Силабус освітнього компонента
Програма навчальної дисципліни

Теорія інформації і кодування

Шифр та назва спеціальності
257 –Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Управління інформаційною безпекою

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Обов'язкова

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: "Моделювання систем інформаційної безпеки", "Штучний інтелект і бізнес-аналітика", "Стандартизація та сертифікація в галузі інформаційної безпеки", "Технологія управління безпекою бізнес-процесів" 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 – екзамен.

Компетентності

КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ–4. Здатність спілкуватися державною мовою як усно, так і письмово.
КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ФК–1. Здатність використовувати безпекові режими під час виконання службових обов'язків.
ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
ФК-4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.
ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
ФК-6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.
ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
ФК-9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.
ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

ПРН-3. 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.
ПРН-4. Вільно спілкуватися державною мовою.
ПРН-5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.
ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
ПРН-8. Вміти використовувати сучасне програмно апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
ПРН-9. Вміти використовувати безпекові режими під час виконання службових обов'язків.
ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
ПРН-11. 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.
ПРН-12. Вміти використовувати програмні та програмно апаратні комплекси захисту інформаційних ресурсів.
ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в. т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно комунікаційних системах.
ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно комунікаційних систем.
ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 16 год., лабораторні роботи – 16 год., самостійна робота – 58 год.

Передумови вивчення дисципліни (пререквізити)

Інтернетика. Теорія пошуку. Моделі та алгоритми, 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.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Математичні основи теорії інформації.
Тема 2. Інформація та її кількісні оцінки. Ентропія джерела інформації.
Тема 3. Ефективне кодування та стиснення даних.
Тема 4. Інформаційні характеристики каналів зв'язку.
Тема 5. Принципи та методи завадостійкого кодування.
Тема 6. Циклічні коди. Методи кодування та декодування.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Подання числової інформації в різних системах числення.
Тема 2. Характеристики дискретного каналу передавання інформації.
Тема 3. Використання статистичних методів стиснення інформації.
Тема 4. Математичні моделі каналів зв'язку.
Тема 5. Дослідження та вивчення критеріїв оцінки завадостійкого кодування.
Тема 6. Коди Ріда-Соломона та їх використання в кодуванні та декодуванні.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних

робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

Основна література:

1. Теорія інформації і кодування: курс лекцій [Електронний ресурс] : навч. посіб. для здобувачів ступеня бакалавра за спеціальністю 124 «Системний аналіз» /; уклад.: А.Є. Коваленко. Київ : КПІ ім. Ігоря Сікорського, 2020. 248 с.
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
https://ekt.elit.sumdu.edu.ua/wp-content/uploads/2023/05/Teoriia-informatsii-ta-koduvannia_Odesa_2020.pdf
3. Подлевський Б. М. Теорія інформації в задачах. Центр навчальної літератури. 2019. 271 с.
https://www.libr.dp.ua/text/kraj/1552407.pdf

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 305 за кредитно-модульною організацією навчального процесу. Київ: ННІТІ ДУТ, 2018. 91с.
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. для студ. спеціальності 171 «Електроніка», спеціалізації «Електронні та інформаційні технології кінематографії та аудіовізуальних систем» / М. І. Романюк, Г. Г. Власюк; КПІ ім. Ігоря Сікорського. – Електронні текстові данні (1 файл: 2,09 Мбайт). Київ : КПІ ім. Ігоря Сікорського, 2018. 81 с.
https://ela.kpi.ua/items/1cc27217-226a-484b-b8ac-9497fffe37b5

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% семестрової оцінки;
•екзамен: 40% семестрової оцінки.

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 (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент 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

28.08.2024 Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024 Гарант ОП
Роман КОРОЛЬОВ