Міністерство освіти і науки України
Західноукраїнський національний університет

Затверджую
Проректор з наукової роботи
_____ З.-М. Задорожний

ПРОГРАМА
вступного іспиту на здобуття наукового ступеня
доктора філософії зі спеціальності
123 – Комп'ютерна інженерія

Схвалено
на засіданні приймальної комісії
ЗУНУ 22.02.2023 р. протокол №2

Схвалено на засіданні кафедри
комп'ютерної інженерії,
протокол № 7
від «30» січня 2023 р.

Завідувач кафедри,
к.т.н., доцент _____ Леся Дубчак

КОМП'ЮТЕРНА КРИПТОГРАФІЯ

Задачі криптографії. Основні поняття та положення комп'ютерної криптографії. Принципи криптографічного захисту інформації. Криптоаналітичні атаки, їх види. Шифри перестановки: скитала, частоколу, шифруючі таблиці, шифр магічних квадратів, шифр Кардано. Шифри простої заміни: атбаш, полібіанський квадрат, шифр Цезаря, шифр Цезаря з ключовим словом, шифруючі таблиці Трисемуса.

Біграмний шифр Плейфейра. Подвійний квадрат Уїтстона. Шифр чотирьох квадратів. Шифр ADFGVX. Шифр Гронсфельда. Шифр Гронсфельда з ключовим словом. Шифр Віженера. Шифр Віженера з ключовим словом. Роторні шифрувальні машини, Enigma. Шифр одноразового блокноту.

Структура алгоритму DES, його переваги та недоліки. Операції алгоритму DES, функція шифрування алгоритму DES. Генерація підключів алгоритму DES. Режими роботи алгоритму DES. Структура алгоритму IDEA, його переваги та недоліки. Операції алгоритму IDEA. Генерація підключів алгоритму IDEA. Загальна структура алгоритму ГОСТ28147–89, його переваги та недоліки. Операції алгоритму ГОСТ28147–89. Генерація підключів алгоритму IDEA. 1Режими роботи алгоритму ГОСТ28147–81. Галузі застосування алгоритмів IDEA та ГОСТ28147–89.

Основні поняття. Алгоритм Евкліда, його наслідок, пошук оберненого елемента, китайська теорема про остачі. Функція Ейлера. Теореми Ейлера та Ферма.

Опис криптосистеми RSA. Генерування ключів. Шифрування та дешфрування. Коректність, ефективність та надійність криптосистеми.

Генерування ключів криптосистеми Рабіна. Шифрування та дешифрування в криптосистемі Рабіна. Коректність, ефективність та надійність криптосистеми. Криптосистема Ель–Гамаля. Шифрування та дешифрування в криптосистемі Ель–Гамаля. Коректність, ефективність та надійність криптосистеми.

Поняття електронного цифрового підпису. Електронний цифровий підпис в системах RSA та Ель–Гамаля. Алгоритм DSA. Система Шнорра. Ефективність, достовірність та конфіденційність підписів у різних алгоритмах.

Поняття криптографічного протоколу. Протоколи обміну ключем, жеребу по телефону, розподілу таємниці.

Поняття криптоаналізу. Частотний аналіз. Метод зустрічі посередині. Метод «парадоксу днів народження».

Література

1. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко,В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.

2. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

3. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Проведення робіт.

4. Закон України «Про державну таємницю» від 21.01.1994 // Відомості Верховної Ради України, 1994, No 16. – Ст. 93.

5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від Відомості Верховної Ради України, 1994, No 31. – Ст. 286, із змінами 2005 р.

6. Закон України «Про інформацію» // Відомості Верховної Ради, 1992, No 48. – Ст. 650 – 651.

7. Остапов С.Е. Кібербезпека: сучасні технології захисту / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – К.:.Новий світ-2000, 2020. – 678 с. 17. Хорошко В. О. Проєктування комплексних систем захисту інформації./ В.О. Хорошко. – Львів: Видавництво Львівської політехніки, 2020. – 317 с.

СИНТЕЗ ТА МОДЕЛЮВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Поняття про об'єкт моделювання (проектування) та його основні параметри. Поняття моделі та моделювання. Види моделей. Поняття алгоритму та види алгоритмів. Поняття методу та види методів. Поняття гіпотези та теорії. Поняття методології та технології моделювання.

Види опису математичних моделей. Класифікація математичних моделей. Вимоги до математичних моделей. Алгоритм побудови математичної моделі. Основні параметрі математичних моделей. Поняття точності, адекватності та області адекватності ММ. Основні параметри методів та алгоритмів. Поняття достовірності результатів моделювання. Поняття про обчислювальний експеримент. Приклади побудови математичних моделей елементів СКС. Моделі, алгоритми та методи для багаторівневого моделювання СКС.

Особливості мереж Петрі. Прості мережі Петрі. Параметри мереж Петрі. Розширення мереж Петрі. Особливості побудови моделей для аналізу СКС на основі мереж Петрі. Приклади використання моделей на основі мереж Петрі для аналізу СКС. Основи систем масового обслуговування. Класифікація систем масового обслуговування. Відкриті системи масового обслуговування. Закриті системи масового обслуговування. Особливості розв'язання задач аналізу СКС з використанням моделей на основі систем масового обслуговування. Приклади використання моделей СМО для аналізу СКС.

Основні відомості та поняття про оптимізацію. Поняття критерія оптимізації та цільової функції. Поняття обмежень цільової функції. Постановка оптимізаційної задачі. Алгоритм постановки оптимізаційної задачі. Геометрична інтерпритація цільової функції. Поняття глобального та локального оптиуму. Класифікація методів рішення оптимізаційних задач.

Особливості задач одновимірної оптимізації. Умови існування екстремуму функції однієї змінної. Класифікація методів одновимірної оптимізації. Метод Ньютона-Рафсона, метод Пауела, метод ділення інтервалу наполовину та метод золотого січення. Порівняльна характеристика методів одновимірного пошуку.

Поняття багатопараметричної оптимізації. Умови існування екстремуму функції багатьох змінних. Класифікація методів рішення задач нелінійного програмування. Особливості методів прямого пошуку. Метод пошуку по

симплексу. Метод Нелдера-Міда. Метод Хука-Джівса. Особливості градієнтних методів оптимізації. Методи першого порядку. Метод Коші. Методи 2-го порядку. Метод Ньютона та його модифікація. Квазіньютонівські методи. Метод Девідона. Метод Флетчера-Пауела. Метод Флетчера-Рівса. Узагальнений алгоритм градієнтних методів. Особливості методів умовної оптимізації. Метод множників Лагранжа. Метод штрафних функцій.

Класифікація методів синтезу. Алгоритм розв'язання задач структурного синтезу. Морфологічний метод. Метод гілок та границь. Приклади розв'язання задач структурного синтезу складних систем та мереж. Класифікація евристичних методів синтезу. Метод "мозкового штурму". Методи асоціацій та аналогій. Синектика. Методи контрольних запитань та колективного блокноту. Метод "матриць відкриття". Засоби автоматизованого синтезу комп'ютерних систем та мереж.

Література

1. Березький О.М., Теслюк В.М., Дубчак Л.О., Мельник Г.М., Батько Ю.М.Дослідження і проектування комп'ютерних систем та мереж: навчальний посібник. Тернопіль: ЗУНУ, 2022. 251 с.
2. Ловейкін В.С., Ромасевич Ю.О. Теорія технічних систем. К.: ЦП „КОМПРИНТ", 2017. 291 с.
3. Моделювання та оптимізація систем: підручник /[Дубовой В. М., Квєтний Р. Н., Михальов О. І., А.В.Усов А. В.]. Вінниця : ПП «ТД«Еднльвейс», 2017. 804 с.
4. Системний підхід і моделювання в наукових дослідженнях [текст] :підручник. / За заг. ред. Бутка М. П. [М. П. Бутко, І. М. Бутко, М. Ю.Дітковська та ін.]. К.: «Центр учбової літератури», 2014. 360 с
5. Виклюк Я.І., Камінський Р.М., Пасічник В.В. Моделювання складних систем: посібник. Львів: Видавництво «Новий Світ – 2000», 2020. 404 с.11
6. Стеценко, І.В. Моделювання систем: навч. посіб. [Електронний ресурс, текст] / І.В. Стеценко; М-во освіти і науки України, Черкас. держ. технол.ун-т. Черкаси : ЧДТУ, 2010. 399 с.
7. Теслюк В.М. Математичне моделювання в САПР: Ч.1. Конспект лекцій з курсу "Математичне моделювання в САПР" для студентів базового напрямку "Комп'ютерні науки". Львів: Видавництво Національного університету "Львівська політехніка", 2009. 64 с.
8. Jensen K., Kristensen L.M., Coloured Petri Nets: modelling and validation of concurrent systems: 1st edition – 2009, Springer. 395 p.
9. Teslyuk V., Hamza Al-Shavabkeh, Pereyma M., Al Omari Tarik The formalization of the MEMS automated design process by usage of Petri Networks. Proc.of the IIId International Conference of Young Scientists (MEMSTECH'2007). Lviv - Polyana, May, 23-26, 2007. P.133 - 134.
10. Теслюк В.М., Андрійчук М.І. Конспект лекцій з курсу «Методи синтезу та оптимізації» для студентів базового напряму «Комп'ютерні науки», Ч.1. Львів, 2018. 64 с.
11. Теслюк В.М., Пелешко Д.Д. Методи цілочисельного програмування та нульового порядку. Конспект лекцій з курсу «Методи синтезу та

оптимізації» для студентів базового напряму 6.050101 «Комп'ютерні науки», Ч.2. Львів, 2018. 84 с.

ДОСЛІДЖЕННЯ МЕРЕЖЕВИХ ОПЕРАЦІЙНИХ СИСТЕМ»

Основні терміни та визначення ОС. Архітектура сучасних ОС. Мережеві функції ОС. Архітектури мікропроцесорів. Адміністрування ОС. Віртуалізація

Основні функції ОС Windows 2008. Вимоги до обладнання. Процес завантаження. Архітектура ОС Windows 2008. Підсистеми режиму ядра. Диспетчер процесів. Ресурси прикладних програм.

Основні функції ОС. Вимоги до обладнання. Архітектура ОС. Модулі ядра ОС Linux. Ресурси прикладних програм. Процес завантаження. Емулятор терміналу. Пакети прикладних програм. Диспетчери файлів.

BIOS та завантажувачі системи. Процес завантаження ядра та драйверів ОС Linux. Програми завантажувачі ОС Linux GRUB, syslinux, lilo. Завантажувач ОС Windows ntldr. Процес завантаження ядра та драйверів ОС Windows. Робота зі службами.

Служби ОС Windows Server 2008. Системні утиліти Windows. Служби ОС Linux. Команди ОС Linux. Аналіз продуктивності серверів. Аналіз продуктивності прикладних програм (застосувань).

Призначення та функції. Службові символи. Змінні і параметри. Перевірка умов. Оператори та числові константи. Цикли. Зовнішні та внутрішні команди, програми та утиліти.

Призначення та функції. Змінні і параметри. Члени та змінні об'єктів. Перевірка умов. Цикли. Функції Зовнішні та внутрішні команди, програми та утиліти.

Управління обліковими записами і ресурсами в середовищі Microsoft Windows Server 2008. Управління користувацьким та системним середовищем за допомогою групової політики. Управління користувачами і групами ОС Linux. Управління правами доступу до файлів і каталогів.

Основні характеристики жорстких дисків. Програмні та апаратні RAID масиви. Файлові системи сучасних операційних систем. Основні характеристики продуктивності мережевого обладнання. Фактори впливу на завантаженість мережі.

Критерії визначення безпеки комп'ютерних систем. Критерії цінності інформації. Резервування інформації. Безпечне знищення даних на жорсткому диску. Антивірусний захист. Мережевий фільтр. Обмеження прав користувачів. Системні бази даних. Захист у безпровідних комп'ютерних мережах. Системи виявлення та протидії вторгнень на базі ОС Linux.

Встановлення і налаштування веб-сервера Apache. Встановлення і налаштування веб-сервера IIS. Системні вимоги веб-серверів. Розподіл дискового простору. Адміністрування прав користувачів. Налаштування мережевого екрану. Моделювання навантаження при впровадженні сервера.

Сервери Microsoft SQL та PostgreSQL. Системні вимоги серверів баз даних. Розподіл дискового простору. Адміністрування прав користувачів.

Налаштування мережевого екрану. Моделювання навантаження при впровадженні сервера.

Література

1. Stallings W. Operating Systems: Internals and Design Principles (8th Ed). William – Pearson, 2015. 800 p.

2. Шеховцов В. А. Операційні системи : підруч. для студ. вищ. навч. закладів, які навч. за напрямами "Комп'ютерні науки", "Комп'ютеризовані системи, автоматика і управління", "Комп'ютерна інженерія", "Прикладна математика". К.: ВНV, 2008. 576 с.

3. Arpaci-Dusseau R. H., Arpaci-Dusseau A. C. Operating Systems: Three Easy Pieces. Arpaci-Dusseau Books, 2018. 714p. URL: https://pages.cs.wisc.edu/~remzi/OSTEP/

4. Shotts W. The Linux Command Line, 2nd Edition: A Complete Introduction. 2019. 555 p. URL: http://linuxcommand.org/tlcl.php

МЕТОДИ РОЗПІЗНАВАННЯ ЗОБРАЖЕНЬ І КОМП'ЮТЕРНИЙ ЗІР

Поняття цифрової обробки зображень. Приклади областей застосування цифрової обробки зображень: формування зображень за допомогою гамма-променів, рентгенівські зображення, зображення в ультрафіолетовому діапазоні, зображення у видимому та інфрачервоному діапазонах, зображення в мікрохвильовому діапазоні, зображенні в діапазоні радіохвиль. Основні стадії обробки цифрових зображень. Компоненти системи обробки цифрових зображень.

Світло і електромагнітний спектр. Зчитування та регістрація зображень: регістрація за допомогою одиночного, лінійки і матриці сенсорів. Модель формування зображень. Дискретизація та квантування зображень. Представлення зображення. Просторова і яскравістна роздільна здатність. Ефекти муара і накладання спектрів. Збільшення та зменшення цифрових зображень. Співвідношення між пікселами. Лінійні та нелінійні перетворення.

Градаційні перетворення. Логарифмічні перетворення. Степеневі перетворення. Кусково-лінійні функції перетворення. Перетворення гістограми. Покращення зображень на основі арифметично-логічних операцій. Методи просторової фільтрації.

Вступ до фур'є-аналізу. Згладжувальні частотні фільтри. Частотні фільтри підвищеної різкості. Гомоморфна фільтрація. Швидке перетворення Фур'є.

Піраміди зображень. Субсмугове кодування. Перетворення Хаара. Кратномасштабний розклад. Вейвлет-функції. Одномірне вейвлет-перетворення. Дискретне вейвлет-перетворення. Швидке вейвлет-перетворення. Двомірне вейвлет-перетворення.

Виявлення розривів яскравості. Зв'язування контурів і знаходження границь. Порогова сегментація. Сегментація з глобальним порогом. Сегментація з адаптивним порогом.

Сегментація на основі нарощування областей. Алгоритми центроїдного зв'язування. Алгоритми злиття-розщеплення. Морфологічна сегментація. Сегментація на основі кластеризації. Сегментація на основі водоподілу.

Поняття контура зображень. Алгоритми проходження контуром. Алгоритм «жука». «Moore-Neighbor Tracing» алгоритм. „Redial Sweep" алгоритм. «Theo Pavlidi's Algorithm» алгоритм. Алгоритм проходження контуром з можливістю зворотного ходу.

Представлення контурів за допомогою ланцюгового коду. Апроксимація контурів за допомогою ломаних ліній. Сигнатури. Опис за допомогою скелету області. Дескриптори границь.

Поняття текстури зображення. Дескриптори областей. Статистичні підходи до оцінювання текстури. Структурний підхід. Спектральний підхід. Метод головних компонент. Реляційні дескриптори.

Проблема розпізнавання. Основні поняття. Гнесологічні аспекти розпізнавання. Загальна характеристика розпізнавання і їх типи. Математична теорія розпізнавання образів. Математична постановка задачі розпізнавання образів і зображень.

Формулювання байєсівських задач. Дві властивості байєсівських стратегій. Ймовірність помилкового рішення про стан. Байєсівська стратегія відмови від розпізнавання.

Обмеженість байєсівського підходу. Формулювання небайєсівських задач. Задача Неймана –Пірсона. Мінімаксна задача. Задача Вальда. Двоїсті задачі лінійного програмування. Розв'язок небаєсівських задач на основі теорії двоїстості.

Загальність статистичного розпізнавання. Структрне розпізнавання зображень. Множина спостережень. Множина скритих параметрів зображень. Основні поняття структурного розпізнавання.

Неформальне пояснення двомірних граматик і мов. Двомірні контестно-вільні граматики і мови. Задача на відповідність. Узагальнений алгоритм Кока-Янгера-Касамі. Структурна конструкція для визначення множин об'єктів розпізнавання.

Передумови до використання нейронних мереж. Персептрон для двох класів. Алгоритми навчання. Багатошарові нейронні мережі без зворотного зв'язку та зі зворотнім зв'язком.

Основи методу опорних векторів. Машина опорних векторів для лінійно сепарабельних набрів даних. Алгоритм машини опорних векторів для лінійно сепарабельних даних. Знаходження машини опорних векторів.

Література.

1. Scott Krig. Computer Vision Metrics. Survey, Taxonomy, and Analysis-Apress Berkeley, CA - Scott Krig 2014 – pp. 508

2. Miroslav Kubat. An Introduction to Machine Learning - Springer International Publishing AG 2017 – pp. 348

3. Peter Corke. Robotics, Vision and Control Fundamental Algorithms In MATLAB® Second, Completely Revised, Extended And Updated Edition - Springer

Tracts in Advanced Robotics (STAR, volume 118) – Springer International Publishing AG 2017 – pp. 693

4. Wilhelm Burger , Mark J. Burge. Digital Image Processing An Algorithmic Introduction Using Java - Part of the book series: Texts in Computer Science (TCS) - Springer-Verlag London Ltd., part of Springer Nature 2016 – pp. 811

5. Esteva, A., Chou, K., Yeung, S. et al. Deep learning-enabled medical computer vision. npj Digit. Med. 4, 5 (2021). https://doi.org/10.1038/s41746-020-00376-2 .

6. O'Mahony, Niall, Sean Campbell, Anderson Carvalho, Suman Harapanahalli, Gustavo Velasco Hernandez, Lenka Krpalkova, Daniel Riordan, and Joseph Walsh. "Deep learning vs. traditional computer vision." In Advances in Computer Vision: Proceedings of the 2019 Computer Vision Conference (CVC), Volume 1 1, pp. 128-144. Springer International Publishing, 2020..

7. Yuan, Lu, Dongdong Chen, Yi-Ling Chen, Noel Codella, Xiyang Dai, Jianfeng Gao, Houdong Hu et al. "Florence: A new foundation model for computer vision." arXiv preprint arXiv:2111.11432 (2021).

ДОСЛІДЖЕННЯ І ПРОЕКТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Основні поняття та задачі курсу. Особливості розроблення КСМ. Методологія та методика наукового дослідження КСМ. Методика роботи над рукописом дослідження, особливості підготовки і оформлення результатів дослідження.

Основні поняття та визначення курсу проектування КСМ. Принципи системного підходу до проектування. Поняття системотехніки. Класифікація методів та технологій проектування складних систем та мереж.

Ієрархічні рівні проектування. Стадії проектування. Типові проектні процедури. Елементи технічного завдання на проектування.

Поняття задачі багатокритеріальної оптимізації. Причини багатокритеріальності. Класифікація методів розв'язання задач багатокритеріальної оптимізації. Метод головної компоненти. Метод поступок. Метод комплексного критерію. Метод Гермейєра. Метод справедливого компромісу. Метод умовного центра мас. Метод ідеальної точки. 1Парето множина, оптимальність за Парето. 1Застосування генетичних алгоритмів при розв'язанні задач багатокритеріальної оптимізації.

Методи згортки векторних критеріїв. Особливості методів згортки векторних критеріїв. Побудова функції корисності. Адитивний та мультиплікативний критерії. Мінімаксний та максі мінний критерії. Методи рішення задач векторної оптимізації при наявності інформації про важливість критерія.

Класифікація методів синтезу. Алгоритм розв'язання задач структурного синтезу. Методи генерування множини альтернативних рішень. Метод генерування множини альтернативних рішень на основі І-АБО дерев. Морфологічні таблиці. Методи зменшення потужності множини

альтернативних рішень. Метод гілок та границь. Приклади розв'язання задач структурного синтезу складних систем та мереж.

Класифікація евристичних методів синтезу. Метод "мозкового штурму". Методи асоціацій та аналогій. Синектика. Методи контрольних запитань та колективного блокноту. Метод "матриць відкриття".

Алгоритм розв'язання задач параметричного синтезу. Класифікація типових задач параметричного синтезу. Методи параметричного синтезу з використанням теорії кореляції та чутливості. Приклади розв'язання задач параметричного синтезу систем та мереж.

Література

1. Березький О.М., Теслюк В.М., Дубчак Л.О., Мельник Г.М., Батько Ю.М. Дослідження і проектування комп'ютерних систем та мереж: навчальний посібник. – Тернопіль: ЗУНУ, 2022. 251 с.

2. Теслюк В.М., Загарюк Р.В. Методи багатокритеріальної оптимізації. Конспект лекцій з курсу «Методи багатокритеріальної оптимізації» для студентів базового напряму «Комп'ютерні науки», Ч.1. Львів, 2019. 52с.

3. Теслюк В.М., Андрійчук М.І. Конспект лекцій з курсу «Методи синтезу та оптимізації», Ч.1. Львів, 2018. 64 с.

4. Теслюк В.М., Пелешко Д.Д. Методи цілочисельного програмування та нульового порядку. Конспект лекцій з курсу «Методи синтезу та оптимізації», Ч.2. Львів, 2018. 84 с.

5. Теслюк В.М. Градієнтні методи розв'язання оптимізаційних задач. Конспект лекцій з курсу «Методи синтезу та оптимізації»,Ч.3.Львів, 2018. 67 с.

6. Математичні методи дослідження операцій : підручник / Є. А. Лавров, Л. П. Перхун, В. В. Шендрик та ін. – Суми : Сумський державний університет, 2017. 212 с. https://essuir.sumdu.edu.ua/bitstream-download/123456789/68212/1/Lavrov_matematychni_metody.pdf;jsessionid=A51A5455A8D00EABFFECAC79D1DA66AB.

7. Методи оптимізації та дослідження операцій [Текст] : навчальний посібник / Укладачі: Я. Б. Сікора, А.Й. Щехорський, Б.Л. Якимчук. Житомир: Вид-во ЖДУ ім. Івана Франка, 2019. 148 с.

8. Дослідження операцій. Конспект лекцій / Уклад.: О.І. Лисенко, І.В. Алєксєєва, К: НТУУ «КПІ», 2016. 196 с.

9. Теслюк В.М. Моделі та інформаційні технології синтезу мікроелектромеханічних систем: Монографія. Львів: Видавництво ПП "Вежа і Ко", 2018. 192 с.