

Дек: _____

Принес

« _____ » _____

Декан факультету IT

Ім'я, ПРІЗВИЩЕ

08 2024 p.

Алгоритми та структури даних

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС			Залік	Іспит
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття					
Очна (денна)	-	-	8	240	85	34	34	17		155			+	

Хмельницький 2024

АЛГОРИТМИ ТА СТРУКТУРИ ДАНИХ У СИСТЕМАХ ЗАХИСТУ

Тип дисципліни	Вибіркова
Рівень вищої освіти	Перший (бакалаврський)
Мова викладання	Українська
Семестр	-
Кредити ЄКТС	8,0
Форми навчання, для яких викладається дисципліна	Денна

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати* та аналізувати різні фундаментальні та вдосконалені алгоритми для розв'язування задач захисту інформації, *адаптуватися* в умовах частой зміни технологій професійної діяльності; *вміти* самостійно опановувати нові методи та технології розробки інформаційних систем, формалізувати обчислювальні та логічні задачі та *давати* оцінку результативності якості прийнятих рішень, ефективності організації структур даних та алгоритмів в системах захисту; *виконувати* пошук інформації в структурах даних використовуючи різні способи пошуку (послідовний, ділення навпіл, хешування, пошук підрядків різними методами), *використовувати* різні методи сортування даних в масивах на лінійних списках; *володіти* навичками розробки та налагодження програм на одній з алгоритмічних процедурних мов програмування високого рівня (Python, C++), практичними навичками проектування захищених систем. сучасними технологія розробки алгоритмів і програм, способами конструювання складних структур даних на базі простих структур даних, методами сортування даних, умінням самостійно опановувати нові алгоритми і структури даних, методи та технології розробки систем захисту.

Зміст навчальної дисципліни. Перетворення інформації з метою захисту, базові структури даних, динамічні структури даних, стеки і черги, зв'язані списки, хеш-таблиці, бінарні дерева пошуку, червоно-чорні дерева, рекурентні співвідношення, методи сортування динамічне програмування, жадібні алгоритми, алгоритми пошуку підрядків, геометричні алгоритми, алгоритми на графах.

Пререквізити: технології безпечного програмування.

Кореквізити: - .

Запланована навчальна діяльність: лекції 34 год., лабораторних робіт 34 год., практичних 17 год, самостійної роботи 155 год., разом 240 год.

Форми (методи) навчання: пояснювально-ілюстративні, продуктивні та репродуктивні, практичні, застосування інформаційно-комп'ютерних технологій.

Форми оцінювання результатів навчання: усне опитування, тестування, захист лабораторних робіт.

Вид семестрового контролю: залік

Навчальні ресурси:

1. Крєневич А.П. Алгоритми та структури даних: навчальний посібник / А.П. Крєневич. – К.: ВПЦ "Київський Університет", 2018. – 777 с.
2. Мелешко Є.В. Алгоритми та структури даних: навчальний посібник / Є.В. Мелешко, М.С. Якименко, Л.І. Поліщук. – Кропивницький: Видавець – Лисенко В.Ф., 2019. – 156 с
3. Data Structures And Algorithmic with Python / Editors: Kent D. Lee• Steve Hubbard. – Switzerland: Springer International Publishing, 2015, – 369 p.
4. Ткачук В.М. Алгоритми і структура даних: навчальний посібник / В.М.Ткачук. – Івано-Франківськ: Видавництво Прикарпатського національного університету імені Василя Стефаника, 2016. – 286 с.
5. Євсєєв С.П. КІБЕРБЕЗПЕКА: КРИПТОГРАФІЯ З PYTHON: навч. посібн. / С.П. Євсєєв, О.В. Шматко, О.Г. Король – Харків: Видавництво «Новий Світ – 2000», 2021. – 120 с.
6. Модульне середовище для навчання Доступ до ресурсу: <https://msn.khnu.km.ua/course/view.php?id= 5941>
7. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php

Викладач: кандидат технічних наук, доцент Муляр І.В.

ВСТУП

Дисципліна «Алгоритми та структури даних в системах захисту» - вибіркова складова професійної підготовки бакалаврів в галузі інформаційних технологій зі спеціальності „Кібербезпека”, що охоплює сучасні методи представлення даних в пам’яті комп’ютера та основних алгоритмів їх опрацювання для практичного використання при проектуванні систем захисту інформації.

Мета дисципліни. Формування системи знань та розуміння теоретичних, методичних і алгоритмічних основ інформаційних технологій їх використання під час вирішення прикладних і наукових завдань у сфері інформаційних систем і технологій та захисту інформації. Ознайомити студентів з сучасними та ефективними структурами даних та алгоритмами комп’ютерного оброблення інформації, а також методами їх дослідження та аналізу.

Предмет дисципліни. Сучасні методи проектування структур даних та алгоритми їх опрацювання в системах захисту.

Завдання дисципліни. Застосовувати знання до вирішення задач інформаційної безпеки, самостійних практичних задач в галузі захисту комп’ютерних систем та мереж. Забезпечити набуття компетентностей та досягнення програмних результатів навчання:

компетентності:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.

ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

результати навчання:

ПРН 1(5). Адаптуватися в умовах часткої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН 2(47). Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного захисту інформації.

ПРН 3(53). Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

ПРН 4. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН 5. Самостійно опановувати нові методи та технології розробки інформаційних систем.

ПРН 6. Використовувати прикладні системи програмування, розробляти складні програмні комплекси з функціями захисту даних..

ПРН 7. Визначати функціональні вимоги до розроблюваної програми, розробляти набори тестових даних та давати оцінку результативності якості прийнятих рішень.

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати* та аналізувати різні фундаментальні та вдосконалені алгоритми для розв’язування задач захисту інформації, *адаптуватися* в умовах часткої зміни технологій професійної діяльності; *вміти* самостійно опановувати нові методи та технології розробки інформаційних систем, формалізувати обчислювальні та логічні задачі та *давати* оцінку результативності якості прийнятих рішень, ефективності організації структур даних та алгоритмів в системах захисту; *виконувати* пошук інформації в структурах даних використовуючи різні способи пошуку (послідовний, ділення навпіл, хешування, пошук підрядків різними методами), *використовувати* різні методи сортування даних в масивах на лінійних списках; *володіти* навичками розробки та налагодження програм на одній з алгоритмічних процедурних мов програмування високого рівня (Python, C++), практичними навичками проектування захищених систем. сучасними технологія розробки алгоритмів і програм, способами конструювання складних структур даних на базі простих структур даних, методами сортування даних, умінням

самостійно опановувати нові алгоритми і структури даних, методи та технології розробки систем захисту.

СТРУКТУРА ЗАЛКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин, відведених на:			
	лекції	лабораторні роботи	Практичні заняття	самостійну роботу
Тема 1. Статичні структури даних	6	8	4	20
Тема 2. Динамічні та нелінійні структури даних	6	12	6	40
Тема 3. Основні алгоритми обробки і шифрування інформації	18	14	6	70
Тема 4. Аналіз алгоритмів як базис криптоаналізу	4	-	1(1/2)*	25
Разом:	34	34	17 (18/16)*	155

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
Тема 1. Статичні структури даних		
1	Python, як мова етичного хакінгу і інструмент кібербезпеки. Типи даних. Арифметичні вирази, управляючі конструкції та масиви у мові Python. Функції у мові Python. Файли. Особливості Python як інструментарію фахівця з кібербезпеки Літ.: [3] с.1-41; [9] с.5-83; [15].	2
2	Алгоритми та дані. Структурування і абстракція програм. Алгоритми. Формалізація алгоритмів. Ефективність алгоритмів. Алгоритм та оцінка його складності. Асимптотична оцінка складності алгоритмів. . Способи реалізації алгоритмів. Документація алгоритмів. Методи розробки алгоритмів. Літ.: [1] с.22-36; [2] с.5-16; [4] с.204-220; [5] с.18-22; [8] с.12-16; [10] с.16-29.	2
3	Прості, статичні та напівстатичні структури даних. Основні поняття та термінологія, структур даних, вимоги до структур даних. Концепція структур даних. Класифікація структур даних. Операції над структурами даних. Масиви даних, розріджені масиви. Множини. Структури. Об'єднання. Бітові типи. Таблиці. Рядки. Літ.: [4] с.4-103; [9] с.84-141; [10] с.30-48.	2
Тема 2. Динамічні та нелінійні структури даних		
4	Списки. Односпрямовані і двоспрямовані списки. Структура і типі лінійних списків. Операції із списками. Літ.: [1] с.94-98; [3] с.91-122; [4] с.105-138; [6] с.8-121.	2
5	Стеки, деки, черги. Реалізація на мові Python. Особливі види черг (деки та черги з пріоритетами). Використання стеків для обчислення виразів. Літ.: [1] с.72-93; [3] с.123-136; [4] с.138-143; [5] с.48-95	2
6	Нелінійні структури даних. Визначення дерева. Бінарне дерево. Подання дерев у пам'яті комп'ютера. Правила побудови бінарного дерева з будь-якого дерева. Поняття графу. Подання графу у пам'яті комп'ютера. Список суміжних вершин. Матриця суміжності. Використання динамічних і нелінійних структур при написанні захищених програм. Літ.: [2] с.70-116; [3] с.163-185, с.261-280; [4] с.143-167; [5] с.135-210.	2
Тема 3. Основні алгоритми обробки і шифрування інформації		
7	Алгоритми сортування. Задача сортування. Сортування вибіркою. Сортування бульбашкою (bubble sort). Сортування Шелла. Сортування включенням (insertion sort). Швидке сортування Хоара. Сортування злиттям. Сортування купою (пірамідальне сортування). Сортування впорядкованим бінарним деревом. Сортування підрахунком. Літ.: [1] с.54-64; [2] с.28-69; [4] с.234-265; [5] с.287-309; [8] с.7-24.	2
8	Комбінаторні та рекурсивні алгоритми. Ханойська вежа. Числа Фібоначчі. Перестановки. Підрахунок кількості можливих перестановок. Метод повного перебору. Методи сортування з використанням рекурсії. Літ.: [1] с.9-21; [2] с.5-16; [3] с.71-88; [4] с.227-233.	2

9	Алгоритми пошуку. Послідовний (лінійний) пошук. Бінарний пошук. Бінарний пошук з використанням дерев. Метод інтерполяції. Метод „золотого перерізу”. Алгоритми пошуку послідовностей. Алгоритм Кнута, Моріса, Пратта. Літ.: [1] с.40-54, с.99-130; [4] с.267-275; [5] с.310-334.	2
10	Динамічне програмування. Використання динамічного програмування. Дерево Фібоначчі. Задача про стрибунця. Літ.: [1] с.169-171; [5] с.416-452.	2
11	Фундаментальні алгоритми на графах і деревах. Способи задання графів. Пошук в ширину. Пошук у глибину. Алгоритм визначення компонент двозв’язності. Літ.: [1] с.130-156; [2] с.117-130; [4] с.167-184.	2
12	Пошук найкоротших шляхів на графах. Жадібні алгоритми. Алгоритм Дейкстри. Алгоритм Прима. Алгоритм Краскала. Алгоритм Флойда - Фелкерсона. Використання алгоритмів на графах при побудові захищених програм. Літ.: [1] с.157-168; [2] с.131-136; [3] с.185-205; [4] с.184-203; [5] с.242-286, 390-398.	2
13	Алгоритми і структури даних в задачах криптографічного шифрування. Класифікація криптографічних алгоритмів. Таблиці шифрування та алгоритми шифрування за таблицями. Одноалфавітні та поліалфавітні таблиці шифрування. Функція Ейлера і її застосування в криптографії. Літ.: [7] с.15-25; [7] с.62-72; [16] с.48-76; [24].	2
14	Методи швидкого доступу до даних. Хеш-функції, хеш-таблиці і алгоритми хешування даних. Хешування даних. Колізії. Методи розв’язання колізій. Поняття хеш-функції. Алгоритми хешування. Відкрите і закрите хешування. Літ.: [2] с.93-100; [3] с.145-151; [5] с.347-361; [16] с.284-308; [22, 23].	2
15	Алгоритми рандомізації як спосіб руйнування статистичних залежностей і захисту структурованих даних. Організація даних для прискорення пошуку за вторинними ключами. Метод часткових цілей. Метод сходження. Алгоритми стиснення без втрат. Реалізація алгоритму Хаффмана з використанням кодових дерев. Алгоритмічна реалізація симетричної криптосистеми з нелінійним шифруванням та можливістю контролю шифротексту з метою маскування. Літ.: [3] с.281-296; [7] с.15-25; [24].	2
Тема 4. Аналіз алгоритмів як базис криптоаналізу		
16	Побудова і аналіз алгоритмів. Покрокове проектування алгоритмів. Характеристики алгоритму. Ефективність алгоритмів. Правила аналізу складності алгоритмів. Способи реалізації алгоритмів. Документація алгоритмів. Методи розробки алгоритмів. Асимптотичні позначення. Швидкість росту функцій. Логарифмічний ріст. Лінійний ріст. Квадратичний ріст. Експоненційний ріст. Літ.: [4] с.204-220; с.18-22; [5] с.387-415.	2
17	Класи складності P й NP. Поліноміальний час. Ефективний алгоритм. Абстрактна задача. Поліноміальна задача. Формальні мови для задач розв’язуваності. Перевірка належності до мови та клас NP. Задача про гамільтоновий цикл у графі. Алгоритм перевірки. NP-важкі й NP-повні задачі. Клас NP. Літ.: [5] с.255-286, с.453-470.	2
Разом:		34

Зміст лабораторних робіт

№ з/п	Тема лабораторного заняття	Кількість годин
1	Способи організації списків (масивів) у Python. Функції. Літ.: [1] с.94-98; [5] с.48-95; [6] с.8-21; [8] с.25-32.	4
2	Квадратичні алгоритми впорядкування масивів. Рекурсивні алгоритми. Літ.: [1] с.54-64; [5] с.287-309	4
3	Оптимізовані алгоритми хешування в Python для роботи з словниками. Літ.: [3] с.139-145; [5] с.347-361; [9] с.127-151.	4
4	Одно та двоспрямовані списки. Стеки та черги у Python. Літ.: [1] с.72-98; [3] с.91-122; [3] с.123-136; [5] с.96-134; [6] с.21-35; [8] с.33-40.	4
5	Використання бінарних дерев в алгоритмах захищених групових комунікацій. Опрацювання нелінійних структур даних, представлених у вигляді бінарних дерев. Літ.: [1] с.99-130; [2] с.70-116; [3] с.163-185, с.261-280; [4] с.143-167; [6] с.35-47; [8] с.41-45.	4
6	Способи задання графів. Неорієнтовані графи. Способи обходу графів: DFS та BFS алгоритми. Літ.: [1] с.130-156; [2] с.117-130; [4] с.167-184; [8] с.45-54;	4
7	Використання алгоритмів пошуку найкоротших шляхів на графах для моделювання поширення забороненої інформації. Літ.: [1] с.157-168; [2] с.131-136; [3] с.185-205; [4] с.184-203; [5] с.242-286; [8] с.55-61.	4
8	Використання бібліотеки BeautifulSoup для парсингу сайтів на присутність забороненого контенту. Літ.: [9] с.185-200.	4
9	Підсумкове заняття	2
Разом:		34

Перелік практичних занять

№ п/п	Тема практичного заняття	Кільк. годин
1	Аналіз алгоритмів впорядкування Літ.: [4] с. 31-147, с.257-323; [6] с. 47 – 193	2
2	Вдосконалені алгоритми впорядкування (пірамідальний, швидкий, злиття) Літ.: [4] с. 349-403; [6] с. 97 – 193	2
3	Робота з однозв'язними та двозв'язними списками Літ.: [4] с. 141-169; [6] с. 193 – 280	2
4	Особливі види черг (деки та черги з пріоритетами). Використання стеків для обчислення виразів Літ.: [4] с. 375-429; [6] с. 193 – 280	2
5	Правила побудови бінарного дерева з будь-якого дерева Літ.: [4] с. 429-453; [6] с. 97 – 280	2
6	Способи задання графів. Орієнтовані графи Літ.: [4] с. 429-453; [6] с. 193 – 280	2
7	Способи обходу графів (алгоритми в глибину та алгоритми в ширину) Літ.: [1] с.130-156; [2] с.117-130; [4] с.167-184; [8] с.45-54;	2
8	Пошук найкоротших шляхів на графах. Алгоритм Флойда Літ.: [1] с.157-168; [2] с.131-136; [3] с.185-205; [4] с.184-203; [5] с.242-286; [8] с.55-61.	2
9	Підсумкове заняття	1 (1/2)*
Разом:		17(16/18)*

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу аудиторних занять)

ЗМІСТ САМОСТІЙНОЇ (ІНДИВІДУАЛЬНОЇ) РОБОТИ

Об'єм самостійної роботи становить 155 годин. Він включає опрацювання лекційного матеріалу, підготовку до виконання лабораторних робіт і їх захисту, підготовку до поточного контролю, а також самостійну роботу студентів.

Номер тижня	Теми самостійної роботи	Кількість годин
1	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №1.	5
2	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №1.	6
3	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №2	4
4	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 2	10
5	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи № 3.	10
6	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 3.	10
7	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №4.	10
8	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №4.	10
9	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи № 5	10
10	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №5	10
11	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи № 6.	10
12	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №6.	10
13	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №7.	10
14	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №7	10
15	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи № 8	10
16	Опрацювання лекційного матеріалу, Підготовка до захисту лабораторної роботи № 8	10
17	Опрацювання лекційного матеріалу. Підготовка до тестування.	10
Разом за семестр:		155

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу аудиторних занять)

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів, зокрема: лекції з використанням пояснювально-ілюстративних та репродуктивних методів і візуалізації; лабораторні роботи з використанням продуктивних та практичних методів, з застосування інформаційно-комп'ютерних технологій.

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: спілкування під час лекцій, прилюдні захисти лабораторних робіт з обґрунтуванням прийнятих рішень щодо вибору методів рішення завдань в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики; адаптованість, вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел передбачені специфікою дисципліни, що передбачає рішення проблемних завдань із застосуванням творчих підходів; обмежений час на виконання лабораторних робіт, і тестових завдань, чітко визначені і надані в силабусі терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту).

При вивченні дисципліни можуть бути зараховані результати навчання, здобуті у неформальній освіті. Визнання результатів навчання, здобутих у неформальній освіті, реалізується згідно з чинним законодавством і регулюється Положенням про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ <https://www.khnu.km.ua/root/files/01/10/03/006.pdf>.

МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- усне опитування;
- захист лабораторної роботи;
- тестування.

При виведенні підсумкової семестрової оцінки враховуються результати поточного контролю (залік за рейтингом формується автоматично за результатами поточного контролю).

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів у семестрі за ваговими коефіцієнтами

	Аудиторна робота	Контрольні заходи	Підсумковий контрольний захід
Вид заняття	Лабораторні роботи	Тестування	
Тема	1-4	1-4	
Ваговий коефіцієнт	0,8	0,2	

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення протоколу і звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторне заняття викладач оголошує одразу після захисту звіту з лабораторної роботи і проставляє в електронний журнал дисципліни.

Оцінювання тестових завдань. Тематичний тест для кожного студента складається з п'ятнадцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 15.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1–5	6–10	11–13	14–15
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 15 хвилин (для закритої форми тестів – по одній хвилині на кожне завдання). Правильні відповіді студент записує у талоні відповідей. При цьому усі граfi для відповідей мають бути заповнені цифрами, що відповідають правильним, на погляд студента, відповідям. Через 15 хвилин студенти здають викладачу завдання з талонами відповідей.

Тестування студент може також пройти і в он-лайн режимі в модульному середовищі для навчання.

Оцінку за тестування викладач проставляє в електронний журнал дисципліни.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями оцінювання знань.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	Узагальнений критерій
1	2
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві-три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка „задовільно”.

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Залік вважається зданим при отриманні студентом за зведеними результатами поточного контролю підсумкової оцінки з дисципліни від 3,00 до 5,00 балів. При цьому за вітчизняною шкалою ставиться оцінка за двобальною шкалою, а за шкалою ECTS – оцінка, що відповідає набраній студентом кількості балів.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ECTS встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	Інституційна інтервальна шкала балів	Інституційна оцінка, критерії оцінювання		
A	4,75–5,00	5		Відмінно – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4		Добре – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4		Добре – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3		Задовільно – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3		Задовільно – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2		Незадовільно – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2		Незадовільно – необхідна серйозна подальша робота і повторне вивчення дисципліни

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ЗДОБУТИХ СТУДЕНТАМИ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Особливості Python як інструментарію фахівця з кібербезпеки.
2. Концепція структур даних.
3. Класифікація структур даних.
4. Прості та статичні структури даних.
5. Динамічні структури даних.
6. Нелінійні структури даних.
7. Стандартна бібліотека шаблонів: призначення та основні поняття.
8. Основні типи контейнерів стандартної бібліотеки шаблонів.
9. Поняття ітератора та основні операції роботи із ним.
10. Поняття алгоритму стандартної бібліотеки шаблонів.
11. Вектор: поняття та приклади реалізації.
12. Масив як структура даних.
13. Динамічні масиви даних.
14. Розріджені масиви: основні поняття та способи представлення.
15. Граф: основні поняття та визначення.
16. Способи представлення графів.
17. Мінімальне покриваюче дерево та алгоритм його побудови.
18. Алгоритм пошуку в ширину.
19. Алгоритм пошуку в глибину.
20. Ейлерів цикл та алгоритм його побудови.
21. Гамільтонів цикл та алгоритм його побудови.
22. Найкоротший шлях на графі та алгоритми його побудови.
23. Складений тип даних структура.
24. Динамічні структури даних. Структури в якості полів структури. Елементи – функції структури.
25. Об'єднання.
26. Дерева: основні поняття та визначення.
27. Бінарне дерево та способи його представлення.
28. Способи обходу бінарного дерева.
29. Бінарне дерево пошуку.
30. Алгоритми вставки та видалення вузла в бінарному дереві.
31. Множина: основні поняття та операції. Основні операції над множинами.
32. Стек: поняття, основні операції та реалізація.
33. Черга: поняття, основні операції та реалізація.
34. Дек: поняття, основні операції та реалізація.
35. Лінійний список: поняття, основні операції.
36. Реалізація лінійного списку.
37. Алгоритми обробки елементів лінійного списку: створення списку, вставка та видалення елементів.
38. Різновиди списків.
39. Лінійний двозв'язний список.
40. Циклічний однозв'язний список.
41. Циклічний двозв'язний список.
42. Квадратичні алгоритми сортування.

43. Алгоритм шейкерного сортування
44. Алгоритм швидкого сортування.
45. Алгоритм сортування злиттям
46. Алгоритм пошуку найкоротшого шляху Флойда.
47. Алгоритм пошуку найкоротшого шляху Дейкстри;
48. Критерії оцінки ефективності алгоритмів.
49. Алгоритм послідовного пошуку.
50. Алгоритм бінарного пошуку.
51. Алгоритм прямого пошуку в тексті.
52. Алгоритм Кнута, Морріса і Пратта пошуку в тексті.
53. Алгоритм Бойєра і Мура пошуку в тексті.
54. Бінарне сортування пірамідою.
55. Алгоритм сортування Шелла.
56. Алгоритм швидкого сортування Хоара.
57. Таблиці шифрування та алгоритми шифрування за таблицями.
58. Методи швидкого доступу до даних. Хеш-функції, хеш-таблиці і алгоритми хешування даних.
59. Алгоритми і структури даних в задачах криптографічного шифрування.
60. Алгоритмічна реалізація симетричної криптосистеми з нелінійним шифруванням та можливістю контролю шифротексту з метою маскування.
61. Алгоритми рандомізації як спосіб руйнування статистичних залежностей і захисту структурованих даних.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни „Алгоритми та структури даних у системах захисту” повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, розміщеною в електронному варіанті в модульному середовищі.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Крєневич А.П. Алгоритми та структури даних: навчальний посібник / А.П. Крєневич. – К.: ВПЦ "Київський Університет", 2018. – 777 с.
2. Мелешко Є.В. Алгоритми та структури даних: навчальний посібник / Є.В. Мелешко, М.С. Якименко, Л.І. Поліщук. – Кропивницький: Видавець – Лисенко В.Ф., 2019. – 156 с
3. Data Structures And Algorithmic with Python / Editors: Kent D. Lee• Steve Hubbard. – Switzerland: Springer International Publishing, 2015, – 369 p.
4. Ткачук В.М. Алгоритми і структура даних: навчальний посібник / В.М.Ткачук. – Івано-Франківськ: Видавництво Прикарпатського національного університету імені Василя Стефаника, 2016. – 286 с.
5. Євсєєв С.П. КІБЕРБЕЗПЕКА: КРИПТОГРАФІЯ З PYTHON: навч. посібн. / С.П. Євсєєв, О.В. Шматко, О.Г. Король – Харків: Видавництво «Новий Світ – 2000», 2021. – 120 с.
6. Data Structures And Algorithmic Thinking With Python / Edited by Narasimha Karumanchi. – Carecr Monk Publications, 2016. – 471 p
7. Алгоритми та структури даних: конспект лекцій. Частина 1. Структури даних / О.Д. Воробйова, Л.В. Глазунова – Одеса: ОНАЗ ім.О.С. Попова, 2017. – 48с.
8. Алгоритми та структури даних: конспект лекцій. Частина 2. Алгоритми пошуку, стиснення даних, внутрішнього та зовнішнього сортування, алгоритми на графах / О.Д. Воробйова, Л.В. Глазунова – Одеса: ОНАЗ ім. О.С. Попова, 2017. – 52 с.
9. Власій О.О. Алгоритми та структури даних: лабораторний практикум / О. О. Власій. – Івано-Франківськ: ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», 2015. – 68 с.
10. Крєневич А.П. Python у прикладах і задачах. Частина 1. Структурне програмування: навчальний посібник / А.П. Крєневич. –К.: ВПЦ "Київський Університет", 2017. – 206 с.
11. Алгоритми, дані і структури: навчальний посібник / В.М. Ільман, О.П. Іванов, Л.О. Панік.Дніпропет. нац.. ун-т залізн. трансп.ім. акад. В. Лазаряна. – Дніпро, 2019. – 134 с.

Додаткова

12. Data Structures And Algorithms Made Easy / Edited by Narasimha Karumanchi. – Carecr Monk Publications, 2017. – 828 p
13. Python & Algorithms 2.0. A Guide to Learn how to Fly / Edited by Marina Wahl. – NY, 2014. – 244 p.
14. Data Structures And Algorithmic in Python / Editors: Michael T. Goodrich, Roberto Tamassia, Michael H. Goldwasser. – John Wiley & Sons, Inc, 2013. – 770 p
15. Алгоритми та структури даних: методичні вказівки до виконання лабораторних робіт / Н.К. Стратієнко, І.О. Бородіна. – Харків : НТУ «ХПІ», 2017. – 36 с.
16. Hacking: Hacking Practical Guide for Beginners / Edited by Jeff Simon. – NY, 2016. – 94 p.
17. Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
18. Pauly Bernadette. Null-Safe Programming: The Kotlin Way / Bernadette Pauly, Erin Gray//Harm Reduction Journal volume 13, Article number: 15 (2016)
19. Муляр І. В. Ієрархічна мережева модель інформаційного забезпечення подання предметної області / В. М. Джулій, І. В. Муляр, О. В. Селюков, В. М. Чешун, Д. В. Коровченко, А. А. Берназ // Збірник наукових праць Військового інституту Київського національного університету

імені Тараса Шевченка. – Київ : ВІКНУ, 2019. – Вип. 65. – С. 27–39.

20. Муляр І.В. Адаптивний метод проектування програмного забезпечення / І. В. Муляр, Є. С. Ленков, С. М. Жовнір, С. Л. Кушнірук // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка.- 2018. – Вип. 61. – С. 124-135.

21. Муляр І.В. Ітераційно-геометричний метод для стійкого перцептуального хешування зображення / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун // Вісник Хмельницького національного університету. Технічні науки. – 2020. – № 1. – С. 76–79.

22. Муляр І.В. Використання розподілених хеш-таблиць надання доступу до хмарних сервісів / Ю. П. Кльоц, І. В. Муляр, В. М. Чешун, О. В. Бурдюг // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Київ : ВІКНУ, 2020. – Вип. 67. – С. 85–95.

23. Муляр І.В. Симетрична криптосистема з нелінійним шифруванням та можливістю контролю шифротексту з метою маскування / В. А. Анікін, В. М. Джулій, І.В. Муляр, В.С. Орленко, В.Ю. Тітова // Вісник Хмельницького національного університету. Технічні науки. – 2020. – № 6. – С. 12-16.

24. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. – Хмельницький: ХмНУ, 2020. – 196 с.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань) Доступ до ресурсу: <https://msn.khmnu.edu.ua/course/view.php?id=5941>

2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/plage_lib.php.