



ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ (ФІС)

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

1. Загальна інформація про дисципліну:

Назва дисципліни	ОСНОВИ ТЕОРІЇ ІНФОРМАЦІЇ
Викладач	Приймак Микола Володимирович
Профайл викладача	https://tntu.edu.ua
Контактний тел.	Комутатор (0352) 51-97-00, внутрішній 1706 (із зовнішніх телефонів через комутатор, тоді в режимі тонального набору набрати внутрішній номер), 380931688324
E-mail:	pmw.ukr@ukr.net
Сторінка дисципліни в A-Tutor	https://dl.tntu.edu.ua , ID1493
Консультації	Згідно графіку консультацій у другому семестрі

2. Коротка анотація до дисципліни

Навчальна дисципліна «**Основи теорії інформації**» належить до вибіркових дисциплін циклу професійної підготовки освітньої програми «Інформаційні системи та технології» першого (бакалаврського) рівня вищої освіти. Галузь знань 12 «Інформаційні технології», спеціальності 126 «Інформаційні системи та технології». Викладається у 4 семестрі (другий курс) обсягом 6,0 кредитів ECTS. Формою підсумковою контролю є екзамен.

3. Мета та завдання дисципліни

Мета дисципліни «Основи теорії інформації» – сформувати теоретичні знання і практичні навички щодо кількісної оцінки інформації, методів її кодування та захисту. Під час освоєння дисципліни студентом вивчаються три основних розділи теорії інформації. 1) Поняття невизначеності та одиниця її вимірювання – БАЙТ; інформація як засіб ліквідації невизначеності. 2) Кодування інформації та швидкість її передачі каналами зв'язку. 3) Криптологія та шифрування інформації, поняття кеш-функції та цифрового підпису.

Завданням дисципліни є оволодіння студентом основних понять теорії інформації, методами її кодування, шифрування та дешифрування.

4. Формат дисципліни:

Дисципліна передбачає проведення лекційних, лабораторних занять та консультацій. Для кращого розуміння та засвоєння викладеного матеріалу дисципліна має супровід у вигляді електронного навчального курсу в системі A-Tutor (<https://dl.tntu.edu.ua>). Електронний навчальний курс має лекційний матеріал, лабораторні роботи, питання підсумкового контролю та систему оцінювання.

5. Результати навчання:

В результаті вивчення дисципліни студент повинен **знати**:

- ✓ складові світобудови, третьою з яких є інформація;
- ✓ основну властивість повсякденного життя – невизначеність;
- ✓ засіб ліквідації невизначеності – інформація;
- ✓ підхід Хартлі до вимірювання невизначеності (ентропії) та формулу Хартлі;
- ✓ підхід Шеннона до вимірювання невизначеності (ентропії) та формулу Шеннона;
- ✓ поняття одиниці міри невизначеності – байт;
- ✓ основні властивості ентропії незалежних подій;
- ✓ основні властивості ентропії залежних подій;

- ✓ визначення інформації як різницю ентропії на вході каналу зв'язку та на його виході.
- ✓ основні методи кодування;
- ✓ проблеми та задачі захисту інформації;
- ✓ основні терміни захисту інформації; криптологія, криптографія, криптоаналіз, шифр, ключ, хеш-функція, цифровий підпис;
- ✓ класифікація шифрів в їх історичному розвитку;
- ✓ основні класичні шифри;
- ✓ шифри перестановки та заміни;
- ✓ симетричні та несиметричні шифри;
- ✓ шифр RSA;
- ✓ поняття та кеш-функції та її формування;
- ✓ поняття та цифрового підпису та його створення (формування).

В результаті вивчення дисципліни студент повинен **вміти**:

- ✓ знаходити величину невизначеності за формулою Хартлі;
- ✓ знаходити величину невизначеності за формулою Шеннона;
- ✓ здійснювати побудову кодів букв алфавіту методом Шеннона-Фано;
- ✓ здійснювати побудову кодів букв алфавіту методом Хафмана;
- ✓ знаходити середню довжину кодів букв алфавіту, порівнювати її (довжину) з ентропією алфавіту та вносити відповідні пропозиції;
- ✓ шифрувати повідомлення (інформацію) з використанням шифру Цезаря;
- ✓ шифрувати повідомлення (інформацію) з використанням шифру Віженера;
- ✓ шифрувати повідомлення (інформацію) з використанням шифру RSA;
- ✓ створювати хеш-функцію повідомлення;
- ✓ створювати цифровий підпис на основі шифру RSA;

Вивчення навчальної дисципліни передбачає формування та розвиток у студентів **загальних компетентностей (КЗ) та спеціальних (фахових) компетентностей (КС)** згідно освітньої програми.

Загальні:

- ЗК 1.** Здатність до абстрактного мислення, аналізу та синтезу;
- ЗК 2.** Здатність застосовувати знання у практичних ситуаціях;
- ЗК 3.** Здатність до розуміння предметної області та професійної діяльності;
- ЗК 5.** Здатність вчитися і оволодівати сучасними знаннями;
- ЗК 6.** Здатність до пошуку, оброблення та узагальнення інформації з різних джерел.

Спеціальні (фахові):

- КС 1.** Здатність аналізувати об'єкт проектування або функціонування та його предметну область;
- КС 11.** Здатність до аналізу, синтезу і оптимізації інформаційних систем та технологій з використанням математичних моделей і методів;
- КС 12.** Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет);
- КС13.** Здатність проводити обчислювальні експерименти, порівнювати результати експериментальних даних і отриманих рішень;
- КС 14.** Здатність формувати нові конкурентоспроможні ідеї й реалізовувати їх у проектах (стартапах).

Вивчення навчальної дисципліни передбачає формування у студента таких **прикладних результатів навчання (ПР)** згідно освітньої програми:

- ПР 1.** Знати лінійну та векторну алгебру, диференціальне та інтегральне числення, теорію функцій багатьох змінних, теорію рядів, диференціальні рівняння для функції однієї та багатьох змінних, операційне числення, теорію ймовірностей та математичну статистику в обсязі, необхідному для розробки та використання інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.
- ПР 4.** Проводити системний аналіз об'єктів проектування та обґрунтовувати вибір структури, алгоритмів та способів передачі інформації в інформаційних системах та технологіях;

ПР 7. Обґрунтовувати вибір технічної структури та розробляти відповідне програмне забезпечення, що входить до складу інформаційних систем та технологій.

ПР 10. Розуміти і враховувати соціальні, екологічні, етичні, економічні аспекти, вимоги охорони праці, виробничої санітарії, пожежної безпеки та існуючих державних і закордонних стандартів під час формування технічних завдань та рішень;

ПР 11. Демонструвати вміння розробляти техніко-економічне обґрунтування розроблення інформаційних систем та технологій та вміти оцінювати економічну ефективність їх впровадження.

6. Обсяг дисципліни

Вид заняття	Загальна кількість годин
лекції	36
лабораторні заняття	54
самостійна робота	90
Всього за дисципліну	180

7. Ознаки дисципліни:

Рік викладання	Семестр	Курс	Спеціальність	Нормативна/ вибіркова
2020	4	2	122 «Комп'ютерні науки»	Вибіркова
2020	4	2	126 «Інформаційні системи та технології»	Вибіркова

8. Пререквізити

Студенти повинні володіти базовими знаннями теорії ймовірностей і математичної статистики, програмування.

9. Технічне й програмне забезпечення /обладнання:

Студент повинен мати рівень впевненого користувача прикладних програм пакету Microsoft Office 365, графічних редакторів (CorelDRAW тощо).

10. Політика дисципліни

Усі процедури навчального процесу під час викладання дисципліни відповідають положенню про академічну доброчесність учасників освітнього процесу та недопущення академічного **плагіату** (укр.: **злодійства**) в Тернопільському національному технічному університеті імені Івана Пулюя.

11. Схема дисципліни

Тиж./ дата/ год.	Тема, підтеми	Форма заняття, формат	Матеріали	Література, ресурси в інтернеті	Завдання, год	Засоби діагностики	Вага оцінки
1	2	3	4	5	6	7	8

Тиж. 1/ 11.02/ 2 акад. год.	Тема 1. Інтуїтивне поняття інформації. Інформація як третя складова основ світобудови. Аспекти інформації: соціальний, релігійний, філософський, політичний, економічний, військовий, моральний (думка говорить одне, а совість інше). Невизначеність. Гра «Бар-Кохба» як шлях подолання невизначеності. Зв'язок між невизначеністю та інформацією.	Лекція 01 Лаб. р. № 1	Лекц. мат.	Дистанц. курс	Опрацюв лек. 4	Експрес-тестування	
Тиж. 2/ 18.02/ 2 акад. год.	Тема 2. Формула Хартлі. Гра про відгадування задуманого числа та її зв'язок з інформацією. Способи (методи) відгадування. Оптимальний спосіб відгадування. Формула Хартлі як міра невизначеності.	Лекція 02 Лаб. р. № 1	Лекц. мат., лаб. р. № 1	Дистанц. курс	Опрацюв. лек. 4	Експрес-тест.	
Тиж. 3/ 25.02/ 2 акад. год.	Тема 3. Формула Шеннона. Невизначеність та ентропія. Сукупність подій (повідомлень) та ймовірності їх появи. Випадкова величина як модель сукупності подій. Формула Шеннона. Приклади. Зв'язок формули Хартлі і Шеннона. Невизначеність та ентропія. Визначення біта як одиниці міри невизначеності.	Лекція 03 Лаб. р. № 2	Лекц. мат., лаб. р. № 2	Дистанц. курс	Опрацюв лек. 4 лаб. р. 2	Експрес-тест. захист лаб. р.	2
Тиж. 4/ 03.03/ 2 акад. год.	Тема 4. Ентропія сукупності подій. Ентропія незалежних випадкових величин. Приклади. Ентропія залежних випадкових величин. Приклади. Ентропія українського алфавіту: статистично-ймовірнісний метод (алгоритм) її визначення.	Лекція 04 Лаб. роб. № 2	Лекц. матер., лаб. р. № 2	Дистанц. курс	Опрац. лек. 4 лаб. р. 2	Експрес-тест.	
Тиж. 5/ 10.03/ 2 акад. год.	Тема 5. Математична модель каналу зв'язку. Канальні матриці. Канальна матриця вхідного і вихідного алфавітів каналу зв'язку. Канальні матриці із сторони джерела інформації та із сторони прийому інформації. Умовна ентропія вхідного алфавіту каналу зв'язку та ентропія вихідного алфавіту.	Лекція 05 Лаб. роб. № 3	Лекц. матер., лаб. р. № 3	Дистанц. курс	Опрац. лек., 4 лаб. р. 2	Експрес-тест захист лаб. р.	5
Тиж. 6/ 17.03/ 2 акад. год.	Тема 6. Кількість інформації. Ентропія сукупності вхідного і вихідного алфавітів канальної матриці. Прикладд. Кількість інформації як різниця безумовної і умовної ентропій вхідного і вихідного алфавіту (повідомлення) каналу зв'язку.. Приклади.	Лекція 06	Лекц. матер., лаб. р. № 3	Дистанц. курс.	Опрац. лек., 4 лаб. р. 10	Експрес-тест	

Тиж. 7/ 24.03/ 2 акад. год.	Тема 7. Код та кодування інформації. Приклади кодів і кодування в повсякденному житті та в різноманітних сферах людської діяльності. Основна причина виникнення необхідності кодування. Каналі зв'язку для передачі інформації. Приклади. Елементарні сигнали (букви), придатні для передачі каналом зв'язку. Приклади. Узгодження елементарних букв для кодування із властивостями каналів зв'язку. Визначення термінів код та кодування.	Лекція 07 Лаб. роб. № 3	Лекц. матер., лаб. р. № 3	Дистанц. курс	Опрац. лек., 4 лаб. р. 10	Експрес-тест	
Тиж. 8/ 31.03/ 2 акад. год.	Тема 8 Коди та їх класифікація. Двійковий, трійковий, R -ковий коди. Їх переваги та недоліки. Рівномірний та нерівномірний коди. Код Бодоо та код Морзе. Код Шеннона-Фано. Код Хафмана.. Середня довжина коду. Приклад.	Лекція 08	Лекц. Матер., лаб. р. № 3	Дистанц. курс	Опрац. лек., 4 лаб. р. 4	Експрес-тест	
Тиж. 9/ 7.04/ 2 акад. год.	Тема 9. Кодування із виправленням помилок. Коди із виявленням та виправленням помилок: однієї помилки. Код із виправленням до однієї помилки. Приклад. Код із виявленням та виправленням до двох помилок. Приклад.	Лекція 09 Лаб. роб. № 4	Лекц. матеріал, лаб. р. № 4	Дистанц. курс	Опрац. лек., 4 лаб. р. 6	захист лаб. р.	5
					Тест. завд. модуля 1, 30	Модульний контроль 1	25
Тиж. 10/ 14.04/ 2 акад. год.	Тема 10. Дискретизація та квантування сигналів. Теорема Найквіста-Котельникова. Спектр неперервного сигналу та вибір кроку дискретизації. Приклад.	Лекція 10	Лекц. матер., лаб. р. № 4	Дистанц. курс	Опрац. лек., 4 лаб. р. 4	Експрес-тест	
Тиж. 11/ 21.04/ 2 акад. год.	Тема 11. Коливні процеси як носії передачі сигналів. Математичний маятник та маятник поздовжніх коливань. Акустичні коливання. Рівняння Максвелла та електромагнітні коливання.	Лекція, F2F Лаб. роб. № 5	Лекц. матер., лаб. р. № 5	Дистанц. курс	Опрац. лек., 4 лаб. роб., 4	Каhoot!, захист звіту з лаб. роб.	3
Тиж. 12/ 28.04/ 2 акад. год.	Тема 12. Швидкість передачі інформації. Амплітудна, частотна та фазова модуляції електромагнітних коливань. Тривалість елементарного сигналу 2-ГО, 3-ГО, R -ГО КОДІВ. Швидкість передачі сигналів.	Лекція 12	Лекц. матер., лаб. р. № 5	Дистанц. курс	Опрац. лек., 4 лаб. р. 4	Експрес-тест	

Тиж. 13/ 5.05/ 2 акад. год.	Тема 13. Криптологія. Загальні поняття. Загальні поняття криптології та її складових – криптографії (шифрування) і криптоаналізу (дешифрування). Основні термінологічні поняття (визначення) криптології.	Лекція 13 Лаб. роб. № 6	Лекц. матер., лаб. р. № 6	Дистанц. курс	Опрац. Лек., 4 лаб. роб., 4	Kahoot!, захист звіту з лаб. роб.	2
Тиж. 14/ 12.05/ 2 акад. год.	Тема 14. Загальна задача та схема захисту інформації. Історичні приклади шифрів (тайно передачі). Загальна задача та схема захисту інформації. Шифр «Сцیتال»». Шифр Цезаря. Шифр (квадрат) Полібія. . Шифр Віженера. Шифр «решітка». (Кардано). Шифр частоколу. Шифр масонів. Стеганографія. Історичні приклади стеганографії.	Лекція 14	Лекц. матер., лаб. р. № 6	Дистанц. курс	Опрац. лек., 4 лаб. р. 4	Експрес-тест	
Тиж. 15/ 19.05/ 1 акад. год.	Тема 15. Шифри із симетричним ключем. Шифр DSA. Класифікація шифрів. Копм'ютерна криптографія. Шифри із симетричним ключем. Шифр DSA.	Лекція, 15	Лекці. матер., лаб. р. № 6	Дистанц. курс	Опрац. лек., 2	Експрес-тест	
Тиж. 16/ 26.05/ 1 акад. год.	Тема 16. Шифри із асиметричним ключем. Шифр RSA. Загальна схема шифрування RSA. Формування ключа шифру RSA. Алгоритм шифрування тексту в шифрі RSA. Алгоритм дешифрування тексту в шифр RSA.	Лекція 16	Лекці. матер., лаб. р. № 6	Дистанц. курс	Опрац. лек., 4 лаб. р. 4	Експрес-тест	
Тиж. 17/ 02.06/ 1 акад. год.	Тема 17. Хеш-функція. Цифровий підпис. Поняття хеш-функцій. Алгоритм утворення хеш-функції. Цифровий підпис в системі RSA.	Лекція 17	Лекц. мат., лаб. р. № 6	Дистанц. курс	Опрац. лек., 2	Експрес- тест	
Тиж. 18/ 09.06/ 2 акад. год.	Тема 18. Основні задачі та методи дешифрування.	Лекція 18 Лаб. роб. № 7	Лекц. матер., лаб. р. № 7	Дистанц. курс	Опрац. л., 4 лаб. роб., 4	Експ.-тест захист звіту з лаб. роб.	5
					Тест. завд. модуля 2, 30	Модульний контроль 2	25

12. Система оцінювання та вимоги

Форма підсумкового семестрового контролю – залік.

Підсумкова семестрова оцінка заліку складається з суми балів, отриманих студентом при проведенні проміжних (модульних) контролів рівня засвоєння теоретичних знань (за перший та другий модулі) та отриманих балів за лабораторні роботи.

МОДУЛЬ 1			МОДУЛЬ 2			ПІДСУМКОВА СЕМЕСТРОВА ОЦІНКА	РАЗОМ З ДИСЦИПЛІНИ
АУДИТОРНА ТА САМОСТІЙНА РОБОТА			АУДИТОРНА ТА САМОСТІЙНА РОБОТА				
ТЕОРЕТИЧНИЙ КУРС (ТЕСТУВАННЯ)	ЛАБОРАТОРНА РОБОТА		ТЕОРЕТИЧНИЙ КУРС (ТЕСТУВАННЯ)	ЛАБОРАТОРНА РОБОТА			
СЕМЕСТРОВА ОЦІНКА						25	100
19	21		19	16			
№ ЛЕКЦІЇ (ТЕМИ)	ВИД РОБІТ	БАЛ	№ ЛЕКЦІЇ (ТЕМИ)	ВИД РОБІТ	БАЛ	за кожних три бали семестрової оцінки студент отримує 1 бал підсумкової	
Лекція 1	Лаб. роб. №1	3	Лекція 10	Лаб. роб. №8	4		
Лекція 2	Лаб. роб. №2	3	Лекція 11	Лаб. роб. №9	4		
Лекція 3	Лаб. роб. №3	3	Лекція 12	Лаб. роб. №10	4		
Лекція 4	Лаб. роб. №4	3	Лекція 13	Лаб. роб. №11	4		
Лекція 5	Лаб. роб. №5	3	Лекція 14				
Лекція 6	Лаб. роб. №6	3	Лекція 15				
Лекція 7	Лаб. роб. №7	3	Лекція 16				
Лекція 8			Лекція 17				
Лекція 9			Лекція 18				
Лекція 10							
Лекція 11							
Лекція 12							
Лекція 13							
19		215	19		16		

До підсумкового семестрового контролю (складання семестрового заліку) допускаються студенти, які протягом семестру виконали всі види навчальної роботи, успішно пройшли проміжні (модульні) контролю і набрали не менше 45 балів семестрової бальної оцінки та за умови отримання не менше 60% (15) балів за результатами кожного проміжного (модульного) контролю рівня знань.

Підсумкова оцінка записується за 100-бальною шкалою із подальшим переведенням її у шкалу Європейської кредитно-трансферної системи (ECTS) відповідно А, В, С, D, E, F, FX при цьому чотирибальна шкала оцінок (з записом семестрової оцінки «відмінно» - А, «добре» - В,С, «задовільно» - D, E відповідають підсумковому результату «зараховано», «незадовільно» - F, FX відповідає підсумковому результату «незараховано»).

13. Навчально-методичне забезпечення

1. Конспект лекцій з курсу «Основи теорії інформації» для здобувачів освітнього ступеня «бакалавр», спеціальностей: 122 «Комп'ютерні науки», 126 «Інформаційні системи та технології», всіх форм навчання. Автори М.В.Приймак, Л.П.Дмитроца. – ТНТУ, 2019 р
2. Методичні вказівки до виконання лабораторних робіт з дисципліни «Основи теорії інформації» для здобувачів освітнього ступеня «бакалавр», спеціальностей: 122 «Комп'ютерні науки», 126 «Інформаційні системи та технології», всіх форм навчання. Автори М.В.Приймак, Л.П.Дмитроца. – ТНТУ, 2019 р.

14. Рекомендована література

Базова

1. Яглом А.М., Яглом И.М. Вероятность и информация. – М.: Наука, 1973. – 512 с.
2. Хинчин А.Я. Понятие энтропии в теории информации. // УМН. – 1953. – Т. 8, вып. 3 (55). – С.3-20.
3. Колмогоров А.Н. Теория информации и теория алгоритмов. М.: Наука, 1987. – 304 с.
4. Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования. Киев: Вища школа, 1977. – 280 с.
5. Цымбал В.П. Теория информации и кодирования. - 4-е изд., перераб. и доп. – К.: Вища школа, 1992. – 263 с.
6. Хинчин А.Я. Об основных теоремах теории информации // УМН, – 1956. –Т.11, вып. 1 (67). – С. 17-75.
7. Бабак В.П., Ключников А.А. Теоретические основы защиты информации. – Чернобыль (Киев. обл.): Институт проблем безопасности АЭС, 2012. – 776 с.
8. Шеннон Р. Математическая теория связи / Работы по теории вероятностей и кибернетике. М.: Иностранная литература, 1963. – 829 с. / С. 243-332.
9. Боровков А.А. Теория вероятностей. – М.: Эдиториал УРСС, 1999. – 472 с.

Допоміжна література.

1. Агидеев М.Г. Введение в криптографию. – Ростов-на-Дону: Ростовский гос. университет, 2003. – 35 с. (Шифрування + Гамування + RSA)
2. Андреева Е.Б., Босова Л.Л., Филина И.Н. Математические основы информатики. – М.: БИНОМ. Лаборатория знаний, 2005. – 328 с. (Під код 32 біти + Кодування зображень).
3. Хемминг Р.В. Теория кодирования и теория информации. М.: Радио и связь, 1983. – 1765 с.
4. Тарасов Л.В. Закономерности окружающего мира. В 3 кн. Кн 2. Вероятность в современном обществе. М.: Физматлит, 2004. – 360 с.
5. Игнатов В.А. Теория информации и передачи сигналов. М.: Сов. радио, 1979. – 280 с.

15. Інформаційні ресурси

1. <http://dl.tntu.edu.ua> Електронні навчальні курси ТНТУ імені І. Пулюя.