

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем



Підтверджую

Тетяна ГОВОРУЩЕНКО
2024 р.

Навчальна дисципліна Обробка інформації та мультимедійні системи

Освітньо-професійна програма Комп'ютерна інженерія та програмування

Рівень вищої освіти перший (бакалаврський)

Загальна інформація

Позиція	Зміст інформації
Викладач(і)	Корецька Людмила Олександрівна
Профайл викладача	http://kiis.khmnu.edu.ua/personnel/koreczka-kovtun-lyudmyla-oleksandrivna/
E-mail викладача(ів)	koretskal@khmnu.edu
Контактний телефон	заповнюється за домовленістю
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=6764
Навчальний рік	2024-2025
Консультації	Очні: среда, 5-а пара, 1-114 онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Статус дисципліни	Форма навчання	Курс	Семестр	Загальне навантаження		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
				Кредити ЄКТС	Години	Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, в т.ч. ІРС			Залік	Іспит
						Разом	Лекції	Лабораторні роботи	Практичні заняття						
О	Д	3	5	5	150	68	17	17	34		82	-	-		+

Анотація дисципліни

Дисципліна "Обробка інформації та мультимедійні системи" відноситься до циклу дисциплін професійної підготовки, викладається для здобувачів першого (бакалаврського) рівня вищої освіти очної денної форми навчання спеціальності «Комп'ютерна інженерія» за освітньо-професійною програмою «Комп'ютерна інженерія та програмування».

Пререквізити: вища математика; дискретна математика; теорія ймовірності та математична статистика; інформаційні технології.

Кореквізити: комп'ютерні мережі, системне адміністрування та кібербезпека

Мета і завдання дисципліни

Мета викладання дисципліни. Метою дисципліни "Обробка інформації та мультимедійні системи" є: 1) надання основ прикладної теорії інформації та кодування для розуміння питань побудови, функціонування та експлуатації комп'ютерних систем та мереж, а також різних систем обробки інформації та керування на їх основі; 2) вивчення основних методів оптимального та завадостійкого кодування, які широко використовуються в сучасних комп'ютерних системах та мережах; 3) надати фундаментальні знання з основ криптографічного захисту та шифрування інформації; 4) оволодіння студентами алгоритмами створення сучасних мультимедійних продуктів; сучасними методами та технологіями; комп'ютерними програмними, технічними засобами у сфері мультимедіа: графічних, текстових, звукових та відео-редакторів і т. п. та набуття практичних навичок, необхідних для розробки мультимедіа проектів.

Завдання дисципліни. Надати студентам знання і практичні навички з основ побудови оптимальних та завадостійких методів кодування інформації, оволодіння методами криптографічного захисту та шифрування інформації у комп'ютерних системах та мережах, опанування основними технологіями та засобами розробки мультимедійних систем.

Очікувані результати навчання.

Студент, який успішно завершив вивчення дисципліни, повинен: обґрунтовувати вибір способів збору, зберігання, передачі та захисту інформації в програмних і технічних засобах комп'ютерних систем та мереж, в тому числі й у мультимедійних системах; адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та технології комп'ютерної інженерії із забезпеченням захисту інформації; забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки; використовувати організаційні, технічні, алгоритмічні та інші методи і засоби захисту інформації.

Компетентності, на формування яких спрямовано ОК:

Інтегральна. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми під час професійної діяльності в комп'ютерній галузі або навчання, що передбачає застосування теорій та методів комп'ютерної інженерії і характеризується комплексністю та невизначеністю умов.

ЗК3. Здатність застосовувати знання у практичних ситуаціях

ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово

ЗК11. Здатність до розуміння предметної галузі та професійної діяльності

ЗК13. Здатність розв'язувати поставлені задачі та приймати відповідні рішення

ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії.

ФК4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки

ФК10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

ФК19. Здатність організувати збір та зберігання даних у базах та сховищах даних, передачу та захист інформації в програмних і технічних засобах комп'ютерних систем та мереж, в тому числі й у мультимедійних системах

Програмні результати навчання, на забезпечення яких спрямовано ОК:

ПРН3. Знати новітні технології в галузі комп'ютерної інженерії.

ПРН6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

ПРН11. Вміти здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії.

ПРН15. Вміти виконувати експериментальні дослідження за професійною тематикою.

ПРН17. Спілкуватись усно та письмово з професійних питань українською мовою та однією з іноземних мов (англійською, німецькою, італійською, французькою, іспанською).

ПРН18. Використовувати інформаційні технології для ефективного спілкування на професійному та соціальному рівнях.

ПРН19. Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.

ПРН20. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

ПРН21. Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.

ПРН24. Обґрунтовувати вибір способів збору, зберігання, передачі та захисту інформації в програмних і технічних засобах комп'ютерних систем та мереж, в тому числі й у мультимедійних системах.

ПРН25. Адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та технології комп'ютерної інженерії із забезпеченням захисту інформації в комп'ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема лабораторно ї роботи	Тема практичної роботи	Самостійна робота студентів		
				Зміст	Год.	Література
1	Основні положення теорії інформації. Вимірювання інформації		Ентропія. Об'єм інформації	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №1 та підготовка до виконання практичної роботи №1.	4	[1 - 6, 10]
2		Кількісна оцінка інформації в системах з рівномірним та нерівномірним розподілом ймовірностей появи у тексті		Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №1, підготовка до виконання практичної роботи №1 (продовження).	4	[1 - 6, 10]
3	Оптимальне кодування. Методи оптимального стиску Хаффмана та Шенона-Фано		Методи оптимального стиску. Метод Хаффмана	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №2, захисту практичної роботи №1 та до виконання практичної роботи №2.	4	[1 - 6, 10]
4		Словникові методи стиску інформації (I група методів - з ковзним вікном)		Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №2, підготовка до виконання практичної роботи №2 (продовження).	4	[1 - 6, 10]
5	Кодування для каналу зв'язку із завадами.		Методи оптимального стиску. Метод Шенона-Фано	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №3, захисту практичної роботи №2 та до виконання практичної роботи №3.	4	[1 - 6, 10]
6		Словникові методи стиску (II група - методи з доповненням словника)		Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №3, підготовка до виконання практичної роботи №3 (продовження).	4	[1 - 6, 10]
7	Основи безпеки інформації. Методи і засоби захисту інформації в комп'ютерних системах.		Арифметика Галуа у задачах завадостійкого кодування	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №4, захисту практичної роботи №3 та до виконання практичної роботи №4.	4	[6, 7]

8		Завадостійке кодування. Метод Хеммінга		Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №4, підготовка до виконання практичної роботи №4 (продовження).	4	[6, 7]
9	Симетричні криптосистеми . Види симетричних шифрів		Основи шифрування. Криптоаналіз шифрів перестановки. Шифри трафарети	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №5, захисту практичної роботи №4 та до виконання практичної роботи №5.	4	[6, 7]
10		Відновлення частини пошкоджених файлів із використанням кодів Ріда-Соломона		Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №5, підготовка до виконання практичної роботи №5 (продовження).	4	[6, 7]
11	Асиметричні криптосистеми . Цифровий підпис. Технологія блокчейн		Потокові шифри. Адитивне шифрування	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №6, захисту практичної роботи №5 та до виконання практичної роботи №6.	4	[6, 7]
12		Обробка звукових даних		Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №6, підготовка до виконання практичної роботи №6 (продовження).	4	[6, 7]
13	Засоби мультимедійних технологій. Апаратні та програмні складові мультимедіа-систем		Шифри заміни. Криптоаналіз шифру Цезаря. Поліграмні шифри. Шифр Playfair	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №7, захисту практичної роботи №6 та до виконання практичної контрольної роботи.	9	[8, 9]
14		Обробка графічних даних		Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №7, підготовка до виконання практичної роботи №7 (продовження).	4	[8, 9]
15	Обробка звукової, графічної та відео інформації. Мультимедійні проекти		Асиметрична криптосистема RSA. Цифровий підпис	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №8, захисту практичної роботи №7 та до виконання практичної роботи №8	4	[8, 9]
16		Створення мультимедійного проекту		Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №8, підготовка до	8	[8, 9]

				виконання практичної роботи №8 (продовження). Підготовка до підсумкового тестового контролю		
17				Опрацювання лекційного матеріалу. Підготовка до захисту практичної роботи №8. Підготовка до підсумкового контрольного заходу	9	[8, 9]

Примітка: *Лекції, практичні заняття проводяться по дві години; послідовність проведення занять визначається розкладом (може не відповідати нумерованим тижням)

Політика дисципліни.

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції, практичні та лабораторні заняття згідно з розкладом, не запізнюватися на заняття, завдання виконувати відповідно до графіка. Пропущене практичне та лабораторне заняття студент зобов'язаний опрацювати самостійно у повному обсязі і відвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. До практичних та лабораторних занять студент має підготуватися за відповідною темою і проявляти активність. Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання у ХНУ.

Критерії оцінювання результатів навчання.

Кожний вид роботи з дисципліни оцінюється за **чотирибальною** шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з врахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих її видів робіт. При оцінюванні знань студентів використовуються різні засоби контролю, зокрема: усне опитування перед допуском до виконання лабораторної та практичної робіт – здійснюється на їх початку; засвоєння теоретичного матеріалу з тем перевіряється тестовим контролем; якість виконання, набуття теоретичних знань і практичних навичок перевіряється шляхом захисту кожної лабораторної та практичної роботи та індивідуального завдання згідно з робочою програмою дисципліни і робочим навчальним планом.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів денної форми навчання у семестрі за ваговими коефіцієнтами

Аудиторна робота		Самостійна, індивідуальна робота		Семестровий контроль (іспит)
Лабораторні роботи №: 1-8	Практичні роботи №: 1-8	Контрольні заходи:		Підсумковий контрольний захід
		КР	ТК	
ВК: 0,15	ВК: 0,1	ВК: 0,25	ВК: 0,1	ВК: 0,4

Умовні позначення: ВК – ваговий коефіцієнт.

Оцінювання тестових завдань. Тематичний тест для кожного студента складається з двадцяти п'яти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 25. На тестування відводиться 30 хвилин. Тестування проводиться з використанням модульного середовища для навчання MOODLE.

Оцінювання здійснюється за чотирибальною шкалою.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту, представлена у нижченаведеній таблиці.

Сума балів за тестові завдання	1–13	14–16	17–22	23–25
Оцінка за 4-бальною шкалою	2	3	4	5

Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	Інституційна інтервальна шкала балів	Вітчизняна оцінка, критерії	
A	4,75–5,00	5	Відмінно – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4	Добре – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4	Добре – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3	Задовільно – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3	Задовільно – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	Незадовільно – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2	Незадовільно – необхідна серйозна подальша робота і повторне вивчення дисципліни

Питання для підсумкового контролю з дисципліни

- Відповідність мір інформації напрямкам теорії інформації. Структурні міри інформації.
- Геометрична міра інформації.
- Комбінаторна міра інформації.
- Поняття та основні задачі теорії кодування, методи вирішення основних задач. Рівномірні та нерівномірні коди
- Оптимальне кодування: визначення; властивості; принципи.
- Адитивна міра Хартлі.
- Кількісна оцінка інформації.
- Дискретизація і квантування сигналів.
- Оптимальне кодування Хаффмена.
- Завадостійке кодування: основні поняття та загальні принципи побудови завадостійких кодів.
- Коди Хеммінга.
- Класифікація повідомлень за вміщеною інформацією.
- Поняття кодової відстані. Перевіряючі та корегуючі характеристики коду.
- Узагальнена структура інформаційної системи.
- Теорема Шеннона для дискретного каналу за умови наявності перешкод.
- Надлишковість інформації. Семантична та статистична надлишковість.
- Пропускна здатність дискретного каналу зв'язку за умови наявності перешкод.
- Циклічні коди. Загальні поняття та визначення.
- Основні параметри сигналів. Умова узгодження сигналів з каналом зв'язку.
- Оптимальні нерівномірні коди. Терма Шеннона.
- Пропускна здатність дискретного каналу за умови відсутності перешкод.
- Паритетне кодування. Паритетне кодування блоків даних.
- Канал для передачі дискретних повідомлень за умови наявності перешкод. Особливості впливу перешкод на передачу повідомлень.
- Використання циклічних кодів для виявлення та корегування помилок.
- Основні принципи побудови циклічних кодів.
- Ентропія та надлишковість. Поняття недовантаженості та надлишковості.
- Формування циклічних кодів методом множення поліномів.
- Загальні принципи використання надлишковості при побудові корегуючих кодів.
- Методи автоматичного виявлення помилок.
- Поняття кодової відстані. Зв'язок перевіряючих та корегуючих характеристик коду з кодовою відстанню.
- Формування циклічних кодів методом ділення поліномів.
- Стиснення інформації. Словникові методи Лемпела-Зіва.
- Основи безпеки інформації.
- Методи і засоби захисту інформації в комп'ютерних системах.
- Криптографічні методи захисту інформації.
- Технічні методи і засоби захисту інформації. Програмні методи і засоби захисту.

37. Симетричні криптосистеми – проста перестановка, одиночна перестановка по ключу, подвійна перестановка, перестановка «магічний квадрат».
38. Види симетричних шифрів.
39. Симетричні криптосистеми DES, AES. Блочні шифри.
40. Симетрична система DES. Перетворення Мережею Фейстеля.
41. Схема шифрування алгоритму DES.
42. Симетрична система AES.
43. Асиметричні криптосистеми.
44. Порівняння симетричних та асиметричних криптосистем: переваги, недоліки.
45. Основні принципи побудови криптосистем з відкритим ключем.
46. Криптографія з декількома відкритими ключами.
47. Криптографічний протокол Діффі-Хелмана.
48. Алгоритм Діффі-Хелмана з трьома і більше учасниками.
49. Криптографічний алгоритм RSA. Алгоритм створення відкритого і секретного ключів.
50. Цифровий підпис.
51. Атаки на алгоритм RSA.
52. Технологія блокчейн. Реалізація в системі біткойнів.
53. Блок транзакцій. Ланцюжок блоків. Підтвердження транзакцій. «Подвійне витрачання».
54. Застосування поза сферою криптовалют: банківський сектор, інвестиції і біржі, земельний реєстр, посвідчення особи, платіжний засіб.
55. Класифікація мультимедіа-систем.
56. Засоби мультимедійних технологій.
57. Системи мультимедіа, їх класифікація.
58. Апаратні та програмні складові мультимедіа-систем.
59. Обробка текстової та графічної інформації.
60. Обробка зображень. Формати кодування зображень.
61. Технології звукового моделювання. Оцифрування аналогового сигналу.
62. Формати звукових файлів.
63. MIDI і цифровий звук: переваги й недоліки.
64. Види модуляції при роботі з аудіоінформацією.
65. Види й формати кодування даних. Втрати інформації при кодуванні.
66. Відновлення аудіоінформації. Цифро-аналогове перетворення.
67. Формати аудіостиснення. Переваги й недоліки цифрового звуку.
68. Загальні положення синтезу звуку.
69. Аналогова та цифрова відеоінформація.
70. Формати збереження відеоінформації. Технології відеомодельювання.
71. Особливості створення мультимедійних проектів.
72. Особливості використання текстових, графічних, аудіо- та відеоінформації у мультимедійних проектах.

Методичне забезпечення

Навчальний процес з дисципліни забезпечений необхідними навчально-методичними розробками в модульному середовищі.

Рекомендована література

1. Корецька Л. О. Теорія інформації, кодування та шифрування : навчальний посібник. Хмельницький : Символ, 2021. 208 с.
2. Лабораторний практикум з навчальної дисципліни “Теорія інформації та кодування” : навчальний посібник / Г. І. Гайдур та ін. Київ: ДУТ : ННІЗІ, 2021. 50 с.
3. Основи інформаційних технологій : навчальний посібник / А. М. Гуржій та ін. Київ : Літера ЛТД, 2023. 288 с.
4. Теорія інформації та обробка сигналів (конспект лекцій) [Електронний ресурс] : навчальний посібник / уклад.: Ю. С. Ямненко, К. С. Клен. Київ : КПІ ім. Ігоря Сікорського, 2019. 120 с.
5. Теорія передавання інформації : конспект лекцій / уклад. В. А. Литвиненко. Кам’янське : ДДТУ, 2024. 77 с.
6. Остапов С., Євсєєв С., Мілов О. Кібербезпека: основи кодування та криптографії. Київ : Новий світ-2000, 2024. 658 с.
7. Інтерактивні медіа технології (комп’ютерний практикум) [Електронний ресурс] : навчальний посібник / уклад.: К. І. Золотухіна, О. Л. Благодір. Київ : КПІ ім. Ігоря Сікорського, 2020. 39 с.
8. Основи теорії інформації та кодування : навчальний посібник / І. А. Прокопишин та ін. Львів : ЛНУ ім. Ів. Франка, 2023. 156 с.

9. Основи кіберпростору, кібербезпеки та кіберзахисту : навчальний посібник / В. М. Богуш та ін. ; ред. В. М. Богуша. Київ : Ліра-К, 2020. 554 с.

10. Основи теорії інформації та кодування. Конспект лекцій: [Електронний ресурс] : навчальний посібник / уклад.: М. І. Романюк, Ю. Г. Савченко. Київ : КПІ ім. Ігоря Сікорського, 2019. 70 с.

11. Остапов С. Е., Євсєєв С. П., Король О. Кібербезпека : сучасні технології захисту : навчальний посібник. Львів : Новий Світ- 2000, 2020. 678 с.

Розробник:

канд. техн. наук, доц. Людмила КОРЕЦЬКА

Погоджено:

Зав. каф. КПС

канд. техн. наук, доц. Ірина ЗАСОРНОВА

Гарант ОПШ «КІП»

д-р техн. наук, проф. Сергій ЛИСЕНКО