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

НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

ЗАТВЕРДЖЕНО:

Методичною радою
КПІ ім. Ігоря Сікорського
(протокол №5 від «26» червня 2025 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 та захист інформації

УХВАЛЕНО:

Вченою радою НН ФТІ
КПІ ім. Ігоря Сікорського
(протокол №7 від «12» червня 2025 р.)

Київ – 2025

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

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

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

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

Перелік позначень

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

Дисципліни для вибору на перший рік навчання		
Студенти першого курсу магістратури (ОПП і ОНП) 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.
* Захист інформації в спеціалізованих інформаційно-телекомунікаційних системах	ІБ	5
Методи аналізу великих гетерогенних даних	ММАД	9
Методи глибокого навчання на різнорідних даних	ММАД	11
* Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	ІБ	13
*Теорія і методи соціальної інженерії в кібербезпеці	ІБ	16
Рефлексивний аналіз поведінки вибору	ІБ	19
Технологія блокчейн та розподілені системи	ММЗІ	21

*Складові сертифікатної програми «Кібербезпека об'єктів критичної інфраструктури»

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

ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ ПЕРШОГО КУРСУ НАВЧАННЯ

(ЕКЗАМЕНАЦІЙНІ ДИСЦИПЛІНИ)

Захист інформації в спеціалізованих інформаційно-телекомунікаційних системах

(Проф. Зубок В.Ю.)

Сертифікатна програма	Кібербезпека об’єктів критичної інфраструктури
Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**5 кредити ЄКТС, 150 год** Лекційних занять: 30 год Практичних занять: 30 год Самостійна робота студентів: 90 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	*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.
Що буде вивчатися	Навчальна дисципліна «Захист інформації в спеціалізованих інформаційно-телекомунікаційних системах» 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 розглянуто 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. Для досягнення мети передбачається опрацювання значної кількості розрахункових та аналітичних задач, які ілюструють та розширюють лекційний матеріал.
Чому це цікаво/треба вивчати	Навчальна дисципліна розглядає законодавчі вимоги до кіберзахисту спеціалізованих систем, нормативне забезпечення, міжнародні стандарти на кращі світові практики цієї діяльності, перш за все, в аспекті кібербезпеки так званих Операційних технологій (ICS/SCADA систем). Безпека операційних технологій, “Промисловості 4.0”, промислового Інтернету речей (IIoT) є одним з головних завдань кібербезпеки, особливо під час відновлення інфраструктури та промисловості України.
Чому можна навчитися	Сучасні технологічні тренди захисту інформації спеціалізованих ІКС. Загальні напрями технічної політики з забезпечення кібербезпеки спеціалізованих ІКС. Спеціалізовані ІКС в державному та банківському секторі, в промисловості. Міжнародні документи з кіберзахисту промислових ІКС. Ключові аспекти спеціалізованих комунікаційних

	технологій в промисловості. Кіберінциденти в промисловості. Огляд та архітектурно-функціональне порівняння відомих платформ та систем кіберзахисту спеціалізованих ІКС в промисловості. Архітектури та топології промислових ІКС. Порівняння вимог до безпеки загальних IT систем та ІКС управління технологічними процесами (АСУТП). Архітектура кіберзахисту спеціалізованих промислових ІКС. Сегментація, сегрегація, засоби впровадження. Заходи з забезпечення кібербезпеки в промисловості. Реагування на інциденти. Побудова політики безпеки спеціалізованої ІТС з використанням «контролів безпеки».
Як можна користуватися набутими знаннями та вміннями	Вивчення дисципліни дозволяє поглибити розуміння технологій та моделей захисту інформації в інформаційно-телекомунікаційних системах та мережах, їх властивостей, внутрішніх зв'язків та інтерпретацій у термінах різних дисциплін.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1oYhaM7ZS7vCQHO-JcPR-yJXs5cecCRWG?usp=sharing
Вид семестрового контролю	екзамен

Методи аналізу великих гетерогенних даних

(Доцент Колотій А.В.)

Кафедра, яка забезпечує викладання	ММАД
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**5 кредити ЄКТС, 150 год** Лекційних занять: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 106 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Для вивчення дисципліни студент має бути знайомий з основами програмування, бажано на Python, структурами даних. Бажано розуміти принципи побудови та функціонування програмних систем, володіти навичками підготовки та аналізу даних, бути знайомим з методами штучного інтелекту, зокрема, нейронними мережами.
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 різнорідних 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 та вміннями	Для вирішення задач розподіленої обробки великих обсягів дани

Інформаційне забезпечення дисципліни	Силабус, Google Classrom з матеріалами https://drive.google.com/file/d/1prPUSfL_dTGyGTedy1rjooBdbSBiSig2/view?usp=sharing
Вид семестрового контролю	екзамен

Методи глибокого навчання на різнорідних даних

(Асистент Яворський О.А.)

Кафедра, яка забезпечує викладання	ММАД
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**5 кредити ЄКТС, 150 год** Лекційних занять: 14 год Лабораторних занять: 30 год Самостійна робота студентів: 106 год
Мова викладання	українська
Вимоги для 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	- Основні архітектури глибинних мереж - Методи fine-tuning (покращення) моделей - Методи дистиляції знань - Проблеми побудови RAG систем - Фізично-обгрунтовані архітектури - Проблеми оцінки якості та ефективності моделей - Методи інженерії даних (feature engineering) - Мультимодальні архітектури - Вступ до роботи з CUDA
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	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
Як можна користуватися набутими знаннями та вміннями	- 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 https://drive.google.com/file/d/1wYbZuWZe3k1UKRIgNUA0z-khT35cwnbh/view
Вид семестрового контролю	екзамен

Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем

(Доц. Барановський О.М.)

Сертифікатна програма	Кібербезпека об’єктів критичної інфраструктури
Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**5 кредити ЄКТС, 150 год** Лекційних занять: 30 год Практичних занять: 30 год Самостійна робота студентів: 90 год
Мова викладання	Українська
Вимоги для початку вивчення дисципліни	Для успішного оволодіння матеріалом потрібно мати знання щодо методів захисту інформації в інформаційно — комунікаційних системах та підходів до захисту web-ресурсів.
Що буде вивчатися	Метою навчальної дисципліни 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
Чому це цікаво/треба вивчати	Отримання знань та навичок щодо архітектури, налаштування та супроводу технологій захисту сучасних інформаційно-комунікаційних систем
Чому можна навчитися	В процесі вивчення дисципліни студенти засвоять 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
Як можна користуватися набутими знаннями та вміннями	В результаті вивчення навчальної дисципліни студенти зможуть застосувати отримані знання для аналізу захищеності інформаційно-комунікаційних систем, формування рекомендацій щодо підвищення ступеню їх захисту, а також роботи над обраними темами магістерських дисертацій
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1_zarwriqpQx7j4VWCVt4zzfXjp5j_cb1?

	usp=sharing
Вид семестрового контролю	екзамен

Теорія і методи соціальної інженерії в кібербезпеці

(Доцент Стьопочкіна І.В.)

Сертифікатна програма	Кібербезпека об’єктів критичної інфраструктури
Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**5 кредити ЄКТС, 150 год** Лекційних занять: 30 год Практичних занять: 30 год Самостійна робота студентів: 90 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Бажане уміння програмувати на мовах Java, Python.
Що буде вивчатися	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 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. • 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.
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. Відповідно, проходження даного курсу дозволяє розширити знання студентів щодо ефективній протидії таким атакам.
Чому можна навчитися	Технікам соціальної інженерії (для задач offensive security), опанувати засоби та методи протидії.
Як можна користуватися набутими знаннями та вміннями	В результаті виконання практикумів студенти набувають 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.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1bEgTKqgB95O4C0MY6UfZ96twY5CxMa0-?usp=sharing Платформа “Сікорський”: курс «Теорія та методи соціальної інженерії в кібербезпеці» https://do.ipo.kpi.ua/course/view.php?id=1713
Вид семестрового контролю	екзамен

Рефлексивний аналіз поведінки вибору

(Доцент Смирнов С.А.)

Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**5 кредити ЄКТС, 150 год** Лекційних занять: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 106 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Для розуміння змісту курсу студентам достатньо мати базові знання з основ математичного моделювання, дискретного аналізу та теорії імовірностей.
Що буде вивчатися	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.
Чому це цікаво/треба вивчати	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, політтехнології, фішинг та соціальна інженерія), але також дозволяють знайти

	інструменти для захисту від таких маніпуляції.
Чому можна навчитися	Студенти зможуть 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 них.
Як можна користуватися набутими знаннями та вміннями	Отримані знання дозволяють моделювати та аналізувати рефлексивну структуру людської взаємодії, знаходити та блокувати загрози, спроби маніпуляції та рефлексивного керування.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1kZeQQ4YQGwkgll5Gxr1kNnX-BTMWvKb0?usp=sharing Посилання на дистанційний ресурс: Платформа “Сікорський”, курс “Рефлексивний аналіз поведінки вибору” https://classroom.google.com/u/1/c/ODIyNTE2ODIzNjZa
Вид семестрового контролю	екзамен

Технологія блокчейн та розподілені системи

(Проф. Кудін А.М.)

Кафедра, яка забезпечує викладання	ММЗІ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**5 кредити ЄКТС, 150 год** Лекційних занять: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 106 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Бажані знання щодо методів симетричної та асиметричної криптографії, сучасних криптосистем та протоколів
Що буде вивчатися	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». Теоретичний матеріал супроводжується комп'ютерними практикумами, на яких ви зможете самостійно розгорнути деякі блокчейн-системи та опанувати механізми їх роботи.
Чому це цікаво/треба вивчати	За результатами вивчення даного курсу студенти будуть ознайомлені з принципами функціонування новітніх blockchain-технологій, огляд сучасних протоколів консенсусу при формуванні геш-ланцюгів блоків. Це дозволить поглибити знання студентів щодо сучасних методів криптографічного

	захисту інформації.
Чому можна навчитися	У дисципліні буде розглянуто такі теми: • «низова» структура блокчейнів; • протоколи консенсусу: Proof of Work, Proof of Stake, Proof of Activity та ін.; • децентралізовані та централізовані блокчейни (private ledgers); • принципи роботи криптовалют та смарт-контрактів.
Як можна користуватися набутими знаннями та вміннями	Отримані знання дозволяють проводити аналіз та практично використовувати blockchain-технології для побудови розподілених баз даних із властивостями незмінюваності та спостережуваності
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1dsXa76wYk9R5qbs1Sb6z8gvANb7KrNdr?usp=sharing
Вид семестрового контролю	екзамен

Основи теорії ідентифікації систем

(професор, д.т.н. Мачуський Є.А.)

Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**5 кредити ЄКТС, 150 год** Лекційних занять: 30 год Лабораторних занять: 30 год Самостійна робота студентів: 106 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	● знання основ математичного аналізу; ● знання основ спектрального аналізу сигналів; ● знання пакетів для моделювання на мові програмування Python; ● знання принципів обробки мультимедійних даних (стиснення, фільтрація від завад, підвищення якості).
Що буде вивчатися	Метою навчальної дисципліни є розширення 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	За результатами вивчення дисципліни проводиться поглиблення розуміння сучасних підходів до ідентифікації систем обробки даних за наявними (частковими) даними. Це надає можливість щодо використання новітніх методів для непрямого визначення параметрів системи обробки даних, що є одним з найбільш складних випадків

	при проведенні спеціальних досліджень.
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 та вміннями	Побудова статистичних моделей та методів визначення параметрів систем обробки сигналів за наявними даними. Оцінка якості роботи даних моделей та методів.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1NjzPAxnku7W_3KdXL-CPjeaArudZdk0c?usp=sharing
Вид семестрового контролю	екзамен

Моделі та методи криптоаналізу блокових шифрів

(Доц. Яковлев С.В.)

Кафедра, яка забезпечує викладання	ММЗІ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**5 кредити ЄКТС, 150 год** Лекційних занять: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 106 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Базові знания з наступних дисциплін: теорія ймовірності, симетрична криптографія, математична статистика, методи криптоаналізу
Що буде вивчатися	Основною метою дисципліни є формування у студентів глибинного розуміння сучасних статистичних методів 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) модифікаці'і 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) модифікаці'і та узагальнення лінійного криптоаналізу: білінійний криптоаналіз, узагальнений лінійний криптоаналіз на довільних абелевих групах, аналіз нульових кореляцій, диференціально-лінійні розпізнавачі; 7) методи автоматизованого пошуку високоймовірних та неможливих диференціалів, високймовірних лінійних апроксимацій; 8) інтегральний криптоаналіз та йога узагальнення: аналіз лінійних підпросторів, властивості подільності.
Чому це цікаво/треба вивчати	Багато сучасних інформаційних систем використовують блокові шифри, зокрема AES та DES. Для успішного аналізу рівня захищеності та пошуку вразливостей таких систем, необхідно знати відповідні криптографічні властивості блокових шифрів та вміти здійснювати 'іх криптоаналіз.
Чому можна навчитися	Студенти отримують знания моделей та методів криптоаналізу блокових шифрів, параметрів стійкості до криптоаналітичних атак та 'іх поведінку; вміння будувати статистичні атаки на ітеративні блокові шифри та одержувати аналітичні чи розрахункові оцінки стійкості до таких атак.
Як можна користуватися набутими знаннями та вміннями	Створювати та аналізувати сучасні методи блокового шифрування, оцінювати та контролювати гарантований рівень захисту при шифруванні.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/luUogeDExAda2Wsvs7BJo7K0gt1EjzmBY?usp=sharing
Вид семестрового контролю	екзамен

Загальна теорія ігор

(Доц. Терещенко І.М.)

Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**5 кредити ЄКТС, 150 год** Лекційних занять: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 106 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Для розуміння змісту курсу студентам достатньо мати базові знання з наступних навчальних дисциплін: математичне моделювання, дискретний аналіз, теорія ймовірностей.
Що буде вивчатися	В курсі вивчаються особливості процесів прийняття рішень, пов’язані із структурою конфліктної взаємодії, можливостями щодо впливу та оцінювання результатів з боку сторін, що приймають рішення.
Чому це цікаво/треба вивчати	Навчальна дисципліна «Загальна теорія ігор» присвячена формуванню у студентів здатності застосовувати спеціальні математичні поняття, означення, алгоритми та методи, що необхідні для вивчення наступних спеціальних дисциплін, вивчення найважливіших професійно корисних результатів прикладної математики.
Чому можна навчитися	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.
Як можна користуватися набутими знаннями та вміннями	В результаті навчання 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.
Інформаційне забезпечення дисципліни	- Посилання на силабус: https://drive.google.com/file/d/18Z_SSCo8hhYHJ30cgwzMmFa4qiLNBrsJ/view?usp=sharing Посилання на дистанційний ресурс: Платформа "Сікорський", курс "Загальна теорія ігор" https://classroom.google.com/c/MTQyNDc1MjgwOTg2
Вид семестрового контролю	екзамен

ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ ПЕРШОГО КУРСУ НАВЧАННЯ

(ЗАЛІКОВІ ДИСЦИПЛІНИ)

Web - аналітика

(Доц. Ткач В.М.)

Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**4 кредити ЄКТС, 120 год** Лекційних занять: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 76 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Предмет базується на знаннях в галузі програмного забезпечення ЕОМ, програмування та створення web-застосунків.
Що буде вивчатися	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.
Чому це цікаво/треба вивчати	Ознайомлення з принципами пошуку аномалій в даних веб-аналітики, основами поведінкового аналізу користувачів в мережі Інтернет
Чому можна навчитися	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.
Як можна користуватися набутими знаннями та вміннями	Отримані знання можуть використовуватися при підготовці магістерської дисертації, зокрема аналізу даних, що збираються в Інтернет, принципи пошуку аномалій в даних веб-аналітики
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1TGbOCpNYMUGSSk64N8LSX4aHISBNLEDV?usp=sharing
Вид семестрового контролю	залік

Проектування розподілених систем

(Доцент Родіонов А.М.)

Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**4 кредити ЄКТС, 120 год** Лекційних занять: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 76 год
Мова викладання	українська
Вимоги для 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-застосувань
Що буде вивчатися	Навчальна дисципліна присвячена теоретичним та практичним аспектам створення масштабованих, високонавантажених та високодоступних розподілених систем, а також програмного забезпечення на їх основі. Практичні завдання присвячені розробці невеликих застосувань на основі шаблонів мікросервісів. У груповому проекті необхідно реалізувати розподілене та відмовостійке застосування на основі мікросервісної архітектури.
Чому це цікаво/треба вивчати	У курсі розглядається базова теорія пов’язана з розподіленими системами і велика частина курсу присвячена мікросервісній архітектурі та

	шаблонам мікросерівів.
Чому можна навчитися	Основні теми курсу: • Масштабованість, продуктивність, доступність сучасних застосувань • Шаблони зв'язку в розподілених системах: RPC, Async, Messaging, gRPC • Проблеми комунікації повідомленнями: Duplicate, Delay, Drop, Reorder • Distributed systems: Communication, Failure Modes, Leader, Consensus, Quorums, Time, Order • Монолітна та мікросервісна архітектура - переваги та недоліки • Шаблони мікросервісної архітектури: Service Discovery & Service Registry, Deployment Strategy, Microservice chassis, Distributed tracing, DB per service, API Gateway, Circuit Breaker, Testing, Backpressure • Розподілені транзакції • Системи обміну повідомленнями • Архітектура на основі обміну повідомленнями
Як можна користуватися набутими знаннями та вміннями	Отримані знання та навички можуть використовуватися для реалізації розподілених та відмовостійких високонавантажених систем, зокрема із застосуванням мікросервісної архітектури.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1WjA1CoO6UZC2nPrLK5GhGlkMxHLUwIkt?usp=sharing
Вид семестрового контролю	залік

Рішення в умовах невизначеності та ризиків

(Доцент Смирнов С.А.)

Сертифікатна програма	Кібербезпека об’єктів критичної інфраструктури
Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**4 кредити ЄКТС, 120 год** Лекційних занять: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 76 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Для успішного засвоєння курсу потрібні базові знання з математичного аналізу, алгебри і геометрії, дискретного аналізу, математичного моделювання.
Що буде вивчатися	Метою курсу є вивчення теоретичних основ та практичних методів прийняття рішень в умовах невизначеностей різної природи: множинної, ймовірністної, конфліктної. Обговорюються також методи контролю та подолання різних форм складності, ризику та невизначеності, що містяться в практичних ситуаціях прийняття рішень.
Чому це цікаво/треба вивчати	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.
Чому можна навчитися	Розв’язувати задачі оцінювання та прийняття рішень в умовах

	невизначеності та ризику від виникнення проблеми до отримання результату
Як можна користуватися набутими знаннями та вміннями	Набуті знання та вміння щодо сучасних методів підтримки прийняття рішень в умовах невизначеності можуть бути використані для розв'язання широкого кола задач за темою магістерської дисертації.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/14Q8h3tj3SPojyXIVIZtb9SWGap_2_OIN?usp=sharing Посилання на дистанційний ресурс: Платформа "Сікорський", курс "Рішення в умовах невизначеності та ризику" https://classroom.google.com/u/1/c/OTk3MTgyNzQzNDNa?hl=uk
Вид семестрового контролю	залік

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ АНАЛІЗУ ВЕЛИКИХ ГЕТЕРОГЕННИХ ДАНИХ

(Професор Шелестов А.Ю.)

Сертифікатна програма	Моделі та методи інтелектуального аналізу

	гетерогенних даних
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: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 76 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	Наразі дані великого об’єму аналізуються та обробляються великою кількістю систем. Одним з сучасних підходів до розв’язання таких задач на основі великих даних є використання хмарних інфраструктур, які дозволяють використовувати набір віддалених обчислювальних компонентів для обробки даних як одну з інформаційних підсистем. Саме вивченню таких технологічних рішень і присвячено даний освітній компонент.
Чому можна навчитися	Володінню методами та засобами аналізу великих гетерогенних даних
Як можна користуватися набутими знаннями та вміннями	Знання та вміння, набуті в процесі вивчення дисципліни "Інформаційні технології аналізу великих гетерогенних даних" дозволять використовувати сучасні інструменти побудови розподілених додатків та використовувати хмарні ресурси для розв’язання прикладних задач на мультимодальних даних.
Інформаційне забезпечення дисципліни	Силабус, монографія, навчальний посібник
Вид семестрового контролю	Залік

Проактивний захист персональних даних 1

(доцент, к.т.н. Прогонов Д.О.)

Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
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	**4 кредити ЄКТС, 120 год** Лекційних занять: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 76 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	● знання основ математичного аналізу; ● знання основ спектрального аналізу сигналів; ● знання пакетів для моделювання на мові програмування Python; ● знання принципів обробки мультимедійних даних (стиснення, фільтрація від завад, підвищення якості)
Що буде вивчатися	Метою навчальної дисципліни є розширення 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.
Як можна користуватися набутими знаннями та вміннями	Підвищення точності імітаційного моделювання фізичних процесів та явищ.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1GZNyZQqJyPptRSVOrhYP3ChKcn6rhIKx?usp=sharing
Вид семестрового контролю	залік

Проактивний захист персональних даних 2

(доцент, к.т.н. Прогонов Д.О.)

Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
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	**4 кредити ЄКТС, 120 год** Лекційних занять: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 76 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	● знання основ математичного аналізу; ● знання основ спектрального аналізу сигналів; ● знання пакетів для моделювання на мові програмування Python; ● знання принципів обробки мультимедійних даних (стиснення, фільтрація від завад, підвищення якості)
Що буде вивчатися	Метою навчальної дисципліни «Проактивний захист персональних даних 2» є поглиблення у студентів компетентностей з синтезу елементів систем обробки інформації з врахуванням заданих вимог щодо їх взаємодії з іншими елементами та системами. Предметом дисципліни є методи синтезу систем.
Чому це цікаво/треба вивчати	Поглиблення розуміння принципів, методів та засобів імітаційного моделювання систем обробки сигналів. Розуміння методів синтезу даних систем за наявними вимогами/параметрами.
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.
Як можна користуватися набутими знаннями та вміннями	Підвищення якості моделювання систем обробки сигналів, синтезу даних систем за наявними параметрами/вимогами.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1znaRw_uqqhFwlfeH-TDuik9GGg9o7fDH?usp=sharing
Вид семестрового контролю	залік

Інфраструктури відкритих ключів

(Доц. Яковлев С.В.)

Кафедра, яка забезпечує викладання	ММЗІ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**4 кредити ЄКТС, 120 год** Лекційних занять: 30 год Самостійна робота студентів: 90 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Знання основ криптографії
Що буде вивчатися	Навчальна дисципліна «Інфраструктури відкритих ключів» знайомить студентів з принципами, методами та механізмами організації: систем керування ключами та захищеного докvментообігv.
Чому це цікаво/треба вивчати	Основною метою дисципліни є формування у студентів знань основних принципів роботи центрів сертифікаці'і ключів, організаці'і життевого циклу ключів, форматів основних структур даних, які використовуються у механізмах захисту систем захищеного документообігу
Чому можна навчитися	Основні теми, які розглядаються у курсі: електронні довірчі послуги, класифікація електронних підписів та "іх функціональність; механізми eIDAS; життевий цикл криптографічних ключів, організація керування життевим циклом ключів, різні варіанти будови інфраструктур відкритих ключів, Центри сертифікаці"і ключів; - мова ASN.1, стандарти кодування BER,

	CER, DER; - формат сертифікатів відкритих ключів X.509v3; перевірка статусу сертифікатів, атрибутні сертифікати, списки відкликаних сертифікатів, протокол OCSP; - протоколи керування сертифікатами (PKCSl0, CMC, CMP); - формати криптографічних повідомлень (CMS), підписані повідомлення, часові штемпелі; розширені формати підписаних повідомлень (CAdES); - dюомати захишених повіломлень
Як можна користуватися набутими знаннями та вміннями	Знания основних принципів роботи центрів сертифікаці'і ключів, організаці'і життєвого циклу ключів, форматів основних структур даних, дозволяють ввільно почуватися у роботі з механізмами захисту систем захищеного докvментообігv
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.cor/ drive/f olders/lrkBBOVirSi3zT4j fL7zy2nЬILAVuY-z?usp=sharing Посилання на дистанційний ресурс: Платформа "Сікорський", курс "Інфраструктури відкритих ключів" https://classroom.google.com/u/1/c/ NTI3MTM0MDcxNjc5
Вид семестрового контролю	залік

Аналіз кібернетичних загроз в інформаційно-телекомунікаційних системах із застосуванням методів машинного навчання

(Доц. Прогонов Д.О.)

Сертифікатна програма	Кібербезпека об’єктів критичної інфраструктури
Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**4 кредити ЄКТС, 120 год** Лекційних занять: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 76 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	- знання основ математичного аналізу; - знання основ спектрального аналізу сигналів; - знання пакетів для моделювання на мові програмування Python; - знання 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 в інформаційно-комунікаційних системах в умовах опрацювання значних об’ємів даних. Предметом дисципліни є методи статистичного аналізу та статистичного моделювання числових даних
Чому це цікаво/треба вивчати	Поглиблення розуміння принципів роботи, області застосування та обмежень сучасних статистичних моделей даних. Підвищення точності роботи статистичних моделей в умовах зашумленості та/або даних.

Чому можна навчитися	- Знання термінології в галузі аналізу та класифікації (кластеризації) даних; - Знання методів моделювання багатовимірних сигналів в умовах обмеженості або відсутності даних щодо їх статистичних характеристик; - Знання поширених методів класифікації (кластеризації) багатовимірних даних; - Навички практичної роботи у сучасних програмних комплексах аналізу та обробки даних. - Вміння вибору статистичних моделей багатовимірних сигналів з врахуванням наявної інформації щодо їх статистичних та кореляційних характеристик; - Вміння застосування методів класифікації (кластеризації) даних в умовах обробки реальних (зашумлених) сигналів; - Вміння проведення оцінювання якості роботи систем класифікації (кластеризації) даних
Як можна користуватися набутими знаннями та вміннями	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	Google classroom: https://classroom.google.com/c/NjE4ODkxMDE1MTUz?cjc=ccbtwcx
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: 30 год Практичних занять: 14 год Самостійна робота студентів: 76 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 уміннями	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

ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ ДРУГОГО КУРСУ НАВЧАННЯ

(ЗАЛІКОВІ ДИСЦИПЛІНИ)

Безпека кіберфізичних систем

(Доцент Смирнов С.А.)

Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**4 кредити ЄКТС, 120 год** Лекційних занять: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 76 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 убезпечення 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	Отримати *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); класифікації загроз для систем управління та методів їх аналізу, виявлення та попередження; 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, вразливість, керованість, спостережуваність); будувати алгоритми управління на основі градієнтних методів та методу швидкісного градієнту; перевіряти алгоритми керування на загрози та вразливості.
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	Посилання на силабус: https://drive.google.com/drive/folders/1CVEEybuGa9n_LD1bACSEGEwBxxTH-OmA?usp=sharing Посилання на дистанційний ресурс: Платформа “Сікорський”, курс “Безпека кіберфізичних систем” https://classroom.google.com/u/1/c/NTI3MTM0MDcxNjc5
Вид семестрового контролю	залік

Моделювання складних систем забезпечення безпеки

(д.т.н., професор Качинський А. Б.)

Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**4 кредити ЄКТС, 120 год** Лекційних занять: 30 год Практичних занять: 14 год Самостійна робота студентів: 76 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Основними інструментами дисципліни «Моделювання складних систем забезпечення безпеки» є теорія ймовірностей і математична статистика, теорія графів, теорія клітинних автоматів, агентне моделювання.
Що буде вивчатися	Курс «Моделювання складних систем забезпечення безпеки» дає змогу оволодіти умінням застосовувати значну кількість математичних методів і адаптивних інструментів моделювання для дослідження взаємодії технічних і соціальних систем. Теоретичні матеріали курсу дають студенту знання про: 1) лінійні моделі та методи їх регуляризації; 2) методи побудови нелінійних моделей; 3) моделі змішаного типу (SWM метод); 4) байєсівські моделі складних структурних відношень; 5) ансамблі моделей (випадковий ліс, бустінг, бегінг).
Чому це цікаво/треба вивчати	Дисципліна «Моделювання складних систем забезпечення безпеки» 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.
Чому можна навчитися	Внаслідок виконання практичних завдань студент набуває такі уміння: 1) застосовувати багатомодельний підхід до розуміння складних явищ і процесів; 2) оцінювати параметри моделей; 3) відбирати підмножини змінних; 4) знижувати розмірність ознакового простору; 5) отримувати додаткову інформацію про параметри моделі за допомогою перехресної перевірки та бутстреп методу; 6) оцінювати ефективність розробленої моделі.
Як можна користуватися набутими знаннями та вміннями	В роботі з складними системами допоможуть знання та навички з декомпозиції та спрощення, агрегування систем, вміння розділяти та поєднувати, досліджувати окремі компоненти. Знання, набуті студентами під час вивчення курсу «Моделювання складних систем забезпечення безпеки», дозволять ліпше розуміти, пояснювати, розробляти, прогнозувати і досліджувати складні явища та процеси, що відбуваються у реальних системах.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1wqIWYN4guBZIwYRFvKifP5UO0wZMu6Zx?usp=sharing
Вид семестрового контролю	залік

Технології штучного інтелекту у системах інформаційної безпеки

(доцент, к.т.н. Прогонов Д.О.)

Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
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	**4 кредити ЄКТС, 120 год** Лекційних занять: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 76 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Навчання на програмі дуальної освіти з Samsung R&D Україна
Що буде вивчатися	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 шкідливого програмного забезпечення (ШПЗ) в умовах обмеженості апріорних даних щодо його особливостей.
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 основ математичної статистики та теорії ймовірності, 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) • Знання принципів функціонування операційних систем мобільних пристроїв, зокрема Android. Знання основ розробки додатків для операційної системи Android.
Як можна користуватися набутими знаннями та вміннями	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.
Інформаційне забезпечення дисципліни	Посилання на силабус: • https://drive.google.com/drive/folders/1Ihu6JKrgQgGmjZvhmtCuvvbLycZ6cuyq?usp=sharing
Вид семестрового контролю	залік

Технології захисту персональних даних

(доцент, к.т.н. Прогонов Д.О.)

Кафедра, яка забезпечує викладання	ІБ
Рівень вищої освіти	2
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	**4 кредити ЄКТС, 120 год** Лекційних занять: 30 год Практичнихзанять: 14 год Самостійна робота студентів: 76 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Навчання на програмі дуальної освіти з Samsung R&D Україна
Що буде вивчатися	Метою дисципліни є формування компетентностей з застосування методів машинного навчання розробки автоматизованих систем обробки персональних даних, зокрема поведінкових систем автентифікації
Чому це цікаво/треба вивчати	Досліджуються задачі щодо оцінки ефективності сучасних систем поведінкової автентифікації користувачів на мобільних пристроях
Чому можна навчитися	Знання основ математичної статистики та теорії ймовірності, 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); знання принципів функціонування операційних систем мобільних пристроїв, зокрема Android OS. Знання основ розробки додатків для операційної системи Android OS.
Як можна користуватися набутими знаннями та вміннями	За результатами вивчення дисципліни студенти отримають знання та навички щодо розробки та оцінки ефективності методів поведінкової автентифікації користувачів на мобільних пристроях з використанням штучних нейронних мереж.
Інформаційне забезпечення дисципліни	Посилання на силабус: • https://drive.google.com/drive/folders/1iTQyc9eVKU8c1jfqEjXyv937C2paMPng?usp=sharing
Вид семестрового контролю	залік

Методи реалізації криптографічних механізмів

(Проф. Кудін А.М.)

Кафедра, яка забезпечує викладання	ММЗІ
Рівень вищої освіти	2
Можливі обмеження	Без обмежень
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	**4 кредити ЄКТС, 120 год** Лекційних занять: 30 год Лабораторних занять: 14 год Самостійна робота студентів: 76 год
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Знання основ криптографії
Що буде вивчатися	Метою вивчення дисципліни єознайомлення 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 встановлення взаємозв'язку між теоретичними моделями та реалізаціями криптографічних механізмів в автоматизованих системах.
Чому це цікаво/треба вивчати	Перехід людства до інформаційного суспільства супроводжуеться 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 досліджуються 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.
Чому можна навчитися	Метою вивчення дисципліни е ознайомлення студентів з сучасними моделями, що застосовуються в криптології та їх практичною реалізацією, надання інформації про алгоритми реалізації криптосистем. Завданням дисципліни - засвоєння студентами вміння адекватно оцінювати стійкість реальних криптосистем, основних алгоритмів "їх реалізації, а також встановлення взаемозв 'язку між теоретичними моделями та реалізаціями криптографічних механізмів в автоматизованих системах.
Як можна користуватися набутими знаннями та вміннями	Курс може бути використаний при створенні та експлуатації систем захисту інформації, а також при проведенні сертифікації та експертизи засобів захисту інформації.
Інформаційне забезпечення дисципліни	• Посилання на силабус: https://drive.google.com/drive/folders/1WSYvmD97XeUe9rrc_ptiK7gqaySL6kWZ? usp=sharing
Вид семестрового контролю	залік

АЛГОРИТМИ КОДУВАННЯ ДВІЙКОВИХ ДАНИХ

Кафедра	Математичних методів захисту інформації

Рівень вищої освіти	Другий (магістерський)
Курс, семестр	2 курс, 3 семестр
Обсяг дисципліни та розподіл годин	**4 кредити ЄКТС (120 годин)** Лекційних занять: 30 год Практичних занять: 14 год Самостійна робота студентів: 76 год
Мова викладання	Українська
Вимоги до початку вивчення дисципліни	Базові знання з дискретної математики, лінійної прикладної алгебри, програмування. Знання теорії інформації та кодування суттєво посилить розуміння даної дисципліни, хоча не є обов'язковим для вивчення.
Що буде вивчатися	Основні теми, які розглядаються у курсі: 1) коди та алгоритми представлення двійкових даних; 2) алгоритми стискання інформації та методи посилення їх ефективності; 3) контрольні суми та алгоритми завадостійкого кодування.
Чому це цікаво/треба вивчати	Теорія мертва без практики (драматична пауза). Дуже часто теоретичні знання про поведінку алгоритмів в ідеальних модельних умовах стикаються на практиці із суворою реальністю, коли особливості обчислювального середовища, архітектури системи чи мови програмування перегортають поведінку алгоритмів з ніг на голову. У даному курсі основний фокус буде зосереджено саме на реалізації алгоритмів та аналізі ефективності таких реалізацій при взаємодії із різнорідними даними, що прокладе місток між теорією та практикою.
Чому можна навчитися	Курс повністю присвячено відомим спеціалізованим алгоритмам, заточеним під розв'язання конкретних задач кодування: перетворення у різних схемах кодування, стискання даних без втрат, виправлення помилок у даних. Опанування курсу передбачає систематичне виконання практичних завдань на програмування усіх алгоритмів, які розглядаються. Окремою навичкою, яка буде розвиватись у курсі, є планування та виконання обчислювальних експериментів для порівняння різних алгоритмів та їх реалізацій.
Як можна користуватися набутими знаннями і уміннями	Набуті знання та навички дозволяють створювати ефективні програмні системи та/або їх складові (системні бібліотеки) як на етапі проектування, так і на етапі реалізації, за рахунок порівняльного аналізу різних можливих підходів до розв'язання конкретних задач із урахуванням можливостей архітектури та середовища обчислення.
Інформаційне забезпечення	Силабус: https://mmis.ipt.kpi.ua/education/education-master-syllabi/
Вид семестрового контролю	Залік

КВАНТОВІ ОБЧИСЛЕННЯ ТА КВАНТОВА КРИПТОГРАФІЯ

Лектор	Старший викладач 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: 30 год Практичних занять: 14 год Самостійна робота студентів: 76 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