



Силабус освітнього компонента

Програма навчальної дисципліни

Агентне моделювання

**Шифр та назва спеціальності**

F5 – Кібербезпека та захист інформації

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Спеціалізація**Кафедра**

Кібербезпеки (328)

Освітня програма

Кібербезпека

Тип дисципліни

Професійна підготовка, Вибіркова

Рівень освіти

Другий (магістерський)

Форма навчання

Денна, заочна

Семестр

2

Мова викладання

Українська, англійська

Викладачі, розробники

**АКСЬОНОВА Ірина Вікторівна**

Iryna.Aksonova@khpі.edu.ua

Кандидат економічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 150, з них свідоцтв на авторський твір - більше 15, розділів у монографіях - 10, статей, що реферуються у науково метричних базах Scopus та WoS - 9. Лектор з дисциплін: "Штучний інтелект і бізнес-аналітика", "Теорія інформації і кодування", "Технологія управління безпекою бізнес-процесів, "Агентне моделювання" та інших у студентів бакалавріата та магістратури.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна програма дисципліни "Агентне моделювання" 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 вивчення дисципліни – це створення теоретичної основи для розробки та використання інтелектуальних агентно-орієнтованих систем. Наведені у роботі приклади застосування програмних агентів та мультиагентних систем мають показати ефективність агентного підходу та підкреслити сферу його застосування.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований 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. Проводити 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.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Основи програмування, Технології програмування, Алгоритми та структури даних. Основи математичного моделювання систем безпеки, Основи кібербезпеки.

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

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Системи, засновані на знаннях. Інтелектуальні системи: основні визначення та проблеми. Символьні обчислення. Знання і моделі їх подання. Рівні розуміння інформації. Онтологічне подання знань. Засоби здобуття знань. Експертні системи.	4
Тема 2. Теоретичні основи інтелектуальних програмних агентів. Основні властивості програмних агентів. Архітектури агентів. Мультиагентні системи. Мови комунікації агентів. Агентно-орієнтоване програмування. Методології розробки мультиагентних систем. Засоби інтелектуалізації поведінки програмних агентів.	4
Тема 3. Застосування агентних технологій для пошуку інформації в Інтернеті. Інформаційні ресурси Інтернету. Засоби формального подання метазнань про інформаційні ресурси Інтернету. Інформаційно-пошукові агенти. Мультиагентні інформаційно-пошукові системи.	4
Тема 4. Застосування агентних технологій. Інформаційна економіка як сфера застосування агентних технологій. Програмні агенти е-комерції. Програмні агенти логістики. Програмні агенти електронних ринків. Програмні агенти дистанційної освіти. Програмні агенти електронного урядування. Програмні агенти систем кібербезпеки. Програмні агенти електронної медицини.	4
Загальна кількість годин	16

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти α
Тема 1. Установка програмного забезпечення для розробки та тестування додатків. Ознайомлення з інструментами та середовищами розробки, необхідними для створення агентних систем. Встановлення середовищ програмування (наприклад, Eclipse, IntelliJ IDEA), налаштування Java Development Kit (JDK) та бібліотек для агентного моделювання (JADE, AnyLogic тощо). Перевірка коректності роботи програмного середовища.	8	0,2
Тема 2. Розробка програми моделювання агента. Створення базового програмного модуля агента, визначення його поведінки, ролей і станів. Реалізація взаємодії агентів через обмін повідомленнями. Тестування моделей на простих прикладах середовища моделювання.	8	0,2
Тема 3. Ознайомлення з JADE. Вивчення структури та архітектури платформи JADE (Java Agent DEvelopment Framework). Створення простого агентного застосунку, який реалізує обмін повідомленнями між агентами,	8	0,2

дослідження механізмів реєстрації, пошуку та комунікації агентів у системі.

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

8

0,2

Розробка прикладу мобільного застосунку, що використовує агентну архітектуру. Інтеграція JADE з Android-платформою. Аналіз можливостей застосування мультиагентних систем у мобільних і розподілених середовищах.

Загальна кількість годин

32

$$\sum_{i=1}^n a_i = 0,8$$

Контрольні роботи

Теми контрольних робіт

Вагові
коефіцієнти b

Тема 1. Системи, засновані на знаннях. Теоретичні основи інтелектуальних програмних агентів.

0,1

Контрольна робота спрямована на закріплення знань про принципи побудови інтелектуальних систем і програмних агентів. Розглядаються основні поняття систем, заснованих на знаннях, методи подання знань, експертні системи та особливості їх функціонування.

Особлива увага приділяється теоретичним основам програмних агентів: їх властивостям, архітектурам, мовам комунікації, а також методологіям розробки мультиагентних систем. Студенти повинні продемонструвати розуміння принципів інтелектуальної поведінки агентів та підходів до створення гнучких агентних архітектур.

Тема 2. Застосування агентних технологій у сучасних інформаційних системах.

0,1

У роботі розглядаються практичні аспекти застосування агентних технологій у різних галузях діяльності. Аналізуються інформаційно-пошукові агенти, принципи їх роботи та роль у сучасних Інтернет-технологіях.

Досліджуються приклади застосування агентних технологій в економіці, логістиці, електронній комерції, освіті, урядуванні, медицині та кібербезпеці. Метою є формування у студентів системного уявлення про можливості та переваги використання агентних підходів для автоматизації процесів пошуку, аналізу та обробки інформації.

Загалом

$$\sum_{i=1}^m b_i = 0,2$$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення

Кількість годин

Тема 1 Історія розвитку агентних технологій.

8

Розглядаються етапи становлення агентного підходу — від ранніх експертних систем до сучасних мультиагентних платформ. Аналізуються ключові наукові школи та концепції, що вплинули на розвиток агентних систем.

Тема 2. Класифікація агентів і типи агентних систем.

8

Вивчаються різновиди агентів: реактивні, когнітивні, адаптивні, навчальні. Описуються критерії класифікації агентних систем і сфери їх застосування.

Тема 3. Архітектури агентів: реактивні, розумні та гібридні моделі. Пояснюються відмінності між різними архітектурами агентів, принципи їх проектування, а також способи реалізації поведінки на основі правил, логіки або навчання.	7
Тема 4. Комунікація між агентами. Мови та протоколи взаємодії. Розглядаються основи обміну повідомленнями між агентами, мови типу ACL (Agent Communication Language) та протоколи взаємодії (FIPA, KQML тощо).	7
Тема 5. Онтології в агентних системах. Вивчаються принципи побудови онтологій для формального опису знань у мультиагентних системах, роль онтологічного моделювання для взаєморозуміння агентів.	7
Тема 6. Координація, планування та переговори між агентами. Аналізуються методи узгодження дій агентів, алгоритми колективного планування, розподілу ресурсів і ведення переговорів між агентами в умовах конфлікту інтересів.	7
Тема 7. Агентні системи в Інтернеті речей (IoT). Розглядається застосування агентних технологій у смарт-середовищах, зокрема в інтернеті речей, для автономного управління пристроями та оптимізації процесів.	7
Тема 8. Агентні технології в системах кібербезпеки. Досліджуються підходи до використання агентів для виявлення вторгнень, моніторингу трафіку, аналізу загроз і реагування на інциденти безпеки.	7
Тема 9. Мультиагентне моделювання соціальних та економічних процесів. Описується застосування агентного моделювання для аналізу поведінки людей, ринкових процесів, розповсюдження інформації, конфліктів і співпраці.	7
Тема 10. Перспективи розвитку агентного моделювання та штучного інтелекту. Розглядаються сучасні тренди в інтеграції агентних технологій зі штучним інтелектом, машинним навчанням та хмарними обчисленнями.	7
Загальна кількість годин	72

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.

Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Плєскач В.Л., Рогушина Ю.В. Агентні технології: Монографія. – К.: Київ. нац. торг.-екон. ун-т, 2005. – 344 с. (Табл.10. Рис.58. Бібліограф.361) [Електронний ресурс]. – Режим доступу: <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. [Електронний ресурс]. – Режим доступу:
<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. [Електронний ресурс]. – Режим доступу:
<https://axon.cs.byu.edu/~martinez/classes/778/Papers/GP.pdf>.

Додаткова література

4. Bigus J., Constructing Intelligent Agents Using Java: Second Edition. – New York: Addison-Wesley, 2002. – 520 p. [Електронний ресурс]. – Режим доступу:
https://books.google.com.ua/books/about/Constructing Intelligent Agents Using Ja.html?id=RxTN7rgf19gC&redir_esc=y
5. Subrahmanian V.S. Heterogeneous agent systems. – The MIT Press, Cambridge, Massachusetts, London, England, 2000. – 580 p. [Електронний ресурс]. – Режим доступу:
https://books.google.com.ua/books/about/Heterogeneous Agent Systems.html?hl=ca&id=2YMUNKuq8mYC&redir_esc=y.

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k :

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,8	0,2		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.

Розрахунок підсумкової оцінки проводиться за формулою:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \Pi_k \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль

I – оцінка за виконання індивідуального завдання

K – середньозважена оцінка за контрольні роботи

Π_k – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + \dots + K_m \cdot b_m}{\sum_{i=1}^m b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Шкала оцінювання

Поточні оцінки за кожну складову (Π , K , I , ...) виставляються за 100-бальною шкалою згідно з [положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої](#)

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B

освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

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

Здобувач вищої освіти 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

30.08.2025



Завідувач кафедри
Сергій ЄВСЕЄВ

30.08.2025



Гарант ОП
Ольга КОРОЛЬ