Силабус освітнього компонента
Програма навчальної дисципліни

Теорія інформації і кодування

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

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

Освітня програма
Кібербезпека

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 1. Здатність застосовувати знання у практичних ситуаціях.
КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

Результати навчання

РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їх ефективність.
РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН 7 – діяти на основі законодавчої та нормативно правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
РН 10 – виконувати аналіз та декомпозицію інформаційнотелекомунікаційних систем.
РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
РН 12 – розробляти моделі загроз та порушника.
РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно телекомунікаційних системах.
РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз.
РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

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)

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.

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
Сергій ЄВСЕЄВ