



Основи теорії кодування та шифрування сигналів (RE-185).

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Перший (бакалаврський)</i>
Галузь знань	<i>17 - Електроніка, автоматизація та електронні комунікації</i>
Спеціальність	<i>172 "Електронні комунікації та радіотехніка"</i>
Освітня програма	Всі ОП
Статус дисципліни	<i>Вибіркова</i>
Форма навчання	<i>Заочна</i>
Рік підготовки, семестр	<i>3 курс, 6 семестр</i>
Обсяг дисципліни	<i>Загальна кількість: (4 кредитів) 120 год. Лекційних занять: 6 год. Практичних занять: 0 год. Лабораторних занять (комп'ютерних практикумів): 4 год. Самостійна робота студентів: 110 год.</i>
Семестровий контроль/ контрольні заходи	<i>ТКР, МКР (ДЗ); ДКР (ДЗ), індивідуальні завдання до лабораторних занять (комп'ютерних практикумів), залік</i>
Розклад занять	https://schedule.kpi.ua/
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектор: старший викладач Павлов Олег Ігорович (pavlov.oleg1@iit.kpi.ua) Лабораторні: старший викладач Павлов Олег Ігорович (pavlov.oleg1@iit.kpi.ua)</i>
Розміщення курсу	https://do.ipk.kpi.ua/course/view.php?id=451

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Дисципліна «Основи теорії кодування та шифрування сигналів» (далі — ОТКШС) відноситься до дисциплін циклу професійної підготовки фахівців першого (бакалаврського) рівня вищої освіти за спеціальністю 172 Електронні комунікації та радіотехніка.

1.1. Предмет та мета вивчення дисципліни

Предмет дисципліни ОТКШС — методи та алгоритми форматування сигналів від аналогового джерела, перетворення їх в дискретну форму, кодування повідомлень дискретного джерела з дозволеними втратами, квантування кодованих даних, шифрування цифрових даних,

канального кодування зашифрованих цифрових даних, а також особливості їх застосування в радіотехнічних системах.

Мета вивчення дисципліни — формування у студентів компетентності щодо:

- використання методів форматування сигналів від аналогового джерела, перетворення їх в дискретну форму, кодування повідомлень дискретного джерела з дозволеними втратами, квантування кодованих даних, шифрування цифрових даних, канального кодування зашифрованих цифрових даних, які застосовуються в сучасних цифрових телекомунікаційних системах;
- володіння теоретичним фундаментом для подальшого самостійного вивчення та вдосконалення набутих знань щодо методів, алгоритмів і особливостей практичної реалізації процесів кодування джерела, шифрування даних та канального кодування в рамках самостійної роботи над бакалаврською роботою;
- використання системи Matlab для моделювання алгоритмів обробки сигналів і даних при кодуванні джерела та шифруванні даних, дослідження їх характеристик та оцінювання їх ефективності та відповідності вимогам.

1.2. Після засвоєння навчальної дисципліни студенти мають продемонструвати такі результати навчання:

ЗНАННЯ (результат вивчення явищ і закономірностей об'єктивного світу, такий, який можна логічно або фактично обґрунтувати, і емпірично або практично перевірити):

- класифікації методів форматування сигналів від аналогового джерела, кодування дискретного джерела, шифрування дискретних повідомлень, канального кодування, їх визначення, властивостей, прикладів реалізації та критеріїв ефективності застосування;
- особливостей кодування дискретного джерела на прикладі кодування мовленнєвих сигналів в сучасних цифрових телекомунікаційних системах; особливостей шифрування дискретних повідомлень сучасними криптографічними методами;
- процесів обробки сигналів на базі методу лінійного прогнозування в задачах аналізу та синтезу, еквівалентного параметричного подання лінійних систем в різних альтернативних просторах параметрів, методів оцінювання параметрів, векторного їх прогнозування, квантування та інтерполяції, методів симетричного та несиметричного шифрування даних, методів криптографічної ідентифікації, верифікації та перевірки цілісності.

НАВИКИ (здатність до діяльності, "навченість виконувати дії", сформована шляхом повторення дії і доведення її до автоматизму):

- кодування джерела методом лінійного прогнозування, виконання векторного квантування кодованих параметрів з використанням системи Matlab;
- використання систем PGP, GPG, OpenSSL та інших для шифрування даних і їх підписування;
- генерації ключів та інших службових даних для їх використання в криптографічних алгоритмах, їх перевірки щодо вимог криптографічної стійкості.

УМІННЯ (опанований спосіб виконання дії, який забезпечується сукупністю придбаних знань та навичок, і який створює можливість виконання дії не тільки в звичних умовах, але і в таких, що змінилися):

- виконувати моделювання кодування джерела методом лінійного прогнозування на прикладі мовленнєвих сигналів;
- виконувати проектування кодової книги векторного квантування кодованих параметрів джерела методом LBG на прикладі мовленнєвих сигналів;
- виконувати шифрування даних методом RSA та AES;
- виконувати підписування шифрованих даних методом RSA та DES.

1.3. **Роль і значення дисципліни в підготовці фахівців** — формування сучасного бачення та досвіду щодо проектування РЕА, здатної забезпечувати ефективне кодування сигналів та даних, а також їх шифрування для досягнення таких властивостей:

- зменшення обсягів даних, що зберігаються або передаються (при фіксованих величинах спотворень, що виникають під час кодування);

- зменшення величин спотворень, що виникають в результаті кодування даних (при фіксованих обсягах даних / швидкостях передачі);
- підвищення надійності прийому / відтворення даних з можливістю виправлення помилок, що виникають в приймачі / відтворювачі в результаті різних чинників;
- забезпечення конфіденційності зберігання та передачі даних відкритими (незахищеними) каналами зв'язку;
- забезпечення можливості перевірки цілісності (незмінності) даних, їх оригінальності та верифікації їх виробника / відправника.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Основується на знаннях, що отримані в рамках вивчення освітніх компонентів; «Математичний аналіз. Частина 1», «Математичний аналіз. Частина 2», «Математичний аналіз. Частина 3», «Інформатика. Частина 1. Основи програмування та алгоритми», «Інформатика. Частина 2. Основи обчислювальної техніки», «Основи теорії електронних комунікацій і радіотехніки. Частина 2. Сигнали та процеси в радіотехніці».

Знання та програмні результати навчання, що отримані в ході опанування освітнього компоненту «Цифрове оброблення сигналів» забезпечують вивчення освітніх компонентів: «Радіонавігаційні системи», «Цифрові телевізійні системи», «Мікрокомп'ютерні вбудовані системи радіокерування».

3. Зміст навчальної дисципліни

Назви розділів і тем
Розділи 1—7: Основи теорії кодування сигналів
Розділ 1. Форматування сигналів джерела та НЧ модуляція (за Склярром)
Тема 1.1. Низькочастотні системи [1, с. 84—87]
Тема 1.2. Форматування текстової інформації (Знакове кодування.) [1, с. 87—87]
Тема 1.3. Повідомлення знаки символи [1, с. 87—91]
Тема 1.4. Форматування аналогової інформації (Теорема відділів. Накладання спектрів. Вибірка з запасом. Класифікація сигналів та процеси їх перетворення при введенні в цифрову систему.) [1, с. 91—104]
Тема 1.5. Джерела спотворень (Вплив дискретизації та квантування. Вплив каналу. Відношення С/Ш для квантованих імпульсів.) [1, с. 104—107]
Тема 1.6. Імпульсно-кодова модуляція [1, с. 107—109]
Тема 1.7. Квантування з постійним та змінним кроком (Статистика амплітуд при передачі мовлення. Нерівномірне квантування. Характеристики компандування.) [1, с. 109—113]
Тема 1.8. Низькочастотна передача (Подання двійкових цифр у формі сигналів. Типи сигналів PCM. Спектральні параметри сигналів PCM. Кількість біт на слово PCM та кількість біт на символ PCM. М-кратні імпульсно-модульовані сигнали.) [1, с. 113—122]
Тема 1.9. Кореляційне кодування (Двубінарна передача сигналів. Двубінарне декодування. Попереднє кодування. Еквівалентна двубінарна передаточна функція. Порівняння бінарного та двубінарного методів передачі сигналів. Полібінарна передача сигналів.) [1, с. 122—127]
Тема 1.10. Підсумки (Література. Задачі. Питання для самоперевірки.) [1, с. 127—132]
Тематична контрольна робота за розділом 1 (Moodle, Завдання 1 до МКР-1) [14]
Розділ 2. Техніка кодування аналогових джерел (за Прокісом)
Тема 2.1. Часово-сигнальне кодування (Імпульсно-кодова модуляція (ІКМ). Диференційна ІКМ. Адаптивні ІКМ та ДІКМ. Дельта-модуляція (ДМ).) [2, с. 108—118]
Тема 2.2. Спектральне кодування сигналу (Кодування підсумг. Адаптивне перетворююче кодування.) [2, с. 118—119]
Тема 2.3. Модельне кодування джерела (Методи кодування мовленнєвих сигналів.) [2, с. 119—125]
Тема 2.4. Підсумки (Література. Задачі. Питання для самоперевірки.) [2, с. 125—130]
Розділ 3. Кодування джерела (за Склярром)
Тема 3.1. Джерела (Дискретні джерела, ентропія двійкового джерела з пам'яттю та без, коди розширення. Джерела неперервних сигналів, функція щільності амплітуд.) [1, с. 822—828]
Тема 3.2. Квантування амплітуди (Шум квантування. Рівномірне квантування. Насичення. Додавання псевдо випадкового шуму. Нерівномірне квантування.) [1, с. 828—852]
Тема 3.3. Диференціальна імпульсно-кодова модуляція (Передбачення з одним відведенням. Передбачення з N-відведеннями. Дельта-модуляція. Сигма-дельта-модуляція. Сигма-дельта АЦП. Сигма-дельта ЦАП.) [1, с. 852—867]
Тема 3.4. Адаптивне прогнозування (Пряма адаптація. Синтетичне/аналітичне кодування.) [1, с. 867—870]
Тема 3.5. Блочне кодування (Векторне квантування.) [1, с. 870—873]
Тема 3.6. Перетворююче кодування (Квантування для перетворюючого кодування. Багато смугове кодування.) [1, с. 873—876]
Тема 3.7. Кодування джерела для цифрових даних (Властивості кодів. Код Хаффмана. Групові коди.) [1, с. 876—887]
Тема 3.8. Приклади кодування джерела (Аудіо стиснення. Стиснення зображень.) [1, с. 887—900]
Тема 3.9. Підсумки (Література. Задачі. Питання для самоперевірки.) [1, с. 900—906]
Розділ 4. Кодування джерела (за Прокісом)
Тема 4.1. Математичні моделі для джерел інформації [2, с. 74—75]

Тема 4.2. Логарифмічна міра інформації (Середня взаємна інформація та ентропія. Вимірювання інформації для неперервних випадкових величин.) [2, с. 75—82]
Тема 4.3. Кодування для дискретних джерел без пам'яті (Кодові слова фіксованої довжини. Теорема кодування джерела №1. Кодові слова змінної довжини. Нерівність Крафта. Теорема кодування джерела №2. Алгоритм кодування Хаффмена.) [2, с. 82—90]
Тема 4.4. Кодування для дискретних джерел з пам'яттю (Дискретні стаціонарні джерела. Алгоритм Земпела-Зіва.) [2, с. 90—94]
Тема 4.5. Кодування для аналогових джерел — основні теореми (Функція "Спотворення/Швидкість" $R(D)$. Теорема про функцію $R(D)$ для гаусового джерела без пам'яті. Теорема про кодування джерела з заданою мірою спотворення. Теорема про верхню межу для функції $R(D)$.) [2, с. 94—98]
Тема 4.6. Кодування для аналогових джерел — оптимальне квантування (Скалярне квантування. Векторне квантування, алгоритм k -середніх.) [2, с. 98—108]
Тема 4.7. Підсумки (Література. Задачі. Питання для самоперевірки.) [2, с. 125—131]
Тематична контрольна робота за розділом 4 (Moodle, Завдання 2 до МКР-1) [14]
Розділ 5. Векторне квантування при кодуванні мовлення (за Максвоулом)
Тема 5.1. Вступні положення (Мета та питання, які розглядаються. Основи кодування мовленнєвих сигналів.) [3, с. 19—22]
Тема 5.2. Векторне квантування (Постановка задачі. Міри спотворень. Побудова кодової книги. Обчислення витрат та потрібної смості пам'яті. Модель векторного квантування.) [3, с. 22—30]
Тема 5.3. Теоретичні характеристики векторного квантування (Теорія передачі з похибкою. Скалярне квантування. Асимптотичні характеристики векторного квантування.) [3, с. 30—38]
Тема 5.4. Порівняння скалярного та векторного квантування векторних джерел (Розподіл біт. Поворот вектора для випадку корельованих джерел. Порівняння з векторним квантуванням.) [3, с. 38—44]
Тема 5.5. Побудова кодової книги (Пошук за методом дихотомії. Каскадне квантування. Мультиплікативні коди. Випадкові кодові книги. Навчання та випробовування.) [3, с. 44—53]
Тема 5.6. Векторне квантування з врахуванням часових залежностей (Вибіркова передача кадрів. Сегментне квантування. Адаптивне ВК.) [3, с. 53—55]
Тема 5.7. Кодування форми мовленнєвого сигналу (Скалярне квантування форми сигналу. Векторне квантування форми сигналу. Література. Задачі. Питання для самоперевірки.) [3, с. 55—58]
Тема 5.8. Підсумки (Література. Задачі. Питання для самоперевірки.) [3, с. 58—61]
Тематична контрольна робота за розділом 5 (Moodle, Завдання 3 до МКР-1) [14]
Розділ 6. Циклічні коди. Ефективність використання завадостійких кодів (за Мазурковим)
Тема 6.1. Алгебраїчний опис циклічних кодів (Просте поле Гауа. Розширене поле Гауа. Конструктивний опис циклічних кодів). Коди Боуза-Чоудхурі-Хоквінгема. [4, с. 120—130]
Тема 6.2. Найважливіші блокові коди та їхні властивості (Досконалі коди. Симплексні коди. Ортогональні та біортогональні коди. Коди максимальної довжини). Мажоритарне декодування циклічних кодів. [4, с. 130—138]
Тема 6.3. Коди Ріда-Соломона. Еквівалентні двійкові коди Ріда-Соломона. [4, с. 142—145]
Тема 6.4. Кодування загорткових кодів. Декодування загорткових кодів. Алгоритм Вітербі. [4, с. 145—151]
Тема 6.5. Кодування у каналах із замираннями. Код Фінка-Хагельбергера. Два способи приймання — в цілому, та поелементне. [4, с. 151—155]
Тема 6.6. Потенційна завадостійкість кодів максимальної довжини при прийманні в цілому. Алгоритм швидкого кореляційного декодування m -кових циклічних кодів. [4, с. 155—160]
Тема 6.7. Завадостійкість коректувальних кодів при прелементному прийманні. Використання кодів у системах із зворотним зв'язком. [4, с. 160—166]
Розділ 7. Завадостійке кодування. Теоретичні межі коректувальних можливостей (за Мазурковим)
Тема 7.1. Коректувальні коди. Загальні властивості [4, с. 104—106]
Тема 7.2. Геометрична модель. Основні параметри коректувальних кодів [4, с. 106—110]
Тема 7.3. Класифікація коректувальних кодів [4, с. 110—111]
Тема 7.4. Межі коректувальних можливостей лінійних кодів (Суттєвість теореми кодування Шеннона для каналів із завадами. Верхня границя Хеммінга. Нижня границя Варламова-Гілберта.) [4, с. 111—114]
Тема 7.5. Лінійні блокові коди. Декодування за методом синдрому (Алгебраїчний опис, кодування та декодування лінійних кодів. Коди Хеммінга. Границя Сінглтона.) [4, с. 114—119]
Розділи 8—13: Основи теорії шифрування даних
Розділ 8. Основи теорії шифрування та дешифрування (за Скляром)
Тема 8.1. Моделі, мета, початкові системи шифрування (Модель процесу шифрування та дешифрування. Задачі системи шифрування. Класичні загрози. Класичні шифри.) [1, с. 908—913]
Тема 8.2. Секретність системи шифрування (Абсолютна секретність. Ентропія та невизначеність. Інтенсивність та надлишковість мови. Відстань єдності та ідеальна секретність.) [1, с. 913—920]
Тема 8.3. Практична захищеність (Суміш та дифузія. Підстановка. Перестановка. Продукційний шифр. Стандарт шифрування даних.) [1, с. 920—931]
Розділ 9. Практичне шифрування та дешифрування (за Скляром)
Тема 9.1. Потокове шифрування (Приклад генерування ключа з використанням лінійного регістру зсуву зі зворотним зв'язком. Слабкі місця регістру зсуву зі зворотним зв'язком. Синхронні та самосинхронізаційні системи поточного шифрування.) [1, с. 931—936]
Тема 9.2. Криптосистеми з відкритим ключем (Перевірка справжності підпису з використанням системи з відкритим ключем. Одностороння функція з "лазівкою". Схема RSA. Задача укладання рюкзака. Криптосистема з відкритим ключем, яка заснована на "лазівці" в рюкзаку.) [1, с. 936—944]
Тема 9.3. Система PGP ("Потрійний" DES, CAST та IDEA. Алгоритм Діффі-Хелмана і варіант Елгамала та RSA. Шифрування повідомлень в системі PGP. Аутентифікація за допомогою PGP і створення підпису.) [1, с. 944—955, 8]
Тема 9.4. Підсумки (Література. Задачі. Питання для самоперевірки.) [1, с. 955—961]
Тематична контрольна робота за розділом 9 (Moodle, Завдання 4 до МКР-1) [14]
Розділ 10. Вступ до теорії криптографії (за Шнайсром)
Тема 10.1. Загальні поняття (Термінологія. Стеганографія. Підстановочні та перестановочні шифри. Просте XOR. Одноразові блокноти. Комп'ютерні алгоритми. Великі числа.) [5, с. 47—71]
Розділ 11. Криптографічні протоколи (за Шнайсром)
Тема 11.1. Елементи протоколів. [5, с. 71—107]
Тема 11.2. Основні протоколи. Проміжні протоколи. [5, с. 107—177]
Тема 11.3. Розвинуті протоколи. Езотеричні протоколи. [5, с. 177—241]
Домашня КР №1
Розділ 12. Криптографічні методи (за Шнайсром)
Тема 12.1. Довжина ключа. Керування ключами [5, с. 241—293]
Тема 12.2. Типи алгоритмів та криптографічні режими [5, с. 293—325]
Тема 12.3. Використання алгоритмів [5, с. 325—347]
Тематична контрольна робота за розділом 12 (Moodle, Завдання 5 до МКР-1) [14]
Розділ 13. Криптографічні алгоритми (за Шнайсром)
Тема 13.1. Математичні основи [5, с. 347—389]
Тема 13.2. Стандарт шифрування DES та інші блочні шифри. Об'єднання блочних шифрів. [5, с. 389—521]
Тема 13.3. Генератори ПІВГ та справжніх ВП. Потоківні шифри. Однонаправлені хеш-функції. [5, с. 521—633]
Тема 13.4. Алгоритми з відкритими ключами. Алгоритми ЕЦП. Схеми ідентифікації. Алгоритми обміну ключами. Спеціальні алгоритми для протоколів [5, с. 633—753]
Тематична контрольна робота за розділом 13 (Moodle, Завдання 6 до МКР-1) [14]

4. Навчальні матеріали та ресурси

Рекомендована література:

Основна до частини 1

1. [Sklar B. Digital communications. Fundamentals and Applications. — 2nd ed. / Communications Engineering Services, Tarzana, California and University of California, Los Angeles // Prentice Hall PTR, 2001. — ISBN 0-13-084788-7.](#)
2. [Proakis J. Digital Communications. — 4th ed. // New York: The McGraw-Hill, 2001. — 928 p. — ISBN 0-07-232111-3., Lecture 01 — Lecture 20.](#)
3. [Makhoul J., Roucos S., Gish H. Vector Quantization in Speech Coding // Proc. of the IEEE, Vol. 73, No. 11. Nov. 1985. — pp. 1551—1588.](#)

Додаткова до частини 1

4. [Мазурков М. І. Основи теорії передавання інформації. Навчальний посібник для вищих навчальних закладів. / М. І. Мазурков; Одес. нац. політехн. ун-т. — О.: Наука і техніка, 2005. — 167 с.: рис., табл. — Бібліогр. у кінці розд. — ISBN 966-8335-08-2.](#)

Основна до частини 2

5. [Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition // 20th Anniversary Edition. — Wiley, 2015. — 784 p. — ISBN 978-1-119-09672-6.](#)

Додаткова до частини 2

6. [Hamming R. Coding and information theory \(2nd ed.\) // USA, NJ: Prentice-Hall, 1986. — ISBN 0-13-139072-4.](#)
7. [Ferguson N. Schneier B. Practical Cryptography // John Wiley & Sons, 2003, 432p. ISBN 047122894X.](#)
8. [Zimmermann P. PGP User's Guide / Public Key Encryption for the Masses, 1990-1994 Philip Zimmermann.](#)
9. [Shannon C.E. A Mathematical Theory of Cryptography // Case 20878, MM-45-110-92, September 1, 1945. Index P0.4. — P.137.](#)
10. [Shannon C.E. 1949. Communication Theory of Secrecy Systems // The Bell System Technical Journal, vol. 28, no. 4, pp. 656-715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.](#)

Додаткова

11. [Korn G. A., Korn T. M. Mathematical Handbook for Scientists and Engineers: Definitions, Theorems, and Formulas for Reference and Review / 2nd ed., enlarged and revised, McGraw-Hill Book Company, 1968. Reprint, Dover Publications, 2013, ISBN 13: 9780486411477.](#)
12. Положення про кредитно-модульну організацію навчального процесу в НТУУ «КПІ» / Уклад. В. П. Головенкін — К.: ІВЦ “Видавництво «Політехніка»”, 2006. — 55 с.

Посібники та методичні вказівки

13. [Методичні вказівки «Спектральні перетворення та методи ЦСА» до дисципліни “Дискретні та цифрові сигнали і процеси в радіотехніці”. Для студентів радіотехнічного факультету усіх форм навчання / Укл. О. І. Павлов. — К.: НТУУ “КПІ”, 2020. — 45 с.](#)

Інформаційні ресурси

14. Сервер СДН з дисципліни ОТКШС за адресою <https://do.ipk.kpi.ua/course/view.php?id=451> (електронні версії літератури, методичні вказівки, завдання, рейтинг).

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

5.1. Лекційні заняття

№	Назва теми лекції та перелік основних питань	Кіль-
---	--	-------

з/п	(перелік дидактичних засобів, посилання на літературу та завдання на СРС)	кількість ауд. годин
	Розділ 2. Техніка кодування аналогових джерел (за Прокісом)	1.00
1.	Тема 2.1. Часово-сигнальне кодування (Імпульсно-кодова модуляція (ІКМ). Диференційна ІКМ. Адаптивні ІКМ та ДІКМ. Дельта-модуляція (ДМ).) [2, с. 108—118]	
	Тема 2.3. Модельне кодування джерела (Методи кодування мовленнєвих сигналів.) [2, с. 119—125]	1.00
	Розділ 5. Векторне квантування при кодуванні мовлення (за Макхоулом)	1.00
2.	Тема 5.1. Вступні положення (Мета та питання, які розглядаються. Основи кодування мовленнєвих сигналів.) [3, с. 19—22]	
	Тема 5.2. Векторне квантування (Постановка задачі. Міри спотворень. Побудова кодової книги. Обчислення витрат та потрібної ємності пам'яті. Модель векторного квантування.) [3, с. 22—30]	
	Тема 5.3. Теоретичні характеристики векторного квантування (Теорія передачі з похибкою. Скалярне квантування. Асимптотичні характеристики векторного квантування.) [3, с. 30—38]	
	Розділ 9. Практичне шифрування та дешифрування (за Склярром)	1.00
	Тема 9.1. Поточкове шифрування (Приклад генерування ключа з використанням лінійного регістру зсуву зі зворотним зв'язком. Слабкі місця регістру зсуву зі зворотним зв'язком. Синхронні та самосинхронізаційні системи поточного шифрування.) [1, с. 931—936]	
3.	Тема 9.2. Криптосистеми з відкритим ключем (Перевірка справжності підпису з використанням системи з відкритим ключем. Одностороння функція з "лазіркою". Схема RSA. Задача укладання рюкзака. Криптосистема з відкритим ключем, яка заснована на "лазірці" в рюкзаку.) [1, с. 936—944]	1.00
	Тема 9.3. Система PGP ("Потрійний" DES, CAST та IDEA. Алгоритм Діффі-Хелмана і варіант Елгамала та RSA. Шифрування повідомлень в системі PGP. Аутентифікація за допомогою PGP і створення підпису.) [1, с. 944—955, 8]	1.00
	ВСЬОГО	6.00

5.2. Лабораторні заняття (комп'ютерні практикуми)

№ з/п	Назва лабораторної роботи	Кількість ауд. годин
1.	Застосування методів ЛП та Проні для визначення параметрів моделі джерела [14]	2.00
2.	Криптографічне шифрування та підписування поточкових даних за алгоритмом AES + RSA. Пакет програм OpenSSL [14]	2.00
	Всього	4.00

6. Самостійна робота здобувача вищої освіти

Самостійна робота студентів передбачає самостійне вивчення теоретичного матеріалу та виконання лабораторних робіт (комп'ютерних практикумів), які не виносяться на аудиторні заняття. Результати виконання лабораторних робіт завантажуються в СДН *Moodle* для перевірки викладачем.

Після вивчення певних розділів матеріалу студенти виконують відповідні тематичні частини (ТКР) модульної контрольної роботи (МКР). ТКР (МКР в цілому) виконуються в формі тестів з використанням СДН *Moodle* (<https://do.ipk.kpi.ua/course/view.php?id=451>) [14].

Після вивчення розділу 11 студенти виконують домашню контрольну роботу (ДКР), результати виконання якої також завантажуються в СДН *Moodle* для перевірки викладачем.

6.1. Самостійне виконання лабораторних робіт

№ з/п	Назва лабораторної роботи	Кількість годин СРС
1.	Оцінювання спектральної обвідної та детального спектра сигналів методом LPC та FFT [14]	2.00
2.	Проектування кодової книги ВК за алгоритмом LBG-VQ (Radix-2 splitting) [14]	2.00

3.	Проектування кодової книги ВК за алгоритмом LBG-VQ (Linear splitting) [14]	2.00
4.	2D-DWT: смугова фільтрація, декомпозиція, децимація та реконструкція зображень [14]	2.00
5.	Криптографічне шифрування та підписування поштових повідомлень на ПК. Додаток Mailvelope [14]	2.00
6.	Криптографічне шифрування та підписування поштових повідомлень на смартфоні з ОС Андроїд. Додатки OpenKeychain + K-9 Mail [14]	2.00
7.	Криптографічне шифрування та підписування файлів на ПК. OpenPGP, Gpg4Win, Gpg4Usb [14]	2.00
	Всього	14.00

6.2. Самостійне вивчення теоретичного матеріалу

№ з/п	Назва теми, що виноситься на самостійне опрацювання	Кількість годин СРС
	Розділ 1. Форматування сигналів джерела та НЧ модуляція (за Скляром)	
1.	Тема 1.1. Низькочастотні системи [1, с. 84—87]	1.00
2.	Тема 1.2. Форматування текстової інформації (Знакове кодування.) [1, с. 87—87]	1.00
3.	Тема 1.3. Повідомлення знаки символи [1, с. 87—91]	1.00
4.	Тема 1.4. Форматування аналогової інформації (Теорема відліків. Накладання спектрів. Вибірка з запасом. Класифікація сигналів та процеси їх перетворення при введенні в цифрову систему.) [1, с. 91—104]	1.00
5.	Тема 1.5. Джерела спотворень (Вплив дискретизації та квантування. Вплив каналу. Відношення С/Ш для квантованих імпульсів.) [1, с. 104—107]	1.00
6.	Тема 1.6. Імпульсно-кодова модуляція [1, с. 107—109]	1.00
7.	Тема 1.7. Квантування з постійним та змінним кроком (Статистика амплітуд при передачі мовлення. Нерівномірне квантування. Характеристики компандування.) [1, с. 109—113]	1.00
8.	Тема 1.8. Низькочастотна передача (Подання двійкових цифр у формі сигналів. Типи сигналів РСМ. Спектральні параметри сигналів РСМ. Кількість біт на слово РСМ та кількість біт на символ РСМ. М-кратні імпульсно-модульовані сигнали.) [1, с. 113—122]	1.00
9.	Тема 1.9. Кореляційне кодування (Двубінарна передача сигналів. Двубінарне декодування. Попереднє кодування. Еквівалентна двубінарна передаточна функція. Порівняння бінарного та двубінарного методів передачі сигналів. Полібінарна передача сигналів.) [1, с. 122—127]	1.00
10.	Тема 1.10. Підсумки (Література. Задачі. Питання для самоперевірки.) [1, с. 127—132]	0.00
	Розділ 2. Техніка кодування аналогових джерел (за Прокісом)	
11.	Тема 2.1. Часово-сигнальне кодування (Імпульсно-кодова модуляція (ІКМ). Диференційна ІКМ. Адаптивні ІКМ та ДІКМ. Дельта-модуляція (ДМ).) [2, с. 108—118]	1.00
12.	Тема 2.2. Спектральне кодування сигналу (Кодування підсмуг. Адаптивне перетворююче кодування.) [2, с. 118—119]	1.00
13.	Тема 2.3. Модельне кодування джерела (Методи кодування мовленнєвих сигналів.) [2, с. 119—125]	1.00
14.	Тема 2.4. Підсумки (Література. Задачі. Питання для самоперевірки.) [2, с. 125—130]	0.00
	Розділ 3. Кодування джерела (за Скляром)	
15.	Тема 3.1. Джерела (Дискретні джерела, ентропія двійкового джерела з пам'яттю та без, коди розширення. Джерела неперервних сигналів, функція щільності амплітуд.) [1, с. 822—828]	1.00
16.	Тема 3.2. Квантування амплітуди (Шум квантування. Рівномірне квантування. Насичення. Додавання псевдо випадкового шуму. Нерівномірне квантування.) [1, с. 828—852]	1.00
17.	Тема 3.3. Диференціальна імпульсно-кодова модуляція (Передбачення з одним відведенням. Передбачення з N-відведеннями. Дельта-модуляція. Сигма-дельта-модуляція. Сигма-дельта АЦП. Сигма-дельта ЦАП.) [1, с. 852—867]	1.00
18.	Тема 3.4. Адаптивне прогнозування (Пряма адаптація. Синтетичне/аналітичне кодування.) [1, с. 867—870]	1.00
19.	Тема 3.5. Блочне кодування (Векторне квантування.) [1, с. 870—873]	1.00
20.	Тема 3.6. Перетворююче кодування (Квантування для перетворюючого кодування. Багато смугове кодування.) [1, с. 873—876]	1.00
21.	Тема 3.7. Кодування джерела для цифрових даних (Властивості кодів. Код Хаффмана. Групові коди.) [1, с. 876—887]	1.00
22.	Тема 3.8. Приклади кодування джерела (Аудіо стиснення. Стиснення зображень.) [1, с. 887—900]	1.00
23.	Тема 3.9. Підсумки (Література. Задачі. Питання для самоперевірки.) [1, с. 900—906]	0.00
24.	Розділ 4. Кодування джерела (за Прокісом)	2.00

	Тема 4.1. Математичні моделі для джерел інформації [2, с. 74—75]	
25.	Тема 4.2. Логарифмічна міра інформації (Середня взаємна інформація та ентропія. Вимірювання інформації для неперервних випадкових величин.) [2, с. 75—82]	2.00
26.	Тема 4.3. Кодування для дискретних джерел без пам'яті (Кодові слова фіксованої довжини. Теорема кодування джерела №1. Кодові слова змінної довжини. Нерівність Крафта. Теорема кодування джерела №2. Алгоритм кодування Хаффмена.) [2, с. 82—90]	2.00
27.	Тема 4.4. Кодування для дискретних джерел з пам'яттю (Дискретні стаціонарні джерела. Алгоритм Земпела-Зіва.) [2, с. 90—94]	2.00
28.	Тема 4.5. Кодування для аналогових джерел — основні теореми (Функція "Спотворення/Швидкість" $R(D)$). Теорема про функцію $R(D)$ для гаусового джерела без пам'яті. Теорема про кодування джерела з заданою мірою спотворення. Теорема про верхню межу для функції $R(D)$.) [2, с. 94—98]	2.00
29.	Тема 4.6. Кодування для аналогових джерел — оптимальне квантування (Скалярне квантування. Векторне квантування, алгоритм k-середніх.) [2, с. 98—108]	2.00
30.	Тема 4.7. Підсумки (Література. Задачі. Питання для самоперевірки.) [2, с. 125—131]	0.00
31.	Розділ 5. Векторне квантування при кодуванні мовлення (за Макхоулом) Тема 5.1. Вступні положення (Мета та питання, які розглядаються. Основи кодування мовленнєвих сигналів.) [3, с. 19—22]	2.00
32.	Тема 5.2. Векторне квантування (Постановка задачі. Міри спотворень. Побудова кодової книги. Обчислення витрат та потрібної ємності пам'яті. Модель векторного квантування.) [3, с. 22—30]	2.00
33.	Тема 5.3. Теоретичні характеристики векторного квантування (Теорія передачі з похибкою. Скалярне квантування. Асимптотичні характеристики векторного квантування.) [3, с. 30—38]	2.00
34.	Тема 5.4. Порівняння скалярного та векторного квантування векторних джерел (Розподіл біт. Поворот вектора для випадку корельованих джерел. Порівняння з векторним квантуванням.) [3, с. 38—44]	2.00
35.	Тема 5.5. Побудова кодової книги (Пошук за методом дихотомії. Каскадне квантування. Мультиплікативні коди. Випадкові кодові книги. Навчання та випробування.) [3, с. 44—53]	2.00
36.	Тема 5.6. Векторне квантування з врахуванням часових залежностей (Вибіркова передача кадрів. Сегментне квантування. Адаптивне ВК.) [3, с. 53—55]	2.00
37.	Тема 5.7. Кодування форми мовленнєвого сигналу (Скалярне квантування форми сигналу. Векторне квантування форми сигналу. Література. Задачі. Питання для самоперевірки.) [3, с. 55—58]	2.00
38.	Тема 5.8. Підсумки (Література. Задачі. Питання для самоперевірки.) [3, с. 58—61]	0.00
39.	Розділ 6. Циклічні коди. Ефективність використання завадостійких кодів (за Мазурковим) Тема 6.1. Алгебраїчний опис циклічних кодів (Просте поле Галуа. Розширене поле Галуа. Конструктивний опис циклічних кодів). Коди Боуза-Чоудхурі-Хоквінгема. [4, с. 120—130]	1.00
40.	Тема 6.2. Найважливіші блокові коди та їхні властивості (Досконалі коди. Симплексні коди. Ортогональні та біртогональні коди. Коди максимальної довжини). Мажоритарне декодування циклічних кодів. [4, с. 130—138]	1.00
41.	Тема 6.3. Коди Ріда-Соломона. Еквівалентні двійкові коди Ріда-Соломона. [4, с. 142—145]	1.00
42.	Тема 6.4. Кодування загорткових кодів. Декодування загорткових кодів. Алгоритм Вітербі. [4, с. 145—151]	1.00
43.	Тема 6.5. Кодування у каналах із завмираннями. Код Фінка-Хагельбергера. Два способи приймання — в цілому, та поелементне. [4, с. 151—155]	1.00
44.	Тема 6.6. Потенційна завадостійкість кодів максимальної довжини при прийманні в цілому. Алгоритм швидкого кореляційного декодування m-кових циклічних кодів. [4, с. 155—160]	1.00
45.	Тема 6.7. Завадостійкість коректувальних кодів при прелементному прийманні. Використання кодів у системах із зворотним зв'язком. [4, с. 160—166]	1.00
46.	Розділ 7. Завадостійке кодування. Теоретичні границі коректувальних можливостей (за Мазурковим) Тема 7.1. Коректувальні коди. Загальні властивості [4, с. 104—106]	1.00
47.	Тема 7.2. Геометрична модель. Основні параметри коректувальних кодів [4, с. 106—110]	1.00
48.	Тема 7.3. Класифікація коректувальних кодів [4, с. 110—111]	1.00
49.	Тема 7.4. Границі коректувальних можливостей лінійних кодів (Суттєвість теореми кодування Шеннона для каналів із завадами. Верхня границя Хеммінга. Нижня границя Варламова-Гілберта.) [4, с. 111—114]	1.00
50.	Тема 7.5. Лінійні блокові коди. Декодування за методом синдрому (Алгебраїчний опис, кодування та декодування лінійних кодів. Коди Хеммінга. Границя Сінглтона.) [4, с. 114—119]	1.00
51.	Розділ 8. Основи теорії шифрування та дешифрування (за Склярром) Тема 8.1. Моделі, мета, початкові системи шифрування (Модель процесу шифрування та дешифрування. Задачі системи шифрування. Класичні загрози. Класичні шифри.) [1, с. 908—913]	1.00

52.	Тема 8.2. Секретність системи шифрування (Абсолютна секретність. Ентропія та невизначеність. Інтенсивність та надлишковість мови. Відстань єдності та ідеальна секретність.) [1, с. 913—920]	1.00
53.	Тема 8.3. Практична захищеність (Суміш та дифузія. Підстановка. Перестановка. Продукційний шифр. Стандарт шифрування даних.) [1, с. 920—931]	1.00
		0.00
	Розділ 9. Практичне шифрування та дешифрування (за Скляром)	
54.	Тема 9.1. Поточкове шифрування (Приклад генерування ключа з використанням лінійного регістру зсуву зі зворотним зв'язком. Слабкі місця регістру зсуву зі зворотним зв'язком. Синхронні та самосинхронізаційні системи поточного шифрування.) [1, с. 931—936]	1.00
55.	Тема 9.2. Криптосистеми з відкритим ключем (Перевірка справжності підпису з використанням системи з відкритим ключем. Одностороння функція з "лазіркою". Схема RSA. Задача укладання рюкзака. Криптосистема з відкритим ключем, яка заснована на "лазірці" в рюкзаку.) [1, с. 936—944]	1.00
56.	Тема 9.3. Система PGP ("Потрійний" DES, CAST та IDEA. Алгоритм Діффі-Хелмана і варіант Елгамала та RSA. Шифрування повідомлень в системі PGP. Аутентифікація за допомогою PGP і створення підпису.) [1, с. 944—955, 8]	1.00
57.	Тема 9.4. Підсумки (Література. Задачі. Питання для самоперевірки.) [1, с. 955—961]	0.00
	Розділ 10. Вступ до теорії криптографії (за Шнайєром)	
58.	Тема 10.1. Загальні поняття (Термінологія. Стеганографія. Підстановочні та перестановочні шифри. Просте XOR. Одноразові блокноти. Комп'ютерні алгоритми. Великі числа.) [5, с. 47—71]	2.00
	Розділ 11. Криптографічні протоколи (за Шнайєром)	
59.	Тема 11.1. Елементи протоколів. [5, с. 71—107]	2.00
60.	Тема 11.2. Основні протоколи. Проміжні протоколи. [5, с. 107—177]	2.00
61.		0.00
62.	Тема 11.3. Розвинуті протоколи. Езотеричні протоколи. [5, с. 177—241]	0.00
		0.00
	Розділ 12. Криптографічні методи (за Шнайєром)	
63.	Тема 12.1. Довжина ключа. Керування ключами [5, с. 241—293]	2.00
64.	Тема 12.2 Типи алгоритмів та криптографічні режими [5, с. 293—325]	2.00
65.	Тема 12.3. Використання алгоритмів [5, с. 325—347]	2.00
	Розділ 13. Криптографічні алгоритми (за Шнайєром)	
66.	Тема 13.1. Математичні основи [5, с. 347—389]	2.00
67.	Тема 13.2. Стандарт шифрування DES та інші блочні шифри. Об'єднання блочних шифрів. [5, с. 389—521]	2.00
68.	Тема 13.3. Генератори ПВП та справжніх ВП. Поточкові шифри. Однонаправлені хеш-функції. [5, с. 521—633]	2.00
69.	Тема 13.4. Алгоритми з відкритими ключами. Алгоритми ЕЦП. Схеми ідентифікації. Алгоритми обміну ключами. Спеціальні алгоритми для протоколів [5, с. 633—753]	2.00
	Разом	84.00
	Модульна контрольна робота (складається з 6 ТКР)	
70.	Тематична контрольна робота за розділом 1 (Moodle, Завдання 1 до МКР-1) [14]	1.00
71.	Тематична контрольна робота за розділом 4 (Moodle, Завдання 2 до МКР-1) [14]	1.00
72.	Тематична контрольна робота за розділом 5 (Moodle, Завдання 3 до МКР-1) [14]	1.00
73.	Тематична контрольна робота за розділом 9 (Moodle, Завдання 4 до МКР-1) [14]	1.00
74.	Тематична контрольна робота за розділом 12 (Moodle, Завдання 5 до МКР-1) [14]	1.00
75.	Тематична контрольна робота за розділом 13 (Moodle, Завдання 6 до МКР-1) [14]	1.00
	Разом МКР	6.00
76.	ДКР	6.00
	Всього	96.00

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

7.1. Відвідування занять

Лекції: відвідування занять за розкладом, також допускається вивчення матеріалу — самостійно, в дистанційному режимі. Для допомоги студентам в СДН <https://do.ipu.kpi.ua/course/view.php?id=451> містяться посилання на всі необхідні матеріали та відеозаписи всіх лекцій.

Лабораторні роботи: відвідування занять за розкладом. Під час виконання лабораторних робіт можливі ситуації, коли студент не встигає виконати роботу під час заняття. В такому випадку її необхідно виконати самостійно вдома в додатковий час, призначений викладачем. Для допомоги студентам в СДН <https://do.ipu.kpi.ua/course/view.php?id=451> містяться посилання на всі необхідні матеріали та відеозаписи всіх лабораторних занять.

Очні лекції та лабораторні заняття проводяться згідно Положення про організацію освітнього процесу КПІ ім. Ігоря Сікорського та можуть переводитися у дистанційний формат згідно тимчасових розпоряджень.

У разі хвороби студент зобов'язаний представляти довідку про термін проходження лікування, оформлену належним чином, з установи, де проходило лікування. Матеріал занять, які були з тих чи інших причин пропущені, необхідно опанувати самостійно.

7.2. Пропущені контрольні заходи

Подання результатів лабораторних робіт, ТКР (МКР) та ДКР є обов'язковим. Несвоєчасне подання дає нульову оцінку. У разі несвоєчасного подання з поважних причин (наприклад, хвороби), підтверджених відповідними документами, студент має можливість написати контрольний захід в інший узгоджений з викладачем термін без зниження оцінки. З метою самовдосконалення та покращення власних результатів допускається повторне виконання ТКР (МКР).

7.3. Оголошення результатів контрольних заходів

Результати виконання самостійних робіт проставляються в СДН Moodle і оголошуються кожному студенту окремо у присутності або у дистанційній формі та супроводжуються оціночними листами (в СДН Moodle), в яких студенти можуть побачити свою оцінку за певними критеріями, а також позначення основних помилок та коментарі до них.

7.4. Академічна доброчесність

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

7.5. Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

7.6. Процедура оскарження результатів контрольних заходів

Студенти мають можливість поставити будь-яке питання, яке стосується процедури проведення та/або оцінювання контрольних заходів, та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами.

Студенти мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оціночного листа та/або зауважень.

8. Види контролю та рейтингова система оцінювання результатів навчання (PCO)

Поточний контроль: виконання лабораторних робіт, домашньої контрольної роботи, написання модульної контрольної роботи.

Семестровий контроль: залік.

Пояснення до обліку успішності в СДН Moodle:

1. Облік виконання завдань та рейтинг студентів здійснюється в СДН Moodle <https://do.ipk.kpi.ua/course/view.php?id=451>. Студенти з першого дня вивчення дисципліни отримують доступ до всіх матеріалів курсу, в тому числі до правил рейтингової системи та власного журналу оцінок.

2. Рейтинг студента за дисципліну розраховується, виходячи із 100-бальної шкали (100% успішності)

$$R = R_s + R_c; R_{s \max} = 60; R_{c \max} = 40; R_m = 100.$$

де R_s — семестрова складова рейтингу, $R_{s \max}$ — максимальне можливе значення семестрової складової, R_c — складова рейтингу, отримана під час складання заліку (семестрового контролю), $R_{c \max}$ — максимальне можливе значення залікової складової, R — рейтинг студента за дисципліну, R_m — максимальне можливе значення рейтингу за дисципліну.

Семестрова складова рейтингу R_s складається з балів, які студент отримує за:

- виконання 9 лабораторних робіт (ЛР);
- виконання модульної контрольної роботи (МКР), яка складається з 6 тематичних контрольних завдань (ТКР);
- виконання домашньої контрольної роботи (ДКР);
- додаткової активності (розробки тестових питань до тем, які не охоплені ТКР/МКР).

3. Виконання, оформлення і захист звітів про виконання лабораторних робіт (ЛР) (комп'ютерних практикумів), що надають такі рейтингові бали успішності:

Повне виконання лабораторної роботи (комп'ютерного практикуму)	40%
Належне оформлення звіту відповідно до вимог	20%
Повна відповідь (не менше 90% потрібної інформації) під час захисту ЛР	40%
Всього	100%

Примітка:

Неповна відповідь (не менше 60% потрібної інформації та деякі помилки) або несвочасний захист ЛР	20%
Відповідь з істотними помилками	10%
Незадовільна відповідь	0%

Виконання тематичних та модульних контрольних робіт (ТКР та МКР) при ручному оцінюванні:

Повна відповідь (не менше 90% потрібної інформації)	95...100%
Достатньо повна відповідь (не менше 75% потрібної інформації або незначні неточності)	75...94%
Неповна відповідь (не менше 60% потрібної інформації та деякі помилки)	60...74%
Незадовільна відповідь	0...59%

Вклад в семестрову складову рейтингу окремих частин активностей:

за МКР (теоретичні заняття, шість ТКР)	20%
за ДКР (практична складова)	20%
за ЛР (дев'ять робіт)	45%
за додаткову активність (РТП)	5%
за поданням ДНВР	10%
Всього	100%

У випадку відсутності додаткової активності чи/та подання ДНВР відсотки вкладу за обов'язкові активності (ТКР/МКР, ДКР, ЛР) нормуються до $20\%+20\%+45\% = 85\%$.

5. Умовою допуску до заліку є зарахування всіх лабораторних робіт, ТКР/МКР, ДКР та стартовий рейтинг (семестровий рейтинг R_s) не менше 40% успішності (40 балів).

6. У випадку, якщо семестровий рейтинг R_s становить 60% і більше, студенти можуть отримати залік автоматично, або спробувати покращити свій рейтинг шляхом складання підсумкового тесту (піти на складання заліку).

7. Під час складання заліку студенти виконують підсумковий тест та отримують R_e — залікову складову рейтингу. В результаті бали семестрової та залікової складових рейтингу, визначені у відсотках успішності, складаються з ваговими коефіцієнтами відповідно до вказаних значень $R_{s \max}$ та $R_{e \max}$, що робиться у СДН Moodle автоматично.

8. Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

<i>Кількість балів</i>	<i>Оцінка</i>
100...95	Відмінно
94...85	Дуже добре
84...75	Добре
74...65	Задовільно
64...60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

Робочу програму навчальної дисципліни (Силабус):

Склали старший викладач кафедри радіоінженерії Павлов Олег Ігорович,

Ухвалено кафедрою радіоінженерії (протокол №06/2025 від 17.06.2025 р.).

Затверджено Методичною комісією РТФ (протокол №06/2025 від 26.06.2025 р.)