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

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

ЗАТВЕРДЖУЮ

Проректор з навчальної роботи

_____ Анатолій МЕЛЬНИЧЕНКО

«____»_____ 2022 р.

Ф-КАТАЛОГ
ВИБІРКОВИХ НАВЧАЛЬНИХ ДИСЦИПЛІН
ЦИКЛУ ПРОФЕСІЙНОЇ ПІДГОТОВКИ

для здобувачів ступеня магістра

за освітньою програмою «Системи, технології та математичні методи кібербезпеки»

за спеціальністю 125 Кібербезпека

УХВАЛЕНО:

Методичною радою
КПІ ім. Ігоря Сікорського
(протокол №___ від «___»_____2022 р.)

Вченою радою ФТІ
КПІ ім. Ігоря Сікорського
(протокол №___ від «___»_____2022 р.)

Київ – 2022

Процедура вибору освітніх компонент відбувається згідно з «Положенням про реалізацію права на вільний вибір навчальних дисциплін здобувачами вищої освіти КПІ ім. Ігоря Сікорського» (https://kpi.ua/free-choice-of-academic-disciplines-right) та «Тимчасовим положенням 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://is.ipt.kpi.ua/change_fb_mag

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, іспит)	*Кафедра*	*Стор.*
Захист інформації в спеціалізованих інформаційно-телекомунікаційних системах	ІБ	*5*
Оптоволоконні комунікаційні системи	ІБ	*7*
Методи аналізу великих гетерогенних даних	ММАД	*8*
Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	ІБ	*9*
Теорія і методи соціальної інженерії в кібербезпеці	ІБ	*10*
Загальна теорія ігор	ММАД	*11*
Рефлексивний аналіз поведінки вибору	ІБ	*12*
Комплексне управління IT-інфраструктурою	ІБ	*13*
Технологія блокчейн та розподілені системи	ММЗІ	*14*
Другий (весняний) семестр, залікові дисципліни		
Дисципліна (4 кредити, залік)	*Кафедра*	*Стор.*
Web - аналітика	ІБ	*16*
Технології великих даних	ММАД	*17*
*Технології штучного інтелекту у системах інформаційної безпеки 1	ІБ	*18*
*Технології захисту персональних даних 1	ІБ	*19*
Проектування розподілених систем	ІБ	*20*
Моделі та рішення в умовах невизначеності	ІБ	*21*
Стандартизація в галузі захисту інформації	ММЗІ	*22*

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

Дисципліни для вибору на другий рік навчання		
Магістри-науковці першого курсу обирають **дві** залікові дисципліни з наведеного переліку для вивчення у **третьому** семестрі другого курсу		
Третій (осінній) семестр, залікові дисципліни		
Дисципліна (4 кредити, залік)	*Кафедра*	*Стор.*
Моделі кіберфізичних систем	ІБ	*24*
Методи реалізації криптографічних механізмів	ММЗІ	*25*
Інфраструктури відкритих ключів	ММЗІ	*26*
Моделювання складних систем	ІБ	*27*
*Технології штучного інтелекту у системах інформаційної безпеки 2	ІБ	*28*
*Технології захисту персональних даних	ІБ	*29*

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

Перелік позначень

Кафедри:
ІБ – кафедра інформаційної безпеки
ММАД – кафедра математичного моделювання та аналізу даних
ММЗІ – кафедра математичних методів захисту інформації

ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ ПЕРШОГО КУРСУ НАВЧАННЯ

(ЕКЗАМЕНАЦІЙНІ ДИСЦИПЛІНИ)

Дисципліна	**Захист інформації в спеціалізованих інформаційно-телекомунікаційних системах**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, іспит	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	Проф. Зубок В.Ю.		
Вимоги до початку вивчення	Пройдені курси «Інформаційні технології», «Комп'ютерні мережі», «Комплексні системи захисту інформації» та «Кібернетична безпека» *Необхідно знати*: фізичну природу електромагнітних сигналів та середовища передачі даних, архітектуру комп'ютерних систем; операційні системи та їх безпеку; технології програмування; теорію інформації та кодування; нормативно правове забезпечення захисту інформації; методи та засоби забезпечення інформаційної безпеки; міжнародні та національні стандарти в сфері інформаційної безпеки. *Необхідно вміти*: виконувати класифікацію автоматизованих систем; виконувати класифікацію інформації; виконувати аналіз профілю захищеності; визначати межі контрольованої зони; виконувати проектування та знати процедури забезпечення КСЗІ; виконувати класифікацію об'єктів інформаційної діяльності; розробляти політику безпеки для ОІД (об'єкт інформаційної діяльності); оцінювати ефективність мір захисту інформації.		
Анотація дисципліни	Навчальна дисципліна «Захист інформації інформаційно-телекомунікаційних системах спеціального призначення» присвячена окремим напрямкам та методам, які використовуються у напряму комплексного підходу до захисту інформаційних ресурсів на об'єктах інформаційної діяльності. Подається структурований матеріал, що відображає сучасні технології та моделі захисту інформації в телекомунікаційних системах та мережах. Докладно розглянуті основи захисту інформації та основні питання інформаційної безпеки національної мережі телекомунікацій, телекомунікаційних мереж загального користування та спеціального призначення, основні методи і засоби захисту телетрафіку, а також основи організації захисту інформації в галузі інформаційно-телекомунікаційних систем та їх мереж. Основні теми, які розглядаються у курсі: 1) Системи та мережі передачі. Класифікація; загальні моделі та характеристики систем передачі інформації. 2) Моделі канал зв'язку. Поняття динамічного діапазону каналу зв'язку, узгодження характеристик. 3) Сучасні інформаційно-телекомунікаційні мережі. Класифікація мереж та середовища передачі даних, типи протоколів передачі даних в аспекті захисту інформаційних ресурсів та їх властивостей. 4) Інформаційно-телекомунікаційні системи та технології як об'єкти інформаційної безпеки. 5) Нормативно-правове забезпечення захисту інформації в інформаційно-телекомунікаційних системах та мережах згідно вітчизняних та світових вимог і стандартів. 6) Вимоги та критерії безпеки інформаційно-телекомунікаційних систем. 7) Управління інформаційними активами інформаційно-телекомунікаційних систем загального та спеціального призначення. 8) Моделі загроз та моделі порушника в інформаційно-		

	телекомунікаційних системах та мережах. 9) Ризик менеджмент в інформаційно-телекомунікаційних системах загального та спеціального призначення. 10) Профілі захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах та мережах. Технології та архітектура управління забезпеченням. Основною метою дисципліни є формування у студентів глибинного розуміння технологій та моделей захисту інформації в інформаційно-телекомунікаційних системах та мережах, їх властивостей, внутрішніх зв'язків та інтерпретацій у термінах різних дисциплін. Для досягнення мети передбачається опрацювання значної кількості розрахункових та аналітичних задач, які ілюструють та розширюють лекційний матеріал.
Форма проведення занять	Лекційні та практичні заняття

Дисципліна	**Оптоволоконні комунікаційні системи**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, іспит	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	Ас. Балан А.В.		
Вимоги до початку вивчення	Для освоєння курсу студенти повинні мати тверді знання з дисциплін: «Фзика оптика», «Основи оптоволоконних систем», «Компонентна база ТЗІ», «Схемотехніка ТЗІ»,		
Анотація дисципліни	Принципи функціювання, та архітектурної побудови і організації сучасних телекомунікаційних систем на основі технологій волоконно-оптичних ліній зв'язку та систем передачі даних в локальній та глобальній мережі, а також з основними галузями застосування волоконної оптики в системі кіберпростору. Ознайомити з сучасним мережним телекомунікаційним обладнанням та транспортною телекомунікаційною мережею. Формування навичок індивідуальної практичної та пізнавальної діяльності.		
Форма проведення занять	Лекційні та практичні заняття		

Дисципліна	**Методи аналізу великих гетерогенних даних**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, іспит	Мова викладання	Українська
Кафедра	Математичного моделювання та аналізу даних		
Викладачі	Проф. Шелестов А.Ю.		
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. В 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	Лекційні та лабораторні заняття		

Дисципліна	**Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, іспит	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	*уточнюється*		
Вимоги до початку вивчення	Для успішного оволодіння матеріалом потрібно мати знання та навички з дисципліни “Захист інформації в інформаційно — комунікаційних системах” та “Захист Web-ресурсів”.		
Анотація дисципліни	Метою навчальної дисципліни "Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем" є отримання знань та навичок про архітектуру, налаштування та супровід технологій захисту сучасних інформаційно-комунікаційних систем.". В процесі вивчення дисципліни розглядаються такі теми: -Управління ідентифікаціями (Identity management) -Системи контролю привілеїв користувачів (Privileged access management) -Протоколи автентифікації та авторизації -Засоби побудови віртуальних захищених мереж (VPN) -Системи управління інформаційною безпекою та подіями безпеки (Security information and event management) -Використання засобів віртуалізації та хмарних технологій для побудови захищених інформаційно-комунікаційних систем		
Форма проведення занять	Лекційні та практичні заняття		

Дисципліна	**Теорія і методи соціальної інженерії в кібербезпеці**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (2 семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, іспит	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. Передбачається, що практикуми повинні бути здані вчасно, в разі перевищення дедлайну встановлений штраф: практикум захищається на мінімальну позитивну оцінку. Дати дедлайнів обговорюються зі студентами на першому занятті. 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. За курсом передбачено модульну контрольну роботу для контролю засвоєння практичного та теоретичного матеріалу.		
Форма проведення занять	Лекційні та практичні заняття		

Дисципліна	**Загальна теорія ігор**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, іспит	Мова викладання	Українська
Кафедра	Математичного моделювання та аналізу даних		
Викладачі	Доцент Терещенко І.М.		
Вимоги до початку вивчення	1. Навички розв’язування практичних та теоретичних задач з лінійної алгебри та аналітичної геометрії. 2. Практичні навички та засвоєні теоретичні знання, набуті під час вивчення кредитного модулів «Математичний аналіз».		
Анотація дисципліни	Навчальна дисципліна «Загальна теорія ігор» є дисципліною з циклу професійної підготовки і присвячена формуванню у студентів здатності застосовувати спеціальні математичні поняття, означення, алгоритми та методи, що необхідні для вивчення наступних дисциплін спеціальності «Прикладна математика», вивчення найважливіших професійно корисних результатів прикладної математики. Навчальна дисципліна «Дослідження операцій» спирається на дисципліну «Математичний аналіз», а також дисципліну «Алгебра і геометрія». Завдання навчальної дисципліни — навчити студентів використовувати математичні методи теорії ігор для розв’язання різноманітних прикладних задач прикладного характеру, пов’язаних з оптимізацією функцій, які виникають у практичної діяльності. Навчальна дисципліна «Загальна теорія ігор» містить теоретичні матеріали, що викладаються у 18 лекціях, після засвоєння яких студент буде обізнаний у таких основних напрямках: - основні понять теорії ігор; - антагоністичні ігри; - зв'язок між матричними іграми та лінійним програмуванням; - біматричні ігри; - основні поняття кооперативних ігор; - С-ядро; - вектор Шеплі. Також за дисципліною передбачено ? практичних занять, які доповнюють теоретичний матеріал і активують його практичними навичками. Курс побудований таким чином, що для виконання багатьох завдань студентам необхідно застосовувати навички та знання, отримані при вивчені попередніх дисциплін математичного профілю. Особлива увага приділяється принципу заохочення студентів до активного навчання, у відповідності з яким студенти мають працювати над практичними тематичними завданнями, які дозволять в подальшому вирішувати реальні проблеми та завдання. В результаті студент набуває такі уміння: - уміння формалізувати задачу, в межах термінів теорії ігор формулювати її математичну постановку; - уміння зводити матричну гру до задачі лінійного програмування; - уміння застосовувати графо-аналітичний метод; - уміння знаходити рішення гри за допомогою домінуючих стратегій; - уміння знаходити арбітражне рішення Неша; - уміння застосовувати кооперативні ігри, створювати коаліції; - уміння знаходити поділ за допомогою С-ядра або вектора Шеплі. Ці уміння необхідні для розуміння та використання загальних зв’язків між вивченими математичними поняттями і методами та актуальними практичними задачами. За курсом передбачено модульну контрольну роботу, яка складається з двох робіт на теми ”Знаходження рішення ігри. Правило доповнювальної		

	нежорсткості” та “Арбітражне рішення Неша”. Метою є перевірка оволодіння методами розв’язання антагоністичних, біматричних ігор та вміння вирішувати певні практичні задачі за допомогою теорії ігор, і передбачає самостійне розв’язання задач студентами. Також доводиться до відома студентів те, що відсутність написаної модульної контрольної роботи призводить до недопуску до екзамену.
Форма проведення занять	Лекційні та практичні заняття

Дисципліна	**Рефлексивний аналіз поведінки вибору**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, іспит	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	Доцент Смирнов С.А.		
Вимоги до початку вивчення	Для розуміння змісту курсу студентам достатньо мати базові знання з наступних навчальних дисциплін: математичне моделювання, дискретний аналіз, теорія ймовірностей.		
Анотація дисципліни	В курсі вивчаються особливості процесів прийняття рішень (ППР), пов’язані із рефлексивною структурою та станом свідомості людини, що приймає рішення. Завдання навчальної дисципліни — навчити студентів використовувати методи і прийоми моделювання поведінки вибору, аналізувати отримані моделі, визначати загрози та вразливості ППР, пов'язані з їх структурою та наповненням, а також з варіантами доступності інформації про це. Моделі поведінки вибору, як одно- так і багатосуб’єктні, моделі рефлексивного керування на їх основі мають значну цінність в сучасних умовах, бо їх знання створюють можливості маніпуляції вибором (реклама, фішинг та соціальна інженерія), але також дозволяють знайти можливості захисту від таких маніпуляції.		
Форма проведення занять	Лекційні заняття		

Дисципліна	**Комплексне управління IT-інфраструктурою**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, іспит	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	Ас. Кіфорчук К.О.		
Вимоги до початку вивчення	Навички програмування на мовах C, Java, Python.		
Анотація дисципліни	IT-інфраструктура є цінним ресурсом підприємства. Ефективне управління цим компонентом та його захист є одним з найважливіших завдань будь-якої сучасної IT компанії. Навчальна дисципліна «Комплексне управління IT-інфраструктури» розглядає основні компоненти IT-інфраструктури та відповідні інструменти управління ними. Мета викладання дисципліни – формування системи теоретичних знань про сучасні технології, методи та інструментальні засоби, які використовуються для створення та управління IT-інфраструктурою підприємства, а також практичних навичок, які є необхідними для забезпечення її функціонування. За дисципліною передбачено 3 комп’ютерних практикуми, які доповнюють теоретичний матеріал і поглиблюють його за практичним напрямом. Передбачається, що практикуми повинні бути здані вчасно, в разі перевищення дедлайну встановлений штраф: практикум захищається на мінімальну позитивну оцінку. Дати дедлайнів обговорюються зі студентами на першому занятті. В результаті виконання практикумів студент набуває такі уміння: - використання сучасних технологій для управління персоналом та моніторингу діяльності співробітників; - опанування інструментів моніторингу та логування інформаційних подій IT-інфраструктури; - уміння налаштувати та ефективно використовувати сучасні рішення «інфраструктури як сервісу»; - розуміння принципів архітектури підприємства та цінність, яку вона надає бізнесу. За курсом передбачено модульну контрольну роботу для контролю засвоєння практичного та теоретичного матеріалу.		
Форма проведення занять	Лекційні та лабораторні заняття		

Дисципліна	**Технологія блокчейн та розподілені системи**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	5 кредитів ЄКТС, іспит	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 ЄКТС, 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. Структурний підхід», «Програмування. Об'єктно-орієнтований підхід», «Програмування. Основи 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. В 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 та практичні заняття		

Дисципліна	**Технології великих даних**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	4 кредити ЄКТС, залік	Мова викладання	Українська
Кафедра	Математичного моделювання та аналізу даних		
Викладачі	Доц. Орєхов В.А.		
Вимоги до початку вивчення	Програмування, Інтелектуальний аналіз даних		
Анотація дисципліни	В курсі розглядаються наступні алгоритми та технології: 1. Бібліотека обробки великих даних Hadoop та розподілена файлова система HDFS (Hadoop Distributed File System). Технологія Map Reduce. 2. Алгоритм LSH (Locality Sensitive Hashing) пошуку схожих об’єктів. Поняття шингла, мінхеша і відстані Жаккарда. 3. Фільтрування потоків даних. Фільтр Блума. Підрахунок кількості окремих елементів в потоці даних. Алгоритм Алона-Матіаса-Шегеді. 4. Алгоритм ранжування веб-сторінок PageRank. 5. Алгоритми пошуку частих елементів: Apriori, Парка-Чена-Ю. 6. Алгоритми кластеризації: K-means, CURE. 7. Основи аналізу соціальних мереж. Основні метрики графів соціальних мереж. Пошук кластерів, спільнот, перетину спільнот. 8. Алгоритми зниження розмірності. Декомпозиція CUR. 9. Основи роботи з бібліотекою Apache Spark. API PySpark.		
Форма проведення занять	Лекції та лабораторні заняття		

Дисципліна	**Технології штучного інтелекту у системах інформаційної безпеки 1**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	4 кредити ЄКТС, 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 обробляються 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		

Дисципліна	**Технології захисту персональних даних 1**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	4 кредити ЄКТС, 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	**Проектування розподілених систем**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	4 кредити ЄКТС, 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 будт-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 і велика частина курсу присвячена мікросервісній архітектурі та шаблонам мікросерівів. Практичні завдння 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, практичні заняття, груповий проект		

Дисципліна	**Рішення в умовах невизначеності**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	4 кредити ЄКТС, залік	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	Доцент Смирнов С.А.		
Вимоги до початку вивчення	Для успішного засвоєння курсу потрібні попередні знання з наступних дисциплін: математичний аналіз, алгебра і геометрія, дискретний аналіз, математичне моделювання.		
Анотація дисципліни	Метою курсу є вивчення теоретичних основ та практичних методів прийняття рішень в умовах невизначеностей різної природи: множинної, ймовірністної, конфліктної. Викладаються математичні засоби що дозволяють успішно долати шлях від неформалізованої постановки задачі з боку Замовника, через проактивне моделювання ситуації, до варіантів її точного розв’язання Виконавцем. Обговорюються також методи контролю та подолання різних форм складності та невизначеності, що містяться в практичних ситуаціях прийняття рішень.		
Форма проведення занять	Лекційні та практичні заняття		

Дисципліна	**Стандартизація в галузі захисту інформації**		
Рівень ВО	Другий (магістерський)	Курс	Перший курс (другий семестр)
Обсяг, форма контролю	4 кредити ЄКТС, залік	Мова викладання	Українська
Кафедра	Математичних методів захисту інформації		
Викладачі	Доцент Фаль О.М.		
Вимоги до початку вивчення	Пройдені курси «Криптографія» («Симетрична криптографія», «Асиметричні криптосистеми та протоколи»)		
Анотація дисципліни	Поширення інформаційних технологій (ІТ) в усі сфери господарської діяльності потребує взаємодії та сумісності інформаційних систем від різних постачальників. Вирішення цієї проблеми може бути досягнуто шляхом використання стандартних протоколів, інтерфейсів, структур даних тощо. Тому в рамках різних організацій зі стандартизаціїї розробляється велика кількість стандартів в галузі інформаційних технологій. Засоби убезпечення ІТ є дуже важливою компонентою інформаційних систем, що спричиняє необхідність створення стандартів в галузі безпеки ІТ. Дисципліна «Стандартизація в галузі безпеки інформації». охоплює десятки міжнародних та національних стандартів в галузі безпеки ІТ, які уже уведені в дію, а також знайомить з проектами стандартів, що тільки розробляються. Спектр вказаних стандартів дуже широкий: від загальної архітектури безпеки інформаційних систем до конкретних послуг та механізмів безпеки. Значна кількість стандартів стосується криптографічних механізмів, а саме: цифрових підписів, алгоритмів гешування та вироблення кодів автентифікації повідомлень, алгоритмів шифрування, управління ключами та сертифікатами відкритих ключів. Основні теми, які розглядаються у курсі: 1) Процедури розроблення стандартів та архітектура безпеки. 2) Стандарти схем цифрового підпису. 3) Стандарти процедур автентифікації. 4) Управління ключами та інфраструктура відкритих ключів. 5**)** Стандарти алгоритмів гешування. 6) Стандарти алгоритмів шифрування 7) Управління інформаційною безпекою та оцінювання захищеності ІТ. 8) Генерування криптографічних параметрів. Метою дисципліни є ознайомлення студентів з сучасними процедурами створення стандартів в галузі безпеки ІТ та надання студентам інформації щодо існуючих міжнародних та національних стандартів в галузі безпеки ІТ, проектів стандартів що розроблюються.		
Форма проведення занять	Лекції, семінарські доповіді		

ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ ДРУГОГО КУРСУ НАВЧАННЯ

(ЗАЛІКОВІ ДИСЦИПЛІНИ)

Дисципліна	**Моделі кіберфізичних систем**		
Рівень ВО	Другий (магістерський)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	4 кредити ЄКТС, залік	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	Доцент Смирнов С.А.		
Вимоги до початку вивчення	Для розуміння змісту курсу Кіберфізичні системи студентам бажано попередньо володити знаннями з наступних навчальних дисциплін: математичний аналіз, лінійна алгебра, загальна фізика, диференційні рівняння.		
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. вбудуваними 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 синхронизації, 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 синхронизації 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	Лекційні та лабораторні заняття		

Дисципліна	**Методи реалізації криптографічних механізмів**		
Рівень ВО	Другий (магістерський)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	4 кредити ЄКТС, залік	Мова викладання	Українська
Кафедра	Математичних методів захисту інформації		
Викладачі	Професор Кудін А.М.		
Вимоги до початку вивчення	Пройдений курс «Криптографія»		
Анотація дисципліни	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'явились 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. Саме цим питанням присвячена дисципліна «Методи реалізації криптографічних механізмів». Курс може бути використаний при створенні та експлуатації систем захисту інформації, а також при проведенні сертифікації та експертизи засобів захисту інформації. Метою вивчення дисципліни є ознайомлення студентів з сучасними моделями, що застосовуються в криптології та їх практичною реалізацією, надання інформації про алгоритми реалізації криптосистем. Завданням дисципліни є засвоєння студентами вміння адекватно оцінювати стійкість реальних криптосистем, основних алгоритмів їх реалізації, а також установлення взаємозв'язку між теоретичними моделями та реалізаціями криптографічних механізмів в автоматизованих системах.		
Форма проведення занять	Лекції, комп'ютерні практикуми		

Дисципліна	**Інфраструктури відкритих ключів**		
Рівень ВО	Другий (магістерський)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	4 кредити ЄКТС, залік	Мова викладання	Українська
Кафедра	Математичних методів захисту інформації		
Викладачі	Доцент Яковлев С.В.		
Вимоги до початку вивчення	Пройдений курс «Криптографія»		
Анотація дисципліни	Навчальна дисципліна «Інфраструктури відкритих ключів» знайомить студентів з принципами, методами та механізмами організації систем керування ключами та захищеного документообігу. 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, атрибутні сертифікати, списки відкликаних сертифікатів, протокол OCSP; 5) протоколи керування сертифікатами (PKCS10, CMC, CMP); 6) формати криптографічних повідомлень (CMS), підписані повідомлення, часові штемпелі; розширені формати підписаних повідомлень (CAdES); 7) формати захищених повідомлень. Основною метою дисципліни є формування у студентів знань основних принципів роботи центрів сертифікації ключів, організації життєвого циклу ключів, форматів основних структур даних, які використовуються у механізмах захисту систем захищеного документообігу		
Форма проведення занять	Лекційні заняття		

Дисципліна	**Моделювання складних систем**		
Рівень ВО	Другий (магістерський)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	4 кредити ЄКТС, залік	Мова викладання	Українська
Кафедра	Інформаційної безпеки		
Викладачі	Професор Ланде Д.В.		
Вимоги до початку вивчення	Основними інструментами дисципліни «Моделювання складних систем» є теорія ймовірностей і математична статистика, теорія графів, теорія клітинних автоматів, теорія систем, агентне моделювання.		
Анотація дисципліни	Дисципліна «Моделювання складних систем» розглядається як міждисциплінарна область знань на границі інформатики та кібербезпеки, Вона фокусується на системах забезпечення безпеки, що є складними системами з великою кількістю взаємодіючих компонентів. Курс «Моделювання складних систем» дає змогу оволодіти умінням застосовувати значну кількість математичних методів й адаптивних інструментів моделювання для дослідження взаємодії технічних і соціальних систем. Основною його ідеєю є те, що поведінка простих моделей може бути складною, а наслідком – пояснення складної поведінки системи за допомогою простих моделей. Загалом, даний курс про складні системи дає можливість студентам дізнатися не тільки про системи забезпечення кібербезпеки і соціальні системи, але й розвити навики прграмування, математичного моделювання, узагальнити раніше отриманні знання з фундаментальних дисциплін.		
Форма проведення занять	Лекційні та практичні заняття		

Дисципліна	**Технології штучного інтелекту у системах інформаційної безпеки 2**		
Рівень ВО	Другий (магістерський)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	4 кредити ЄКТС, 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** • 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		

Дисципліна	**Технології захисту персональних даних**		
Рівень ВО	Другий (магістерський)	Курс	Другий курс (третій семестр)
Обсяг, форма контролю	4 кредити ЄКТС, 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** • 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 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		