

Міністерство освіти і науки України
Хмельницький національний університет

ЗАТВЕРДЖУЮ
Декан ФІТ  Савенко О.С.
2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ


Обробка інформації та мультимедійні системи

Назва

Галузь знань 12 – Інформаційні технології
Спеціальність 123 – Комп'ютерна інженерія очна денна форма здобуття освіти
Освітня програма Комп'ютерна інженерія та програмування
Статус дисципліни обов'язкова, дисципліна професійної підготовки
Факультет інформаційних технологій
Кафедра Комп'ютерної інженерії та інформаційних систем

Форма здобуття освіти	Курс	Семестр	Загальне навантаження		Кількість годин						Курсовий проєкт	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						
ОД	3	5	5	150	68	17	17	34		82				+
Разом			5	150	68	17	17	34		82				1


Робоча програма складена на основі стандарту вищої освіти зі спеціальності 123 Комп'ютерна інженерія, освітньо-професійної програми та навчального плану

Програма складена  Корецькою Л.О.
Прізвище, ініціали викладача(ів)

Схвалена на засіданні кафедри Комп'ютерної інженерії та інформаційних систем

Протокол № 1 від 12.08.2022 р.

Зав. кафедри комп'ютерної інженерії та інформаційних систем

 Говорухенко Т.О.
Підпис Прізвище, ініціали

Робоча програма розглянута та схвалена Вченою радою факультету інформаційних технологій

Голова Вченої ради  Савенко О.С.
Підпис Прізвище, ініціали

Хмельницький 2022

ВСТУП

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.

Предмет дисципліни. Методи побудови оптимальних та завадостійких кодів, системи криптографічного захисту інформації, технології та алгоритми створення сучасних мультимедійних продуктів.

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.

Після вивчення дисципліни "Обробка інформації та мультимедійні системи" студент має досягти таких результатів навчання (сукупність знань, умінь, навичок, компетентностей):

знати:

- об'єкт дисципліни, предмет дисципліни, задачі дисципліни, проблематику дисципліни та її основні розділи;

- наукові і математичні положення, що лежать в основі функціонування інформаційних систем, комп'ютерних засобів; базові знання технічних характеристик, конструктивних особливостей, застосування і правил експлуатації комп'ютерних систем, мереж та програмно-технічних засобів;

- новітні інформаційні технології у галузі інформаційних технологій;

уміти:

- застосовувати знання для ідентифікації, формулювання і розв'язування задач визначення втрат інформації, завадостійкого кодування інформації у комп'ютерних системах і мережах та каналах зв'язку, криптографії та шифрування даних, формати даних; застосовувати знання з теорії інформації та кодування для розв'язування задач аналізу та синтезу засобів в комп'ютерних системах і мережах; оцінювати отримані результати та аргументовано захищати прийняті рішення;

- здійснювати пошук інформації в різних джерелах для розв'язання задач обробки інформації, її кодування та шифрування у комп'ютерних системах та мережах;

- застосовувати обробку інформації та відомі методи стиску, завадостійкого кодування та шифрування для її достовірної передачі, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань побудови комп'ютерних систем та мереж без втрат інформації;

- використовувати сучасні інформаційні технології для ефективного спілкування на професійному та соціальному рівнях із використанням сучасних мультимедійних систем;

бути здатним:

- використовувати та впроваджувати нові інформаційні технології із застосуванням отриманих знань з обробки інформації та мультимедійних систем, проводити дослідницьку та/або інноваційну діяльність у галузі інформаційних технологій;

- проводити управління та забезпечення якістю продуктів і сервісів інформаційних технологій протягом їх життєвого циклу;

- досліджувати проблему обробки, зберігання та передачі інформації у комп'ютерних системах та мережах.

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 організовувати 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

ОБРОБКА ІНФОРМАЦІЇ ТА МУЛЬТИМЕДІЙНІ СИСТЕМИ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Перший (бакалаврський)
Мова викладання	Українська
Семестр	5
Кількість встановлених кредитів ЄКТС	5
Форми здобуття вищої освіти	Денна очна

Результати навчання. Студент, який успішно завершив вивчення дисципліни, повинен: знати новітні технології в галузі комп'ютерної інженерії; вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей; вміти здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії; вміти виконувати експериментальні дослідження за професійною тематикою; спілкуватись усно та письмово з професійних питань українською мовою та однією з іноземних мов (англійською, німецькою, італійською, французькою, іспанською); використовувати інформаційні технології для ефективного спілкування на професійному та соціальному рівнях; здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення; усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення; якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики; 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 в комп'ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки

Зміст навчальної дисципліни. Основні поняття та визначення теорії інформації. Кодування як процес відображення інформації в цифровому вигляді. Особливості ефективного кодування. Оптимальне кодування. Код Шеннона-Фано. Код Хаффмена. Завадостійке кодування. Теорема Шеннона для дискретного каналу із шумом. Зв'язок коригувальної здатності коду з кодовою відстанню. Завадостійкі коди для виявлення помилок. Коди для корегування помилок. Паритетні коди. Коди Хеммінга. Циклічні коди. Симетричні та асиметричні криптосистеми. Криптосистеми DES, AES, RSA, Діффі-Хелмана. Загальні уявлення про мультимедіа. Текст, графіка, звук та відео в мультимедіа. Обробка текстової, звукової, графічної, відео інформації в мультимедіа.

Запланована навчальна діяльність: лекції – 17 год., лабораторні заняття – 17 год., практичні заняття – 34 год., самостійна робота – 82 год.; разом – 150 год.

Методи навчання: інтерактивні, пояснювально-ілюстративні, репродуктивні, продуктивні, практичні, частково-пошукові.

Форми оцінювання результатів навчання: усне опитування, захист лабораторних та практичних робіт, тестовий контроль, підсумковий контрольний захід

Форма семестрового контролю: іспит

Навчальні ресурси:

1. Корецька Л. Теорія інформації, кодування та шифрування : навчальний посібник / Л.О. Корецька. – Хмельницький: Символ, 2021. – 208 с.
2. Беркман Л.Н.. Кодування джерел інформації та каналів зв'язку : навч. посібник / Л.Н. Беркман, А.П. Бондарчук, Г.І. Гайдур, Н.С. Чумак. – Київ: ННІТІ ДУТ, 2018. – 91с.
3. Дробик О.В. Цифрова обробка аудіо- та відеоінформації у мультимедійних системах: Навчальний посібник / О.В. Дробик, В.В. Кідалов, В.В. Коваль, Б.Я. Костік, В.С. Лазебний, Г.М. Розорінов, Г.О. Сукач. – К.: Наукова думка, 2016. – 144 с.
4. Дробик О.В. Цифрова обробка аудіо- та відеоінформації у мультимедійних системах: Навчальний посібник / О.В. Дробик, В.В. Кідалов, В.В. Коваль, Б.Я. Костік, В.С. Лазебний, Г.М. Розорінов, Г.О. Сукач. – К.: Наукова думка, 2016. – 144 с.
5. Модульне середовище для навчання MOODLE. Доступ до ресурсу: <https://msn.khnu.km.ua>.
6. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php/f/page_lib.php.

Викладач: кандидат технічних наук, доцент Корецька Л.О.

1 СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин, відведених на:			
	лекції	лабораторні роботи	практичні роботи	самостійну роботу
<i>Тема 1.</i> Математичні основи теорії інформації	2	2	4	8
<i>Тема 2.</i> Оптимальне кодування та стиск інформації	2	4	8	8
<i>Тема 3.</i> Завадостійке кодування	2	4	4	8
<i>Тема 4.</i> Криптографія та шифрування даних	6		18	24
<i>Тема 5.</i> Апаратні та програмні компоненти мультимедіа-технологій. Класифікація мультимедіа-систем	6	8		34
<i>Разом за семестр:</i>	16/18	16/18	34	82

2 ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1 Зміст лекційного курсу

№ лекції	Перелік тем лекцій, їх анотації	Кільк. годин
	<i>П'ятий семестр</i>	
Тема 1. Математичні основи теорії інформації		
1	<p>Основні положення теорії інформації. Вимірювання інформації</p> <p>Предмет теорії інформації. Основні поняття, визначення і задачі теорії інформації. Вимірювання інформації. Міра Хартлі. Структурні міри інформації. Класифікація і характеристики кодів. Дві групи кодів: безнадмірні (некоректувальні, первинні, прості) та надмірні (завадостійкі). Рівномірні та нерівномірні коди. Подільні та неподільні, систематичні та несистематичні коди. Способи подання кодів: табличний, у вигляді кодового дерева, зображення комбінацій коду точками дискретного n-вимірного векторного простору, матричний спосіб. Надмірність повідомлень і кодів.</p> <p>Літ.: [1 - 6]</p>	2
Тема 2. Оптимальне кодування та стиск інформації		
2	<p>Оптимальне кодування. Методи оптимального стиску Хаффмана та Шеннона-Фано</p> <p>Метод Шеннона-Фано, алгоритм і побудова таблиці. Метод Хаффмана. Кодове дерево для побудови ОНК. Особливості використання методів оптимального кодування. Передача кодового дерева. Порівняння алгоритмів Хаффмана та Шеннона-Фано.</p> <p>Стиск інформації. Словникові алгоритми Лемпела-Зіва. Арифметичне кодування. Особливості програм-архіваторів. Відмінності статичної і динамічної моделей стиску. Стиск інформації з втратами.</p> <p>Літ.: [1 – 6, 11]</p>	2
Тема 3. Завадостійке кодування		
3	<p>Кодування для каналу зв'язку із завадами.</p> <p>Друга теорема Шеннона. Двійкові коди, що виявляють помилки. Код із перевіркою на парність. Код із перевіркою на непарність. Код із простим повторенням. Інверсний код. Кореляційний код. Код зі сталою вагою. Код із кількістю одиниць у комбінації, кратною трьом.</p> <p>Коди, що виправляють помилки. Двійкові групові коди. Методи виправлення помилок у систематичному груповому коді. Коди Хеммінга. Формування перевірних елементів, співвідношення коректувальних та інформаційних розрядів. Перевірна матриця і система перевірних рівнянь коду Хеммінга. Розширений код Хеммінга.</p> <p>Літ.: [1 - 6, 8, 11]</p>	2
Тема 4. Криптографія та шифрування даних		
4	<p>Основи безпеки інформації. Методи і засоби захисту інформації в комп'ютерних системах.</p> <p>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.</p> <p>Літ.: [9, 10]</p>	2
5	<p>Симетричні криптосистеми. Види симетричних шифрів</p> <p>Симетричні криптосистеми – основні положення: проста перестановка, одиночна перестановка по ключу, подвійна перестановка, перестановка «магічний квадрат». Загальна схема. Параметри алгоритмів. Види симетричних шифрів.</p> <p>Літ.: [9, 10]</p>	2

6	<p>Асиметричні криптосистеми. Цифровий підпис. Технологія блокчейн</p> <p>Асиметричні криптосистеми. Порівняння симетричних та асиметричних криптосистем: переваги, недоліки. Види асиметричних шифрів. Ідея криптосистеми з відкритим ключем. Схема шифрування з відкритим ключем. Основні принципи побудови криптосистем з відкритим ключем. Криптографія з декількома відкритими ключами. Криптоаналіз алгоритмів з відкритим ключем. Застосування, переваги та недоліки. Криптографічний протокол Діффі-Хелмана. Опис алгоритму. Алгоритм Діффі-Хеллмана з трьома і більше учасниками. Шифрування з відкритим ключем. Отримання ключа без передачі ключа. Криптографічна стійкість.</p> <p>Криптографічний алгоритм RSA. Алгоритм створення відкритого і секретного ключів. Шифрування і розшифрування. Алгоритм шифрування сеансового ключа. Цифровий підпис. Швидкість роботи алгоритму RSA. Криптоаналіз RSA. Атаки на алгоритм RSA.</p> <p>Технологія блокчейн. Реалізація в системі біткойнів. Блок транзакцій. Ланцюжок блоків. Підтвердження транзакцій. «Подвійне витрачання». Застосування поза сферою криптовалют: банківський сектор, інвестиції і біржі, земельний реєстр, посвідчення особи, платіжний засіб</p> <p>Літ.: [9, 10]</p>	2
Тема 5. Мультимедійні системи		
7	<p>Засоби мультимедійних технологій. Апаратні та програмні складові мультимедіа-систем</p> <p>Класифікація мультимедіа-систем. Засоби мультимедійних технологій. Системи мультимедіа, їх класифікація. Апаратні та програмні складові мультимедіа-систем.</p> <p>Обробка текстової та графічної інформації. Обробка зображень. Формати кодування зображень.</p> <p>Літ.: [12 - 15]</p>	2
8	<p>Обробка звукової, графічної та відео інформації.</p> <p>Технології звукового моделювання. Оцифрування аналогового сигналу. Формати звукових файлів. MIDI і цифровий звук: переваги й недоліки. Види модуляції при роботі з аудіоінформацією. Види й формати кодування даних. Втрати інформації при кодуванні. Відновлення аудіоінформації. Цифро-аналогове перетворення. Формати аудіостиснення. Переваги й недоліки цифрового звуку. Загальні положення синтезу звуку.</p> <p>Літ.: [12 - 15]</p>	2
9	<p>Мультимедійні проєкти.</p> <p>Аналогова та цифрова відеоінформація. Формати збереження відеоінформації. Технології відеомоделювання.</p> <p>Особливості створення мультимедійних проєктів. Особливості використання текстових, графічних, аудіо- та відеоінформації у мультимедійних проєктах</p> <p>Літ.: [12 - 15]</p>	2
Загалом:		16/18

2.2 Зміст лабораторних занять

№ п/п	Тема лабораторного заняття	Кількість годин
1	Кількісна оцінка інформації в системах з рівномірним та нерівномірним розподілом ймовірностей появи у тексті	2
2	Словникові методи стиску інформації (I група методів - з ковзним вікном)	2
3	Словникові методи стиску (II група - методи з доповненням словника)	2
4	Завадостійке кодування. Метод Хеммінга	2
5	Відновлення частини пошкоджених файлів із використанням кодів Ріда-Соломона	2
6	Обробка звукових даних	2
7	Обробка графічних даних	2
8	Створення мультимедійного проекту	2
9	Підсумкове заняття	2
Загалом:		16/18

2.3 Зміст практичних занять

№ п/п	Тема практичного заняття	Кількість годин
1	Ентропія. Об'єм інформації	4
2	Методи оптимального стиску. Метод Хафмана	4
3	Методи оптимального стиску. Метод Шенона-Фано	4
4	Арифметика Галуа у задачах завадостійкого кодування	4
5	Основи шифрування. Криптоаналіз шифрів перестановки. Шифри графарети	4
6	Потокові шифри. Адитивне шифрування	4
7	Шифри заміни. Криптоаналіз шифру Цезаря. Поліграмні шифри. Шифр Playfair	4
8	Асиметрична криптосистема RSA. Цифровий підпис	6
Загалом:		34

2.4 Зміст самостійної (індивідуальної) роботи

Номер тижня	Вид самостійної роботи	К-ть годин
1	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №1 та підготовка до виконання практичної роботи №1.	4
2	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №1, підготовка до виконання практичної роботи №1 (продовження).	4
3	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №2, захисту практичної роботи №1 та до виконання практичної роботи №2.	4
4	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №2, підготовка до виконання практичної роботи №2 (продовження).	4
5	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №3, захисту практичної роботи №2 та до виконання практичної роботи №3.	4
6	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №3, підготовка до виконання практичної роботи №3 (продовження).	4
7	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №4, захисту практичної роботи №3 та до виконання практичної роботи №4.	4
8	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №4, підготовка до виконання практичної роботи №4 (продовження).	4
9	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №5, захисту практичної роботи №4 та до виконання практичної роботи №5.	4
10	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №5, підготовка до виконання практичної роботи №5 (продовження).	4
11	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №6, захисту практичної роботи №5 та до виконання практичної роботи №6.	4
12	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №6, підготовка до виконання практичної роботи №6 (продовження).	4
13	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №7, захисту практичної роботи №6 та до виконання практичної роботи №7. Підготовка до контрольної роботи.	9
14	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №7, підготовка до виконання практичної роботи №7 (продовження).	4
15	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №8, захисту практичної роботи №7 та до виконання практичної роботи №8	4
16	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №8, підготовка до виконання практичної роботи №8 (продовження). Підготовка до підсумкового тестового контролю	8
17	Опрацювання лекційного матеріалу. Підготовка до захисту практичної роботи №8. Підготовка до підсумкового контрольного заходу	9
	Загалом:	82

3. МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться в основному словесними методами та із застосуванням мультимедійних систем, а практичні заняття проводяться з використанням інформаційних технологій, практикумів і мають за мету – набуття студентами практичних навичок з дисципліни.

4. ФОРМИ І МЕТОДИ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Поточний контроль здійснюється під час лекційних, лабораторних та практичних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни. Семестровий контроль проводиться у формі іспиту. При цьому при виведенні остаточної оцінки враховуються результати поточного контролю.

При викладанні дисципліни використовуються такі види навчальних занять, як лекції, лабораторні роботи, практичні роботи, індивідуальне консультування і керівництво самостійною роботою студента.

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. Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

При оцінюванні знань студентів використовуються різні засоби контролю, зокрема: усне опитування перед допуском до виконання лабораторної та практичної робіт – здійснюється на її початку; якість виконання, набуття теоретичних знань і практичних навичок перевіряється шляхом захисту кожної лабораторної та практичної робіт згідно з робочою програмою дисципліни та робочим навчальним планом.

Оцінка, яка виставляється за *лабораторне та практичне заняття*, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної та практичної робіт; знання теоретичного матеріалу з теми; якість оформлення звіту; вміння студента обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної та практичної робіт. Для виконання програми дисципліни студент повинен отримати 8 позитивних оцінок за лабораторні роботи та 8 позитивних оцінок за практичні роботи в семестрі.

Пропущене лабораторне або практичне заняття студент повинен відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за тиждень до завершення теоретичних занять у семестрі.

При *оцінюванні знань* студентів викладач керується такими критеріями.

Оцінку „відмінно”, за шкалою ECTS – A (див. шкалу оцінок), отримує студент за глибоке і повне опанування змісту навчального матеріалу, в якому він легко орієнтується, понятійного апарату, за уміння зв’язувати теорію з практикою, вирішувати практичні завдання, висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає грамотний, логічний виклад відповіді (як в усній, так і в письмовій формі), якісне зовнішнє оформлення. Студент повинен набути практичних навичок із складання різних алгоритмів та розробки програм за цими алгоритмами. Оцінка "відмінно" виставляється студенту, який глибоко засвоїв предметну область та вміє застосовувати її на практиці. Студент не повинен вагатися при відозміні запитання, повинен робити детальні та узагальнюючі висновки.

Оцінку „добре”, за шкалою ECTS – B, отримує студент за повне засвоєння навчального матеріалу, володіння понятійним апаратом, орієнтування в вивченому матеріалі, свідоме використання знань для вирішення практичних завдань, грамотний виклад відповіді, але у змісті і формі відповіді мали місце окремі неточності (похибки), нечіткі формулювання закономірностей тощо. Відповідь студента повинна будуватись на основі самостійного

мислення.

Оцінку „добре”, за шкалою ECTS – C, отримує студент за правильну відповідь з однією суттєвою помилкою.

Оцінки "задовільно", за шкалою ECTS – D, заслуговує студент, який виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, що справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент слабо знає структуру курсу, допускає помилки у відповіді, засвоїв і набув практичних навичок, але допустив неточності. Вагається при відповіді на видозмінене запитання, разом з тим студент володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.

Оцінки "задовільно", за шкалою ECTS – E, заслуговує студент за неповне опанування програмного матеріалу, але отримані знання і набуті практичні навички.

Оцінка „незадовільно”, за шкалою ECTS – FX, виставляється, коли студент має розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткових знань з курсу.

Оцінка „незадовільно”, за шкалою ECTS – F, виставляється студенту за повне незнання і нерозуміння навчального матеріалу або відмову від відповіді і передбачає повторне навчання студента з дисципліни.

Кожний вид роботи оцінюється за чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання

Аудиторна робота		Самостійна, індивідуальна робота		Форма семестрового контролю
Лабораторні роботи №: 1-8	Практичні роботи №: 1-8	Контрольні заходи:		іспит
		КР	ТК	
ВК: 0,15	ВК: 0,1	ВК: 0,25	ВК: 0,1	ВК: 0,4

Примітка: КР – контрольна робота; ВК – ваговий коефіцієнт; ТК – тестовий контроль

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.

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

На тестування відводиться 30 хвилин. Тестування проводиться з використанням модульного середовища для навчання MOODLE. Правильні відповіді студент реєструє в онлайн режимі в модульному середовищі MOODLE. Через 55 хвилин студенти завершують тестування та надсилають свої відповіді на сервер. Викладач оголошує результати тестування згідно журналу оцінок модульного середовища MOODLE.

Якщо студент отримав негативну оцінку, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

Підсумкова семестрова оцінка за національною шкалою і шкалою ECTS встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу. Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ECTS наведені у таблиці.

Співвідношення вітчизняної 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

5. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ СТУДЕНТІВ

1. Відповідність мір інформації напрямкам теорії інформації. Структурні міри інформації.
2. Геометрична міра інформації.
3. Комбінаторна міра інформації.
4. Поняття та основні задачі теорії кодування, методи вирішення основних задач.
Рівномірні та нерівномірні коди
5. Оптимальне кодування: визначення; властивості; принципи.
6. Адитивна міра Хартлі.
7. Кількісна оцінка інформації.
8. Дискретизація і квантування сигналів.
9. Оптимальне кодування Хаффмена.
10. Завадостійке кодування: основні поняття та загальні принципи побудови завадостійких кодів.
11. Коди Хеммінга.
12. Класифікація повідомлень за вміщеною інформацією.
13. Поняття кодової відстані. Перевіряючі та корегуючі характеристики коду.
14. Узагальнена структура інформаційної системи.
15. Теорема Шеннона для дискретного каналу за умови наявності перешкод.
16. Надлишковість інформації. Семантична та статистична надлишковість.
17. Пропускна здатність дискретного каналу зв'язку за умови наявності перешкод.
18. Циклічні коди. Загальні поняття та визначення.
19. Основні параметри сигналів. Умова узгодження сигналів з каналом зв'язку.
20. Оптимальні нерівномірні коди. Терма Шеннона.
21. Пропускна здатність дискретного каналу за умови відсутності перешкод.
22. Паритетне кодування. Паритетне кодування блоків даних.
23. Канал для передачі дискретних повідомлень за умови наявності перешкод. Особливості впливу перешкод на передачу повідомлень.
24. Використання циклічних кодів для виявлення та корегування помилок.
25. Основні принципи побудови циклічних кодів.
26. Ентропія та надлишковість. Поняття недовантаженості та надлишковості.
27. Формування циклічних кодів методом множення поліномів.
28. Загальні принципи використання надлишковості при побудові корегуючих кодів.
29. Методи автоматичного виявлення помилок.
30. Поняття кодової відстані. Зв'язок перевіряючих та корегуючих характеристик коду з кодовою відстанню.
31. Формування циклічних кодів методом ділення поліномів.
32. Стиснення інформації. Словникові методи Лемпела-Зіва.
33. Основи безпеки інформації.
34. Методи і засоби захисту інформації в комп'ютерних системах.
35. Криптографічні методи захисту інформації.
36. 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-Хеллмана 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 відеомоделювання.
71. Особливості створення мультимедійних проектів.
72. Особливості використання текстових, графічних, аудіо- та відеоінформації у мультимедійних проектах.

6. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

1. Ковтун Л.О. Теорія інформації та кодування : методичні вказівки до практичних робіт для студентів спеціальності 123 - Комп'ютерна інженерія / Л.О. Ковтун. – Хмельницький : ХНУ, 2018. – 104 с.

2. Корецька Л. Теорія інформації, кодування та шифрування : навчальний посібник / Л.О. Корецька. – Хмельницький: Символ, 2021. – 208 с.

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

3. Приходько С. І. Основи теорії інформації та кодування : навчальний посібник / С. І. Приходько, К. А. Трубочанінова, О. П. Батаєв. – Харків : УкрДУЗТ, 2017. – 111 с.

4. Курко А.М. Введення в теорію інформації : посібник до вивчення дисципліни теорія інформації для студентів за напрямом підготовки 6.050202 Автоматизація та комп'ютерно-інтегровані технології / укл. : А.М. Курко , В.Я. Решетник. – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2017. – 108 с.

5. Теорія інформації та обробка сигналів-1: конспект лекцій [Електронний ресурс]: навч. посіб. для студ. спеціальності 171 «Електроніка», освітньої програми «Електронні компоненти і системи» / КПІ ім. Ігоря Сікорського ; уклад.: Ю.С. Ямненко, К. С. Клен. – Київ: КПІ ім. Ігоря Сікорського, 2019. – 120 с.

6. Беркман Л.Н. Кодування джерел інформації та каналів зв'язку : навч. посібник / Л.Н. Беркман, А.П. Бондарчук, Г.І. Гайдур, Н.С. Чумак. – Київ: ННІТІ ДУТ, 2018. – 91с.

7. Технології захисту інформації [Електронний ресурс] : підручник / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

8. Дробик О.В. Цифрова обробка аудіо- та відеоінформації у мультимедійних системах: Навчальний посібник / О.В. Дробик, В.В. Кідалов, В.В. Коваль, Б.Я. Костік, В.С. Лазебний, Г.М. Розорінов, Г.О. Сукач. – К.: Наукова думка, 2016. – 144 с.

9. Шубін І.Ю. Розробка інтерактивного медіа: Навч. посібник / І.Ю. Шубін, І.В. Груздо – Харків: ХНУРЕ., 2016. – 170 с.

10. Основи теорії інформації та кодування. Конспект лекцій: [Електронний ресурс]: навч. посіб. / М.І. Романюк; Ю. Г. Савченко; КПІ ім. Ігоря Сікорського. – Електронні текстові данні (1 файл: 1,86 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2019. –70 с.

Додаткова

1. Інформаційний та кіберпростори : проблеми безпеки, методи та засоби боротьби : посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін. – К. : ДУТ – КНУ, 2016. – 178 с

2. Основи теорії інформації та кодування: лабораторний практикум [Електронний ресурс] : навч. посіб. для студ. спеціальності 171 «Електроніка», спеціалізації «Електронні та інформаційні технології кінематографії та аудіовізуальних систем» / М. І. Романюк, Г. Г. Власюк; КПІ ім. Ігоря Сікорського. – Електронні текстові данні (1 файл: 2,09 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 81 с.

3. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

4. Правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.

8. ІНФОРМАЦІЙНІ РЕСУРСИ

Електронний університет:

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі тестові завдання для поточного та семестрового контролю знань).

2. Електронна бібліотека університету