

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут»

ЗАТВЕРДЖЕНО

вченою радою
Національного аерокосмічного
університету ім. М.Є. Жуковського
«Харківський авіаційний інститут»
Ректор університету

професор

«22» січня



М.В. Нечипорук

2020 р. протокол № 6

**ПРОГРАМА
ВСТУПНОГО ВИПРОБУВАННЯ**

для конкурсного відбору вступників до аспірантури
для здобуття ступеня доктора філософії зі спеціальностей

- 121 – Інженерія програмного забезпечення**
- 122 – Комп'ютерні науки**
- 123 – Комп'ютерна інженерія**
- 125 – Кібербезпека**

Вступ

Вступне випробування для конкурсного відбору вступників до аспірантури для здобуття ступеня доктора філософії зі спеціальностей 121 – Інженерія програмного забезпечення, 122 – Комп'ютерні науки, 123 – Комп'ютерна інженерія, 125 – Кібербезпека відбувається відповідно до Правил прийому до аспірантури та докторантури Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» у формі індивідуального письмового іспиту, який приймає екзаменаційна комісія, склад якої затверджується наказом ректора Університету.

До іспиту входять питання за розділами та темами:

I. Загальний блок.

1. Методи математичного моделювання.
2. Методи прийняття рішень і оптимізації.

II. Інженерія програмного забезпечення.

1. Архітектура та проектування програмного забезпечення.
2. Аналіз вимог до програмного забезпечення.
3. Бази даних.
4. Проектування програмного забезпечення систем реального часу.
5. Формальний аналіз програмного забезпечення систем.

III. Комп'ютерні науки.

1. Проектування інформаційних систем.
2. Технології комп'ютерного проектування.
3. Методи та системи штучного інтелекту.
4. Інтегровані автоматизовані системи управління.
5. Технології розподілених систем та паралельних обчислень.

IV. Комп'ютерна інженерія.

1. Комп'ютерні мережі та розподілені обчислення.
2. Мікропроцесорні системи.
3. Системне програмування.
4. Організація баз даних.
5. Проектування програмних систем.

V. Кібербезпека.

1. Загрози кібербезпеці.
2. Криптографія.
3. Комплексна система захисту від кіберзагроз.
4. Технології адміністрування та експлуатації систем кіберзахисту.
5. Управління кібербезпекою.

Перелік питань за розділами та темами наведений у програмі.

Критерії оцінювання знань

1. Результати іспиту визначаються за 5 – бальною шкалою.
2. Екзаменаційний білет складається з трьох питань.
3. Мінімальна кількість балів з вступного випробування, з якими вступник допускається до участі у конкурсі складає 3 бала.

Питання за розділами та темами

1. Загальний блок

1. Методи математичного моделювання

Вимоги до математичних моделей (ММ) систем (процесів) і класифікація систем (процесів) з точки зору побудови математичних моделей. Принципи побудови математичних моделей, верифікація та валідація ММ. Характеристика основних етапів побудови ММ. Моделювання систем (процесів) на основі математичного апарату безперервних марковських ланцюгів. Моделювання систем (процесів) масового обслуговування. Моделювання систем (процесів) на основі мереж Петрі. Сутність імітаційного моделювання (ІМ) систем (процесів) і характеристика основних етапів ІМ. Принципи побудови моделюючих алгоритмів (моделювання із постійним кроком та моделювання за особистими станами) та їх порівняльна характеристика.

2. Методи прийняття рішень і оптимізації

Класифікація методів прийняття рішень з точки зору умов визначеності і невизначеності (стохастичної та нестохастичної). Класифікація і загальна характеристика задач оптимізації (математичного програмування). Постановка найбільш розповсюджених задач дискретної оптимізації та особливості методів їх вирішення. Загальна ідея і область застосування методу динамічного програмування, постановка задачі динамічного програмування. Застосування генетичних алгоритмів для рішення задач оптимізації. Використання систем комп'ютерної математики для вирішення задач математичного моделювання і оптимізації.

II. Інженерія програмного забезпечення

1. Архітектура та проектування програмного забезпечення

Призначення і основна мета дисципліни архітектура програмного забезпечення (ПЗ). Основні принципи проектування архітектури ПЗ. Типова архітектура програми. Основні рівні архітектури, їх призначення. Шаблони проектування (Design pattern), їх класифікація та призначення. Шаблони проектування, їх класифікація та призначення. Багатопоточність і особливості її використання в програмному забезпеченні. Основні принципи ідентифікації і реєстрації серверів в СОМ-технології.

2. Аналіз вимог до програмного забезпечення

Вимоги. Класифікація вимог. Атрибути вимог. Процес розробки вимог до ПЗ. Управління вимогами. Низхідний спосіб внесення змін в специфікації вимог.

Способи запису специфікацій вимог до програмного забезпечення. Документування вимог. Документ-концепція. Структура документа-концепції. Методи прототипування вимог до ПЗ.

3. Бази даних

Архітектури баз даних і особливості їх застосування. Модель «сутність – зв'язок» і її використання у базах даних. Цілі і методи нормалізації/денормалізації даних. Цілісність бази даних, методи і засоби її забезпечення. Мови визначення даних (Data definition language) та маніпулювання даними (Data manipulation language) і їх використання для побудови баз даних. Транзакції, збережені процедури, тригери і їх використання у базах даних.

4. Проектування програмного забезпечення систем реального часу

Загальні принципи побудови систем реального часу. Організація вводу-виведення. Особливості побудови систем реального часу. Взаємодія та синхронізація процесів. Забезпечення надійності, реактивності, детермінованості. Планування задач. Служба часу в ОС. Шаблони проектування систем реального часу: архітектура, управління ресурсами, шаблони для забезпечення надійності та функціональної безпеки. Програмні засоби систем супервізорного управління та збору даних (SCADA - Supervisory Control And Data Acquisition). Область застосування.

5. Формальний аналіз програмного забезпечення систем

Моделі і методи прийняття ідентифікаційних і прогнозних рішень як інструмент формального аналізу ПЗ. Прийняття рішень в умовах визначеності/невизначеності, ризику. Критерії прийняття рішень. Еволюція методів формального аналізу у контексті розвитку програмної інженерії загалом. Аналіз ПЗ на основі класичних методів аналізу програмного забезпечення систем. Методи обробки нечіткої інформації при формальному аналізі ПЗ. Нечіткі відношення та нечітке логічне виведення. Аналіз нечітких експертних заключень. Прийняття рішень в нечітких умовах.

III. Комп'ютерні науки

1. Проектування інформаційних систем

Стилі проектування "зверху вниз" і "знизу вгору". Багаторівнева архітектура інформаційних систем. Структурний і об'єктно-орієнтований підходи в проектуванні інформаційних систем. Проектування на основі даних і проектування на основі тестів. Компонентне і сервіс-орієнтоване проектування.

2. Технології комп'ютерного проектування

Сучасні стандарти розробки інформаційних систем. Типове проектування інформаційних систем. Методи і засоби прототипного проектування. Методології моделювання предметної галузі. Структурна модель предметної галузі. Моделювання бізнес-процесів засобами Bpwin. Уніфікована мова візуального моделювання UML.

3. Методи та системи штучного інтелекту

Коефіцієнт розгалуження. Фактор розгалуження. Диз'юнктивна нормальна форма. Алгоритм нормалізації. Принцип резолюцій. Алгоритм Девіса і Патнема. Механізм доповнення для обчислення коефіцієнта визначеності укладення.

4. Інтегровані автоматизовані системи управління

Існуючі підходи до інтеграції в сучасних інформаційних системах. Основні поняття сервісно-орієнтованої архітектури (SOA). Web-сервіси. Стандарти для Web-сервісів: SOAP, WSDL, UDDI. Мова BPEL для опису бізнес-процесів. Інтеграційні платформи: особливості, класифікація та типова структура.

5. Технології розподілених систем та паралельних обчислень

Розподілені та паралельні обчислення: основні поняття. Шляхи досягнення паралелізму. Класифікація сучасних обчислювальних систем. Систематика Фліна та її деталізація. Архітектура GRID: рівні та головні компоненти, протоколи та інтерфейси. Хмарні обчислення та GRID-комп'ютинг. Характеристики та особливості мультиагентних систем.

IV. Комп'ютерна інженерія

1. Комп'ютерні мережі та розподілені обчислення

Кабельна система комп'ютерних мереж. Структурована кабельна система (СКС): структура, підсистеми, вимоги щодо протяжності кабельних сегментів, стандарти СКС. Технології бездротових мереж. Бездротові мережі Wi-Fi сімейства IEEE802.11. Метод доступу CSMA/CA. Частотні канали. Режими роботи: Ad-hoc, Infrastructure. Принципи розгортання бездротових мереж. Протоколи маршрутизації. Дистанційно-векторні протоколи. Протоколи стану лінії зв'язку. Різниця у принципах роботи. Протоколи внутрішньої та зовнішньої маршрутизації. Особливості реалізації протоколів RIP, OSPF, EIGRP. СКС Віртуальні приватні мережі. Типи та протоколи віртуальних приватних мереж. Протокол IPSec. Користування VPN-з'єднанням для доступу до Internet. Розподілені та паралельні обчислення. Шляхи досягнення паралелізму. Класифікація сучасних обчислювальних систем. Систематика Фліна та її деталізація. Хмарні технології та Інтернет речей (IoT). Архітектури хмарних сервісів. Побудова та технології створення IoT-систем.

2. Мікропроцесорні системи

Інтерфейси мікропроцесорних систем (МПС). Системні інтерфейси. Інтерфейси розширення. Інтерфейси ISA, PCL, PCIN. Інтерфейси периферійного обладнання МПС, інтерфейси USB, CAN, SATA. Управління енергоспоживанням в МПС системі, способи зниження енергоспоживання. Робота МПС в режимі реального часу, таймери, лічильники, процесори подій. Мультимікропроцесорні системи: класифікація, способи організації, синхронізація. Технології програмування вбудованих систем.

3. Системне програмування

Механізми віртуальної пам'яті в ОС Windows. Менеджер віртуальної пам'яті та його алгоритм роботи. API для роботи з пам'яттю за прямими віртуальними адресами. Багаторівнева модель додатків Windows. Ресурси, пов'язані з процесами і потоками. Градація пріоритетів для процесів і потоків. Архітектура віконних додатків Windows. Цикли обробки віконних повідомлень. Віконні процедури та повідомлення Windows. Загальна характеристика Win32 API. Створення віконного інтерфейсу на Win32 API, базові функції і структури. Створення багато потокових додатків на Win32 API. Загальні принципи побудови ОС реального часу. Взаємодія та синхронізація процесів. Забезпечення надійності, реактивності, детермінованості. Планування задач. Служба часу в ОС. Шаблони проектування систем реального часу: архітектура, управління ресурсами, шаблони для забезпечення надійності та функціональної безпеки.

4. Організація баз даних

Теоретичні основи реляційних БД: загальні поняття, таблиці та зв'язки між ними, типи зв'язків. Мови визначення даних (Data definition language) та маніпулювання даними (Data manipulation language) і їх використання для побудови баз даних. Транзакції, збережені процедури, тригери і їх використання у базах даних. Проектування сховищ баз даних, нормалізація, приведення сховищ даних до нормальних форм та денормалізація. Сучасні технології доступу до баз даних на стороні клієнта. Загальні принципи роботи з базами даних із клієнтських додатків. Бібліотека JDBC. Класи та методи бібліотек JDBC и ADO.NET. Основи технологій Big data.

5. Проектування програмних систем

Моделі, каркаси і зразки проектування програмних систем (ПС). Стандарти, нотація і інструментальні засоби детального проектування ПС. Якість і надійність програмних систем. Тестування ПС на основі підходів чорного ящика, білого ящика і сірого ящика. Інструментальні засоби інтегрального і системного тестування ПС. Організація процесу супроводження ПС і методи супроводження.

V. Кібербезпека

1. Загрози кібербезпеці

Типи атак на інформаційні ресурси та системи. Атаки доступу. Атаки модифікації. Комбіновані атаки. Переповнення буферу. DoS-атака. SQL-ін'єкція. Шкідливе програмне забезпечення. Типи вірусів. Механізми зараження. Пошук вірусів. Системи антивірусного захисту. Трояни. Комп'ютерні «черв'яки». Сканери атак. Евристичні аналізатори. Аналіз коду підозрілих об'єктів. Поведінковий аналіз.

2. Криптографія

Криптосистеми та криптопротоколи: базові поняття, призначення, класифікація. Симетричні криптоалгоритми. Асиметричні криптоалгоритми.

Цифровий підпис. Автентифікація користувачів. Механізми розподілу ключів. Методи побудови і аналізу криптосистем. Основні стандарти щодо реалізації криптосистем.

3. Комплексна система захисту від кіберзагроз

Нормативно-правова база. Програмні засоби захисту. Технічні засоби захисту. Механізми захисту мереж. Аналіз трафіку. Безпека в безпроводних мережах. Безпека в операційних системах. Функціональна безпека і кібербезпека. Стандарти, методи оцінювання та забезпечення функціональної безпеки.

4. Технології адміністрування та експлуатації систем кіберзахисту

Основи технології адміністрування та експлуатації систем кіберзахисту (СКЗ). Адміністрування процесу проектування СКЗ. Адміністрування процесу вводу в експлуатацію СКЗ. Технічна експлуатація та обслуговування СКЗ. Надійність СКЗ.

5. Управління кібербезпекою

Система моніторингу. Система аналізу уразливостей. Система виявлення вторгнень. Управління комплексними системами захисту. Стандартизація у галузі моніторингу кіберсистем. Аналіз і управління ризиками.

Література:

1. Мартин Р., Мартин М. Принципы, паттерны и методики гибкой разработки на языке C#. – СПб: Символ плюс, 2011.
2. Соммервилл Иан. Инженерия программного обеспечения, 6-е издание: пер. с англ. – М.: Вильямс, 2002. – 624с.
3. Microsoft Corporation. Принципы проектирования и разработки программного обеспечения. Учебный курс MCSD. Пер. с англ. – М.: Русская редакция. – 2006. – 606 с.
4. Якобсон А., Буч Г., Рамбо Дж. Унифицированный процесс разработки программного обеспечения. – СПб.: Питер, 2002. – 496 с.
5. Орлов С.А. Технология разработки программного обеспечения. Учебник. – СПб.: Питер, 2002. – 464 с.
6. Крёнке Д. Теория и практика построения баз данных. 8-е изд. – СПб.: Питер, 2003. – 800 с.
7. Системы баз данных. Полный курс / Гарсия-Молина, Гектор; Ульман, Джеффри; Уидом, Дженнифер: Пер. с англ. – М.: Вильямс, 2003. – 1088 с.
8. Рефакторинг баз данных: эволюционное проектирование / Скотт В. Эмблер, Прамодкумар Дж. Садаладж: Пер. с англ. – М.: Вильямс, 2007. – 672 с.
9. Туркин И.Б., Лучшев П.А., Василенко Т.В. Методы и алгоритмы обработки данных в задачах реального времени: лабораторный практикум. – Х.: Нац. аэрокосм. ун-т, 2007. – 110 с.

10. Вороновский Г.К., Махотило К.В., Петрашев С.Н., Сергеев С.Н. Генетические алгоритмы, искусственные нейронные сети и проблемы виртуальной реальности. – Х.: Основа, 1997. – 112 с.
11. Проектирование информационных систем / Т.В. Гвоздева, Б.А. Баллод. – Ростов н/Д: Феникс, 2009. – 508 с.
12. Данилин А., Слюсаренко А. Архитектура и стратегия. "Инь" и "янь" информационных технологий. Интернет-университет информационных технологий. – ИНТУИТ.ру, 2005. – 504 с.
13. Гамма Э., Хелм Р., Джонсон Р., Влиссидес Дж. Приемы объектно-ориентированного проектирования. Паттерны проектирования. – СПб: Питер, 2007. – 230 с.
14. Вендров А.М. Современные методы и средства проектирования программного обеспечения. – М, 2008. – 183 с.
15. Люгер Джорж Ф. Искусственный интеллект: стратегии и методы решения сложных проблем. Пер. с англ. – М.: Вильямс, 2003. – 864 с.
16. Тей А., Грибомон П., Луи Ж. и др. Логический подход к искусственному интеллекту: от классической логики к логическому программированию. – Пер. с франц. – М.: Мир, 1990. – 432 с.
17. Марселлус Д. Программирование экспертных систем на ТУРБО ПРОЛОГЕ. – М.: Финансы и статистика. 1994. – 256 с.
18. Прохоров А.В., Пахнина Е.М. Технологии распределенных систем и параллельных вычислений: учеб. пособие. – Х.: Нац. аэрокосм. ун-т им. Н.Е. Жуковского «Харьк. авиац. ин-т», 2013. – 184 с.
19. Прохоров А.В. Технологии интеграции корпоративных приложений: учеб. пособ. по лаб. практ. – Х.: Нац. аэрокосм. ун-т им. Н.Е. Жуковского "Харьк. авиац. ин-т", 2011. – 84 с.
20. Федорович О.Є., Прохоров О.В., Головань К.В. Системи обробки інформації і управління розподіленими виробництвами: навч. посібник (Гриф Міністерства освіти і науки України). – Х.: Нац. аерокосм. ун-т "Харк. авиац. ін-т", 2006. – 236 с.
21. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. – СПб.: Питер, 2009. – 864 с.
22. Таненбаум Э. Компьютерные сети. – СПб.: Питер, 2008. – 848 с.
23. Липовецкий Г. П. Однокристалльные микро-ЭВМ. – М.: Бином, 1992.
24. Коффрон Дж. Технические средства микропроцессорных систем. – М.: Мир, 1983.
25. Джонсон М. Харг. Системное программирование в среде Win32. Пер. с англ. – М.: Вильямс, 2005. – 592 с.
26. Рихтер Дж. Windows для профессионалов: создание эффективных Win32 приложений с учетом специфики 64-разрядной версии Windows. Пер. с англ. – СПб.: Питер; М.: Русская Редакция, 2001. – 752 с.
27. Пирогов В. SQL Server 2005. Программирование клиент-серверных приложений. – СПб: БХВ-Петербург, 2006. – 336 с.
28. Дейт К. Дж. Введение в базы данных. – М.: Вильямс, 2006. – 1328 с.
29. Брауде Э. Технология разработки программного обеспечения. – СПб: Питер, 2004. – 655 с.

30. Орехов А. А., Харченко Л.Д., Лямец В.И. Проектирование программных систем с применением Case-технологий Учеб. пособие.– Х.: Нац. аэрокосм. ун-т «Харьк. авиац. ин-т», 2005. – 83 с.
31. Кобозева А.А. Аналіз захищеності інформаційних систем. Підручник [Текст] / А.А. Кобозева, І.О. Мачалін, В.О. Хорошко.– К.: ДУІКТ, 2010. – 316 с.
32. Єжова Л.Ф. Управління інформаційною безпекою. Підручник. У 2-х томах [Текст] / Л.Ф. Єжова, І.О. Мачалін, Я.В. Невоїт, В.О. Хорошко. – Севастополь: СНУ, 2010.
33. Павлов І.М. Проектування комплексних систем захисту інформації [Текст] / І.М. Павлов, В.О. Хорошко. – К.: ВІПІ, 2011. – 245 с.
34. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учеб. пособие [Текст] / Г.Н Устинов. – М.: Синтег, 2000. – 248с.
35. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие [Текст] / А.А. Малюк . – М: Горячая линия-Телеком, 2004. – 280 с.
36. Романец Ю.В. Защита информации в компьютерных системах и сетях [Текст] / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин.–М.: Радио и связь, 2001. – 376 с.
37. Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика. Монографія [Текст] / Ю.І. Горбенко, І.Д. Горбенко. – Х.: Форт, 2010. – 608с.
38. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. – Х.: ХНУРЕ, Форт, 2013. – 878 с.
39. Кузнецов А.А. Безопасность информационных систем и технологий [Текст] / В.И. Есенин, А.А. Кузнецов, Л.С. Сорока . – Х.: ООО «ЭДЭНА», 2010. – 656с.
40. Остроухов В.В. Информационно-психологическая безопасность в эпоху глобализации. Учеб. пособие [Текст] / В.М. Петрик, В.В. Остроухов, А.А. Штоквиш. – К., 2008. – 544 с.
41. Томашевський В.М. Моделювання систем. – К.: Видавнича група ВНУ, 2005. – 352 с.
42. Крайников А.В. и др. Вероятностные методы в вычислительной технике. – М.: Высшая школа, 1986. – 312 с.
43. Гудман С., Хидетниемеи С. Введение в разработку и анализ алгоритмов. – М.: Мир, 1981. – 368 с.
44. Вентцель Е.С. Исследование операций. – М.: Радио и связь, 1972. – 552 с.
45. Гладков Л.А., Курейчик В.В., Курейчик В.М. Генетические алгоритмы. Учебное пособие. – М.: Физматлит, 2006. – 320 с.
46. Лысенко И.В. Решение задач дискретной оптимизации в среде Matlab: сб. практ. заданий. – Х.: Нац. аэрокосм. ун-т им. Н. Е. Жуковского «Харьк. авиац. ин-т», 2014. – 47 с. [Электронное издание]
47. Даншина С.Ю., Харченко В.С. (ред.) та ін. Методи системного аналізу у комп'ютерній інженерії та радіоелектроніці. Підручник. – Х.: Міносвіти та науки України, Нац. аэрокосм. ун-т им. Н. Е. Жуковского «Харьк. авиац. ин-т», 2015. – 345с.

48. Кейс-методы оценивания программных систем. В 3-х томах. Качество. Надежность. Безопасность / Под ред. Харченко В.С. – Х.: Нац. аэрокосм. ун-т им. Н. Е. Жуковского «Харьк. авиац. ин-т», 2012. – 869 с.
49. Технологии Grid, Web, Cloud для гарантоспособных ИТ-инфраструктур/ Под ред. Харченко В.С., Горбенко А.В. – Х.: Нац. аэрокосм. ун-т им. Н. Е. Жуковского «Харьк. авиац. ин-т», 2013. – 821 с.

Програму розглянуто й узгоджено на сумісному засіданні кафедр комп'ютерні системи, мереж і кібербезпеки, інженерія програмного забезпечення, комп'ютерних наук та інформаційних технологій

Протокол № 5 від «13» 01 2020 р.

Завідувач кафедри
комп'ютерні системи, мереж і кібербезпеки
д.т.н., професор

В.С. Харченко

Завідувач кафедри
інженерія програмного забезпечення
д.т.н., професор

І.Б. Туркін

Завідувач кафедри
комп'ютерних наук та інформаційних технологій
д.т.н., професор

О.Є. Федорович