Силабус освітнього компонента
Програма навчальної дисципліни

Теорія інформації і кодування

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320

Спеціалізація
-

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
1

Мова викладання
Українська

Викладачі, розробники

АКСЬОНОВА Ірина Вікторівна

Iryna.Aksonova@khpi.edu.ua
Кандидат економічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 150, з них свідоцтв на авторський твір - більше 15, розділів у монографіях - 10, статей, що реферуються у науково метричних базах Scopus та WoS - 9. Лектор з дисциплін: "Штучний інтелект і бізнес-аналітика", "Теорія інформації і кодування", "Технологія управління безпекою бізнес-процесів, "Агентне моделювання" та інших у студентів бакалавріата та магістратури.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

У межах даної дисципліни здобувачі вищої освіти вивчають процеси зберігання, перетворення і передачі інформації а також властивості кодів та їхньої придатності для вирішення специфічних задач. Крім того, студенти опановують методи визначення пропускної здатності каналів зв'язку, достатньої для передачі всієї інформації, що надходить без затримок і спотворень; вивчають основні алгоритми побудови різних кодів, використовуваних як для захисту даних, так і для їх стиснення.

Мета та цілі дисципліни

Метою дисципліни «Теорія інформації і кодування» є ознайомлення з технологіями роботи з інформацією; формування знань та вмінь потрібних для використання моделей і методів

перетворення повідомлень і сигналів; обробки та захисту інформації при наявності завад, побудови кодів, управління потоками в інформаційних мережах.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
СК1. Здатність використовувати безпекові режими під час виконання службових обов'язків.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.
СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
СК6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.
СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
СК9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.
СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
РН4. Вільно спілкуватися державною мовою.
РН5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.
РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
РН8. Вміти використовувати сучасне програмно апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
РН9. Вміти використовувати безпекові режими під час виконання службових обов'язків.
РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
РН12. Вміти використовувати програмні та програмно апаратні комплекси захисту інформаційних ресурсів.
РН13. Вміти вирішувати задачі забезпечення та супроводу (в. т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно комунікаційних системах.
РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності. РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Іноземна мова, Математичні основи криптології.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Математичні основи теорії інформації. Теоретико-ймовірнісні основи теорії інформації. Випадкові величини та їх розподіли. Математичне сподівання, дисперсія та їх роль у вимірюванні інформації. Математичні моделі джерела інформації. Основні поняття теорії множин та комбінаторики для задач кодування.	4
Тема 2. Інформація та її кількісні оцінки. Ентропія джерела інформації. Поняття інформації в класичному та сучасному розумінні. Оцінка кількості інформації: міра Хартлі, міра Шеннона. Ентропія як міра невизначеності. Властивості ентропії. Надлишковість повідомлень і її практичне значення.	4
Тема 3. Ефективне кодування та стиснення даних. Принципи побудови кодів без втрат. Коди префіксного типу. Алгоритм Хаффмана. Алгоритм Шеннона–Фано. Методи стиснення з втратою інформації. Практичні приклади стиснення тексту, зображень і аудіо.	4
Тема 4. Інформаційні характеристики каналів зв'язку. Канал зв'язку та його основні параметри. Ймовірність помилок у каналі зв'язку. Пропускна здатність каналу. Теорема Шеннона про пропускну здатність.	4

Канали з шумами та без шумів. Баланс між швидкістю передачі та надійністю.	
Тема 5. Принципи та методи завадостійкого кодування. Загальні принципи завадостійкості. Виявлення та виправлення помилок. Методи побудови завадостійких кодів. Лінійні коди. Коди Хеммінга. Мінімальна кодова відстань та її значення.	6
Тема 6. Циклічні коди. Методи кодування та декодування. Визначення та властивості циклічних кодів. Поліноміальне представлення кодів. Генераторні та перевірочні багаточлени. Алгоритми побудови циклічних кодів. Методи декодування циклічних кодів. Приклади використання CRC у сучасних комунікаційних системах.	4
Тема 7. Аналітичні та математичні методи теорії інформації. Основні поняття: інформація, кількість інформації. Аналітичні методи в теорії інформації. Ентропія та надійність пароля. Взаємна інформація та її схема. Математичні методи в теорії інформації. Теорія ймовірностей, теорія кодування, середня довжина коду, надлишковість, канальна модель Шеннона, ємність каналу, міра невизначеності джерела.	6
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. . Математичні основи теорії інформації. Вирішення завдань на подання числової інформації в різних системах числення.	6	0,15
Тема 2. . Інформація та її кількісні оцінки. Ентропія джерела інформації. Вирішення завдань на характеристики дискретного каналу передавання інформації.	6	0,15
Тема 3. Ефективне кодування та стиснення даних. Вирішення завдань на використання статистичних методів стиснення інформації.	5	0,15
Тема 4. Інформаційні характеристики каналів зв'язку. Вирішення завдань на інформаційні характеристики каналів зв’язку.	5	0,15
Тема 5. Принципи та методи завадостійкого кодування. Класифікація кодів. Вирішення завдань на визначення критеріїв оцінки завадостійкого кодування.	5	0,15
Тема 6. Циклічні коди. Методи кодування та декодування. Вирішення завдань на коди Ріда-Соломона та їх використання в кодуванні й декодуванні.	5	0,15
Тема 7. Аналітичні та математичні методи теорії інформації. Підсумкові заняття, контрольне опитування.	4	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 1$

Контрольні роботи

За наявності

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Інформація, ентропійні міри та ефективне кодування в теорії інформації. Питання охоплюють матеріал за темами 1-4.	0,5
Тема 2. Методи та класифікація завадостійких кодів: блокові, згорткові та циклічні коди. Питання охоплюють матеріал за темами 5-7.	0,5
Загалом	$\sum_{i=1}^{m} b_i=1$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу, підготовка до лабораторних занять, контрольних робіт та екзамену.

Опрацювання теоретичного матеріалу

Теми самостійного вивчення	Кількість годин
Тема 1. Математичні основи теорії інформації. Історичні етапи становлення теорії інформації (Гартлі, Шеннон, Колмогоров). Використання теорії чисел у криптографії (прості числа, модульна арифметика). Асиметричні системи числення (залишкові класи, китайська теорема про залишки). Представлення інформації у квантових системах (кубіти як аналог двійкових розрядів).	12
Тема 2. Інформація та її кількісні оцінки. Ентропія джерела інформації. Алгоритмічна міра інформації (Колмогоровська складність). Взаємна інформація та її застосування у теорії зв'язку. Перехресна ентропія та відстань Кульбака–Лейблера. Ентропійні критерії у машинному навчанні (інформаційний виграш).	12
Тема 3. Ефективне кодування та стиснення даних. Методи стиснення мультимедійних даних (JPEG, MPEG, MP3) — принципи і відмінності. Адаптивні методи кодування. Використання кодів у криптографічних протоколах (стеганографія, приховане кодування). Порівняння ефективності сучасних алгоритмів стиснення.	14
Тема 4. Інформаційні характеристики каналів зв'язку. Математичне моделювання завад (білий шум, гаусівські та імпульсні завади). Канали з пам'яттю та марковські моделі передачі. Використання кодів корекції помилок (LDPC, Turbo, Polar codes). Інформаційні характеристики квантових каналів (ентанґлмент, квантова пропускна здатність).	12
Тема 5. Принципи та методи завадостійкого кодування. Класифікація кодів. Еволюція завадостійкого кодування: від класичних до сучасних кодів (LDPC, Turbo, Polar). Порівняння застосування згорткових та блокових кодів у мобільних мережах 5G/6G. Використання кодової відстані для оцінки стійкості криптографічних систем. Методи візуалізації процесів кодування та декодування (треєкові діаграми, графові структури). Роль завадостійких кодів у протоколах автентифікації та цифрового підпису.	12
Тема 6. Циклічні коди. Методи кодування та декодування. Еволюція завадостійкого кодування: від класичних до сучасних кодів (LDPC,	12

Turbo, Polar). Порівняння застосування згорткових та блокових кодів у мобільних мережах 5G/6G. Використання кодової відстані для оцінки стійкості криптографічних систем. Методи візуалізації процесів кодування та декодування (треєкові діаграми, графові структури). Роль завадостійких кодів у протоколах автентифікації та цифрового підпису.	
Тема 7. Аналітичні та математичні методи теорії інформації. Використання ентропії для оцінки стійкості сучасних криптографічних протоколів. Зв'язок інформаційної ємності каналу з пропускною здатністю систем кіберзахисту. Адаптація моделей Шеннона для аналізу мереж із криптографічним захистом. Використання математичних методів (теорія графів, матричний аналіз) у сучасній теорії кодування. Роль надлишковості у виявленні прихованих каналів витоку інформації.	12
Загальна кількість годин	**86**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

1. Онлайн-курс «Програмування для всіх: основи Python»
https://prometheus.org.ua/prometheus-free/python-fundamentals-for-everyone/
2. Онлайн-курс «Git для розподіленої розробки програмного забезпечення»
https://prometheus.org.ua/prometheus-free/git-for-distributed-software/

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Теорія інформації і кодування: курс лекцій [Електронний ресурс] : навч. посіб. /; уклад.: А.Є. Коваленко. Київ : КПІ ім. Ігоря Сікорського, 2020. 248 с. Режим доступу: https://ela.kpi.ua/items/a07a480f-f5ec-4cbd-9e92-34ffc453b10c
2. Бойко В.Д., Василенко М.Д., Слатвінська В.М. Теорія інформації та кодування: навчально-методичні рекомендації(в допомогу до самостійної роботи для здобувачів вищої освіти кваліфікації бакалавр факультету кібербезпеки та інформаційних технологій). Одеса : Видавничий дім «Гельветика». 2020. 34 с. Режим доступу:
https://ekt.elit.sumdu.edu.ua/wp-content/uploads/2023/01/Teoriia-informatsii-ta-koduvannia_Odesa_2020.pdf
3. Подлевський Б. М. Теорія інформації в задачах. Центр навчальної літератури. 2019. 271 с. Режим доступу:
https://book-ye.com.ua/dovidnikova-literatura/navchal-na-literatura/pidruchnyky-ta-posibnyky/teoriya-informatsiyi-v-zadachakh-pidruchnyk/?srsltid=AfmBOop1F8d3WFRJoiafQYf2Fx2qmbCCrb33tU0yB1LpNiNGYv6HjXnn

Додаткова література

1. Курко А. М. Введення в теорію інформації [Електронний ресурс]: Посібник до вивчення дисципліни «Теорія інформації» / А. М. Курко, В. Я. Решетняк. – Тернопіль: Тернопільський національний технічний університет ім. Івана Пулюя, 2017. 108 с. Режим доступу: http://elartu.tntu.edu.ua/handle/lib/21919

2. Беркман Л.Н., Бондарчук А.П., Гайдур Г.І., Чумак Н.С. Кодування джерел інформації та каналів зв'язку. Навч. посібник підготовлено для самостійної роботи студентів вищих навчальних закладів. Київ: НННТІ ДУТ, 2018. 91с. Режим доступу: https://duikt.edu.ua/ua/lib/1/category/2530/view/1619?lang=ua&act=view&page=1&category=2530&id=1619
3. Основи теорії інформації та кодування: лабораторний практикум [Електронний ресурс] : навч. посіб. / М. І. Романюк, Г. Г. Власюк; КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2018. 81 с. Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/5b1188ab-b6ce-42fd-8103-9e0dc10971cb/content

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,7	0,2		0,1

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно	F

(потрібне повторне вивчення)

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Роман КОРОЛЬОВ