

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки



ЗАТВЕРДЖУЮ

Декан ФІТ

Гетяна ГОВОРУЩЕНКО

«31» серпня 2024 р.

СИЛАБУС

Навчальна дисципліна: “ Алгоритми та структури даних ”

Освітньо-професійна програма: «Кібербезпека»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Муляр Ігор Володимирович
Профайл викладач(ів)	https://kb.khmnu.edu.ua/mulyar-igor-volodymyrovych
Е-mail викладача(ів)	muliariv@khmnu.edu.ua
Контактний телефон	+3 8 067 938-15-44
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=5941
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/5011940672 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр V (осінньо-зимовий)
Консультації	Очні: згідно графіку консультацій Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

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

Анотація дисципліни

Дисципліна «Алгоритми та структури даних» є вибірковою, викладається для студентів очної денної форми навчання, рекомендована для здобувачів вищої освіти за освітньо-професійною програмою «Кібербезпека» першого (бакалаврського) рівня, охоплює сучасні методи представлення даних в пам'яті комп'ютера та основних алгоритмів їх опрацювання для практичного використання при проектуванні систем захисту інформації.

Пререквізити –.

Кореквізити –.

Анотація дисципліни

Дисципліна «Алгоритми та структури даних» - 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.

При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні та репродуктивні, застосування інформаційно-комп’ютерних технологій.

Мета і завдання дисципліни

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:

- вміння застосовувати та аналізувати різні фундаментальні та вдосконалені алгоритми для розв’язування задач захисту інформації,
- здатність будувати та здійснювати раціональний вибір алгоритму для конкретної складної спеціалізованої задачі з відомих класів алгоритмів на основі обраних критеріїв.

результати навчання:

- застосовувати знання алгоритмів та структур даних у практичних ситуаціях;
- розробляти алгоритми розв’язання прикладних задач, на підставі базових алгоритмічних структур;
- знати методи представлення даних в пам’яті комп’ютера та основні алгоритмів їх опрацювання;
- розробляти та аналізувати ефективність алгоритмів в системах захисту;
- володіти навичками розробки та налагодження програм на одній з алгоритмічних процедурних мов програмування високого рівня (Python, C++);
- володіти способами конструювання складних структур даних на базі простих структур даних.

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

Тематичний і календарний план вивчення дисципліни

Номер тижня	Номер теми	Тема лекції*	Тема лабораторної роботи**	Самостійна робота студента		
				Зміст	Години	Лігера-тура
1	2	3	4	5	6	7
1	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		Опрацювання теоретичного матеріалу, підготовка до виконання ЛР1	8	Літ.: [3] с.1-41; [9] с.5-83; [15]..
2	1	Алгоритми та дані. Структурування і абстракція програм. Алгоритми. Формалізація алгоритмів. Алгоритм та оцінка його складності. Асимптотична оцінка складності алгоритмів.	ЛР1. Способи організації списків (масивів) у Python. Функції.	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР1	8	Літ.: [1] с.94-98; [5] с.48-95; [6] с.8-21; [8] с.25-32.
3	1	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.		Опрацювання теоретичного матеріалу, підготовка до виконання ЛР2	8	Літ.: [4] с.4-103; [9] с.84-141; [10] с.30-48.

4	2	Списки. Односпрямовані і двоспрямовані списки. Структура і типі лінійних списків. Операції із списками.	ЛР2. Квадратичні алгоритми впорядкування масивів. Рекурсивні алгоритми.	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР2	8	Літ.: [1] с.54-64; [5] с.287-309
5	2	Стеки, деки, черги. Реалізація на мові Python. Особливі види черг (деки та черги з пріоритетами). Використання стеків для обчислення виразів.		Опрацювання теоретичного матеріалу, підготовка до виконання ЛР3	8	Літ.: [1] с.72-93; [3] с.123-136; [4] с.138-143; [5] с.48-95
6	2	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.	ЛР3. Оптимізовані алгоритми хешування в Python для роботи з словниками.	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР3	8	Літ.: [3] с.139-145; [5] с.347-361; [9] с.127-151.
7	2	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		Опрацювання теоретичного матеріалу, підготовка до виконання ЛР4	8	Літ.: [1] с.54-64; [2] с.28-69; [4] с.234-265; [5] с.287-309; [8] с.7-24.

		впорядкованим бінарним деревом. СОРТУВАННЯ ПІДРАХУНКОМ.				
8	3	Комбінаторні та рекурсивні алгоритми. Ханойська вежа. Числа Фібоначчі. Перестановки. Підрахунок кількості можливих перестановок. Метод повного перебору. Методи сортування з використанням рекурсії.	ЛР4. Одно та двоспрямовані списки. Стеки та черги у Python.	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР4	8	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.
9	3	Алгоритми пошуку. Послідовний (лінійний) пошук. Бінарний пошук. Бінарний пошук з використанням дерев. Метод інтерполяції. Метод „золотого перерізу”. Алгоритми пошуку послідовностей. Алгоритм Кнута, Моріса, Пратта. Алгоритм Боуєра та Мура.		Опрацювання теоретичного матеріалу, підготовка до виконання ЛР5	8	Літ.: [1] с.40-54, с.99-130; [4] с.267-275; [5] с.310-334.
10	3	Динамічне програмування. Використання динамічного програмування. Дерево Фібоначчі. Задача про стрибунця.	ЛР5. Використання бінарних дерев в алгоритмах захищених групових комунікацій. Опрацювання нелінійних структур даних, представлених у вигляді бінарних дерев.	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР5	8	Літ.: [1] с.169-171; [5] с.416-452.
11	3	Фундаментальні алгоритми на графах і деревах. Способи задання графів. Пошук в ширину. Пошук у глибину. Алгоритм визначення компонент		Опрацювання теоретичного матеріалу, підготовка до виконання ЛР6	8	Літ.: [1] с.130-156; [2] с.117-130; [4] с.167-184.

		двоzv'язності.				
12	3	Пошук найкоротших шляхів на графах. Жадібні алгоритми. Алгоритм Дейкстри. Алгоритм Прима. Алгоритм Краскала. Алгоритм Флойда - Фелкерсона. Використання алгоритмів на графах при побудові захищених програм.	ЛР6. Способи задання графів. Неорієнтовані графи. Способи обходу графів: DFS та BFS алгоритми.	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР6	8	Літ.: [1] с.157-168; [2] с.131-136; [3] с.185-205; [4] с.184-203; [5] с.242-286, 390-398.
13	3	Алгоритми і структури даних в задачах криптографічного шифрування. Класифікація криптографічних алгоритмів. Таблиці шифрування та алгоритми шифрування за таблицями. Одноalfавітні та поліalfавітні таблиці шифрування. Функція Ейлера і її застосування в криптографії.		Опрацювання теоретичного матеріалу, підготовка до виконання ЛР7	10	Літ.: [7] с.15-25; [7] с.62-72; [16] с.48-76; [24].
14	3	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.	ЛР7 Використання алгоритмів пошуку найкоротших шляхів на графах для моделювання поширення забороненої інформації.	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР7	10	Літ.: [2] с.93-100; [3] с.145-151; [5] с.347-361; [16] с.284-308; [22, 23].
15	3	Алгоритми рандомізації як спосіб руйнування статистичних		Опрацювання теоретичного матеріалу, підготовка до до	10	Літ.: [3] с.281-296; [7] с.15-25; [24].

		<p>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 маскуванню.</p>		виконання ЛР8		
16	4	<p>Побудова і аналіз алгоритмів. Проектування алгоритмів. Характеристики алгоритму. Ефективність алгоритмів. Правила аналізу складності алгоритмів. Способи реалізації алгоритмів. Документація алгоритмів. Методи розробки алгоритмів.</p>	<p>ЛР8. Використання бібліотеки BeautifulSoup для парсингу сайтів на присутність забороненого контенту.</p>	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР8.	8	Літ.: [4] с.204-220; с.18-22; [5] с.387-415.
17	4	<p>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.</p>	Тестування.	Опрацювання теоретичного матеріалу, підготовка до тестування	8	Літ.: [1] с.22-36; [5] с.18-22; [16] с.80-93.

18	4	Класи складності P і NP. 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.	Підсумкове заняття	Опрацювання теоретичного матеріалу.	8	Літ.: [5] с.255-286, с.453-470.
----	---	---	--------------------	-------------------------------------	---	---------------------------------

* лекції проводяться по 2 години.

** лабораторні роботи проводяться раз у два тижні по 6 годин.

Політика дисципліни.

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції і лабораторні роботи згідно з розкладом, не запізнюватися на заняття, самостійну роботу та інші домашні завдання виконувати відповідно до графіка. Пропущену лабораторну роботу студент зобов'язаний опрацювати самостійно у повному обсязі і відзвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. До лабораторних робіт студент має підготуватися за відповідною темою і проявляти активність. Набутті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ <https://www.khnu.km.ua/root/files/01/10/03/006.pdf>.

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 графи 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 MOODLE.

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 задачі підсумкового контрольного заходу не допускається.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС 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 студентів

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 маскуваня.
61. Алгоритми рандомізації як спосіб руйнування статистичних залежностей і захисту структурованих даних.

Методичне забезпечення

Навчальний процес з дисципліни забезпечений необхідними навчально-методичними розробками в модульному середовищі на сторінці дисципліни <https://msn.khnu.km.ua/course/view.php?id=5941>

Рекомендована література

Основна

№	Назва	Режим доступу
1.	Кренивч А.П. Алгоритми та структури даних: навчальний посібник / А.П. Кренивч. – К.: ВПЦ "Київський Університет", 2018. – 777 с.	https://drive.google.com/drive/folders/0AOwk3E6vGowtUk9PVA
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.	http://dSPACE.kntu.kr.ua/jspui/bitstream/123456789/8944/1/Алгоритми%20та%20структури%20даних.pdf
3.	Data Structures And Algorithmic with Python / Editors: Kent D. Lee• Steve Hubbard. – Switzerland: Springer International Publishing, 2015, – 369 p.	https://www.pdfdrive.com/data-structures-and-algorithms-with-python-d157864792.html
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.	http://194.44.152.155/elib/local/2399.pdf
5.	Data Structures And Algorithmic Thinking With Python / Edited by Narasimha Karumanchi. – Carecr Monk Publications, 2016. – 471 p.	https://www.pdfdrive.com/data-structure-and-algorithmic-thinking-with-python-data-structure-and-algorithmic-puzzles-d158071362.html
6.	Алгоритми та структури даних: конспект лекцій. Частина 1. Структури даних / О.Д. Воробйова, Л.В. Глазунова – Одеса: ОНАЗ ім.О.С. Попова, 2017. – 48с.	https://metod.onat.edu.ua/download/417
7.	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.	https://metod.onat.edu.ua/download/418
8.	Власій О.О. Алгоритми та структури даних: лабораторний практикум / О. О. Власій. – Івано-Франківськ: ДВНЗ «Прикарпатський національний університет імені Василя Стефаника», 2015. – 68 с.	http://194.44.152.155:8080/bitstream/123456789/2516/1/Vlasi%20ASD.pdf
9.	Кренивч А.П. Python у прикладах і задачах. Частина 1. Структурне програмування: навчальний посібник / А.П. Кренивч. –К.: ВПЦ "Київський Університет", 2017. – 206 с.	http://www.matfiz.univ.kiev.ua/uploads/books/python2017.pdf
10.	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.	http://eadnurt.diit.edu.ua/bitstream/123456789/11146/1/Iyman_et_al_2019.pdf

Додаткова

11.	Data Structures And Algorithms Made Easy / Edited by Narasimha Karumanchi. – Carecr Monk Publications, 2017. – 828 p	https://www.pdfdrive.com/data-structures-and-algorithms-made-easy-data-structures-and-algorithmic-puzzles-d158226594.html
12.	Python & Algorithms 2.0. A Guide to Learn how to Fly / Edited by Marina Wahl. – NY, 2014. – 244 p.	https://www.pdfdrive.com/algorithms-and-data-structure-in-python-d25944697.html
13.	Data Structures And Algorithmic in Python / Editors: Michael T. Goodrich, Roberto Tamassia, Michael H. Goldwasser. – John Wiley &	https://www.pdfdrive.com/data-structures-and-algorithms-

	Sons, Inc, 2013. – 770 p	in-python-d25119593.html
14.	Алгоритми та структури даних: методичні вказівки до виконання лабораторних робіт / Н.К. Стратієнко, І.О. Бородіна. – Харків : НТУ «ХПІ», 2017. – 36 с.	http://repository.kpi.kharkov.ua/bitstream/KhPI-Press/26426/1/prohramy_2017_Alhorytmy_i_struktury_danykh.pdf
15.	Hacking: Hacking Practical Guide for Beginners / Edited by Jeff Simon. – NY, 2016. – 94 p.	https://www.pdfdrive.com/hacking-hacking-practical-guide-for-beginners-hacking-with-python-d182434771.html
16.	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.	https://drive.google.com/file/d/1jACvCh2O4duJOYA3uLUID8cdVf2EFSWU/view?usp=sharing
17.	Pauly Bernadette. Null-Safe Programming: The Kotlin Way / Bernadette Pauly, Erin Gray//Harm Reduction Journal volume 13, Article number: 15 (2016)	https://dzone.com/articles/null-safe-programming-the-kotlin-way
18.	Благирев А. П. Big Data простим язиком./ А. П. Благирев. – АСТ, 2019г. – 256с	http://loveread.ec/view_global.php?id=79998
19.	Простой Python. Современный стиль программирования / Любанович Билл – СПб.: Питер, 2016. – 480 с.	https://ru.pdfdrive.com/Простой-python-Современный-стиль-программирования-d186869656.html
20.	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	http://elar.khnu.km.ua/jspui/handle/123456789/9618
21.	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.	http://elar.khnu.km.ua/jspui/handle/123456789/7046
22.	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	http://elar.khnu.km.ua/jspui/handle/123456789/8940
23.	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	http://elar.khnu.km.ua/jspui/handle/123456789/9620
24.	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. 12-19.	http://journals.khnu.km.ua/ve-stnik/wp-content/uploads/2021/03/VKNU-TS-2020-N6-291.pdf
25.	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.	https://drive.google.com/file/d/1-ZmFMuTkL5VnBgh1bXNfD6nODchxWI4U/view?usp=sharing

ІНФОРМАЦІЙНІ РЕСУРСИ

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

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

Розробник

_____ Підпис к.т.н., доцент І.В. Муляр
Вчений ступінь, звання Ініціали, прізвище викладача(ів)

Погоджено

Гарант освітньої програми

_____ Підпис к.т.н., доцент В.М. Чешун
Вчений ступінь, звання Ініціали, прізвище

Зав. кафедри кібербезпеки та комп'ютерних систем і мереж

_____ Підпис к.т.н., доцент Ю.П. Кльоц
Вчений ступінь, звання Ініціали, прізвище