

Національний університет біоресурсів і природокористування України
Кафедра комп'ютерних систем, мереж та кібербезпеки

“ЗАТВЕРДЖУЮ”

Декан факультету інформаційних технологій



проф. О.Г. Глазунова
_____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем, мереж та кібербезпеки
Протокол № 10 від «17» травня 2023 р.

Касаткін Д.Ю.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП
«Кібербезпека»

Лахно В.А.
Гарант ОП
(проф. Лахно В.А.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

“Теорія інформацій та кодування”
зі спеціальності 125 – «Кібербезпека»
(шифр і назва напрямку підготовки)
Освітня програма «Кібербезпека»

факультет інформаційних технологій
(назва факультету)

Опис навчальної дисципліни
Теорія інформації та кодування
(назва)

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень		
Галузь знань	Інформаційні технології	
Спеціальність	125 – «Кібербезпека»	
другий (магістерський) рівень	Бакалавр	
Характеристика навчальної дисципліни		
Вид	Обов'язкова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	Іспит	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2023-2024	
Семестр	2	
Лекційні заняття	30 год.	
Практичні, семінарські заняття		
Лабораторні заняття	30 год.	
Самостійна робота	60 год.	
Індивідуальні завдання		
Кількість тижневих годин для денної форми навчання: аудиторних	4 год.	

1. Мета та завдання навчальної дисципліни

Мета - “Теорія інформації та кодування” полягає в ознайомленні студентів з теоретичними основами оцінки інформаційних процесів, організації ефективного завадостійкого кодування з виявленням і виправленням помилок, алгоритмів кодування та декодування даних, сучасних методів кодування даних в каналах зв'язку, а також отриманні студентами практичних навичок в створенні як апаратних так і програмних кодерів і декодерів з використанням сучасних програмних і апаратних засобів. Вивчаються: принципи та методи оцінки інформативності повідомлень, формування кодів та оцінки їх ефективності, завдання завадостійкого кодування, розробка апаратних та програмних кодерів-декодерів, сучасні методи кодування даних..

Основними завданнями вивчення дисципліни «Теорія інформації та кодування» є формування у студентів систематичних знань в області методів підвищення надійності зберігання та передачі даних; ознайомлення студентів з перспективними напрямками в області проектування високонадійних обчислювальних систем; ознайомлення студентів з питаннями побудови ефективних кодів, використовуваних для виявлення та виправлення помилок в кодових комбінаціях.

Місце і роль дисципліни в системі підготовки фахівців відповідно до навчального плану. Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області захисту інформації управляючих систем в різних

галузях, а також сприяє здачі єдиного державного кваліфікаційного іспиту зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти.

Вимоги щодо знань і вмінь, набутих внаслідок вивчення дисципліни

Внаслідок вивчення дисципліни студенти повинні:

знати основні поняття теорії кодування, класифікацію та характеристики кодів, використовуваних в обчислювальній техніці; основні принципи оптимального кодування повідомлень, основні алгоритми, які використовуються для стиснення даних, класифікацію перешкодостійких кодів, принципи їх побудови і використання для виявлення і виправлення помилок

вміти використовувати різні коди для представлення інформації і виконання різних арифметичних операцій із застосуванням зазначених способів кодування; використовувати різні методи побудови оптимальних кодів і їх використання для розробки і реалізації різних алгоритмів стиснення даних; використовувати принципи завадостійкого кодування для побудови кодів, що дозволяють виявляти і виправляти помилки різної кратності в кодових комбінаціях.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Знання та розуміння предметної області та розуміння професії.

КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові) компетентності:

СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів кодування.

СК3. Здатність до використання сучасних методів кодування в інформаційно-телекомунікаційних (автоматизованих) системах.

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК10. Здатність застосовувати методи та засоби завадостійкого кодування на об'єктах інформаційної діяльності.

СК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

СК13. Здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем захисту інформації пов'язаних з Perezдачою повідомлень .

В результаті вивчення навчальної дисципліни студент набере певні програмні результати, а саме:

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами кодування та Perezдачою повідомлень та давати оцінку результативності якості прийнятих рішень.

ПРН 19. Застосовувати теорії, методи та засоби кодування для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПРН 23. Реалізувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки.

ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання алгоритмів та методів кодування в умовах реалізації загроз різних класів.

ПРН 31. Застосовувати теорії та методи кодування для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

В контексті зазначених вище компетентностей та програмних результатів навчання задачі викладання дисципліни визначають необхідний комплекс знань і вмінь, що отримують студенти під час вивчення дисципліни.

Навчальна програма розрахована на здобувачів вищої освіти, які навчаються за освітньою програмою підготовки бакалаврів за спеціальністю 125 «Кібербезпека».

Робоча програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Навчальна програма з курсу «Теорія інформації та кодування» є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни «Теорія інформації та кодування» розроблена на підставі наступних документів:

-освітньо-професійна програма підготовки фахівців за спеціальністю «Кібербезпека»;

-навчальний план підготовки бакалаврів за спеціальністю «Кібербезпека».

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчення курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Теоретичною базою для вивчення курсу «Теорія інформації та кодування» є курси «Інформатика»; «Комп'ютерні системи»; «Безпека інформації в інформаційно-комунікаційних системах»; «Основи криптографічного та стеганографічного захисту інформації»; «Комп'ютерні мережі».

2. Програма навчальної дисципліни

Змістовий модуль №1. Основи теорії інформації.

Тема лекційного заняття 1. Предмет, методи і задачі дисципліни.

Поняття інформації, кількість інформації, ентропії, середня кількість інформації, пропускна здатність каналу для дискретних повідомлень.

Тема лекційного заняття 2. Визначення кількості інформації та ентропії

Фізична суть та міри інформації. Етапи проходження інформації. Інформаційна ентропія. Формула Шеннона. Визначення кількості інформації та ентропії за Хартлі, Шенноном та іншими оцінками

Тема лекційного заняття 3. Моделі сигналів.

Математичні моделі сигналів. Ортогональне зображення сигналів. Частотна форма зображення сигналів. Часова форма зображення сигналів.

Тема лекційного заняття 4. Цифрові системи передавання інформації.

Принципи побудови інформаційних систем. Ентропія джерел повідомлення. Загальні характеристики каналів зв'язку. Теорема Шеннона.

Змістовий модуль № 2. Ефективне та завадостійке кодування.

Тема лекційного заняття 5. Кодування інформації при передачі по дискретному каналу без перешкод

Технічні засоби кодування даних в дискретних каналах без перешкод. Способи подання кодів. Надмірність повідомлень і кодів. Основні теореми кодування для каналів без перешкод. Оптимальне кодування. Призначення і особливості рефлексних кодів. Код Грея: призначення, правила кодування та декодування.

Тема лекційного заняття 6. Ефективне кодування.

Ефективне кодування. Ефективне кодування Шеннона-Фано. Ефективне кодування Хаффмена. Порівняльна характеристика кодів. Префіксність кодів. Методи ефективного кодування корельованої послідовності.

Тема лекційного заняття 7. Лінійні групові коди.

Лінійні групові коди. Завадостійке кодування, поняття відстані Хемінга та визначення надлишковості коду на основі мінімальної відстані Хемінга та коректуючих властивостей коду. Загальна характеристика лінійних групових кодів. Коди Хемінга, методика їх побудови та виправлення помилок. Лінійні групові коди, методика їх побудови та виправлення помилок.

Тема лекційного заняття 8. Циклічні коди.

Неприводимі многочлени та побудова на їх основі циклічних кодів. Побудова циклічних кодів на основі утворюючої матриці. Принципи формування синдрому помилок в циклічних кодах. Побудова циклічних кодів шляхом множення на утворюючий многочлен. Виявлення та виправлення помилок в циклічних кодах.

Тема лекційного заняття 9. Недвійкові коди.

Надмірне кодування. Кодування з перевіркою парності. Кодова відстань по Хеммінгу. Кордон Хеммінга. Класифікація недвійкових кодів. Узагальнений код Хеммінга. Код Ріда-Соломона.

Тема лекційного заняття 10. Основи переведення даних в системі залишкових класів (СЗК) та навпаки.

Основи переведення даних в системі залишкових класів (СЗК) та навпаки. Типи кодувань в СЗК.

Тема лекційного заняття 11. Коди Галуа.

Методика побудови кодів Галуа.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Основи теорії інформації.												
Тема 1. Предмет, методи і задачі дисципліни.	12	2		2		8						
Тема 2. Визначення кількості інформації та ентропії.	12	2		2		8						
Тема 3. Моделі сигналів	12	2		2		8						
Тема 4. Цифрові системи передавання інформації.	10	2		2		6						
Разом за змістовим модулем 1	46	8		8		30						
Змістовий модуль 2. Ефективне та завадостійке кодування.												
Тема 5. Кодування інформації при передачі по дискретному каналу без перешкод.	8	2		2		4						
Тема 6. Ефективне кодування	8	2		2		4						
Тема 7. Лінійні групові коди	12	4		4		4						
Тема 8. Циклічні коди	12	4		4		4						
Тема 9. Недвійкові коди	12	4		4		4						
Тема 10. Основи переведення даних в системі залишкових класів (СЗК) та навпаки.	10	2		2		6						
Тема 11. Коди Галуа.	12	4		4		4						
Разом за змістовим модулем 2	74	22		22		30						
Усього годин за курс	120	30		30		60						

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Сигнали. Дослідження амплітудної модуляції	2
2.	Дослідження амплітудно-імпульсних модуляторів. Амплітудна та частотна маніпуляції.	2
3.	Дослідження основних інформаційних характеристик джерел повідомлень	2
4.	Спектральне представлення сигналів. Дослідження спектру сигналу при різній частоті його дискретизації	4
5.	Дослідження квантування сигналу за рівнем	4
6.	Перетворювачі інформації. Дослідження перетворювача коду в напругу	4
7.	Дослідження цифро-аналогових перетворювачів сходового типу	4
8.	Ефективне кодування з втратою інформації	4
9.	Дослідження та вивчення критеріїв оцінки завадостійкого кодування	4
	Разом за семестр	30
	Разом	30

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1.	Основні визначення, поняття і характеристики щодо систем передачі інформації.	3
2.	Властивості інформації як об'єкту захисту.	3
3.	Типова структура системи обміну інформацією.	3
4.	Процеси, які забезпечують передачу інформації, її доступність і цілісність.	3
5.	Математичні моделі повідомлень, сигналів та завад; їх характеристики.	3
6.	Векторне представлення повідомлень, сигналів та завад.	3
7.	Кореляційні характеристики сигналів і завад.	3
8.	Управління інформаційними параметрами сигналів: однократні та багатократні види модуляції.	3
9.	Роль складних сигналів у вирішенні задач забезпечення якості передачі та захисту інформації.	3
10.	Дискретні канали, їх математично-інформаційні моделі і характеристики.	3
11.	Безперервні канали, їх математично-інформаційні моделі і характеристики.	3
12.	Спотворення і завади в каналах та їх вплив на доступність і цілісність інформації.	3
13.	Власна та максимальна ентропія дискретного повідомлення.	3
14.	Пропускна здатність безперервних каналів; її вплив на доступність та скритність інформації.	3
15.	Алгоритм та структура оптимального демодулятора при когерентному прийомі двійкових сигналів.	4
16.	Показники якості і завадостійкість когерентного прийому двійкових сигналів з амплітудною, частотною та фазовою модуляціями.	4
17.	Шляхи підвищення завадостійкості, скритності та інших показників якості.	6
18.	Перспективи розвитку захищених інформаційних систем.	4
	Разом	60

9. Індивідуальні завдання (ПЕРЕЛІК ПИТАНЬ ДЛЯ САМОСТІЙНОЇ РОБОТИ)

1. Статистичні методи стиснення.
2. Метод Хафмена.
3. Арифметичне кодування.
4. Словникові методи стиснення.
5. Алгоритм LZ77.
6. Алгоритм LZSS.
7. Алгоритм LZ78.
8. Алгоритм LZW.
9. Стиснення зображень. Алгоритм RLE.
10. Диференціальне кодування.
11. Кольорові моделі. Алгоритм стиснення JPEG
12. Коди без пам'яті. Нерівність Крафта.
13. Теореми по символного нерівномірного кодування.
14. Оптимальні методи статистичного кодування Хафмена та Шеннона-Фано.
15. Коди з пам'яттю.
16. Метод блокування повідомлень.
17. Типи кодів.
18. Кодова відстань.

19. Властивості завадостійких кодів.
20. Код з перевіркою на парність.
21. Ітеративний код.
22. Твірна та перевірка на матриці лінійного блокового коду.
23. Кодовий синдром.
24. Арифметичне кодування.
25. Словникові методи стиснення Зіва-Лемпела.
26. Стиснення без втрат інформації.
27. Стиснення із втратами інформації.
28. Факсимільне стиснення.
29. Сучасні архіватори. Призначення, принципи побудови, характеристики. Програми-архіватори: WinZip, WinRAR.
30. Системи кольорів RGB, CMYK, HSB, LAB та їх використання для кодування кольорових зображень.
31. Коди Боуза – Чоудхурі – Хоквінгема.
32. Коди Галуа.
33. Коди Грея.
34. Коди в системі залишкових класів.
35. Завадостійке кодування інформації
36. Основні визначення крипто лінгвістики.
37. Лінгвістичні схеми у криптографії.
39. Ансамблі та джерела повідомлень.
40. Потенційна завадостійкість каналів зв'язку.
41. Коди, що виявляють помилки.
42. Коди, що виправляють помилки.
43. Інформаційні характеристики джерел повідомлень та каналів зв'язку.

10. Методи навчання

Проведення лекцій з використанням технічних засобів навчання. Проведення лабораторних робіт та самостійної роботи засобами інформаційно-комунікаційних технологій в освіті. Використовується електронний навчальний курс на платформі Moodle «Теорія інформації та кодування».

11. Форми контролю

Наприкінці кожного змістовного модуля проводиться контрольна робота у вигляді тесту, що створений у комп'ютерному навчальному середовищі. Підсумкова атестація: іспит.

12. Розподіл балів, які отримують студенти

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «ПОЛОЖЕННЯ про екзамени та заліки у НУБіП України» (наказ про уведення в дію від «26» квітня 2023 р. протокол № 10):

Рейтинг здобувача вищої освіти, бали	Оцінка національна за результати складання екзаменів заліків	
	Екзамен	Залік
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Для визначення рейтингу студента із засвоєння дисципліни $R_{\text{дис}}$ (до 100 балів) одержаний рейтинг з атестації $R_{\text{АТ}}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{\text{НР}}$ (до 70 балів): $R_{\text{дис}}=R_{\text{НР}}+R_{\text{АТ}}$.

Оцінка виконання та захисту лабораторних робіт за кожний модуль здійснюється у наступній відповідності:

№ лабораторної роботи	Кількість балів	Загальна кількість балів
1 модуль		
Лабораторна робота № 1	20	70
Лабораторна робота № 2	20	
Лабораторна робота № 3	20	
Лабораторна робота № 4	10	
Самостійна робота	10	
Модульна контрольна		20
2 модуль		
Лабораторна робота № 5	10	70
Лабораторна робота № 6	10	
Лабораторна робота № 7	10	
Лабораторна робота № 8	10	
Лабораторна робота № 9	30	
Модульна контрольна		20

13. Методичне забезпечення

1. Електронний навчальний курс на платформі Moodle вміщує повне методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо.

14. Рекомендовані джерела інформації

Базові

1. Жураковський Ю.П., Полторак В.П. Теорія інформації та кодування: Підручник.- К.:Вища школа, 2011. — 255 с.
2. Тулякова Н. О. Теорія інформації: Навчальний посібник. - Суми: Вид-во СумДУ, 2008.- 212 с.
3. Кулик А.Я., Кривогубченко С.Г. Теорія інформації і кодування / Навчальний посібник. – Вінниця: ВНТУ, 2008. - 145 с.
- 4.Теорія інформації та кодування : підручник для студ. ВНЗ / В.І. Барсов, В.А. Красобаєв, О.І. Тиртишніков та ін. - Полтава: ПолтНТУ, 2011. – 320 с.
5. Подлевський Б. М. Теорія інформації в задачах. Центр навчальної літератури. 2019. – 271 с.
- 6.Основи теорії інформації та кодування : підручник для студентів ВНЗ, які навчаються за напрямом підготовки "Радіоелектронні апарати", "Телекомунікації", "Комп'ютерна інженерія" / Іван Васильович Кузьмін, Іван Висильович Троцишин, Андрій Іванович Кузьмін. За ред. Івана Васильовича Кузьміна. – 3-те вид.– Хмельницький : ХНУ, 2009.– 373 с.
- 7.Подлевський Б. М. Теорія інформації : підручник / Б. М. Подлевський, Р. Є. Рикалюк. – Львів: Видавничий центр ЛНУ ім. І. Франка, 2016. – 342

Допоміжні

1.Бойко Ю. М. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад : монографія / Ю. М. Бойко, В. А. Дружинінін, С. В. Толюпа. - Київ : Логос, 2018. - 227 с.

15. Інформаційні ресурси

1. Project Jupyter | Home [Електронний ресурс]. – Режим доступу : <https://jupyter.org/> (дата звернення: 2021-10-27). – Назва з екрана.
2. GitHub - dit/dit: Python package for information theory. [Електронний ресурс]. – Режим доступу : <https://github.com/dit/dit> (дата звернення: 2021- 10-27). – Назва з екрана.
3. dit: discrete information theory — dit 1.2.3 documentation [Електронний ресурс]. – Режим доступу : <http://docs.dit.io/en/latest/> (дата звернення: 2019-10-27). – Назва з екрана.
4. Signalprocessing (scipy.signal) — SciPy v1.3.1 ReferenceGuide [Електронний ресурс]. – Режим доступу : <https://docs.scipy.org/doc/scipy/reference/signal.html> (дата звернення: 2021- 10-27). – Назва з екрана.
5. PythonTutorial - SignalProcessingwithNumPyarraysiniPython - 2018 [Електронний ресурс]. – Режим доступу : https://www.bogotobogo.com/python/OpenCV_Python/python_opencv3_NumPy_Arrays_Signal_Processing_iPython.php (дата звернення: 2021-10-27). – Назва з екрана.
6. Plotting a Spectrogramusing Python and Matplotlib | Pythontic.com [Електронний ресурс]. – Режим доступу : <https://pythontic.com/visualization/signals/spectrogram> (дата звернення: 2021-10-27). – Назва з екрана.
7. Overview — NumPy v1.17 Manual [Електронний ресурс]. – Режим доступу : <https://docs.scipy.org/doc/numpy/index.html> (дата звернення: 2021-10-27). – Назва з екрана.

16. Нормативна література

1. ДСТУ ISO/IEC 11770-3:2002 «Інформаційні технології. Методи захисту».
2. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
3. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.