Силабус освітнього компонента
Програма навчальної дисципліни

Моделі і аналіз мультиагентних систем

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Освітньо-наукова програма Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Науково-професійного спрямування, Вибіркова

Семестр
3

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

Навчальна програма дисципліни “ Моделі і аналіз мультиагентних систем ” розглядає теоретичні основи та застосування агентних технологій. Висвітлено сучасні підходи до подання й обробки знань, на яких базуються інтелектуальні програмні агенти. Наведено моделі та технології створення програмних агентів і мультиагентних систем, їх застосування для пошуку інформації та підтримки електронного бізнесу та забезпечення необхідного рівня захищеності ресурсів. Програма орієнтована на науковців і спеціалістів, які займаються дослідженнями та розробками в галузі кібербезпеки, інтелектуальних інформаційних систем, бізнес- застосунків інформаційної економіки.

Мета та цілі дисципліни

Метою викладання навчальної дисципліни «Моделі і аналіз мультиагентних систем» є формування у студентів цілісної системи знань про агентні технологій та мультиагентні системи, навчання студентів методам і засобам проектування, створення і роботи з програмними агентами та мультиагентними системами.

Формат занять

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

Компетентності

КФ1. 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.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ4. 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.
КФ5. 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.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Результати навчання

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. 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.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН15. 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.
РН16. 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.
РН17. 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.
РН19. 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.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. 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.
РН23. 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.
РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.
РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

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)

Вища математика, Основи моделювання.

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. Предмет і задачі ТКП. Основні ідеї та визначення.

Предмет і задачі теорії. Інтелектуальна система (агент). Поняття функціональної цілісності. Принцип колективної дії. Поняття елементарного поведінкового акту. Гіпотеза М.Л. Цетліна про простоту. Наукові напрямки, що складають ТКП.

Тема 2. Поняття агента. Узагальнена функціональна структура агента.

изначення інтелектуальної системи (агента). Поняття середовища агента. Типи середовища. Узагальнена функціональна структура агента. Формальний опис системи <середовище, колектив>. Цільовоа функція агента (agent utility function). Класифікація агентів. Приклади змістовної інтерпретації.

Тема 3. Поняття колективу в ТКП.

Визначення колективу агентів (багатоагентної системи). Основні характеристики колективу агентів. Цільова функція колективу (world utility function). Способи опису колективної поведінки. Основна проблема ТКП.

Тема 4. Децентралізоване та централізоване управління. Самоорганізація.

Визначення централізованого та децентралізованого управління. Порівняння централізованого та децентралізованого управління на прикладі. Ентропія (невизначенність) за К. Шеноном (C. Shannon). Визначення самоорганізації. Міра порядку (фон Фьорстер). Правило самоорганізації.

Тема 5. Однорідність та неоднорідність колективу агентів.

Поняття однорідності та неоднорідності. Адаптивне управління з механізмом наслідування. Гнучкість та цілеспрямованість колективної поведінки. Приклад моделі колективної поведінки з адаптивним управлінням. Спеціалізація (формування груп взаємодоповнюючих стратегій).

Тема 6. Співпраця та суперництво в колективі агентів.

Поняття співпраці (cooperation) та суперництва (competition). Співвідношення між індивідуальною та колективною продуктивністю. Ітераційна ділема ув'язненого (Iterated Prisoners Dilemma, IPD).

Тема 7. Колективні моделі реальності. Колективне знання.

Визначення колективної моделі реальності (КМР). Приклад організації пам'яті агента на основі його узагальненої функціональної структури. Колективне знання. Схема утворення колективного знання. Способи збереження даних колективних моделей.

Тема 8. Колективне прийняття рішень.

Поняття колективного прийняття рішень. Функія колективного вибору. Теорема Ерроу про неможливість (парадокс Ерроу, K.J.Arrow).

Тема 9. Спілкування в колективі агентів.

Основна проблема розподілених систем. Поняття інформаційної зв'язності. Мови спілкування агентів.

Частина 2. Базові алгоритми колективної поведінки (5 лекцій)

Тема 10. Утворення колективу. Самоіменування. Самоузгодження.

Архітектура інтегрального підпорядкування (subsumption architecture, Р.Брукс). Основні вимоги до базових алгоритмів колективної поведінки. Утворення колективу: самовиявлення (detecting). Самоіменування: генерація унікальних імен агентів. Самоузгодження: домовленність про однакову для всіх величину.

Тема 11. Самоорганізація колективу агентів у просторі (самовпорядкування).

Загальна постановка задачі самовпорядкування. Класифікація задач самовпорядкування за складністю. Самоорганізація в задачах самовпорядкування. Впорядковане розміщення у просторі (ordered placement). Формування правильних геометричних фігур (geometric pattern formation). Приклад алгоритму формування сегменту лінії (К.Сугіхара, І.Сузукі). Управління впорядкованим переміщенням (motion control). Приклад алгоритму узгодженого групового переміщення (Д.Кромбі).

Тема 12. Самоорганізація колективу агентів у часі (самосинхронізація).

Постановка задачі самосинхронізації колективу. Дискретний та аналоговий варіанти задачі самосинхронізації. Задача синхронізації ланцюжку стрільців (firing squad synchronization problem, Дж. Майхіл). Приклад алгоритму самосинхронізації ланцюжку агентів. Самосинхронізація агентів поєднаних статичною мережею зв'язків. Самосинхронізація агентів за наявності затримок.

Тема 13. Навчання з підкріпленням (самонавчання).

Зміст та елементи навчання з підкріпленням (Р.Саттон, А.Барто). Стаціонарне випадкове середовище (n-armed bandit problem). Цілеспрямованість поведінки (М.Л.Цетлін). Співвідношення долідження (exploring) та користування (exploiting). Метод зваженої оцінки дій (Action-Value

Method). Середовище з перемиканням (Markov Decision Processes). Навчання за методом часових різниць (Temporal Difference Learning). Q-навчання (Q-learning).

Тема 14. Колективне навчання з підкріпленням (колективне самонавчання).

Проблема формування відгуку середовища (credit-assignment problem). Одночасне ізольоване навчання з підкріпленням (concurrent isolated RL). Інтерактивне самонавчання узгодженим діям (interactive RL of coordination). Самонавчання та спілкування. Зменшення спілкування за рахунок навчання. Покращення навчання за рахунок спілкування.

Частина 3. Моделі колективної поведінки (8 лекцій)

Тема 15. Опис моделей колективної поведінки в термінах теорії ігор.

Основні властивості ігор з нулевою сумою. Рівновага за Нешем. Ігри з послідовним повторенням партій. Стохастичні ігри. Рекурсивні ігри. Ігри на виживання. Ігри на виснаження. Ігри з непротележними інтересами гравців. Кооперативні ігри.

Тема 16. Однорідні симетричні ігри цілеспрямованих автоматів.

Однорідні ігри з обмеженою взаємодією. Однорідна гра на колі. Гра в розміщення. Гра в розподілення. Процедура "спільної каси" (common cash). Гра Гура. Співпраця та суперництво в грі Гура.

Тема 18. Економічні моделі колективної поведінки.

Поняття ринкової рівноваги (general equilibrium theory). Моделі ринкових механізмів (general equilibrium market mechanisms). Проблема "відвідування барів" (El Farol Bar problem). Мінорна гра (minority game). Створення механізмів взаємодії (mechanism design). Аукціони (auctions). Досягнення домовленностей шляхом переговорів (nagotiations).

Тема 19. Еволюційні моделі колективної поведінки.

Природний відбір. Поняття екологічної рівноваги. Штучне життя (Artificial life). Популяційна динаміка. Еволюційні обчислення (evolutionary computation). Генетичні алгоритми (genetic algorithms). Еволюційне програмування (evolutionary programming). Генетичне програмування (genetic programming). Кліткові автомати (celular automata, Дж. фон Нейман).

Тема 20. Методи пошуку припустимого рішення. Колективний пошук в реальному часі.

Проблема розподіленого пошуку припустимого рішення (constraint satisfaction). Методи розподіленого пошуку припустимого рішення. Алгоритми пошуку в реальному часі. Пошук рухомої цілі (moving target search). Співпраця в умовах нестачі інформації. Організація колективу для вирішення проблем (forming problem solving organizations). Задача побудови башти (tower building task).

Тема 21. Задача механічного врівноваження. Узагальнене поняття рівноваги.

Постановка задачі механічного врівноваження. Аналіз задачі врівноваження. Граф розміщень. Узагальнене поняття рівноваги. Критерії ефективності алгоритмів врівноваження. Централізоване врівноваження. Децентралізоване врівноваження несамовиявленим колективом. Децентралізоване врівноваження самовиявленим колективом.

Тема 22. Колективна поведінка обчислювальних агентів. Мобільні обчислення.

Моделі розподілених обчислень. Мобільний код (mobile code) та мобільні агенти (mobile agents). Мобільні обчислення (mobile computing). Концепція обчислювальних екологій (computational ecologies, XEROX). Самоорганізація динамічних розподілених обчислювальних систем (HP). Концепція автономних обчислень (autonomic computing, IBM).

Тема 23. Колективна поведінка вимірювальних агентів. Мобільні вимірювання.

Розподілені вимірювально-обчислювальні системи. Картографування (mapping). Колективний пошук (search), локалізація (localization) та відслідковування траекторій (tracking). Розподілені контактні вимірювання (distributed sensing). Інтерполяційна модель колективної поведінки вимірювальних агентів. Проблема розміщення вимірювальних агентів. Алгоритми поведінки вимірювальних агентів.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Установка ПЗ для розробки та тестування додатків
Тема 2. Розробка програми моделювання агента
Тема 3. Ознайомлення з JADE

Тема 4. Приклад мультиагентного додатку з JADE-агентом на платформі ANDROID

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. Плескач В.Л. , Рогушина Ю.В. Агентні технології: Монографія. – К.: Київ. нац. торг.–екон. ун–т, 2005. – 344 с. (Табл.10. Рис.58. Бібліограф.361). URL: https://core.ac.uk/download/pdf/38468943.pdf
2. Jones, Owen, Robert Maillardet, and Andrew Robinson. Introduction to Scientific Programming and Simulation Using R. Chapman and Hall, 2009.
URL:https://nyu-cdsc.github.io/learningr/assets/simulation.pdf
3. Segaran, Toby. Programming Collective Intelligence: Building Smart Web 2.0 Applications. O'Reilly Media, 2007. URL: https://axon.cs.byu.edu/~martinez/classes/778/Papers/GP.pdf

Додаткова література

4. Bigus J., Bigus J. Constructing Intelligent Agents Using Java: Second Edition. – New York: Addison-Wesly, 2002. – 520 p. URL:
https://books.google.com.ua/books/about/Constructing_Intelligent_Agents_Using_Ja.html?id=RxTN7rgf19gC&redir_esc=y
5. Subrahmanian V.S. Heterogeneos agent systems. – The MIT Press, Cambridge, Massachusetts, London, England, 2000. – 580 p. URL:
https://books.google.com.ua/books/about/Heterogeneous_Agent_Systems.html?hl=ca&id=2YMUNKuq8mYC&redir_esc=y

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% 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
Станіслав МІЛЕВСЬКИЙ