (ідентифікації) невідомих систем за частковими даними. Предметом дисципліни є методи статистичного моделювання динамічних систем.
Чому це цікаво / треба вивчати	Поглиблення розуміння сучасних підходів до ідентифікації систем обробки даних за наявними (частковими) даними. Розуміння методів непрямого визначення параметрів системи обробки даних
Чому можна навчитися	Знання термінології в галузі моделювання динамічних систем; Знання методів моделювання динамічних систем за відомими даними; Знання підходів до ідентифікації динамічних систем за повними або частковими даними; Вміння вибору підходів до розробки математичних моделей динамічних систем; Вміння застосування методів підпросторів та похибки передбачення в задачах ідентифікації систем; Вміння проведення оцінювання точності розробленої математичної моделі динамічної системи; Навички практичної роботи у сучасних програмних комплексах аналізу та обробки даних.
Як можна користуватися набутими знаннями і уміннями	Побудова статистичних моделей та методів визначення параметрів систем обробки сигналів за наявними даними. Оцінка якості роботи даних моделей та методів.
Інформаційне забезпечення дисципліни	Силабус
Вид семестрового контролю	Залік

ТЕХНОЛОГІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ 2

Лектор	Доцент Прогонов Д.О.
Кафедра, яка забезпечує викладання	Інформаційної безпеки
Рівень вищої освіти	Другий (магістерський)
Можливі обмеження	Тільки для магістрів, які навчаються за програмою дуальної освіти з Samsung R&D Institute Ukraine
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	Загальна кількість: (4 кредити ЄКТС) 120 год Лекційних занять: 0 год Лабораторних занять: 0 год Самостійна робота студентів: 120 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Прослухані курси «Математичний аналіз», «Програмування» Рекомендовані знання: Основ спектрального аналізу сигналів Сучасних систем комп'ютерної математики (MATLAB, MathCAD) та пакетів для моделювання на мові програмування Python Принципів обробки мультимедійних даних (стиснення, фільтрація від завад, підвищення якості)
Що буде вивчатися	Поглиблення розуміння принципів, методів та засобів імітаційного моделювання систем обробки сигналів. Розуміння методів синтезу даних систем за наявними вимогами/параметрами.
Чому це цікаво / треба вивчати	Поглиблення розуміння методів синтезу складних систем.
Чому можна навчитися	Знання методів декомпозиції та порівняльного аналізу складних систем; Знання основ конструювання та проектування елементів систем обробки (захисту) інформації; Знання методів проведення імітаційного моделювання елементів та систем обробки даних; Вміння побудови імітаційної моделі та синтезу елементів систем обробки (захисту) даних; Навички практичної роботи з сучасними системами комп'ютерної математики для проведення імітаційного моделювання (MATLAB Simulink, LabVIEW, Wolfram System Modeler, Modelica).
Як можна користуватися набутими знаннями і вміннями	Підвищення якості моделювання систем обробки сигналів, синтезу даних систем за наявними параметрами/вимогами.
Інформаційне забезпечення дисципліни	Силабус
Вид семестрового контролю	Залік