Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ Дмитро УЗУН
(підпис) (ім'я та ПРІЗВИЩЕ)

«_____» _____ 2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Методи моделювання та оптимізації безпечних комп'ютерних систем
(назва навчальної дисципліни)

Галузь знань: F «Інформаційні технології»
(шифр і найменування галузі знань)

Спеціальність: F5 «Кібербезпека та захист інформації»
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Рівень вищої освіти: ***другий (магістерський)***

Силабус введено в дію з 01.09.2025

Харків – 2025 р.

Розробник: Морозова О. І., професор, д.т.н., професор
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри _____ комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

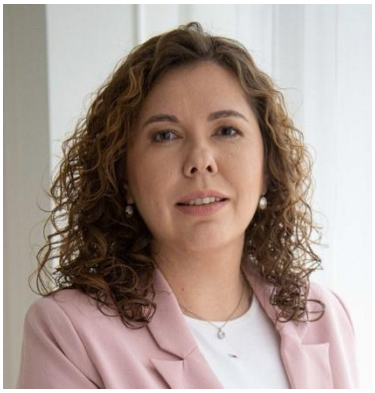
Протокол №1 від «29» 08 2025 р.

Завідувач кафедри д.т.н., професор _____ Вячеслав ХАРЧЕНКО
(науковий ступінь і вчене звання) (підпис) (ім'я та ПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:

_____ Іван ОЛЕФІРЕНКО
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача



ПІБ: Морозова Ольга Ігорівна

Посада: професор

Науковий ступінь: доктор технічних наук

Вчене звання: професор

Перелік дисциплін, які викладає:
Python для кібербезпеки, Безпека засобів штучного інтелекту, Теорія і методи Інтернет-обчислень, Python для систем штучного інтелекту, Програмування засобів штучного інтелекту на Python

Напрями наукових досліджень:
Гарантоздатність флотів БПЛА та інтелектуальних систем індустріального інтернету речей. Методи та технології університетсько-індустріальної співпраці в процесі навчання, у тому числі дуального, проведення тренінгів та виконання спільних R&D проєктів, інтелектуальні засоби підтримки прийняття рішень щодо генерування і вибору моделей кооперації та впровадження інтелектуальних систем індустріального інтернету речей.

Контактна інформація:
o.morozova@khai.edu

2. Опис навчальної дисципліни

Форма здобуття освіти	Денна
Семестр	1-й
Мова викладання	Українська
Тип дисципліни	Обов'язкова
Обсяг дисципліни: кредити ЄКТС/ кількість годин	денна: 3 кредити ЄКТС / 90 годин (48 аудиторних, з яких: лекції – 32, практичні – 16; СРЗ – 42)
Види навчальної діяльності	Лекції, лабораторні заняття, самостійна робота
Види контролю	Поточний контроль, модульний контроль, семестровий контроль – залік
Пререквізити	Дисципліна є обов'язковим компонентом освітньої програми і базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності

3. Мета та завдання навчальної дисципліни, переліки компетентностей та очікуваних результатів навчання

Мета – надання студентам необхідних знань, навичок та вмінь з отримання, оброблення, зберігання та ефективного використання даних при створенні систем з використанням методів моделювання та оптимізації безпечних комп'ютерних систем інформаційної безпеки та/або кібербезпеки.

Завдання – формування у студентів базових системних понять і навичок, цілісного бачення сучасного рівня основних характеристик проєктування та розроблення систем з використанням методів моделювання та оптимізації безпечних комп'ютерних систем інформаційної безпеки та/або кібербезпеки; формування знань і навичок володіння сучасними середовищами розроблення.

Компетентності, які набуваються:

Інтегральна компетентність:

Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності

Після закінчення цієї програми здобувач освіти буде здатен:

– ЗК1. Здатність до адаптації та дій в новій ситуації.
– ЗК2. Здатність до абстрактного мислення, аналізу і синтезу.
– ЗК3. Здатність проводити дослідження на відповідному рівні.
– ЗК4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
– ЗК5. Здатність генерувати нові ідеї (креативність).
– ЗК6. Здатність виявляти, ставити та вирішувати проблеми.
– ЗК7. Здатність приймати обґрунтовані рішення.

Спеціальні компетентності

Після закінчення цієї програми здобувач освіти буде здатен:

– СК1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
– СК4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
– СК5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків

та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Програмні результати навчання:

– ПРН 1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

– ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

– ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

– ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

– ПРН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.

– ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

– ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

– ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

– ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

– ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

– ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

– ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

– ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

– ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

4. Зміст навчальної дисципліни

МОДУЛЬ 1

Змістовний модуль 1. *Методи математичного моделювання безпечних комп'ютерних систем*

Тема 1. Вступ до дисципліни «Методи моделювання та оптимізації безпечних комп'ютерних систем»

- стисла анотація: буде розглянуто такі питання: Предмет, мета вивчення й завдання дисципліни. Структура та зміст дисципліни й методичні рекомендації щодо її вивчення. Міждисциплінарні зв’язки. Програмні компетентності й результати навчання. Перелік україномовної та англійської термінології дисципліни. Перелік державних та міжнародних стандартів ISO/IEC/ДСТУ. Характеристика рекомендованих під час вивчення дисципліни джерел інформації.

- тема лабораторного заняття: Використання програмного середовища MATLAB в режимі прямих обчислень і основи роботи з редактором М-файлів.

- самостійна робота здобувача освіти: опрацювання матеріалу лекцій, опрацювання матеріалу щодо «Методи статистичної обробки і аналізу результатів обчислювального експерименту в сфері інформаційної безпеки та/або кібербезпеки», яке відносяться до теми лекції; підготовка до захисту лабораторної роботи.

Тема 2. Базові положення й принципи математичного моделювання безпечних комп'ютерних систем

- стисла анотація: буде розглянуто такі питання: Поняття про математичні моделі (ММ) й математичне моделювання задач інформаційної безпеки та/або кібербезпеки. Вимоги до ММ систем і процесів. Класифікація систем (процесів) з точки зору побудови ММ. Принципи побудови ММ.

Характеристика основних етапів побудови ММ. Верифікація та валідація ММ. Критерії якості ММ.

- тема лабораторного заняття: Використання програмного середовища MATLAB в режимі прямих обчислень і основи роботи з редактором М-файлів.

- самостійна робота здобувача освіти: опрацювання матеріалу лекцій, опрацювання матеріалу щодо «Порівняльна характеристика методів дослідження математичних моделей для задач інформаційної безпеки та/або кібербезпеки», яке відносяться до теми лекції; підготовка до захисту лабораторної роботи.

Тема 3. Імітаційне моделювання безпечних комп'ютерних систем

- стисла анотація: буде розглянуто такі питання: Сутність імітаційного моделювання систем. Характеристика основних етапів імітаційного моделювання. Принципи побудови моделюючих алгоритмів (моделювання із постійним кроком та моделювання за особистими станами) для рішення задач інформаційної безпеки та/або кібербезпеки.

- тема лабораторного заняття: Імітаційне моделювання складова, розподільчих центрів з використанням системної динаміки в NetLogo.

- самостійна робота здобувача освіти: опрацювання матеріалу лекцій, опрацювання матеріалу щодо «Приклади використання імітаційного моделювання в сфері інформаційної безпеки та/або кібербезпеки», яке відносяться до теми лекції; підготовка до захисту лабораторної роботи.

Тема 4. Аналітичне моделювання безпечних комп'ютерних систем

- стисла анотація: буде розглянуто такі питання: Моделювання на основі систем масового обслуговування (СМО) для вирішення задач інформаційної безпеки та/або кібербезпеки. Моделювання систем на основі математичного апарату Марківських процесів.

- тема лабораторного заняття: Імітаційне моделювання складова, розподільчих центрів з використанням системної динаміки в NetLogo.

- самостійна робота здобувача освіти: опрацювання матеріалу лекцій, опрацювання матеріалу щодо «Імітаційне моделювання систем масового обслуговування за допомогою програмної системи General Purpose Simulation System – GPSS», яке відносяться до теми лекції; підготовка до захисту лабораторної роботи.

Тема 5. Інтелектуальні агенти

- стисла анотація: буде розглянуто такі питання: Мультиагентні системи. Поняття «агент». Структура агентів. Взаємодія агентів. Агенти засновані на знаннях. Інтелектуальні агенти. Використання інтелектуальних агентів для рішення задач інформаційної безпеки та/або кібербезпеки.

- тема лабораторного заняття: Використання мультиагентної середовища NetLogo для моделювання оптимізаційних задач.

- самостійна робота здобувача освіти: опрацювання матеріалу лекцій, опрацювання матеріалу щодо «Середовище моделювання мультиагентних

систем NetLogo», яке відносяться до теми лекції; підготовка до захисту лабораторної роботи.

Тема 6. Машинне навчання

- стисла анотація: буде розглянуто такі питання: Основні поняття машинного навчання. Загальна постановка завдання навчання по прецедентах. Метричні методи класифікації. Вирішальні дерева. Лінійні методи класифікації. Метод опорних векторів. Логістична регресія. Баєсові методи класифікації. Наївний баєсів класифікатор. Використання методів машинного навчання для рішення задач інформаційної безпеки та/або кібербезпеки.
- тема лабораторного заняття: Використання мультиагентної середовища NetLogo для моделювання оптимізаційних задач.
- самостійна робота здобувача освіти: опрацювання матеріалу лекцій, опрацювання матеріалу щодо «Ранжування в машинному навчанні для задач інформаційної безпеки та/або кібербезпеки», яке відносяться до теми лекції; підготовка до захисту лабораторної роботи.

Тема 7. Нейроні мережі

- стисла анотація: буде розглянуто такі питання: Нейробіологія. Нейронні мережі. Типи нейронних мереж. Формальний нейрон. Види активаційних функцій. Навчання нейронної мережі. Алгоритми навчання нейронних мереж. Перцептрон. Робота багатошарового перцептрона. Застосування математичного апарату нейронних мереж для рішення задач інформаційної безпеки та/або кібербезпеки.
- тема лабораторного заняття: Реалізація нейронечіткого виведення в системі ANFIS в середовищі MATLAB.
- самостійна робота здобувача освіти: опрацювання матеріалу лекцій, опрацювання матеріалу щодо «Особливості пакету Neural Network Toolbox для рішення задач інформаційної безпеки та/або кібербезпеки», яке відносяться до теми лекції; підготовка до захисту лабораторної роботи, підготовка до модульної контрольної роботи.

Модульний контроль 1

Змістовний модуль 2. *Методи оптимізації безпечних комп'ютерних систем*

Тема 8. Загальна характеристика методів оптимізації безпечних комп'ютерних систем

- стисла анотація: буде розглянуто такі питання: Постановка задачі оптимізації. Особливості оптимізаційного підходу з точки зору проблематики прийняття рішень. Приклад, що ілюструє перехід від вербальної постановки задачі оптимізації до її формальної постановки. Класифікація і загальна

характеристика оптимізаційних задач інформаційної безпеки та/або кібербезпеки. Можливості програмного середовища MATLAB щодо рішення задач оптимізації.

- тема лабораторного заняття: Реалізація нейронечіткого виведення в системі ANFIS в середовищі MATLAB.

- самостійна робота здобувача освіти: опрацювання матеріалу лекцій, опрацювання матеріалу щодо «Особливості пакетів Optimization Toolbox та Global Optimization Toolbox для рішення задач інформаційної безпеки та/або кібербезпеки», яке відносяться до теми лекції; підготовка до захисту лабораторної роботи.

Тема 9. Нелінійна оптимізація безпечних комп'ютерних систем

- стисла анотація: буде розглянуто такі питання: Класифікація та загальна характеристика методів рішення задач нелінійної оптимізації в сфері інформаційної безпеки та/або кібербезпеки. Постановка задачі квадратичного програмування. Безумовна нелінійна оптимізація: метод найскорішого спуску. Умовна нелінійна оптимізація: метод невизначених множників Лагранжа.

- тема лабораторного заняття: Реалізація нейронечіткого виведення в системі ANFIS в середовищі MATLAB.

- самостійна робота здобувача освіти: опрацювання матеріалу лекцій, опрацювання матеріалу щодо «Умовна нелінійна оптимізація: метод невизначених множників Лагранжа», яке відносяться до теми лекції; підготовка до захисту лабораторної роботи.

Тема 10. Лінійна оптимізація безпечних комп'ютерних систем

- стисла анотація: буде розглянуто такі питання: Базові поняття з області лінійного програмування: приклади задач лінійного програмування (ЗЛП) в сфері інформаційної безпеки та/або кібербезпеки. Основна ЗЛП та умови наявності у неї допустимого рішення; ЗЛП з обмеженнями-нерівностями та перехід від неї до канонічної форми ЗЛП. Геометрична інтерпретація ЗЛП.

- тема лабораторного заняття: Рішення задач нелінійної оптимізації з використанням пакета Optimization Toolbox програмного середовища MATLAB.

- самостійна робота здобувача освіти: опрацювання матеріалу лекцій, опрацювання матеріалу щодо «Симплекс-метод рішення задачі лінійного програмування (ЗЛП): загальна ідея симплекс-методу та її зв’язок з геометрично інтерпретацією ЗЛП, стандартна форма представлення загальної ЗЛП, алгоритм рішення ЗЛП симплекс-методом», яке відносяться до теми лекції; підготовка до захисту лабораторної роботи.

Тема 11. Дискретна оптимізація безпечних комп'ютерних систем

- стисла анотація: буде розглянуто такі питання: Загальна постановка задачі дискретної оптимізації в сфері інформаційної безпеки та/або кібербезпеки. Постановка найбільш розповсюджених задач дискретної

оптимізації (задача про призначення, задача про рюкзак, задача комівояжера) та особливості методів та алгоритмів їх вирішення.

- тема лабораторного заняття: Рішення задач нелінійної оптимізації з використанням пакета Optimization Toolbox програмного середовища MATLAB.

- самостійна робота здобувача освіти: опрацювання матеріалу лекцій, опрацювання матеріалу щодо «Алгоритми рішення задачі цілочисельної лінійної оптимізації за допомогою методів гілок та границь та Гоморі», яке відносяться до теми лекції; підготовка до захисту лабораторної роботи.

Тема 12. Динамічне програмування безпечних комп'ютерних систем

- стисла анотація: буде розглянуто такі питання: Загальна ідея і область застосування методу динамічного програмування для задач інформаційної безпеки та/або кібербезпеки. Постановка задачі динамічного програмування. Вирішення задач комбінаторної оптимізації методом динамічного програмування.

- тема лабораторного заняття: Рішення задач дискретної оптимізації з використанням пакета Optimization Toolbox програмного середовища MATLAB.

- самостійна робота здобувача освіти: опрацювання матеріалу лекцій, опрацювання матеріалу щодо «Рішення задачі оптимального розподілу ресурсів методом динамічного програмування для рішення задач інформаційної безпеки та/або кібербезпеки», яке відносяться до теми лекції; підготовка до захисту лабораторної роботи.

Тема 13. Рішення задач оптимізації за допомогою генетичних алгоритмів

- стисла анотація: буде розглянуто такі питання: Загальна ідея і області застосування генетичних алгоритмів (ГА). Класичний ГА. Приклад використання простого ГА для рішення оптимізаційних задач інформаційної безпеки та/або кібербезпеки. Характеристика можливостей ГА щодо рішення оптимізаційних задач.

- тема лабораторного заняття: Рішення задач дискретної оптимізації з використанням пакета Optimization Toolbox програмного середовища MATLAB.

- самостійна робота здобувача освіти: опрацювання матеріалу лекцій, опрацювання матеріалу щодо «Використання генетичних алгоритмів для рішення оптимізаційних задач на графах», яке відносяться до теми лекції; підготовка до захисту лабораторної роботи.

Тема 14. Рішення задач оптимізації за допомогою мурашиних алгоритмів

- стисла анотація: буде розглянуто такі питання: Біологічні принципи поведінки мурашиної колонії. Історія створення мурашиних алгоритмів.

Концепція мурашиних алгоритмів. Узагальнений алгоритм. Етапи виконання завдання за допомогою мурашиних алгоритмів. Застосування математичного апарату мурашних алгоритмів для рішення задач інформаційної безпеки та/або кібербезпеки.

- тема лабораторного заняття: Рішення задач дискретної оптимізації з використанням пакета Optimization Toolbox програмного середовища MATLAB.

- самостійна робота здобувача освіти: опрацювання матеріалу лекцій, опрацювання матеріалу щодо «Області застосування і можливі модифікації мурашиних алгоритмів. Переваги та недоліки мурашиних алгоритмів», яке відносяться до теми лекції; підготовка до захисту лабораторної роботи, підготовка до модульної контрольної роботи.

Модульний контроль 2

5. Індивідуальні завдання

Виконання індивідуального завдання: «Рішення завдання комівояжера за допомогою різних методів», а саме:

а) методом динамічного програмування (частина 1);
б) методом гілок і границь (частина 2);
в) жадібним методом (частина 3).

6. Методи навчання

Проведення лекцій, лабораторних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

7. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

8. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Виконання і захист	0…5	3	0…15

лабораторних робіт. Своєчасність та виконання всіх завдань лабораторної роботи оцінюється у максимальну оцінку 5 балів.			
Модульний контроль складається з трьох блоків: перший блок – розгорнута відповідь на одне питання (максимум 10 балів), другий блок – п’ять тестових питань по 1 балу, третій блок – п’ять визначень по 2 бали.	0…25	1	0…25
Змістовний модуль 2			
Виконання і захист лабораторних робіт. Своєчасність та виконання всіх завдань лабораторної роботи оцінюється у максимальну оцінку 5 балів.	0…5	3	0…15
Модульний контроль складається з трьох блоків: перший блок – розгорнута відповідь на одне питання (максимум 10 балів), другий блок – п’ять тестових питань по 1 балу, третій блок – п’ять визначень по 2 бали.	0…25	1	0…25
Виконання індивідуального завдання. Своєчасність та виконання індивідуального завдання у повному обсязі оцінюється у максимальну оцінку 20 балів.	0…20	1	0…20
Усього за семестр			**0…100**

Семестровий контроль (*іспит*) проводиться у разі відмови здобувача освіти від балів підсумкового контролю й за наявності допуску до *іспиту*. Під час складання семестрового *іспиту* здобувач освіти має можливість отримати максимум 100 балів.

Білет для *іспиту* складається з 13 питань. Перше блок (теоретичних питань) складається з одного питання на розгорнуту відповідь (максимум 20 балів), п’яти тестових питань по 2 балу, п’ять визначень по 4 бали. Другий блок (практичних питань) містить два питання по 25 балів.

Таблиця 8.2 – Шкали оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційний залік	Залік

90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

Критерії оцінювання роботи здобувача освіти протягом семестру

Задовільно (60 – 74). Мати мінімум знань та умінь. Відпрацювати та захистити всі лабораторні роботи та домашні завдання. Захистити всі індивідуальні завдання та здати тестування.

Добре (75 – 89). Твердо знать мінімум знань, виконати усі завдання. Показати вміння виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які запропоновано у роботах.

Відмінно (90 – 100). Повно знати основній та додатковий матеріал. Знати усі теми. Орієнтуватися у підручниках та посібниках. Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх. Безпомилково виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з докладним обґрунтуванням рішень та заходів, які запропоновано у роботах.

9. Політика навчального курсу

Відвідування занять. Регуляція пропусків. Інтерактивний характер курсу передбачає обов’язкове відвідування практичних занять. Здобувачі освіти, які за певних обставин не можуть відвідувати практичні заняття регулярно, повинні протягом тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущені заняття мають бути відпрацьовані на найближчій консультації протягом тижня після їх пропуску. Відпрацювання занять здійснюється усно у формі співбесіди за питаннями, визначеними планом заняття. В окремих випадках дозволяється письмове відпрацювання пропущених занять шляхом виконання індивідуального письмового завдання.

Дотримання вимог академічної доброчесності здобувачами освіти під час вивчення навчальної дисципліни. Під час вивчення навчальної дисципліни здобувачі освіти мають дотримуватися загальноприйнятих морально-етичних норм і правил поведінки, вимог академічної доброчесності, передбачених Положенням про академічну доброчесність Національного аерокосмічного університету «Харківський авіаційний інститут» (https://khai.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf). Очікується, що роботи здобувачів освіти будуть їх оригінальними дослідженнями або міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших здобувачів освіти становлять, але не обмежують, приклади можливої академічної недоброчестності. Виявлення ознак

академічної недоброчесності в письмовій роботі здобувача освіти є підставою для її незарахування викладачем незалежно від масштабів плагіату чи обману.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, а також правила етичної поведінки регламентуються Кодексом етичної поведінки в Національному аерокосмічному університеті «Харківський авіаційний інститут» (https://khai.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

10. Методичне забезпечення

1. Морозова О. І. Теоретичне введення до лабораторних робіт.
2. Морозова О. І. Методичні вказівки щодо виконання лабораторних робот.

Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=7661, на якому розміщено навчально-методичний комплекс дисципліни, який включає в себе:

– робоча програма дисципліни;
– перелік посилань на ресурси викладача: приватний телеграм викладача, група в телеграмі з дисципліни, посилання на Google Meet;
– конспект лекцій, в тому числі в електронному вигляді, який за змістом повністю відповідає робочій програмі дисципліни;
– методичні вказівки та рекомендації для виконання лабораторних робіт, а також рекомендації для самостійної підготовки;
– модульний контроль;
– журнал успішності.

11. Рекомендована література

Базова

1. Paul Deitel, Harvey Deitel. Intro to Python for Computer Science and Data Science: Learning to Program with AI, Big Data and The Cloud. – Pearson Education, 2019. – 864 p.
2. Моделювання та оптимізація систем: підручник / В. М. Дубовой, Р. Н. Квєтний, О. І. Михальов, А. В. Усов– Вінниця : ПП «ТД«Еднльвейс», 2017. – 804 с.
3. Лахно В. А. Математичне моделювання та оптимізація в системах кібербезпеки : монографія. Харків : ХНЕУ ім. С. Кузнеця, 2020. – 235 с.

4. Trivedi K. S., Bobbio A. Reliability and Availability Engineering: Modeling, Analysis, and Applications. Cambridge : Cambridge University Press, 2017. – 712 p.

5. Railsback Steven F., Volker Grimm. Agent-based and individual-based modeling: a practical introduction. – Princeton university press, 2019. – 360 p.

Допоміжна

1. Tariq Rashid. Make Your Own Neural Network. – CreateSpace, 2016. – 222 p.

2. Hopgood Adrian A. Intelligent systems for engineers and scientists: a practical guide to artificial intelligence. – CRC press, 2021. – 514 p.

12. Інформаційні ресурси

1. Сайт Національної бібліотеки України імені Вернадського [Ел. ресурс]. URL: http://www.nbuv.gov.ua

2. Національна парламентська бібліотека України [Ел. ресурс]. URL: http://www.nplu.kiev.ua

3. Державна науково-технічна бібліотека [Ел. ресурс]. URL: http://www.gntb.gov.ua