Силабус освітнього компонента
Програма навчальної дисципліни

Алгоритми та структури даних

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
2

Мова викладання
Українська

Викладачі, розробники

ТКАЧОВ Андрій Михайлович
andrii.tkachov@khpi.edu.ua
Кандидат технічних наук, старший науковий співробітник кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: більше 60 публікацій, 25 статей у закордонних виданнях та фахових виданнях України, 6 патентів на корисну модель, гарант освітньо-професійної програми першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: «Мережне програмування», «Розробка та аналіз алгоритмів», «Технології програмування» , «Інструментальні засоби програмування», «Веб безпека», «Основи технічного захисту інформації», у студентів бакалавріата та магістратури.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Алгоритми та структури даних" є обов'язковою навчальною дисципліною. Дисципліна спрямована на ознайомлення студентів з сучасними поглядами на алгоритмічні процеси; навчити основним технологічним засобам розробки та аналізу алгоритмів.

Мета та цілі дисципліни

Формування у студентів системи знань про базові структури даних і основні обчислювальні алгоритми, а також придбання практичних навичок з проектування, розроблення та аналізу алгоритмів, оцінювання їх ефективності та складності.

Формат занять

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

Компетентності

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.
КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації
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 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
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.).
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

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 їхню 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–5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
РН–6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
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 інформаційно-телекомунікаційних систем.
РН–11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
РН–12. Розробляти моделі загроз та порушника.

РН–13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
РН–14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
РН–15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
РН–16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
РН–17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
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–23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
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–25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
РН–26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
РН–27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
РН–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.
РН–29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
РН–30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
РН–31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
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–37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
РН–38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
РН–41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН–42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти 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–45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
РН–46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
РН–47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
РН–48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
РН–49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
РН–50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
РН–51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
РН–52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
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 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Основи програмування.

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

Теми лекційних занять

Тема 1. Вступ до структур даних та алгоритмів.
Поняття структур даних та їх класифікація. Формалізація поняття алгоритму. Основні напрямки в теорії алгоритмів. Практичне застосування результатів теорії алгоритмів.
Тема 2. Базові структури даних.
Масиви. Стеки. Черги. Зв'язні списки. Хеш-таблиці. Пряма адресація. Хеш-функції. Двійкові дерева пошуку. Червоно-чорні дерева.
Тема 3. Алгоритми сортування, злиття та пошуку.
Сортування за квадратичний час. Сортування вибором. Сортування обміном. Сортування за O(n log n). Швидке сортування. Вибір елементу для розділення. Сортування злиттям. Витрати пам’яті при сортуванні злиттям. Злиття послідовностей. Бінарний пошук.Нижні оцінки швидкості сортування. Дерево розв’язків. Сортування підрахунком.
Тема 4. Комбінаторні алгоритми.
Генератори псевдовипадкових чисел. Властивості випадкових та псевдовипадкових чисел. Поширені недоліки генераторів псевдовипадкових чисел. Лінійний конгруентний метод. Вихор Мерсенна.
Тема 5. Фундаментальні алгоритми на графах і деревах.
Представлення графів. Вершини. Ребра. Орієнтовані та неорієнтовані графи. Список суміжних вершин. Матриця суміжності. Розріджений граф. Зважений граф. Пошук в глибину. Пошук в ширину. Дерева пошуку. Рекурсивна та нерекурсивна реалізації пошуку у графі. Топологічне сортування.
Тема 6. Геометричні алгоритми.
Властивості відрізків. Опукла комбінація. Векторний добуток. Напрямок повороту. Перевірка перехрещення відрізків. Обмежуючий прямокутник. Відношення порядку на відрізках. Побудова опуклої оболонки. Алгоритм Грехема. Алгоритм Джарвіса. Метод додавання точок. Складність алгоритмів побудови опуклої оболонки.
Тема 7. Криптографічні алгоритми.
Класифікація криптографічних алгоритмів. Криптосистеми із закритим ключем. Поняття закритого ключа. Шифр Цезаря. Шифр Віжинера. Зламування шифрів Цезаря та Віжинера. Криптосистеми з відкритим ключем. Поняття відкритого ключа. Функція Ейлера. Криптографічні хеш-функції. Необхідність криптографічного шифрування.
Тема 8. Евристичні алгоритми.
Оцінка якості наближеного алгоритму. Схема наближення для заданої оптимізаційної задачі. Задача про покриття вершин. Наближений алгоритм для пошуку покриття вершин. Максимальна помилка наближеного алгоритму для пошуку покриття вершин. Задача комівояжера. Нерівність трикутника. Наближений алгоритм для задачі комівояжера. Максимальна помилка наближеного алгоритму для задачі комівояжера.
Тема 9. Математичні основи аналізу алгоритмів.
Асимптотичні позначення. Швидкість росту функцій. Логарифмічний ріст. Лінійний ріст. Квадратичний ріст. Експоненційний ріст. Стандартні функції та позначення. Суми та їхні властивості. Прогресії. Суми різниць. Оцінки сум. Індукція. Почленне порівняння.
Тема 10. Рекурсія.
Алгоритмічна система на основі рекурсивних функцій. Метод підставки. Способи вгадати оцінку (аналогія, послідовні наближення). Індукція та парадокс винахідника. Заміна змінних. Перетворення на суми. Ітерації співвідношень. Дерево рекурсії. Загальне рішення великого класу рекурентних співвідношень. Основна теорема про рекурсивні оцінки. Приклади використання основної теореми про рекурсивні оцінки.
Тема 11. Алгоритмічні стратегії.
Принцип «Розділяй і пануй». Розподіл на підзадачі. Динамічне програмування.
Задача про множення матриць. Оцінка складності алгоритму розв’язання задачі про множення матриць. Задача про пошук найбільшої спільної підпослідовності. Довжина найбільшої спільної

підпослідовності. Відтворення найбільшої спільної підпослідовності. Жадібні алгоритми. Задача про розподіл заявок. Амортизаційний аналіз. Метод групувань. Метод передплати. Метод потенціалів.
Тема 12. Основи теорії обчислюваності.
Поняття обчислюваності й обчислювальні процедури. Поняття відносного алгоритму й відносної обчислюваності, поняття зведення. Машина Тюринга. Складові частини машини Тюринга. Можливості машини Тюринга. Ілюстрація роботи машини Тюринга для простих алгоритмів. Основна гіпотеза теорії алгоритмів. Алгоритмічно нерозв'язні проблеми.
Тема 13. Класи складності.
Поліноміальний час. Ефективний алгоритм. Абстрактна задача. Поліноміальна задача. Формальні мови для задач розв'язуваності. Перевірка належності до мови та клас NP. Задача про гамільтонов цикл у графі. Алгоритм перевірки. NP-важкі й NP-повні задачі. Клас NP.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Базові структури даних: (список, черга, стек).
Тема 2. Базові структури даних: хеш- таблиці; червоно-чорні дерева.
Тема 3. Алгоритми сортування.
Тема 4. Комбінаторні алгоритми.
Тема 5. Фундаментальні алгоритми на графах і деревах.
Тема 6. Геометричні алгоритми.
Тема 7. Криптографічні алгоритми.
Тема 8. Евристичні алгоритми.
Тема 9. Математичні основи аналізу алгоритмів.
Тема 10. Рекурсія. Рекурсивні оцінки
Тема 11. Динамічне програмування. Жадібні алгоритми
Тема 12. Основи теорії обчислюваності.

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.
Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:
C++ 2, Introduction to Data Science
https://www.netacad.com/catalogs/learn?category=course.

Література та навчальні матеріали

Основна література:

1. Marcello La Rocca. Advanced Algorithms and Data Structures. / Marcello La Rocca. – New York: Manning Publications Co., 2021. – 768 p.
https://books.google.com.ua/books/about/Advanced_Algorithms_and_Data_Structures.html?id=XPQ1EAAAQBAJ&redir_esc=y

2. Креневич А.П. Алгоритми і структури даних. Підручник. / А.П. Креневич. – К.: ВПЦ "Київський Університет", 2021. – 200 с.
https://www.mechmat.univ.kiev.ua/wp-content/uploads/2021/09/pidruchnyk-alhorytmy-i-struktury-danykh.pdf
3. Helmut Knebl. Algorithms and Data Structures: Foundations and Probabilistic Methods for Design and Analysis / Helmut Knebl. – Cham: Springer Nature Switzerland AG, 2020. – 349 p. – Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/50239.
4. Алгоритми та структури даних: практикум: навч. посіб./Н.К. Стратієнко, М.Д. Годлєвський, І.О. Бородіна.- Харків: НТУ "ХПІ", 2017. - 224 с.
https://repository.kpi.kharkov.ua/server/api/core/bitstreams/8be9ee4f-7db1-45d5-8f57-9c8e6d0bd982/content
5. Методичні вказівки до виконання лабораторних робіт з курсу "Алгоритми і структури даних" [Електронний ресурс] / уклад. Н. К. Стратієнко, І. О. Бородіна ; Харківський політехнічний ін-т, нац. техн. ун-т. – Електрон. текстові дані. – Харків, 2017. – 36 с. – Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/26426.
6. Євсеєв С.П. КІБЕРБЕЗПЕКА: КРИПТОГРАФІЯ З PYTHON: навч. посібн. / С.П. Євсеєв, О.В. Шматко, О.Г. Король – Харків: Видавництво «Новий Світ – 2000», 2021. –120 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

Додаткова література :

1. Donald Knuth. The Art of Computer Programming, Volume 4, Fascicle 5: Mathematical Preliminaries Redux; Introduction to Backtracking. / Donald Knuth. – Boston: Pearson Education (US), 2020. – 320 p.
https://api.pageplace.de/preview/DT0400.9780134671833_A39997762/preview-9780134671833_A39997762.pdf
2. Florian Jaton, Geoffrey C. Bowker. The Constitution of Algorithms: Ground-Truthing, Programming, Formulating. / Florian Jaton, Geoffrey C. Bowker. – MIT Press Ltd, United States, 2021. – 400 p.
https://florian-jaton.com/resources/jaton_2021_the-constitution-of-algorithms.pdf
3. Shmuel Tomi Klein. Basic Concepts In Algorithms. / Shmuel Tomi Klein. – Singapore: World Scientific Publishing Co Pte Ltd, 2021. – 364 p.
https://books.google.com.ua/books/about/Basic_Concepts_in_Algorithms.html?id=8NpdzgEACAAJ&redir_esc=y
4. Hemant Jain. Problem Solving in Data Structures & Algorithms Using Python. /Hemant Jain. – Independently Published, 2019. – 416 p.
https://books.google.com.ua/books/about/Problem_Solving_in_Data_Structures_and_A.html?id=XpdKMQAACAAJ&redir_esc=y
5. Hemant Jain, Problem Solving in Data Structures & Algorithms Using C. /Hemant Jain. – Independently Published, 2018. – 556 p.
https://books.google.com.ua/books/about/Problem_Solving_in_Data_Structures_and_A.html?id=6ln_MAAACAAJ&redir_esc=y
6. Steven S. Skiena. The Algorithm Design Manual. 3rd ed. / Steven S. Skiena. – Cham: Springer Nature Switzerland AG, 2020. – 793 p.
https://mimoza.marmara.edu.tr/~msakalli/cse706_12/SkienaTheAlgorithmDesignManual.pdf
7. Мелешко Є.В., Якименко М.С., Поліщук Л.І. Алгоритми та структури даних: Навчальний посібник для студентів технічних спеціальностей денної та заочної форми навчання. – Кропивницький: Видавець – Лисенко В.Ф., 2019. – 156 с.
https://dspace.kntu.kr.ua/server/api/core/bitstreams/46a115be-c271-4ab0-bfb5-62dca34b7d6a/content
8. Алгоритми, дані і структури. [Текст], навч. посіб. / В.М. Ільман, О.П. Іванов, Л.О. Панік. Дніпропет. нац.. ун-т залізн. трансп.ім. акад. В. Лазаряна. – Дніпро, 2019. – 134 с.
https://crust.ust.edu.ua/server/api/core/bitstreams/16eada7c-c082-46f7-af81-1d6e97ac9320/content
9. Бородкіна І.Л. Теорія алгоритмів: посібник для студентів вищих навчальних закладів –Центр навчальної літератури, 2018. – 184 с.
http://irb.nubip.edu.ua/cgi-bin/irbis64r_14/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=BOOKS_READER&P21DBN=BOOKS&Z21ID=&Image_file_name=Borodkina_Teorij%20algorutmiv.pdf&mfn=356&FT_REQUEST=&CODE=213&PAGE=1

10. Allen Downey. Think Data Structures / Allen Downey. – O'Reilly Media, Inc, USA, 2017. – 155 p. https://greenteapress.com/thinkdast/thinkdast.pdf
11. Marcin Jamro. C# Data Structures and Algorithms: Explore the possibilities of C# for developing a variety of efficient applications / Marcin Jamro. – Birmingham: Packt Publishing Limited, 2018. – 292 p. https://books.google.com.ua/books/about/C_Data_Structures_and_Algorithms.html?id=Cd9YDwAAQBAJ&redir_esc=y

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;
- іспит: 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