

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ВІДЕОНАГЛЯДУ»

Лектор курсу			Хаб'юк Наталія Сергіївна		Контактна інформація лектора (e-mail), сторінка курсу в Google Class		e-mail: n.khabiuk@duikt.edu.ua , сторінка курсу в Google Class – https://classroom.google.com/c/NzkyOTk4MjI0OTM5?cjc=2nuobczo	
Галузь знань			G Інженерія, виробництво та будівництво		Рівень вищої освіти		бакалавр	
Спеціальність			G5 Електроніка, електронні комунікації, приладобудування та радіотехніка		Семестр		5	
Освітня програма			Мобільні телекомунікації та системи цифрового телебачення		Тип дисципліни		Обов'язкова	
Обсяг:	Кредитів ECTS	Годин	За видами занять:					
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка	
	3	90	18	-	36	-	36	
АНОТАЦІЯ КУРСУ								
Взаємозв'язок у структурно-логічній схемі								
Освітні компоненти, які передують вивченню			Вища математика, Безпроводові телекомунікаційні мережі, Генерування цифрових модульованих сигналів, Основи теорії систем, Теорія передачі сигналів в інфокомунікаційних мережах.					
Освітні компоненти для яких є базовою			Основи кібербезпеки і захисту інформації, Штучний інтелект, Моніторинг телекомунікаційних мереж.					
Мета курсу:		Навчити студентів теоретичних знань та практичних навичок у сфері розробки програмних рішень для аналізу відеоданих, а також формування у студентів здатності проектувати та реалізовувати інтелектуальні системи відеонагляду з використанням сучасних методів комп'ютерного зору, аналізу відеоданих і машинного навчання для вирішення прикладних задач у сфері безпеки та цифрового розвитку.						
Компетентності відповідно до освітньої програми.								
Soft- skills / Загальні компетентності (ЗК)					Hard-skills / Спеціальні компетентності (СК)			
ЗК 3. Здатність до абстрактного мислення, аналізу та синтезу. ЗК 4. Здатність застосовувати знання у практичних ситуаціях. ЗК 8. Здатність працювати в команді. ЗК 9. Здатність вчитися і оволодівати сучасними знаннями. ЗК 10. Вміння виявляти, ставити та вирішувати проблеми. ЗК-11. Навики здійснення безпечної діяльності.					ПК 1. Здатність розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства. ПК 3.Здатність використовувати базові методи, способи тазасоби отримання, передавання, обробки та зберіганняінформації. ПК 9. Здатність здійснювати приймання та освоєннянового обладнання відповідно до чинних нормативів. ПК 10. Здатність здійснювати монтаж, налагодження, налаштування, регулювання, дослідну перевірку працездатності, випробування та здачу в експлуатацію споруд, засобів і устаткування телекомунікацій та радіотехніки. ПК 17. Здатність контролювати і діагностувати стан обладнання і програмного забезпечення інформаційних та телекомунікаційних мереж, мереж теле- та радіомовлення, систем передачі, систем комутації, кінцевих пристроїв користувача, залежно від методів їхньої технічної експлуатації. ПК 18. Здатність вирішувати задачі оптимізації та використання засобів оброблення, передавання, збереження та відображення інформації в системах цифрового телерадіомовлення.			

Програмні результати навчання (ПР)			
ПРН6. Здатність пояснювати результати, отримані в результаті проведення вимірювань, в термінах їх значущості та пов'язувати їх з відповідною теорією. ПРН7. Мати навички оцінювання, інтерпретації та синтезу інформації і даних. ПРН15. Здатність розуміння і застосовування основних властивостей компонентної бази для забезпечення якості та надійності функціонування телекомунікаційних, радіотехнічних систем і пристроїв. ПРН16. Здатність розуміння і застосовування засобів автоматизації проектування і технічної експлуатації систем телекомунікацій та радіотехніки у професійній діяльності. ПРН18. Здатність знаходити, оцінювати і використовувати інформацію з різних джерел, необхідну для розв'язання професійних завдань, включаючи відтворення інформації через електронний пошук.			
ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
РОЗДІЛ 1. ІННОВАЦІЙНІ НАПРЯМИ РОЗВИТКУ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ.			
Тема 1. Відеонагляд 5.0: Інтелектуальні технології безпеки. Знати: еволюцію систем відеонагляду від класичних до інтелектуальних систем, основні напрями застосування відеонагляду основні принципи побудови ICB, базові алгоритми відеоаналітики, ключові технології відеонагляду: AI, Cloud AI, Deep Learning, Edge computing, Big Data, IoT-інтеграція, типи ШІ в сучасних системах відеоспостереження: CNN, Transformer, YOLO, DETR, ViT тощо, переваги та обмеження інтелектуальних систем відеонагляду. Вміти: пояснювати принцип роботи ICB, розрізняти терміни: object detection, object tracking, re-identification, pose estimation, action recognition, face recognition, attribute analysis, класифікувати функціонал AI-камер, формувати базові вимоги до системи відеонагляду з використанням відеоаналітики, обирати архітектуру системи, формулювати технічне завдання (ТЗ), оцінювати ефективність алгоритмів: розуміти метрики точності: Precision/Recall та ймовірність хибних спрацювань. Формування компетенцій: ЗК3, ЗК4, ЗК8, ЗК9, ЗК10, ЗК11, ПК1, ПК3, ПК9, ПК10, ПК17, ПК18 Програмні результати навчання: ПРН6, ПРН7, ПРН15, ПРН16, ПРН18 Рекомендовані джерела: 1–5			
Заняття 1.1. Використання ШІ у відеоаналітиці. Самонавчальні системи розпізнавання загроз. Глибокі нейронні мережі для аналізу поведінки.	Лекція 1 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 1.2. Огляд, аналіз та класифікація інтелектуальних функцій систем відеонагляду покоління Video Surveillance 5.0	Практичне заняття 1 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Заняття 1.3. Проектування інтелектуальної системи відеонагляду та формування технічного завдання	Практичне заняття 2 2 год	3 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.

Тема 2. Етичний ШІ у відеоспостереженні.

Знати: основні положення законодавства: розуміння вимоги GDPR (General Data Protection Regulation) та EU AI Act (перший у світі закон про штучний інтелект), принципи Privacy by Design: що таке «конфіденційність за проектом» та як закладати захист даних на етапі розробки архітектури, види упередженості: bias, як виникає алгоритмічна упередженість та які її наслідки, методи анонімізації: різниця між деідентифікацією, розмиттям облич (blurring) та повною анонімізацією метаданих.

Вміти аналізувати етичні ризики при впровадженні систем відеонагляду з ШІ, оцінювати відповідність систем відеоспостереження принципам етичного ШІ, розрізняти допустиме та недопустиме використання відеоаналітики, формулювати вимоги до систем відеонагляду з урахуванням етичних і правових аспектів, пропонувати заходи з мінімізації ризиків порушення приватності, аргументовано обговорювати етичні дилеми, пов'язані з відеоспостереженням.

Формування компетенцій: ЗК3, ЗК4, ЗК8, ЗК9, ЗК10, ЗК11, ПК1, ПК3, ПК9, ПК10, ПК17, ПК18

Програмні результати навчання: ПРН6, ПРН7, ПРН15, ПРН16, ПРН18

Рекомендовані джерела: 1–5

Заняття 2.1. Баланс між безпекою та конфіденційністю. Антиупереджені алгоритми у відеоаналітиці. Регулювання ШІ у системах нагляду.	Лекція 2 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 2.2. Аналіз етичних ризиків та оцінка відповідності систем відеоспостереження р ШІ	Практичне заняття 3 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Заняття 2.3. Проектування етично безпечної системи відеонагляду та формування етичних вимог з урахуванням принципів Privacy by Design	Практичне заняття 4 2 год	3 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування

Тема 3. Біометричний відеонагляд наступного покоління.

Знати: методи біометричної ідентифікації, технологію розпізнавання облич, Liveness Detection-перевірка на «живість», математичні метрики точності: що таке FAR — помилковий допуск та FRR — помилкова відмова, біометричні вектори, проблеми точності, стійкості та надійності біометричної ідентифікації, ризики та обмеження використання біометричних даних у системах безпеки.

Вміти: пояснити принципи роботи біометричного відеонагляду, аналізувати переваги та недоліки різних біометричних підходів, оцінювати доцільність застосування біометричних систем для конкретних об'єктів, інтерпретувати результати роботи систем розпізнавання, формувати базові вимоги до біометричної системи відеонагляду, враховувати етичні та правові аспекти при проектуванні біометричних систем.

Формування компетенцій: ЗК3, ЗК4, ЗК8, ЗК9, ЗК10, ЗК11, ПК1, ПК3, ПК9, ПК10, ПК17, ПК18

Програмні результати навчання: ПРН6, ПРН7, ПРН15, ПРН16, ПРН18

Рекомендовані джерела: 1–5

Заняття 3.1. Аналіз мікровиразів обличчя. Поведінкове біометричне розпізнавання. Безконтактні методи ідентифікації.	Лекція 3 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 3.2. Дослідження впливу зовнішніх чинників на метрики FAR та FRR у системах розпізнавання облич	Практичне заняття 5 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.

Заняття 3.3. Порівняльний аналіз та тестування безконтактних біометричних технологій наступного покоління в інтелектуальних системах відеонагляду.	Практичне заняття 6 2 год	3 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Тема 4. Децентралізовані відеосистеми на основі блокчейну. Знати: основні принципи систем та технології блокчейн, архітектуру блокчейн-орієнтованих відеосистем, відмінності між централізованими та децентралізованими системами відеонагляду, способи зберігання та передачі відеоданих у блокчейн-середовищі, механізми забезпечення цілісності, автентичності та незмінності відеоданих, переваги, обмеження та виклики застосування блокчейну у відеоспостереженні. Вміти: пояснювати принцип роботи децентралізованих відеосистем, аналізувати доцільність використання блокчейну у системах відеонагляду, порівнювати централізовані та децентралізовані архітектури відеосистем, формувати базові вимоги до відеосистем з використанням блокчейн-технологій. Формування компетенцій: ЗК3, ЗК4, ЗК8, ЗК9, ЗК10, ЗК11, ПК1, ПК3, ПК9, ПК10, ПК17, ПК18 Програмні результати навчання: ПРН6, ПРН7, ПРН15, ПРН16, ПРН18 Рекомендовані джерела: 1–5			
Заняття 4.1. Безпечне зберігання та передача відеоданих. Блокчейн для перевірки автентичності відео. DAO-управління системами безпеки.	Лекція 4 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 4.2. Порівняльний аналіз та проектування архітектури децентралізованої системи відеоспостереження	Практичне заняття 7 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Заняття 4.3. Моделювання захисту, цілісності та доступу до відеоданих у блокчейн-системі з використанням хешування	Практичне заняття 8 2 год	3 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Тема 5. Відеоспостереження на основі гіперспектрального аналізу. Знати: поняття гіперспектрального зображення та його відмінність від моно- і мультиспектрального, фізичні основи гіперспектрального аналізу, архітектуру гіперспектральних систем відеоспостереження, методи обробки та аналізу гіперспектральних відеоданих, застосування гіперспектрального аналізу у системах безпеки та моніторингу, переваги та обмеження гіперспектральних систем порівняно з традиційним відеонаглядом. Вміти: пояснювати принцип роботи гіперспектрального відеоспостереження, аналізувати можливості використання гіперспектральних даних для виявлення об'єктів і аномалій, порівнювати класичний відеонагляд та гіперспектральні системи, оцінювати доцільність застосування гіперспектрального аналізу для конкретних задач, враховувати технічні, економічні та практичні обмеження таких систем. Формування компетенцій: ЗК3, ЗК4, ЗК8, ЗК9, ЗК10, ЗК11, ПК1, ПК3, ПК9, ПК10, ПК17, ПК18 Програмні результати навчання: ПРН6, ПРН7, ПРН15, ПРН16, ПРН18 Рекомендовані джерела: 1–5			
Заняття 5.1. Нові методи розпізнавання об'єктів. Виявлення прихованих загроз. Аналіз матеріалів за спектральними характеристиками.	Лекція 5 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування

Заняття 5.2. Аналіз спектральних характеристик та проєктування інтелектуальної системи відеоспостереження на основі гіперспектральних технологій	Практичне заняття 9 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Заняття 5.3. Моделювання процесу виявлення та класифікації об'єктів у гіперспектральному відео	Практичне заняття 10 2 год	6 балів	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
САМОСТІЙНА РОБОТА			
ТЕМА 1. <i>Архітектура інтелектуальної системи відеонагляду 5.0</i> ТЕМА 2. <i>Миттєва оцінка етичних ризиків ШІ у відеонагляді за допомогою інструментів self-assessment</i> ТЕМА 3. <i>Біометричні технології у сучасних системах відеонагляду</i> ТЕМА 4. <i>Децентралізовані відеосистеми та захист відеоданих</i>	4.год	1 бал	1.Зробити: проаналізувати типову архітектуру системи відеонагляду 5.0, визначити роль ШІ, та хмарних сервісів. Розглянути: джерела відеоданих, рівні обробки інформації, взаємодію між компонентами системи. Вивчити: відмінності між централізованою та гібридною архітектурами, сучасні платформи відеонагляду. Дослідити: переваги та недоліки різних архітектурних підходів.
	4 год	1 бал	2.Зробити: чек-лист для швидкої оцінки етичних ризиків конкретної системи. Розглянути: Як проводити self-assessment перед впровадженням: DPIA процедура. Розглянути етичні дилеми в українських контекстах: закон про персональні дані. Вивчити: Вивчити інструменти для оцінки етики ШІ. Дослідити: 1-2 випадки етичних непорозумінь з ШІ-відеонаглядом у 2023–2025 рр. Провести аналіз компанії з відеонагляду які адаптувалися до AI Act.
	4год	1 бал	3. Зробити: один із методів біометричної ідентифікації, дослідити фактори, що впливають на точність розпізнавання. Розглянути: розпізнавання облич, аналіз ходи, поведінкову біометрію. Вивчити: принципи роботи біометричних алгоритмів, показники ефективності біометричних систем. Виконати: підготувати порівняльну таблицю біометричних методів, короткий опис щодо їх практичного застосування
	4 год	1 бал	4. Зробити: проаналізувати концепцію децентралізованого відеонагляду. Розглянути: механізми контролю доступу, збереження цілісності відео, використання смарт-контрактів. Вивчити: основи блокчейн-технологій, підходи до зберігання відеоданих (off-chain). Дослідити:

ТЕМА 5. Перспективні технології відеонагляду: від гіперспектрального аналізу до Video Surveillance 6.0			можливості застосування блокчейну в системах безпеки. Виконати: концептуальну схему децентралізованої відеосистеми, описати її переваги та обмеження.
	4 год	1 бал	5. Зробити: узагальнити всі розглянуті технології курсу. Розглянути: гіперспектральний відеонагляд, мультисенсорні системи, інтеграцію ШІ, IoT та великих даних. Вивчити: сучасні тенденції розвитку інтелектуальних систем безпеки. Дослідити: можливі напрями еволюції відеонагляду після 5.0. Виконати: підготувати оглядову роботу або презентацію бачення розвитку відеонагляду.

РОЗДІЛ 2. ПЕРСПЕКТИВНІ ТА БЕЗПЕЧНІ ТЕХНОЛОГІЇ ВІДЕОСПОСТЕРЕЖЕННЯ МАЙБУТНЬОГО.

Тема 6. Квантові та постквантові технології у відеоспостереженні.

Знати: базові поняття квантових та постквантових технологій, відмінності між класичними, квантовими та постквантовими підходами до захисту інформації, принципи квантового розподілу ключів (QKD), загрози для сучасних систем відеоспостереження з боку квантових обчислень, поняття постквантової криптографії та її роль у захисті відеоданих, використання квантових технологій у системах відеонагляду, перспективи розвитку квантово-захищених систем безпеки.

Вміти: пояснювати принципи застосування квантових і постквантових технологій у відеоспостереженні, оцінювати ризики безпеки відеоданих, порівнювати класичні та квантово-захищені системи відеоспостереження, формувати базові вимоги до захисту відеосистем з урахуванням квантових загроз, прогнозувати напрями розвитку систем відеонагляду в умовах квантової епохи.

Формування компетенцій: ЗКЗ, ЗК4, ЗК8, ЗК9, ЗК10, ЗК11, ПК1, ПК3, ПК9, ПК10, ПК17, ПК18

Програмні результати навчання: ПРН6, ПРН7, ПРН15, ПРН16, ПРН18

Рекомендовані джерела: 1–5

Заняття 6.1. Криптографічний захист відеоданих.	Лекція 6 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 6.2. Застосування квантових і постквантових технологій у системах відеоспостереження	Практичне заняття 11 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Заняття 6.3. Впровадження постквантових алгоритмів (PQC) у цифрові підписи відеокамер	Практичне заняття 12 2 год	3 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.

Тема 7. Метавсесвіт та відеоспостереження.

Знати: основні моделі/концепції «метавсесвіту», основні способи зв'язку реального відеоспостереження з метавсесвітом/цифровими двійниками, які технології забезпечують синхронізацію фізичного відео з віртуальним середовищем у реальному часі, перспективи розвитку відеоспостереження у метавсесвіті.

Вміти: пояснювати роль відеоспостереження у метавсесвіті та цифрових двійниках, аналізувати сценарії застосування інтелектуального відеонагляду у віртуальних і гібридних середовищах, оцінювати переваги та обмеження використання відеоданих у метавсесвіті, формувати концептуальні моделі взаємодії фізичного та віртуального відеоспостереження.

Формування компетенцій: ЗКЗ, ЗК4, ЗК8, ЗК9, ЗК10, ЗК11, ПК1, ПК3, ПК9, ПК10, ПК17, ПК18 Програмні результати навчання: ПРН6, ПРН7, ПРН15, ПРН16, ПРН18 Рекомендовані джерела: 1–5			
Заняття 7.1. Віртуальні патрульні. Взаємодія відеонагляду з метавсесвітом.	Лекція 7 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 7.2. Дослідження та використання систем відеоспостереження у метавсесвітах і цифрових двійниках	Практичне заняття 13 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Заняття 7.3. Оцінка впливу відеоспостереження на приватність користувачів Метавсесвіту: від ідентифікації до захисту	Практичне заняття 14 2 год	3 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Тема 8. Доповнена реальність та відеоспостереження. Знати: поняття доповненої реальності (AR) та її відмінність від VR і MR, основні компоненти AR-систем, принципи інтеграції відеоспостереження з AR-технологіями, способи візуалізації відеоаналітики в AR-середовищі, роль штучного інтелекту у поєднанні AR та відеонагляду, сфери застосування AR-відеоспостереження. Вміти: пояснювати принципи роботи AR у системах відеоспостереження, аналізувати сценарії використання AR для підвищення ефективності моніторингу, формувати концепцію AR-інтерфейсу для системи відеонагляду, оцінювати переваги та недоліки впровадження AR у реальних системах безпеки. Формування компетенцій: ЗКЗ, ЗК4, ЗК8, ЗК9, ЗК10, ЗК11, ПК1, ПК3, ПК9, ПК10, ПК17, ПК18 Програмні результати навчання: ПРН6, ПРН7, ПРН15, ПРН16, ПРН18 Рекомендовані джерела: 1–5			
Заняття 8.1. AR/VR-безпеки. Аналіз середовища в режимі реального час.	Лекція 8		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 8.2. Інтеграція доповненої реальності з системами відеоспостереження. Аналіз ефективності та етичних аспектів використання AR у відеоспостереженні.	Практичне заняття 15 2 год	3 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Заняття 8.3. Методологія розробки та верифікації систем доповненої реальності для підтримки прийняття рішень та професійної підготовки персоналу СВН (систем відеоспостереження)	Практичне заняття 16 2 год	3 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Тема 9. Розробка безпечних рішень для досягнення етапів. (Designing Secure Milestone Solutions). Сертифікація. Знати: поняття milestone-підходу у проектуванні систем безпеки, архітектуру Milestone XProtect, життєвий цикл інтелектуальної системи відеонагляду, принципи secure by design та privacy by design, основні загрози інформаційній та фізичній безпеці відеосистем, методологію Milestone Hardening Guide, міжнародні та галузеві підходи до стандартизації й сертифікації систем безпеки.			

<u>Вміти:</u> формувати вимоги до безпечних рішень на різних етапах проєкту, аналізувати ризики та вразливості інтелектуальних систем відеонагляду, проєктувати архітектуру відеосистем з урахуванням безпеки та конфіденційності, планувати етапи (milestones) впровадження системи безпеки. <u>Формування компетенцій:</u> ЗК3, ЗК4, ЗК8, ЗК9, ЗК10, ЗК11, ПК1, ПК3, ПК9, ПК10, ПК17, ПК18 <u>Програмні результати навчання:</u> ПРН6, ПРН7, ПРН15, ПРН16, ПРН18 <u>Рекомендовані джерела:</u> 1–5			
Заняття 9.1. Огляд архітектури системи XProtect VMS.	Лекція 9		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 9.2. Проектування малої та середньої системи управління відео XProtect.	Практичне заняття 17 2 год	3 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування.
Заняття 9.3. Проектування з використанням багатопотокової передачі. Проектування XProtect на рішеннях AWS.	Практичне заняття 18 2 год	5 бали	Виконання завдань на практичне застосування знань і вмінь, тестування та отримання сертифікату (при умові успішного складання тестів).
САМОСТІЙНА РОБОТА			
ТЕМА 6 Квантові та постквантові загрози для систем відеонагляду	4 год	1 бал	6. <u>Зробити:</u> проаналізувати можливі квантові загрози для сучасних відеосистем. <u>Розглянути:</u> уразливості класичних криптографічних алгоритмів, вплив квантових обчислень на захист відеопотоків і архівів. <u>Вивчити:</u> принципи постквантової криптографії, загальні підходи до квантово-стійкого захисту даних. <u>Дослідити:</u> сценарії переходу від класичних до постквантових методів захисту. <u>Виконати:</u> аналітичну записку, сформулювати рекомендації щодо захисту відеосистем
ТЕМА 7 Відеоспостереження у метавсесвіті та цифрових двійниках	4 год	1 бал	7. <u>Зробити:</u> проаналізувати концепцію метавсесвіту з точки зору безпеки. <u>Розглянути:</u> цифрові двійники об'єктів і територій, джерела візуальних даних у метавсесвіті. <u>Вивчити:</u> інтеграцію відеоспостереження з XR-технологіями, роль ШІ у віртуальних просторах. <u>Дослідити:</u> ризики конфіденційності та контролю доступу. <u>Виконати:</u> створити концептуальну схему відеоспостереження у метавсесвіті, підготувати короткий пояснювальний опис.
ТЕМА 8 Доповнена реальність як інтерфейс інтелектуального відеонагляду	4 год	1 бал	8. <u>Зробити:</u> можливості використання AR у відеоспостереженні. <u>Розглянути:</u> AR-візуалізацію подій і об'єктів, інтеграцію відеоаналітики з AR-інтерфейсами. <u>Вивчити:</u> базові принципи побудови AR-інтерфейсів,

			вимоги до апаратного та програмного забезпечення. <u>Дослідити:</u> вплив AR на швидкість і якість прийняття рішень оператором. <u>Виконати:</u> описати переваги та обмеження AR-інтерфейсу для системи відеонагляду.
ТЕМА 9 Проектування безпечної інтелектуальної системи відеонагляду	4 год	1 бал	9. <u>Зробити:</u> сформулювати концепцію ІСВ, обрати об'єкт для впровадження системи відеонагляду (навчальний заклад, підприємство, громадський простір, критична інфраструктура), визначити основні загрози безпеці, сформулювати загальну концепцію ІСВ. <u>Розглянути:</u> архітектуру системи відеонагляду, використання штучного інтелекту та відеоаналітики, інтеграцію з іншими системами безпеки. <u>Вивчити:</u> принципи secure by design та privacy by design, основні загрози інформаційній безпеці відеосистем, вимоги до захисту відеоданих і контролю доступу. <u>Дослідити:</u> потенційні вразливості системи на різних етапах життєвого циклу, вплив обраних технологій на рівень безпеки. <u>Виконати:</u> розробити структурну схему системи, сформулювати функціональні та безпекові вимоги, сформулювати підсумкові висновки.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Комп'ютерний клас для проведення практичних занять.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Обов'язкові для ознайомлення джерела:

1. Гонсалес Р., Вудс Р. Цифрова обробка зображень : пер. з англ. – Київ : Діалектика, 2019.
2. Субботін С. О. Інтелектуальні інформаційні системи : навчальний посібник. – Київ : КНТ, 2016.
3. Палагін О. В., Петренко А. І. Основи штучного інтелекту : підручник. – Київ : Академперіодика, 2018.
4. Коваленко І. І., Литвиненко В. І. Комп'ютерний зір та обробка зображень : навчальний посібник. – Харків : ХНУРЕ, 2020.
5. Білоус О. М. Методи та алгоритми цифрової обробки зображень : навчальний посібник. – Львів : НУ «Львівська політехніка», 2017.

Додаткові для ознайомлення джерела:

1. Офіційна документація OpenCV (українські та англійські матеріали спільноти)
<https://docs.opencv.org>
2. PyTorch Tutorials – приклади реалізації моделей комп'ютерного зору
<https://pytorch.org/tutorials>
3. TensorFlow Vision – бібліотека моделей для аналізу зображень і відео
<https://www.tensorflow.org/vision>
4. Papers with Code – сучасні алгоритми та відкриті реалізації з комп'ютерного зору
<https://paperswithcode.com>
5. Deep Learning for Computer Vision – навчальні матеріали та приклади проєктів
<https://cs231n.stanford.edu>
6. Open Data Portal України – відкриті набори даних для аналізу та навчання моделей

<https://data.gov.ua>

7. IEEE Xplore Digital Library – наукові статті з інтелектуальних систем і відеонагляду

<https://ieeexplore.ieee.org>

8. Zhang Z. Computer Vision and Image Processing: A Practical Approach. – Springer, 2020

9. Gonzalez R. C., Woods R. E. Digital Image Processing. – 4th ed. – Pearson, 2018.

10. Szeliski R. Computer Vision: Algorithms and Applications. – 2nd ed. – Springer, 2022.

11. https://learn.milestonesys.com/home_elearning.htm?tocpath=eLearning%20Courses%7C 0 - навчальні матеріали від Milestone.

11. Електронна бібліотека ДУІКТ.

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації студент повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за завдання 0 балів.
- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.

За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни студент видаляється з заняття, за заняття отримує 0 балів.

КРИТЕРІЙ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є виконання всіх практичних робіт і виконання самостійних завдань, які передбачені структурою освітньої компоненти Дослідження операцій.

Якщо студента не допущено до складання заліку, як такого, що не виконав індивідуальний план, йому надається час до перескладання для виконання всіх вимог допуску. Студент має право на два перескладання. При повторному перескладанні екзамену його у студента може приймати комісія, яка створюється директором ННІТ. Оцінка комісії є остаточною. У випадку отримання студентом 0 балів (неприйнятно), що тягне відрахування за невиконання навчального плану.

Оцінювання студентів здійснюється за накопичувальною 100-бальною системою і складається із двох основних оцінкових блоків і розподіляється в певних пропорціях 60 (бали напрацьовані під час вивчення дисципліни – Поточний контроль), 40 (підсумкове оцінювання - Екзамен)

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	• Виконання практичних робіт	52 бали
	• Самостійна робота	8 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ <i>Екзамен</i>	Екзамен проходить у письмовій формі.	40 балів

Додаткова оцінка

Види навчальної роботи	Оцінювання
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
- Тези доповіді на фаховій конференції	3 бали
- Стаття у фаховому виданні	5 балів
- Стаття в іноземному рецензованому виданні	10 балів

Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти - 10 балів.

Форми контролю	Екзамен проходить у письмовій формі.	40 балів	
ПОТОЧНИЙ КОНТРОЛЬ	●Екзамен проходить у письмовій формі.	40 балів	
	●Оцінювання		
ПІДСУМКОВЕ ОЦІНЮВАННЯ <i>Екзамен</i>			
Додаткова оцінка			
Види навчальної роботи		Оцінювання	
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:			
- Тези доповіді на фаховій конференції		3 бали	
- Стаття у фаховому виданні		5 балів	
- Стаття в іноземному рецензованому виданні		10 балів	
Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти - 10 балів.			
ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ			
бали	Критерії оцінювання	Рівень компетентності	Оцінка /запис в екзаменаційній відомості
90-100	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або студент проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	Високий Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін, а також знання, набуті при самостійному поглибленому вивченні питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82-89	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	Достатній Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивченні дисципліни	Добре / Зараховано (В)
75-81	Студент в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає	Достатній	Добре / Зараховано (С)

	робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	
64-74	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядалися з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	Середній Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, студент з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	Середній Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	Низький Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) <i>В залікову книжку не представляється</i>
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі екзамену/заліку.	Незадовільний Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) <i>В залікову книжку не представляється</i>

