



Силабус освітнього компонента

Програма навчальної дисципліни



Генетичні алгоритми

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 підготовка, 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 "Генетичні алгоритми" спрямована на вивчення підходів, методів і механізмів функціонування та використання генетичних алгоритмів. Необхідність в використанні нових підходів обумовлена тим, що сучасні підходи до вирішення складних завдань, які потребують обробки надзвичайно великого обсягу даних, потребують використання великої кількості обчислювальних ресурсів. Вивчення даної дисципліни майбутніми науковцями дозволить їм набути важливих компетенцій в плані розвитку існуючих і використанню нових підходів проектування, розробки та використання генетичних алгоритмів, а також засвоїти методи їх підготовки для практичного застосування.

Мета та цілі дисципліни

Метою вивчення дисципліни "Генетичні алгоритми" є підготовка фахівців, здатних розв'язувати комплексні проблеми в галузі науково-дослідної діяльності у сфері розробки та використання генетичних алгоритмів, організацію рішень на основі окремих компонентів глибинного навчання, їх способи налаштування та тестування в практичних умовах.

Формат занять

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

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.

Результати навчання

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 частотої 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 різні 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 90 год. (3 кредити ECTS): лекції – 16 год., лабораторні роботи – 16 год., самостійна робота – 58 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 проекти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Вступ до навчальної дисципліни «Генетичні алгоритми».

Історія. Основні поняття. Сфери застосування. Найпростіший генетичний алгоритм. Оператори схрещування, мутації. Елітарна модель.

Тема 2. Типи функцій. Мінімізація.

Мінімізація одновимірної функції. Мінімізація багатовимірної функції.

Тема 3. Конфігурація генетичних алгоритмів. Механізми вибору нащадків: метод рулетки, турнірний метод, розумні ваги.

Налаштування. Оцінка ефективності. Методи генерації початкової популяції. Використання селекційних операторів. Огляд різних методів вибору нащадків. Порівняння методів.

Тема 4. Масштабування функції оцінки індивідів. Елітарна модель.

Визначення функції оцінки. Вибір і формулювання функції оцінки. Методи масштабування. Опис елітарної моделі. Типи елітарних моделей.

Тема 5. Дійснозначні генетичні алгоритми.

Основні принципи. Структура індивідів. Порівняння.

Тема 6. Генетичні алгоритми з динамічним розміром популяції.

Причини використання динамічного розміру популяції. Моделі зміни розміру популяції. Механізми управління.

Тема 7. Застосування генетичних алгоритмів для транспортної задачі.

Основна формулювання транспортної задачі. Мета. Чому генетичні алгоритми підходять для транспортної задачі? Ініціалізація популяції для транспортної задачі.

Тема 8. Генетичний алгоритм для задачі перевезення.

Кодування рішень. Функція пристосованості. Оператори генетичного алгоритму.

Тема 9. Еволюційно-чисельний алгоритм. Чисельне розв'язування інтегрального рівняння першого роду.

Структура еволюційно-чисельних алгоритмів. Інтегральні рівняння першого роду. Оцінка функції пристосованості. Оптимізація параметрів еволюційного алгоритму.

Тема 10. Вступ в генетичне програмування.

Визначення генетичного програмування та його місце серед еволюційних алгоритмів.

Представлення програм у генетичне програмування. Функція пристосованості в генетичному програмуванні. Еволюція програм.

Тема 11. Генетичне програмування для задачі символної регресії.

Визначення символної регресії. Завдання. Роль генетичного програмування у розв'язуванні задач символної регресії.

Тема 12. Семантичне генетичне програмування.

Основи семантики у генетичному програмуванні. Методи представлення семантики. Семантичні операції. Застосування семантичного генетичного програмування.

Тема 13. Паралельні генетичні алгоритми.

Архітектури паралельних генетичних алгоритмів. Методи паралелізації. Операції генетичних алгоритмів у паралельному середовищі.

Тема 14. Збіжність генетичних алгоритмів.

Типи збіжності генетичних алгоритмів. Фактори, що впливають на збіжність. Методи покращення збіжності. Аналіз збіжності генетичних алгоритмів.

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 символічної регресії.
Тема 12. Програмування острівної моделі генетичних алгоритмів
Тема 13. Програмування різних критерії зупинки генетичних алгоритмів.
Тема 14. Оцінка збіжності 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. Goldberg D.E. Genetic Algorithm in Search, Optimisation and Machine Learning / D.E. Goldberg // Addison-Wesley, Reading, MA. 1989. URL: [http://www2.fkit.stuba.sk/~kvasnicka/Free%20books/Goldberg Genetic Algorithms in Search.pdf](http://www2.fkit.stuba.sk/~kvasnicka/Free%20books/Goldberg%20Genetic%20Algorithms%20in%20Search.pdf)
2. Koza J.R. Genetic programming as a means for programming computers by natural selection / J.R. Koza // Stat Comput 4, 87–112. 1994. URL: <https://link.springer.com/article/10.1007/BF00175355>
3. Michalewicz Z. Genetic Algorithms + Data Structures = Evolution Programs, 3rd ed. / Z. Michalewicz // Springer-Verlag, Berlin. 1996. URL: <https://web.ist.utl.pt/adriano.simoese/tese/referencias/Michalewicz%20Z.%20Genetic%20Algorithms%20+%20Data%20Structures%20=%20Evolution%20Programs%20%283ed%29.PDF>
4. Mitchell M. An introduction to genetic algorithm / M. Mitchell // The MIT Press. 1998. URL: <https://www.boente.eti.br/fuzzy/ebook-fuzzy-mitchell.pdf>
5. Vanneschi L. Genetic Programming. In: Lectures on Intelligent Systems / L. Vanneschi, S. Silva // Natural Computing Series. Springer, Cham. 2023. URL: https://books.google.com.ua/books/about/Lectures_on_Intelligent_Systems.html?id=WYqnEAAAQBAJ&redir_esc=y

Додаткова література :

6. 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
7. 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

8. 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>
9. 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>
10. 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
11. 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
12. 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;
- іспит: 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