МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

ЗАТВЕРДЖЕНО:
в.о. президента ДУ «КАІ»
_____Ксенія СЕМЕНОВА
«09» ____04____2025 року

ПРОГРАМА
ВСТУПНОГО ВИПРОБУВАННЯ ДО АСПІРАНТУРИ

зі спеціальності F3 «Комп'ютерні науки»

на здобуття ступеня доктора філософії

третього (освітньо-наукового) рівня вищої освіти

Галузь знань F «Інформаційні технології»

Освітньо-наукова програма «Комп'ютерні науки»

Київ – 2025

Програма вступного випробування до аспірантури за спеціальністю 122 «Комп'ютерні науки» відображає такі розділи теоретичних та практичних основ у сфері комп'ютерних наук:

- архітектура сучасних комп'ютерних систем;
- моделювання систем та процесів;
- машинне навчання та штучний інтелект;
- аналіз та обробка великих даних;
- захист даних в сучасних комп'ютерних системах та мережах.

1. Архітектура сучасних комп'ютерних систем

1.1 Принципи побудови та функціонування комп'ютерних систем;
1.2 Архітектура фон Неймана та гарвардська архітектура комп'ютерних систем;
1.3 Архітектура системи команд, мікроархітектура та системне проектування;
1.4 Таксономія Флінна і її компоненти;
1.5 Архітектура набору команд сучасних процесорів;
1.6 Технології та засоби віртуалізації;
1.7 Паралельні комп'ютерні архітектури;
1.8 Принципи побудови розподілених систем;
1.9 Грід-технології та сервіси;
1.10 Системи і мережі зберігання даних;
1.11 Хмарні та туманні обчислення;
1.12 Суперкомп'ютинг: принципи, компоненти, сфери застосування;
1.13 Квантові обчислення: архітектура, алгоритми та завдання;
1.14 Архітектура та цикл розробки програмного забезпечення;
1.15 Сучасні операційні системи та їх архітектура.

2. Моделювання систем та процесів

2.1. Принципи моделювання складних технічних систем та процесів;
2.2. Класифікація та основні властивості математичних моделей;
2.3. Вимоги до математичних моделей;
2.4. Структурно-функціональне моделювання систем;
2.5. Математичне моделювання систем;
2.6. Імітаційне моделювання систем;
2.7. Аналітичні методи формалізованого представлення систем;
2.8. Статистичні методи формалізованого представлення систем;
2.9. Логічні і графічні методи формалізованого представлення систем;
2.10. Етапи та особливості моделювання технічної системи (процесу);
2.11. Багаточинниковий кореляційно-регресійний аналіз;
2.12. Застосування теорій множин, графів та масового обслуговування для

моделювання технічних систем і процесів;

2.13. Особливості моделювання систем підтримки прийняття рішень;
2.14. Сучасні інструменти комп'ютерного моделювання;
2.15. Технології 3-D моделювання процесів та систем.

3. Машинне навчання та штучний інтелект

3.1. Компоненти та цілі машинного навчання (Machine Learning);
3.2. Навчання за прецедентами (індуктивне) та дедуктивне навчання;
3.3. Машинне навчання з учителем (Supervised Learning);
3.4. Машинне навчання без вчителя (Unsupervised Learning);
3.5. Машинне навчання з підкріпленням (Reinforcement Learning);
3.6. Глибоке навчання (Deep Learning);
3.7. Поняття та види нейронних мереж;
3.8. Класифікація сучасних нейронних мереж;
3.9. Застосування машинного навчання у задачах кібербезпеки;
3.10. Сучасні бібліотеки машинного навчання;
3.11. Методи і моделі штучного інтелекту (Artificial Intelligence);
3.12. Обробка природної мови (Natural-Language Processing);
3.13. Машинний зір (Machine Vision);
3.14. Архітектура і функції нейрокомп'ютерів (Neurocomputer);
3.15. Сучасні виклики і тенденції розвитку штучного інтелекту.

4. Аналіз та обробка великих даних

4.1. Поняття, критерії та характеристики великих даних (концепція 3V);
4.2. Передумови та чинники виникнення поняття Big Data;
4.3. Принципи роботи з великими даними;
4.4. Data Mining як метод аналізу великих даних;
4.5. Crowdsourcing як метод аналізу великих даних;
4.6. Класифікація та кластерний аналіз великих даних;
4.7. Візуалізація як метод аналізу великих даних;
4.8. Застосування машинного навчання для аналізу великих даних;
4.9. Когнітивний аналіз даних;
4.10. Технології обробки великих даних;
4.11. Великі дані в інформаційно-комунікаційних системах;
4.12. Обробка великих даних в концепції IoT;
4.13. Проблеми обробки великих даних у задачах кібербезпеки;
4.14. Захищене зберігання і обробка великих даних;
4.15. Сучасні інструменти роботи з великими даними.

5. Захист даних в сучасних комп'ютерних системах та мережах

5.1. Поняття інформаційної безпеки (кібербезпеки), уразливості, ризику, загроз, атаки та інциденту в комп'ютерних системах та мережах;

5.2. Стандарти та рекомендовані практики щодо захисту інформації в комп'ютерних системах та мережах;

5.3. Моделі інформаційної безпеки (кібербезпеки), основні і додаткові характеристики захищеності даних в комп'ютерних системах та мережах;

5.4. Моделі загроз та порушника в комп'ютерних системах та мережах.

5.5. Класифікація атак на комп'ютерні системи;

5.6. Криптографічний захист інформації: принципи, алгоритми, режими шифрування, обчислювальна, практична та теоретико-інформаційна стійкість криптоалгоритмів, сучасні методи криптоаналізу;

5.7. Симетричні та асиметричні шифри, принципи побудови та особливості їх застосування, проблема розподілу ключів шифрування, особливості використання NP-складних задач в криптографії;

5.8. Поняття ЕЦП та його застосування, алгоритми і стандарти ЕЦП, система ЕЦП України та її застосування для захисту даних;

5.9. Квантова криптографія: базові принципи, основні протоколи, квантовий розподіл ключів та квантовий прямий безпечний зв'язок, побудова та застосування квантових систем захисту інформації, квантовий криптоаналіз;

5.10. Стеганографічний захист даних: критерії стеганостійкості, цифрова та комп'ютерна стеганографія, атаки на стеганографічні системи захисту інформації;

5.11. Аудит кібербезпеки, технології випробування стійкості (Penetration Testing) комп'ютерних систем та мереж;

5.12. Інцидент-менеджмент: базові поняття, фази життєвого циклу, архітектура та функції типової системи управління інцидентами інформаційної безпеки;

5.13. Структура і функції сучасних фаєрволів, антивірусів, IDS / IPS;

5.14. Принципи побудови і функціонування сучасних SIEM систем;

5.15. Особливості захисту даних у різних операційних системах.

Рекомендована література:

1. A. Geron, Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems 2nd ed., 2017, 921 p.
2. Hannah B Higgins, The Grid Book, The MIT Press, January 23, 2009, 312 p.
3. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy" by Cathy O'Neil, 2016, 272 p/
4. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.], К. : Центр навч.-наук. та наук.-пр. видань НА СБУ, 2014, 193 с.
5. Горбенко І.Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: Монографія / І.Д. Горбенко, Ю.І. Горбенко, Х.: Видавництво «Форт», 2010, 608 с.
6. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування / І.Д. Горбенко, Ю.І. Горбенко, Х. : Видавництво «Форт», 2012, 870 с.
7. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія і практика / Конахович Г.Ф., Пузиренко О.Ю, К. : «МК-Пресс», 2006, 288 с.
8. Корченко О., Терейковський І., Білощицький А. Методологія розроблення нейромережевих засобів інформаційної безпеки інтернет-орієнтованих інформаційних систем, 2016, 254 с.
9. Мастицкий С.Э. Анализ временных рядов с помощью R, 2020
   https://ranalytics.github.io/tsa-with-r
10. Математичні основи криптоаналізу: навчальний посібник / С.О. Сушко, Г.В. Кузнецов, Л.Я. Фомичова, А.В. Корабльов, Д.: Національний гірничий університет, 2010, 465 с.
11. Математичні основи криптографії: навчальний посібник / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова, Д.: Національний гірничий університет, 2004, 391 с.
12. О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія, Київ, ЦП «Компринт», 2017 – 435 с/
13. Павленко П.М., Філоненко С.Ф., Чередніков О.М., Трейтяк В.В. Математичне моделювання систем і процесів: навч. посіб., К. : НАУ, 2017, 392 с.
14. Сергієнко А.М. Архітектура комп'ютерів: Конспект лекцій, К.: НТУУ «КПІ», 2015, 198 с.
15. Peter Flach, Machine learning, Cambridge University Press, 2012, 416 p.
16. Jack D. Hidary, Quantum Computing: An Applied Approach, Springer, 2019, 379 p.
17. D. Murdoch, Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter, 2019, 258 p.
18. M. Deisenroth, Mathematics for Machine Learning, Cambridge University Press, 2020, 398 p.
19. Приставка П.О., Чолишкіна О.Г. Поліноміальні сплайни в задачі альтернативної навігації за даними аерозйомки: Монографія, К.: МАУП, 2022, 128 с.
20. Peter Flach, Machine learning, Cambridge University Press, 2012, 416 p.
21. Berdibayev R., Gnatyuk S., Tynymbayev S., Sydorenko V. Advanced Technologies of Cyber Incident Management in Critical Infrastructure: Monograph, Kyiv, "Pro Format" Publishing House, 2022, 125 p.
22. Gnatyuk S., Berdibayev R., Sydorenko V., Berdibayeva G., Yudin O. Methodological Bases of Critical Information Infrastructure Identification and Security Assessment: Monograph, Kyiv, "Pro Format" Publishing House, 2023, 129 p.