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

ЗАТВЕРДЖЕНО:

Методичною радою
КПІ ім. Ігоря Сікорського
(протокол № 8 від « 2 » червня 2023 р.)

Ф-КАТАЛОГ
ВИБІРКОВИХ НАВЧАЛЬНИХ ДИСЦИПЛІН
ЦИКЛУ ПРОФЕСІЙНОЇ ПІДГОТОВКИ

для здобувачів ступеня магістра за освітньою програмою
«Системи технічного захисту інформації»,
за спеціальністю 125 Кібербезпека та захист інформації

УХВАЛЕНО:

Вченою радою ФТІ
КПІ ім. Ігоря Сікорського
(протокол №7 від «15» травня 2023 р.)

Київ – 2023

Процедура вибору освітніх компонент відбувається згідно з «Положення про реалізацію права на вільний вибір навчальних дисциплін здобувачами вищої освіти КПІ ім. Ігоря Сікорського» (https://osvita.kpi.ua/node/185).

Силабуси усіх дисциплін та інша супровідна інформація розміщена на сайті кафедри: http://is.ipt.kpi.ua/is/individualnij-vibir-distsiplin-za-osvitnoyu-programoyu/

Дисципліни для вибору на перший рік навчання		
Магістри першого курсу обирають **три** екзаменаційні дисципліни та **дві** залікові дисципліни з наведеного переліку для вивчення у **другому** семестрі		
Другий (весняний) семестр, екзаменаційні дисципліни		
Дисципліна (5 кредитів, екзамен)	*Кафедра*	*Стор.*
в1.Захист інформації в спеціалізованих інформаційно-телекомунікаційних системах	ІБ	*4*
в2.Методи аналізу великих гетерогенних даних	ММАД	*7*
в3.Методи глибокого навчання на різнорідних даних	ММАД	*8*
в4.Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	ІБ	*9*
в5.Теорія і методи соціальної інженерії в кібербезпеці	ІБ	*11*
в6.Рефлексивний аналіз поведінки вибору	ІБ	*13*
в7.Технологія блокчейн та розподілені системи	ММЗІ	*15*
в8.Захист конфіденційної інформації з використанням методів машинного навчання	ІБ	*17*
в9.Основи теорії ідентифікації систем	ІБ	*19*
в10.Організаційне забезпечення оцінювання захищеності інформації	ІБ	*21*
в11.Проектування комплексів захисту конфіденційної інформації	ІБ	*22*
Другий (весняний) семестр, залікові дисципліни		
Дисципліна (4 кредити, залік)	*Кафедра*	*Стор.*
в12.Web - аналітика	ІБ	*24*
в13.Проектування розподілених систем	ІБ	*26*
в14.Рішення в умовах невизначеності	ІБ	*28*
в15.Інформаційні технології аналізу великих гетерогенних даних	ММАД	*29*
в16.Теорія захисту інформаційних ресурсів обмеженого доступу	ІБ	*30*
в17.Проактивний захист персональних даних 1*	ІБ	*31*
в18.Проактивний захист персональних даних 2*	ІБ	*32*

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

Перелік позначень

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)

1. Захист інформації в спеціалізованих інформаційно-телекомунікаційних системах

(проф. Зубок В.Ю.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС
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 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 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 ІТ 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

2. Методи аналізу великих гетерогенних даних
(проф. Шелестов А.Ю.)

Кафедра, яка забезпечує викладання	Математичного моделювання та аналізу даних
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС
Мова викладання	українська
Вимоги для початку вивчення дисципліни	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.
Що буде вивчатися	Дисципліна присвячена вивченню теоретичних положень і сучасних методів математичного моделювання, аналізу та обробки гетерогенних даних, методів регресійного аналізу та кластеризації, нейронних мереж, тощо.
Чому це цікаво/треба вивчати	Отримання знань щодо теоретичного обґрунтування та навичок практичного застосування новітніх методів аналізу та обробки гетерогенних даних
Чому можна навчитися	За результатами вивчення дисципліни розширюються знання студентів щодо принципів аналізу та обробки великих гетерогенних даних.
Як можна користуватися набутими знаннями та вміннями	Отримані теоретичні знання та практичні навички можуть використовуватися для дослідження джерел гетерогенних даних та принципів їх спільного використання, а також адаптації даних методів до вирішення поставлених задач дисертаційного дослідження.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1JmCUkUOE68kM9TIsCUffZ6UvBs6Otw5k?usp=sharing
Вид семестрового контролю	екзамен

3. Методи глибокого навчання на різнорідних даних (проф. Куссуль Н.М.)

Кафедра, яка забезпечує викладання	Математичного моделювання та аналізу даних
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Для вивчення дисципліни студент має володіти методами лінійної алгебри, теорії ймовірностей і математичної статистики, теорії оптимізації, машинного навчання та аналізу даних, бути знайомим з основами програмування, бажано на Python, а також з класичними алгоритмами та структурами даних.
Що буде вивчатися	Дисципліна "Методи глибокого навчання на різнорідних даних" присвячена вивченню методів та технологій машинного навчання з урахуванням сучасних тенденцій розвитку цієї галузі в епоху цифровізації з використанням великих об'ємів гетерогенних даних.
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	В результаті вивчення навчальної дисципліни студенти зможуть застосувати методи глибокого навчання для обробки гетерогенних даних; будуть володіти практичними навичками використання інструментів глибокого навчання для розв'язання задач на основі гетерогенних даних великого об'єму.
Як можна користуватися набутими знаннями та вміннями	Набуті знання та навички можуть бути використаними для вирішення задач аналізу кіберінцидентів та проведення досліджень за темою дисертаційної роботи.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1XlJH0-S2VcJxn9ZlZq3VADm7JM9VRzkw?usp=sharing Платформа "Сікорський": курс «Методи глибокого навчання на різнорідних даних» https://do.ipo.kpi.ua/course/view.php?id=1713
Вид семестрового контролю	екзамен

4. Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем

(доц. Барановський О.М.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС
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.
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

5. Теорія і методи соціальної інженерії в кібербезпеці

(доц. Стьопочкіна І.В.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС
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.
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

6. Рефлексивний аналіз поведінки вибору

(доц. Смирнов С.А.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС
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 (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

7. Технологія блокчейн та розподілені системи

(проф. Кудін А.М.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС
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

8. Захист конфіденційної інформації з використанням методів машинного навчання

(доц., к.т.н. Прогонов Д.О.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС
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 з обмеженим доступом в умовах опрацювання значних об'ємів даних. Предметом дисципліни є методи статистичного аналізу та статистичного моделювання числових даних.
Чому це цікаво/треба вивчати	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	Посилання на силабус: https://drive.google.com/drive/folders/1q7TbM-IOiLp0MBJ7FLFxAX4xySa_zQ0q?usp=sharing
Вид семестрового контролю	екзамен

9. Основи теорії ідентифікації систем

(проф., д.т.н. Мачуський Є.А.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС
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	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

10.Організаційне забезпечення оцінювання захищеності інформації
(ст. викл., д.т.н. Морщ Є.В.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Необхідні знання, навички та вміння в області компонентної бази пристроїв ТЗІ, а також правових основ захисту інформації.
Що буде вивчатися	Метою дисципліни є вивчення порядку організації та проведення державної експертизи у сфері технічного захисту інформації, принципів державної політики у сфері ліцензування, ліцензійних умов провадження господарської діяльності з надання послуг у галузі технічного захисту інформації, питань нагляду і контролю у сфері ліцензування.
Чому це цікаво/треба вивчати	Ознайомлення з сучасним станом нормативної документації в галузі технічного захисту інформації, розуміння принципів державної політики у сфері ліцензування
Чому можна навчитися	За результатами вивчення курсу здобувачі отримають навички практичної роботи з технічних регламентів і передбачених ними процедур оцінки відповідності, а також здійсненням добровільної оцінки відповідності, організацією стандартизації в Україні
Як можна користуватися набутими знаннями та вміннями	Під час вивчення дисципліни проводиться ознайомлення з організаційними засадами розроблення, прийняття та застосування технічних регламентів і передбачених ними процедур оцінки відповідності, а також здійсненням добровільної оцінки відповідності, організацією стандартизації в Україні.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1sOY4Uk2Xw3hc4qhz1PhATRLesH78mO0j?usp=sharing
Вид семестрового контролю	екзамен

11.Проектування комплексів захисту конфіденційної інформації
(проф., д.т.н. Мачуський Є.А.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	5 кредитів ЄКТС
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Для освоєння курсу студенти повинні мати тверді знання щодо основ програмування, теорії кіл та обробки сигналів, компонентної бази та схемотехніки пристроїв ТЗІ, основи роботи з технічною документацією та протоколами міжнародних стандартів техніки ТЗІ.
Що буде вивчатися	Курс “Комплекси охорони об’єктів інформаційної діяльності” присвячений проектуванню та створенню засобів технічного захисту інформації від несанкціонованого доступу та проектуванню комплексних системи захисту інформації. В основу курсу покладено нормативні документи та рекомендації з технічного захисту інформації, а також світові стандарти.
Чому це цікаво/треба вивчати	Розуміння принципів проектуванню та створенню засобів технічного захисту інформації від несанкціонованого доступу та проектуванню комплексних системи захисту інформації. Ознайомлення з нормативними документами та рекомендаціями з технічного захисту інформації.
Чому можна навчитися	За результатами вивчення курсу студенти отримають навички щодо підготовки та проведення проектуванню комплексних системи захисту інформації.
Як можна користуватися набутими знаннями та вміннями	За результатами навчання студенти отримують практичні навички з проектування комплексних систем захисту інформації та проведення державної експертизи у сфері технічного захисту інформації.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1sNcZ-zNJb87AMrIZXuAOhiAtBVI0Qlo6?usp=sharing
Вид семестрового контролю	екзамен

ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ ПЕРШОГО КУРСУ НАВЧАННЯ

(ЗАЛІКОВІ ДИСЦИПЛІНИ)

12.Web - аналітика

(доц. Ткач В.М.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредити ЄКТС
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

13.Проектування розподілених систем

(доц. Родіонов А.М.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредити ЄКТС
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

14.Рішення в умовах невизначеності

(доц. Смирнов С.А.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредити ЄКТС
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Для успішного засвоєння курсу потрібні попередні 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 початку до кінця
Як можна користуватися набутими знаннями та вміннями	Отримані знання та вміння щодо сучасних методів прийняття рішень в умовах невизначеності можуть бути використані для вирішення 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

15.Інформаційні технології аналізу великих гетерогенних даних

(проф. Шелестов А.Ю.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредити ЄКТС
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	Дисципліна присвячена вивченню сучасних засобів аналізу гетерогенних даних та основних інформаційних технологій для роботи з даними великого об’єму з різних джерел.
Чому це цікаво/треба вивчати	Ознайомлення з новітніми засобами аналізу гетерогенних даних та основних інформаційних технологій щодо обробки значних об’ємів даних
Чому можна навчитися	В межах даної навчальної дисципліни розглядаються сучасні інформаційні технології та програмне забезпечення для обробки гетерогенних даних, підходи до обміну та представлення гетерогенної інформації.
Як можна користуватися набутими знаннями та вміннями	Отримання навичок роботи з інформаційних технологій для роботи з гетерогенними даними великого об’єму
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/122tNDi639lFqMhusIqY2tLc01yPfX7c5?usp=sharing
Вид семестрового контролю	залік

16.Теорія захисту інформаційних ресурсів обмеженого доступу

(доц., к.т.н. Прогонов Д.О.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредити ЄКТС
Мова викладання	українська
Вимоги для початку вивчення дисципліни	Для освоєння курсу студенти повинні мати тверді знання щодо основ електродинаміки, компонентної бази ТЗІ, а також проектування систем ТЗІ
Що буде вивчатися	Метою курсу є вивчення базових понять та принципів функціонування пристроїв з точки зору можливості утворення каналів витоку інформації за рахунок ПЕМВН, протидії НСД до ІзОД електричними та електромагнітними каналами, у тому числі, віброакустичних, а також ознайомлення з їх проектуванням та конструюванням на прикладах найбільш поширених пристроїв.
Чому це цікаво/треба вивчати	Даний курс дозволяє поглибити знання в частині фахової підготовки з технічного захисту інформації разом з дисциплінами «ТЗІ», «ЗІ в телекомунікаційних системах», «Радіопротидія», «Проектування СЗІ» та ін.
Чому можна навчитися	Ознайомлення з базовими принципами утворення каналів витоку інформації за рахунок ПЕМВН, протидії НСД до ІзОД електричними та електромагнітними каналами. Отримання навичок щодо проектуванням та конструюванням найбільш поширених пристроїв з технічного захисту інформації.
Як можна користуватися набутими знаннями та вміннями	Увага приділяється питанням, що складають зміст проблематики технічного захисту інформації (ЗІ), а саме, нелінійним перетворенням, каналам побічних випромінювань та рівням захищеності від завад.
Інформаційне забезпечення дисципліни	Посилання на силабус: https://drive.google.com/drive/folders/1HBCHauz36b9d1eb_c2NxIk6Ngls0UQ8L?usp=sharing
Вид семестрового контролю	залік

17.Проактивний захист персональних даних 1

(доц., к.т.н. Прогонов Д.О.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредити ЄКТС
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

18.Проактивний захист персональних даних 2

(доц.т, к.т.н. Прогонов Д.О.)

Кафедра, яка забезпечує викладання	інформаційної безпеки
Рівень вищої освіти	2
Курс, семестр	1 курс, 2 семестр
Обсяг дисципліни та розподіл годин аудиторної та самостійної роботи	4 кредити ЄКТС
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