Силабус освітнього компонента
Програма навчальної дисципліни

Еволюційне програмування

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Профільна підготока, Вибіркова

Семестр
7

Мова викладання
Українська

Викладачі, розробники

Мілов Олександр Володимирович
oleksandr.milov@khpi.edu.ua
Доктор технічних наук, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 200 наукових та навчально-методичних праць. Науковий керівник з захищених кандидатських робіт, гарант освітньо-професійної програми другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Математичні основи криптології та криптоаналіз», «Структури даних», «Промисловий та офісний шпіонаж» , «Цифрова криміналістика», у студентів бакалавріата та магістратури, Розділ «Методологія наукової та педагогічної діяльності в науках кіберзахисту» для аспірантів.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Дисципліна "Еволюційне програмування" охоплює основи і практичні аспекти використання еволюційних алгоритмів для вирішення складних оптимізаційних задач. Еволюційне програмування (ЕП) є частиною ширшого класу алгоритмів, натхнених природними процесами, зокрема теорією еволюції, що базується на принципах природного відбору і генетичної мутації.

Мета та цілі дисципліни

Дисципліна надає студентам необхідні знання та навички для розробки та впровадження еволюційних алгоритмів, що робить їх підготовленими до вирішення практичних задач у галузі комп'ютерних наук, інформаційних технологій та інженерії. Курс сприяє розвитку аналітичного мислення та творчого підходу до вирішення складних проблем, що є важливими в умовах швидко змінюваного технологічного середовища.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
КЗ 2. Знання та розуміння предметної області та розуміння професії.
КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Компетентності

РН–1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
РН–2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
РН–3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
РН–4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН–5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
РН–6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
РН–7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
РН–8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
РН–9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
РН–10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
РН–11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
РН–12. Розробляти моделі загроз та порушника.
РН–13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
РН–14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

РН–15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
РН–16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
РН–17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
РН–18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН–19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
РН–20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
РН–21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН–22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН–23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН–24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
РН–25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
РН–26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
РН–27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
РН–28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
РН–29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
РН–30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
РН–31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
РН–32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
РН–33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків

РН–34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
РН–35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН–41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН–42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
РН–43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
РН–44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
РН–45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
РН–46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
РН–47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
РН–48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
РН–49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
РН–50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
РН–51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
РН–52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
РН–53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
РН–54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 32 год., лабораторні роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

«Теорія ймовірностей” та “Математична статистика», «Основи програмування».

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Вступ до еволюційного програмування.
Основні принципи еволюційного програмування: біологічна метафора, адаптація та еволюція. Відмінності між еволюційним програмуванням і генетичними алгоритмами. Історія розвитку еволюційного програмування: ключові етапи та вчені.
Тема 2. Генетичне програмування.
Структура індивідів. Етапи процесу генетичного програмування. Методи мутації.
Тема 3. Еволюційні стратегії.
Визначення та особливості еволюційних стратегій. Відмінності між еволюційними стратегіями та генетичним програмуванням. Синергія: використання еволюційних стратегій в генетичному програмуванні.
Тема 4. Еволюційне програмування.
Основні компоненти еволюційного програмування. Еволюційні алгоритми для оптимізації. Порівняння еволюційного програмування з іншими методами.
Тема 5. Машинне навчання.
Алгоритми машинного навчання.
Тема 6. Ройові алгоритми.
Типи ройових алгоритмів. Алгоритм оптимізації рою. Гібридизація ройових алгоритмів. Адаптація ройових алгоритмів.
Тема 7. Мурашкові алгоритми.
Алгоритм колонії мурах. Алгоритм штучної колонії бджіл. Порівняння ройових алгоритмів з іншими методами.
Тема 8. Імунні алгоритми.
Основні компоненти. Методи мутації та селекції в імунних алгоритмах. Оцінка. Застосування. Адаптивні імунні алгоритми.
Тема 9. Алгоритми, інспіровані неживою природою.
Фізичні алгоритми. Алгоритми на основі хімічних процесів. Алгоритми на основі географічних і природних процесів. Алгоритми на основі термодинамічних принципів. Гравітаційні алгоритми. Алгоритми на основі аналітичних методів. Практичні застосування алгоритмів, інспірованих неживою природою.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Кодування \ декодування індивідів. Функція оцінки індивіду. Формування популяції. Побудова ітераційного процесу.
Тема 2. Застосування алгоритму для розв’язання системи нелінійних рівнянь.
Тема 3. Програмування алгоритмів методу рулетки та розумних ваг.
Тема 4. Програмування алгоритмів лінійного та степеневого масштабування.
Тема 5. Програмування дійснозначних генетичних алгоритмів.
Тема 6. Програмування алгоритмів з динамічним розміром популяції.
Тема 7. Програмування алгоритмів для транспортної задачі.
Тема 8. Програмування та апробація алгоритму для задачі перевезення.
Тема 9. Програмування алгоритму розв’язування інтегрального рівняння першого роду..
Тема 10. Програмування подання індивіду у вигляді дерева.
Тема 11. Програмування алгоритму для задачі символьної регресі.
Тема 12. Програмування острівної моделі генетичних алгоритмів
Тема 13. Програмування різних критерії зупинки генетичних алгоритмів.
Тема 14. Оцінка збіжність генетичних алгоритмів.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

Основна література:

1. Holland , J.H., Adaptation in Natural and Artificial Systems.Ann Arbor: Univ. of Michigan Press, 1975. URL: http://repo.darmajaya.ac.id/3794/1/Adaptation%20in%20Natural%20and%20Artificial%20Systems_%20An%20Introductory%20Analysis%20with%20Applications%20to%20Biology%2C%20Control%2C%20and%20Artificial%20Intelligence%20%28A%20Bradford%20Book%29%20%28%20PDFDrive%20%29.pdf
2. Holland , J.H., "Genetic algorithms," Scientific American, pp. 66-72, July, 1992. URL: https://www.jstor.org/stable/24939139
3. Goldberg, D.E., Genetic algorithms in search, optimization and machine learning. Addison Wesley, 1989. URL: http://www2.fiit.stuba.sk/~kvasnicka/Free%20books/Goldberg_Genetic_Algorithms_in_Search.pdf
4. Литвин В. В. Методи та засоби інженерії даних та знань / В. В. Литвин // навчальний посібник з грифом МОНУ. — Львів : «Магнолія-2006», 2012. — 241 с. URL: http://lib.puet.edu.ua/index.php?view=article&catid=16%3A2016-06-07-13-58-31&id=1604%3A2017-12-06-09-04-12&format=pdf&option=com_content&Itemid=100148
5. Лавріщева К.М. Програмна інженерія / К.М. Лавріщева // підручник з грифом НАН України. – Київ : 2008.- 319 с. URL: https://csc.knu.ua/uk/library/books/lavrishcheva-6.pdf
6. E. Skakalina, A. Klochko . PRINCIPLES OF FORMATION OF GENERATIONS IN GENETIC ALGORITHMS / Elena Skakalina // LXXIII – International Scientific Conference “EUROPEAN INTEGRATION IN SCIENCE AND INNOVATIONS”, Chernivtsi, December 15-16, 2020.- P. 20-22. URL: https://reposit.nupp.edu.ua/handle/PoltNTU/9005
7. Skakalina E.V. IMPLEMENTATION OF A GENETIC ALGORITHM FOR OPTIMIZING THE DISTRIBUTION PROCESS / Elena Skakalina // Modern engineering and innovative technologies. – 2020. – Issue 14, Part. 2, pp. 6-13. ISSN 2567-5273, DOI: 10.30890/2567-5273.2020-14-02. URL: https://www.sworldjournal.com/index.php/swj/article/view/swj11-01-072
8. E. Skakalina . INTELLECTUAL CONTROL OF LOGISTIC PROCESSES USING GENETIC ALGORITHMS / Elena Skakalina // Системи управління, навігації та зв’язку.- 2021.- Випуск 1(63).- С. 111-115. URL: https://pdfs.semanticscholar.org/a8ef/900a5e0d46209776c57a42458e1939a75854.pdf
9. Skakalina, E. (2018), «Development of Methodological Foundations of Logistical Intellectual Control of Complex Systems Based on Hybrid Heuristic Algorithms» / International Journal of Engineering & Technology.- 2018.- Vol. 7, No (4.8). – P.534-538. DOI: 10.14419/ijet.v7i4.8.27301 (Scopus) URL: https://reposit.nupp.edu.ua/bitstream/PoltNTU/6562/3/IJET-27301.pdf
10. Skakalina Elena. Modification of ant colonies algorithm for solving the problem of automation scheduling [Електронний ресурс] / E. Skakalina // Матеріали XV міжнародної конференції "Контроль і управління в складних системах (КУСС-2020)", м. Вінниця, 8-10 жовтня 2020 р. – Електрон. текст. дані. – Вінниця : ВНТУ, 2020. – Режим доступу: http://ir.lib.vntu.edu.ua//handle/123456789/30669.

11. Skakalina E. V. (2020). Application of intelligent information technologies in the optimization of transportation. Intellectual capital is the foundation of innovative development: innovative engineering and technology, informatics. Monographic series «European Science». Book 3. Part 3. 2020. Karlsruhe, Germany. URL: https://www.sworld.com.ua/index.php/secciisge3-2/32812-sge4-040.
12. E. Skakalina. Hybridization of the genetic algorithm with the apparatus of fuzzy sets // Fourth International Scientific and Technical Conference "COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES " April 22-23, 2020, Kharkov - Riga - Kiev - Lviv - P.10-11. URL: http://csitic.nure.ua/issue/view/12193/showToc.

Додаткова література :

13. L.D. Whitley, Foundations of Genetic Algorithms // M. Kaufmann Publishers, 1993 - 322 с. URL: https://www.google.com.ua/books/edition/Foundations_of_Genetic_Algorithms_1993_F/vTyeBQAAQBAJ?hl=ru&gbpv=0
14. D.A. Coley, An Introduction to Genetic Algorithms for Scientists and Engineers // World Scientific, 1997 - 244 с. URL: http://ftp.demec.ufpr.br/CFD/bibliografia/an_introduction_to_genetic_algorithms_for_scientists_and_engineers_coley.pdf
15. R.L. Haupt, S.E.Haupt, Practical Genetic Algorithms // John Wiley, 2004 - 272 с. URL: https://stb.iau.ir/faculty/file/download/course/1619191163-randy-l.-haupt-sue-ellen-haupt-practical-geneti-bookfi-.pdf
16. S.N. Sivanandam, S.N. Deepa, Introduction to Genetic Algorithms // Springer, 2007 - 453 с. URL: https://download.e-bookshelf.de/download/0000/0122/17/L-G-0000012217-0002345540.pdf
17. E. Wirsansky, Hands-On Genetic Algorithms with Python // Packt Publishing, 2020 - 309 с. URL: https://books.google.com.ua/books/about/Hands_On_Genetic_Algorithms_with_Python.html?id=A0vODwAAQBAJ&redir_esc=y
18. C. Sheppard, Genetic Algorithms with Python // Goodreads.com, 2019 - 297 с. URL: https://books.google.com.ua/books/about/Genetic_Algorithms_with_Python.html?id=3jNqtAEACAAJ&redir_esc=y
19. L. Jacobson, B. Kanber, Genetic Algorithms in Java Basics // Apress, 2015 - 172 с. URL: https://books.google.com.ua/books/about/Genetic_Algorithms_in_Java_Basics.html?id=m88LCwAAQBAJ&redir_esc=y

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
• лабораторні роботи: 30% семестрової оцінки;
• самостійна робота: 10% семестрової оцінки;
• контрольна робота: 20% семестрової оцінки;
• залік: 40% семестрової оцінки

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність.

Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено

28.08.2024

Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024

Гарант ОП
Сергій ЄВСЕЄВ