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

ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
_____ Анатолій МЕЛЬНИЧЕНКО
«01» 02 2022 р.

Ф-КАТАЛОГ
ВИБІРКОВИХ НАВЧАЛЬНИХ ДИСЦИПЛІН
ЦИКЛУ ПРОФЕСІЙНОЇ ПІДГОТОВКИ

для здобувачів ступеня магістра
за освітньою програмою «Математичні методи криптографічного захисту інформації»
за спеціальністю 113 Прикладна математика

УХВАЛЕНО:
Методичною радою
КПІ ім. Ігоря Сікорського
(протокол №3 від «27» 01 2022 р.)
Вченою радою НН ФТІ
КПІ ім. Ігоря Сікорського
(протокол №22 від «28» 12 2021 р.)

Київ – 2022

Процедура вибору освітніх компонент відбувається згідно «Тимчасового положення про порядок реалізації студентами Фізико-технічного інституту КПІ ім. Ігоря Сікорського права на вільний вибір навчальних дисциплін» (http://ipt.kpi.ua/normatyvni-dokumenty-fti)

Силабуси усіх дисциплін та інша супровідна інформація розміщена на сайті кафедри: http://mmis.ipt.kpi.ua/course_selection

З усіх питань щодо організації процедури вибору освітніх компонент та за консультаціями по формуванню індивідуальної освітньої траєкторії звертатись до в.о. зав. кафедрою ММЗІ Сергія Яковлєва (yasv@rl.kiev.ua, tg: @leonhard_eu).

Дисципліни для вибору на перший рік навчання		
Магістри першого курсу обирають **три** екзаменаційні дисципліни та **дві** залікові дисципліни з наведеного переліку для вивчення у **другому** семестрі		
Другий (весняний) семестр, екзаменаційні дисципліни		
Дисципліна (5 кредитів, екзамен)	*Кафедра*	*Стор.*
Ймовірнісні моделі в задачах розпізнавання образів	ММЗІ	4
Методи аналізу великих гетерогенних даних	ММАД	5
Методи глибокого навчання на різнорідних даних	ММАД	6
Моделі та методи криптоаналізу блокових шифрів	ММЗІ	7
Структурні методи розпізнавання образів	ММАД	8
Теорія і методи соціальної інженерії в кібербезпеці	ІБ	9
Технологія блокчейн та розподілені системи	ММЗІ	10
Другий (весняний) семестр, залікові дисципліни		
Дисципліна (4 кредити, залік)	*Кафедра*	*Стор.*
Web-аналітика	ІБ	12
Вступ до алгебраїчної топології	ММЗІ	13
Інформаційні технології аналізу великих гетерогенних даних	ММАД	14
Моделювання екологічних процесів та систем	ММАД	15
Криптосистеми на еліптичних кривих	ММЗІ	16
Проектування розподілених систем	ІБ	17
* Технології захисту персональних даних 1	ІБ	18
* Технології штучного інтелекту у системах інформаційної безпеки 1	ІБ	19

* Тільки для магістрів, які навчаються за дуальною програмою освіти з Samsung R&D Україна.

Дисципліни для вибору на другий рік навчання		
Магістри першого курсу обирають **дві** дисципліни з наведеного переліку для вивчення у **третьому** семестрі		
Третій (осінній) семестр		
Дисципліна (4 кредитів, залік)	*Кафедра*	*Стор.*
ARX-криптосистеми та їх криптоаналіз	ММЗІ	21
Аналіз мережевих структур	ММАД	22
Методи обробки та розпізнавання даних	ММАД	23
Моделі кіберфізичних систем	ІБ	24
Моделі цінності інформації та ефективність інформаційного захисту	ММЗІ	25
* Технології захисту персональних даних 2	ІБ	26
* Технології штучного інтелекту у системах інформаційної безпеки 2	ІБ	27

* Тільки для магістрів, які навчаються за дуальною програмою освіти з Samsung R&D Україна.

ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ ПЕРШОГО КУРСУ НАВЧАННЯ

(ЕКЗАМЕНАЦІЙНІ ДИСЦИПЛІНИ)

Дисципліна	**Ймовірнісні моделі в задачах розпізнавання образів**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів, екзамен	Мова викладання	Українська
Кафедра	математичного моделювання та аналізу даних		
Викладачі	ст. викл. Рябов Г.В.		
Вимоги до початку вивчення	Пройдені курси «Теорія імовірностей», «Математична статистика»		
Анотація дисципліни	Статистичні постановки задач розпізнавання потребують побудови статистичних моделей об'єктів, що спостерігаються. Дослідження таких моделей спирається 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 образів та машинного навчання.		
Форма проведення занять	Лекції		

Дисципліна	**Методи аналізу великих гетерогенних даних**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів, екзамен	Мова викладання	Українська
Кафедра	математичного моделювання та аналізу даних		
Викладачі	доц. Орєхов О.А.		
Вимоги до початку вивчення	Для вивчення дисципліни студент має бути знайомий з основами програмування, бажано на Python, структурами даних, 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, зокрема, нейронними мережами.		
Анотація дисципліни	Дисципліна «Методи аналізу великих гетерогенних даних» присвячена вивченню теоретичних положень і сучасних методів математичного моделювання, аналізу та обробки гетерогенних даних, методів регресійного аналізу та кластеризації, нейронних мереж, тощо. У межах дисципліни розглядаються такі питання, як основні принципи аналізу великих гетерогенних даних, джерела гетерогенних даних та принципи їх спільного використання, обробки та аналізу.		
Форма проведення занять	Лекції, комп’ютерні практикуми		

Дисципліна	**Методи глибокого навчання на різнорідних даних**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів, екзамен	Мова викладання	Українська
Кафедра	математичного моделювання та аналізу даних		
Викладачі	проф. Куссуль Н.М.		
Вимоги до початку вивчення	Для вивчення дисципліни студент має володіти методами лінійної алгебри, теорії ймовірностей і математичної статистики, теорії оптимізації, машинного навчання та аналізу даних, бути знайомим з основами програмування, бажано на Python, а також з класичними алгоритмами та структурами даних.		
Анотація дисципліни	Дисципліна «Методи глибокого навчання на різнорідних даних» присвячена вивченню методів та технологій машинного навчання з урахуванням сучасних тенденцій розвитку цієї галузі в епоху цифровізації з використанням великих об’ємів гетерогенних даних. У результаті вивчення навчальної дисципліни студенти зможуть застосувати методи глибокого навчання для обробки гетерогенних даних; будуть володіти практичними навичками використання інструментів глибокого навчання для розв’язання задач на основі гетерогенних даних великого об’єму.		
Форма проведення занять	Лекції, комп’ютерні практикуми		

Дисципліна	**Моделі та методи криптоаналізу блокових шифрів**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів, екзамен	Мова викладання	Українська
Кафедра	математичних методів захисту інформації		
Викладачі	доц. Яковлєв С.В.		
Вимоги до початку вивчення	Пройдені курси «Симетрична криптографія» («Криптографія»), «Теорія імовірності», «Математична статистика», «Методи криптоаналізу 1»		
Анотація дисципліни	Навчальна дисципліна «Моделі та методи криптоаналізу блокових шифрів» розглядає сучасні методи побудови блокових шифрів та їх криптоаналізу. У дисципліні будуть детально розглянуті такі теми: 1) будова ітеративних шифрів, схеми блокового шифрування; 2) статистичні атаки на раундові ключі; 3) формальна теорія диференціального криптоаналізу, теоретична (доказова) та практична стійкість шифрів до диференціального криптоаналізу, методи оцінювання стійкості, криптографічні параметри, які впливають на стійкість; 4) модифікації та узагальнення диференціального криптоаналізу: аналіз неможливих диференціалів, аналіз диференціалів вищого порядку, атаки бумерангів та прямокутників, атаки на пов'язаних ключах; 5) формальна теорія лінійного криптоаналізу, теоретична (доказова) та практична стійкість шифрів до лінійного криптоаналізу, методи оцінювання стійкості, криптографічні параметри, які впливають на стійкість; 6) модифікації та узагальнення лінійного криптоаналізу: білінійний криптоаналіз, узагальнений лінійний криптоаналіз на довільних абелевих групах, аналіз нульових кореляцій, диференціально-лінійні розпізнавачі; 7) методи автоматизованого пошуку високоімовірних та неможливих диференціалів, високоімовірних лінійних апроксимацій; 8) інтегральний криптоаналіз та його узагальнення: аналіз лінійних підпросторів, властивості подільності. Основною метою дисципліни є формування у студентів глибинного розуміння сучасних статистичних методів криптоаналізу. Для досягнення мети передбачається опрацювання значної кількості розрахункових та аналітичних задач, які ілюструють та розширюють лекційний матеріал, виконання розрахункової роботи та трьох комп'ютерних практикумів.		
Форма проведення занять	Лекції, практичні заняття, комп'ютерні практикуми		

Дисципліна	**Структурні методи розпізнавання образів**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів, екзамен	Мова викладання	Українська
Кафедра	математичного моделювання та аналізу даних		
Викладачі	проф. Півень О.Б.		
Вимоги до початку вивчення	Пройдений курс «Статистичні методи розпізнавання»		
Анотація дисципліни	Об'єкти на зображеннях зазвичай мають заздалегідь відому форму або правила взаємного розташування, які в сукупності ми називаємо структурою зображення. Прикладом таких правил є зображення, що знімає відеореєстратор: ми знаємо, що знизу є дорога, з боків узбіччя з будівлями, людьми тощо, а зверху небо. Вміння описати правила такого типу помітно покращує роботу системи розпізнавання образів в порівнянні з тією, що використовує лише статистичні властивості зображення. Універсальність методів, що розглядаються в курсі, полягає в тому, що статистична модель, яку використовує система структурного розпізнавання образів, може бути довільною — випадкове поле (вивчається у курсі статистичних методів розпізнавання образів), штучна нейронна мережа, просто формула — будь-що, що може вирахувати, наскільки правдоподібна гіпотеза щодо знаходження певних об'єктів у певних місцях зображення.		
Форма проведення занять	Лекції, практичні заняття		

Дисципліна	**Теорія і методи соціальної інженерії в кібербезпеці**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів, екзамен	Мова викладання	Українська
Кафедра	інформаційної безпеки		
Викладачі	доцент Стьопочкіна І.В.		
Вимоги до початку вивчення	Бажане уміння програмувати на мовах java, python.		
Анотація дисципліни	Соціальна інженерія є одним із найуспішніших напрямків здійснення атак на об'єкти різного типу. Слабкою ланкою кожної системи захисту є людина, саме з участю людського фактору соціальний інженер досягає своєї мети. Уміння та знання, набуті в цьому курсі, можуть бути використані там, де передбачається діяльність із кіберзахисту інформації, в тому числі із використанням наукоємних технологій, на стику із методиками HR-менеджмента. Навчальна дисципліна «Теорія та методи соціальної інженерії в кібербезпеці» розглядає теоретичні основи відповідних атак. В тому числі, розглянуто моделі атак соціальної інженерії, моделі їх виявлення, сценарії різних видів атак соціальної інженерії, ПЗ, яке використовується при цьому та способи протидії цим атакам. Ці знання дають змогу зрозуміти фактори успіху відповідних атак, та попередити їх. Теоретичні матеріали курсу дають студенту знання про: – Моделі та сценарії атак та їх виявлення; – Поведінковий та психологічний портрет потенційних жертв соціального інженера, сценарії поведінки які призводять до успіху подібних атак; – Механізми здійснення різних атак соціальної інженерії; – Нові технології та засоби соціальної інженерії, засновані на ML та AI, в тому числі DeepFake та інші. – Рішення кіберзахисту та підходи до попередження атак соціальної інженерії. Також за дисципліною передбачено 5 комп'ютерних практикумів, які доповнюють теоретичний матеріал і поглиблюють його за практичним напрямом. В результаті виконання практикумів студент набуває такі уміння: – Розробляти сценарії та моделі атак соціальної інженерії та здійснювати імітаційне моделювання; – Уміння розробляти програму тестування на проникнення із використанням різних підходів; – Використовувати наявні програмні засоби, за допомогою яких може діяти соціальний інженер, в цілях тестування на проникнення; – Уміння розробляти методики оцінки персоналу на чутливість до різних атак соціальної інженерії; – Уміння розробляти елементи засобів тестування на проникнення із використанням підходів соціальної інженерії.		
Форма проведення занять	Лекції, комп'ютерні практикуми		

Дисципліна	**Технологія блокчейн та розподілені системи**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів, екзамен	Мова викладання	Українська
Кафедра	математичних методів захисту інформації		
Викладачі	проф. Кудін А.М.		
Вимоги до початку вивчення	Пройдений курс «Криптографія» («Симетрична криптографія», «Асиметрічні криптосистеми та протоколи»)		
Анотація дисципліни	Навчальна дисципліна «Технології блокчейн та розподілені системи» присвячена сучасним криптографічним технологіям побудови розподілених баз даних із властивостями незмінюваності та спостережуваності; такі системи ґрунтуються на основі геш-ланцюгів блоків, більш відомих під назвою «блокчейн». У дисципліні буде розглянуто такі теми. 1) «низова» структура блокчейнів; 2) протоколи консенсусу: Proof of Work, Proof of Stake, Proof of Activity та ін.; 3) децентралізовані та централізовані блокчейни (private ledgers); 4) принципи роботи криптовалют та смарт-контрактів. Теоретичний матеріал супроводжується комп'ютерними практикумами, на яких ви зможете самостійно розгорнути деякі блокчейн-системи та опанувати механізми їх роботи.		
Форма проведення занять	Лекції, комп'ютерні практикуми		

ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ ПЕРШОГО КУРСУ НАВЧАННЯ

(ЗАЛІКОВІ ДИСЦИПЛІНИ)

Дисципліна	**Web-аналітика**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	інформаційної безпеки		
Викладачі	Доц. Ткач В.М.		
Вимоги до початку вивчення	Предмет «Web-аналітика» базується на таких курсах, як «Програмне забезпечення ЕОМ», «Програмування»; також бажане знання особливостей створення web-застосунків		
Анотація дисципліни	Сучасний розвиток світових комунікацій, зокрема всесвітньої мережі Інтернет, а також велика кількість інформаційних ресурсів, що в ній представлено, зумовлюють необхідність досконалого вивчення інформаційних потоків, аналізу джерел інформації, кількісних та якісних характеристик. Сучасний рівень розвитку інформаційних технологій вимагає широкого спектру практичних навичок роботи з застосуванням різних методологій програмування. Програмування є лише інструментом для вирішення практичних та науково-практичних задач. Така підготовка може забезпечити можливість пристосування до нових типів задач, пов'язаних з використанням у тому числі високопродуктивної обчислювальної техніки. Дослідник повинен володіти технологіями програмування, достатніми для отримання та обробки відкритих даних з мережі Інтернет, з систем збору аналітики з їх подальшим використанням для розв'язання складних ресурсоємних наукових задач, що як правило мають міждисциплінарний характер. У межах дисципліни розглянуто основні принципи аналізу даних, що збираються в Інтернет, принципи пошуку аномалій в даних веб-аналітики, принципи визначення нормальної та аномальної поведінки користувачів в мережі Інтернет і т.д.		
Форма проведення занять	Лекції, практичні заняття		

Дисципліна	**Вступ до алгебраїчної топології**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	математичних методів захисту інформації		
Викладачі	доц. Хмельницький М.О.		
Вимоги до початку вивчення	Пройдені курси «Математичний аналіз», «Алгебра та геометрія»; рекомендовано прослухати курс «Прикладна алгебра» або інший курс з абстрактної алгебри		
Анотація дисципліни	Навчальна дисципліна «Вступ до алгебраїчної топології» присвячена введенню в коло ідей та методів по вивченню топологічних просторів шляхом побудови для кожного з них певних алгебраїчних інваріантів, як то груп гомотопій та гомологій. Основні теми, які розглядаються в курсі: 1) Топологічні простори та їх гомеоморфізми; 2) Елементи теорії категорій; 3) Класифікація ліній та поверхонь; 4) Фундаментальна група; 5) Групи гомотопій; 6) Групи гомологій. Основною метою дисципліни є формування у студентів стійкого розуміння глибинних взаємозв'язків між різними галузями математики та впливів, які ці галузі роблять одна на іншу, на прикладі вивчення алгебраїчних методів в топології. Для досягнення мети передбачається опрацювання значної кількості розрахункових та аналітичних задач, які ілюструють та розширюють лекційний матеріал.		
Форма проведення занять	Лекції, практичні заняття		

Дисципліна	**Інформаційні технології аналізу великих гетерогенних даних**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	математичного моделювання та аналізу даних		
Викладачі	проф. Шелестов А.Ю.		
Вимоги до початку вивчення	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.		
Анотація дисципліни	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. У межах даної навчальної дисципліни розглядаються сучасні інформаційні технології та програмне забезпечення для обробки гетерогенних даних, підходи до обміну та представлення гетерогенної інформації.		
Форма проведення занять	Лекції, комп’ютерні практикуми		

Дисципліна	**Моделювання екологічних процесів та систем**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	математичного моделювання та аналізу даних		
Викладачі	проф. Ковалець І.В.		
Вимоги до початку вивчення	Слухачі мають володіти базовими знаннями з математичного аналізу, диференційних рівнянь, програмування (Python або C)		
Анотація дисципліни	Курс присвячений вивченню наукових основ та комп'ютерних технологій моделювання екологічних процесів та систем, які включають у себе моделі популяцій, епідемій, а також фізико-хімічних й перетворення енергії в екосистемах. Метою курсу є засвоєння студентами базових підходів щодо аналізу екосистем, та формування практичних навичок щодо застосування методів моделювання для їх вивчення. Курс складається з двох змістовних модулів. У першій частині курсу вивчаються імітаційні моделі популяційної динаміки, зокрема: - загальні поняття про верифікацію і валідацію моделей; - моделі динаміки популяцій; - моделі динаміки населення та епідемій. У другій частині вивчаються методи моделювання екосистем, зокрема: - моделювання фізико-хімічних трансформацій в екосистемах; - моделювання екосистем на прикладі моделей якості води.		
Форма проведення занять	Лекції, практичні заняття, комп'ютерні практикуми		

Дисципліна	**Криптосистеми на еліптичних кривих**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	математичних методів захисту інформації		
Викладачі	проф. Ковальчук Л.В., ас. Грубіян Є.О.		
Вимоги до початку вивчення	Пройдені курси «Прикладна алгебра» / «Математичні основи криптології»		
Анотація дисципліни	Навчальна дисципліна «Криптосистеми на еліптичних кривих» присвячена вивченню теоретичних основ еліптичних кривих (ЕК) над полями дійсних, раціональних чисел, кінцевими полями, і принципів і алгоритмів побудови асиметричних криптосистем, які застосовують арифметику групи точок еліптичних кривих над кінцевими полями. Вивчаються властивості і структура групи точок еліптичних кривих у формах Вейерштраса, Монтгомері, Лежандра, Едвардса та інші, а також арифметика кривих над простими полями і розширеними полями характеристики 2. Розглядаються методи криптоаналізу і історія стандартизації криптосистем цифрового підпису та ін. Для задач постквантової криптографії (PQC) розглядається перспективний алгоритм CSIDH на ізогеніях еліптичних кривих Едвардса. Основні теми, які розглядаються у курсі: 1) Еліптичні криві над полями дійсних і раціональних чисел. 2) Еліптичні криві у формі Вейерштраса і Едвардса над простими полями. Крипто примітиви. 3) Еліптичні криві над розширеними полями характеристики 2. 4) Безпека криптосистем на еліптичних кривих і методи атак 5) Протоколи і стандарти криптосистем на еліптичних кривих. Основною метою дисципліни є формування у студентів глибинного розуміння властивостей груп точок ЕК у різних формах і над різними полями, які дозволяють застосовувати їх у криптосистемах цифрового підпису, розподілу ключів та інших з потрібним рівнем безпеки і найбільш ефективних при імплементації. Для досягнення мети передбачається розв’язання студентами значної кількості розрахункових та аналітичних задач.		
Форма проведення занять	Лекції, практичні заняття, індивідуальні комп’ютерні практикуми		

Дисципліна	**Проектування розподілених систем**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	інформаційної безпеки		
Викладачі	доцент Родіонов А.М.		
Вимоги до початку вивчення	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-застосувань		
Анотація дисципліни	Навчальна дисципліна «Проектування розподілених систем» присвячена теоретичним та практичним аспектам створення масштабованих, високонавантажених та високодоступних розподілених систем, а також програмного забезпечення на їх основі. У курсі розглядається базова теорія, пов'язана з розподіленими системами; велика частина курсу присвячена мікросервісній архітектурі та шаблонам мікросервісів. Практичні завдання присвячені розробці невеликих застосувань на основі шаблонів мікросервісів. У груповому проекті необхідно реалізувати розподілене та відмовостійке застосування на основі мікросервісної архітектури. Основні теми курсу: 1) Масштабованість, продуктивність, доступність сучасних застосувань 2) Шаблони зв'язку в розподілених системах: RPC, Async, Messaging, gRPC 3) Проблеми комунікації повідомленнями: Duplicate, Delay, Drop, Reorder 4) Distributed systems: Communication, Failure Modes, Leader, Consensus, Quorums, Time, Order 5) Монолітна та мікросервісна архітектура - переваги та недоліки 6) Шаблони мікросервісної архітектури: Service Discovery & Service Registry, Deployment Strategy, Microservice chassis, Distributed tracing, DB per service, API Gateway, Circuit Breaker, Testing, Backpressure 7) Розподілені транзакції 8) Системи обміну повідомленнями 9) Архітектура на основі обміну повідомленнями		
Форма проведення занять	Лекції, комп'ютерні практикуми, груповий проект		

Дисципліна	**Технології захисту персональних даних 1**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	інформаційної безпеки		
Викладачі	доц. Прогонов Д.О.		
Вимоги до початку вивчення	**Навчання на програмі дуальної освіти з Samsung R&D Україна** • знання основ математичної статистики та теорії імовірності, знання основних методів оптимізації функцій однієї та декількох змінних, знання основ теорії складності • навички роботи з поширеними системами комп'ютерної математики та моделювання (Python scipy, MATLAB Simulink, MathCAD) • Знання принципів функціонування операційних систем мобільних пристроїв, зокрема Android OS. Знання основ розробки додатків для операційної системи Android OS.		
Анотація дисципліни	Метою дисципліни є формування компетентностей з застосування методів машинного навчання розробки автоматизованих систем обробки персональних даних, зокрема біометричних систем автентифікації. Досліджуються задачі щодо оцінки ефективності сучасних систем одно- та багатофакторної біометричної автентифікації користувачів на мобільних пристроях. За результатами вивчення дисципліни студенти ознайомляться з сучасними автоматизованими системами біометричної автентифікації на мобільних пристроях, отримають знання щодо розробки та оцінки ефективності даних методів.		
Форма проведення занять	Самостійна робота		

Дисципліна	**Технології штучного інтелекту у системах інформаційної безпеки 1**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	інформаційної безпеки		
Викладачі	доц. Прогонов Д.О.		
Вимоги до початку вивчення	**Навчання на програмі дуальної освіти з Samsung R&D Україна** • знання основ математичної статистики та теорії імовірності, знання основних методів оптимізації функцій однієї та декількох змінних, знання основ теорії складності • навички роботи з поширеними системами комп'ютерної математики та моделювання (Python scipy, MATLAB Simulink, MathCAD) • Знання принципів функціонування операційних систем мобільних пристроїв, зокрема Android OS. Знання основ розробки додатків для операційної системи Android OS.		
Анотація дисципліни	Метою дисципліни є формування компетентностей з застосування методів машинного навчання в задачах захисту конфіденційних даних, що оброблюються на мобільних пристроях. Досліджуються задачі щодо розробки й оцінки ефективності автоматизованих систем виявлення загроз інформаційній безпеці мобільних пристроїв, зокрема шкідливого програмного забезпечення (ШПЗ). За результатами вивчення дисципліни студенти ознайомляться з сучасними автоматизованими системами виявлення ШПЗ, отримають знання щодо роботи та розробки методів поведінкового аналізу, а також навики виявлення ШПЗ при наявності інформації щодо особливостей шкідливого програмного забезпечення.		
Форма проведення занять	Самостійна робота		

ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ ДРУГОГО КУРСУ НАВЧАННЯ

Дисципліна	**ARX-криптосистеми та їх криптоаналіз**		
Рівень ВО	Другий (магістерський)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	математичних методів захисту інформації		
Викладачі	доц. Яковлєв С.В.		
Вимоги до початку вивчення	Пройдені курси «Симетрична криптографія» («Криптографія»), «Дискретна математика», «Теорія імовірності», «Математична статистика»; рекомендовано опанувати курс «Моделі та методи криптоаналізу блокових шифрів»		
Анотація дисципліни	Навчальна дисципліна «ARX-криптосистеми та їх криптоаналіз» присвячена так званим ARX-системам та ARX-архітектурі (від Add-Rotation-XOR – трьох основних операцій у структурі криптографічних перетворень), які наразі широко використовуються для алгоритмів так званого «Інтернету речей». Розглядаються алгебраїчні аспекти ARX-систем та методи побудови криптографічних атак (в першу чергу диференціального та обертального криптоаналізу), а також застосування теорії S-функцій та автоматних моделей для автоматизованої побудови атак на ARX-системи. Основні теми, які будуть розглядатись у курсі: 1) будова ARX-криптосистем, повнота ARX-базису; 2) обертальний криптоаналіз ARX-криптосистем; 3) диференціальний криптоаналіз ARX-криптосистем за операціями побітового та модульного додавання; матричні форми диференціальних імовірностей; бінарні знакові різниці та NAF-форми. 4) S-функції та їх диференціальний криптоаналіз; криптоаналіз складних S-функцій. 5) LRX-криптосистеми та їх криптоаналіз.		
Форма проведення занять	Лекції, практичні заняття, індивідуальні комп’ютерні практикуми		

Дисципліна	**Аналіз мережевих структур**		
Рівень ВО	Другий (магістерський)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	математичного моделювання та аналізу даних		
Викладачі	доц. Орєхов О.А.		
Вимоги до початку вивчення	Пройдені курси «Математична логіка», «Дискретна математика» («Дискретний аналіз»)		
Анотація дисципліни	Курс «Аналіз мережевих структур» складається з двох розділів. У першому розділі розглядаються сучасні підходи до побудови систем формальних знань на базі здатних до розв'язання фрагментів дескрипційної логіки. Наводяться приклади онтологій та формальних мов генерації онтологій. У другому розділі надається інформація про мови опису сучасних інформаційних систем – UML, TOGAF та BPMN 2.		
Форма проведення занять	Лекції, комп'ютерні практикуми		

Дисципліна	**Методи обробки та розпізнавання даних**		
Рівень ВО	Другий (магістерський)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	математичного моделювання та аналізу даних		
Викладачі	доц. Юзефович В.В.		
Вимоги до початку вивчення	Рекомендовано опанувати курси «Статистичні методи розпізнавання», «Моделі та рішення в умовах невизначеності»		
Анотація дисципліни	Навчальна дисципліна «Методи обробки та розпізнавання даних» присвячена методам обробки різнорідних даних, з метою покращення їх якості, та методам вирішення на їх основі задач розпізнавання образів (об'єктів, явищ, процесів, подій тощо). Дисципліна передбачає ознайомлення із методами обробки (формалізації, комплексування, групування, агрегування) даних кількісного та якісного характеру та методами розпізнавання (класифікації, ідентифікації, виявлення) на основі отриманих даних об'єктів зацікавленості. Основною метою дисципліни є отримання необхідних теоретичних та практичних знань щодо вирішення конкретних прикладних задач, які вирішуються фахівцями з обробки даних та розпізнавання образів. Для досягнення мети розглядаються ефективні методи та способи, демонструється, яким чином вони використовуються у сучасних інформаційних технологіях. В процесі навчання будуть застосовуватися методи теорії складних систем, дослідження операцій, обробки вимірювань, теорії ймовірності, нечітка математика, методи кластеризації, методи моделювання, методи обробки зображень.		
Форма проведення занять	Лекції, комп'ютерні практикуми		

Дисципліна	**Моделі кіберфізичних систем**		
Рівень ВО	Другий (магістерський)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	інформаційної безпеки		
Викладачі	доц. Смирнов С.А.		
Вимоги до початку вивчення	Для розуміння змісту курсу “Кіберфізичні системи” студентам бажано попередньо володіти знаннями з наступних навчальних дисциплін: математичний аналіз, лінійна алгебра, загальна фізика, диференційні рівняння, теоретична механіка, теорія керування, основи нелінійного аналізу.		
Анотація дисципліни	Навчальна дисципліна орієнтована на оволодіння сучасними кібернетичними та фізичними принципами побудови і функціонування перспективних компьютерів та широкого спектру кіберфізичних систем. Сучасний стан та перспективи розвітку 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 забезпечує імплементацію керуючих та інформаційних процесів у реальні фізичні системи. Мета курсу полягає в ознайомленні з сучасними принципами та засобами організації кібернетичних процесів в фізичних системах. Після засвоєння навчальної дисципліни студенти мають продемонструвати наступні результати навчання: знання: основних принципів організації інформаційних процесів, зв’язку між сигнально-інформаційною та матеріально-енергетичною складовою реальних процесів та явищ; зв’язку між інформацією, прийняттям рішень та їх реалізацією (управлінням); моделей об’єктів та цілей управління, алгоритмів управління та методів їх побудови для консервативних та дисипативних систем, видів синхронізації, управління синхронізацією та управління хаосом; уміння: вільно володіти і оперувати основними поняттями систем управління у фізичному контексті; вміти визначати цілі управління та засоби їх досягнення, характеристики систем управління (стійкість, керованість, спостережуваність); будувати алгоритми управління на основі градієнтних методів та методу швидкісного градієнту; будувати алгоритми синхронізації та управління хаосом. досвід: вільно орієнтуватися на якісному й кількісному рівні в основних фізичних принципах, умовах, можливостях та обмеженнях, 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.		
Форма проведення занять	Лекції, комп’ютерні практикуми		

Дисципліна	**Моделі цінності інформації та ефективність інформаційного захисту**		
Рівень ВО	Другий (магістерський)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	математичних методів захисту інформації		
Викладачі	проф. Савчук М.М.		
Вимоги до початку вивчення	Пройдені курси «Дискретна математика» та «Теорія імовірностей»; студенти повинні мати базові знання та представлення з теорії інформації та криптографії.		
Анотація дисципліни	У навчальній дисципліні «Моделі цінності інформації та ефективність інформаційного захисту» розглядаються теоретичні поняття інформації, 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) криптосистема 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) імітостійкость та цінність інформації; застосування моделей цінності інформації для автентифікації.		
Форма проведення занять	Лекції, практичні заняття		

Дисципліна	**Технології захисту персональних даних 2**		
Рівень ВО	Другий (магістерський)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	інформаційної безпеки		
Викладачі	доцент Прогонов Д.О.		
Вимоги до початку вивчення	**Навчання на програмі дуальної освіти з Samsung R&D Україна** Пройдений курс «Технології захисту персональних даних 1» • знання основ математичної статистики та теорії імовірності, знання основних методів оптимізації функцій однієї та декількох змінних, знання основ теорії складності, знання основ роботи зі штучними нейронними мережами • навички роботи з поширеними системами комп'ютерної математики та моделювання (Python scipy, Keras/TensorFlow, MATLAB Simulink, MathCAD) • Знання принципів функціонування операційних систем мобільних пристроїв, зокрема Android OS. Знання основ розробки додатків для операційної системи Android OS.		
Анотація дисципліни	Метою дисципліни є формування компетентностей з розробки автоматизованих систем обробки персональних даних, зокрема поведінкових систем автентифікації. Досліджуються задачі щодо оцінки ефективності сучасних систем поведінкової автентифікації користувачів на мобільних пристроях. За результатами вивчення дисципліни студенти отримають знання щодо розробки та оцінки ефективності методів поведінкової автентифікації користувачів на мобільних пристроях з використанням штучних нейронних мереж.		
Форма проведення занять	Самостійна робота		

Дисципліна	**Технології штучного інтелекту у системах інформаційної безпеки 2**		
Рівень ВО	Другий (магістерський)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	4 кредити, залік	Мова викладання	Українська
Кафедра	інформаційної безпеки		
Викладачі	доцент Прогонов Д.О.		
Вимоги до початку вивчення	**Навчання на програмі дуальної освіти з Samsung R&D Україна** Пройдений курс «Технології штучного інтелекту у системах інформаційної безпеки 1» • знання основ математичної статистики та теорії імовірності, знання основних методів оптимізації функцій однієї та декількох змінних, знання основ теорії складності, знання основ роботи зі штучними нейронними мережами • навички роботи з поширеними системами комп'ютерної математики та моделювання (Python scipy, Keras/TensorFlow, MATLAB Simulink, MathCAD) • Знання принципів функціонування операційних систем мобільних пристроїв, зокрема Android OS. Знання основ розробки додатків для операційної системи Android OS.		
Анотація дисципліни	Метою дисципліни є формування компетентностей з застосування методів машинного навчання в задачах захисту конфіденційних даних, що оброблюються на мобільних пристроях. Досліджуються задачі щодо розробки й оцінки ефективності автоматизованих систем виявлення шкідливого програмного забезпечення (ШПЗ) в умовах обмеженості апріорних даних щодо його особливостей. За результатами вивчення дисципліни студенти отримають знання щодо розробки методів поведінкового аналізу на основі штучних нейронних мереж, а також навики виявлення ШПЗ в умовах обмеженості апріорних даних щодо його особливостей.		
Форма проведення занять	Самостійна робота		