Силабус освітнього компонента
Програма навчальної дисципліни

Ігрове та системно-динамічне моделювання кіберконфліктів

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
третій (освітньо-науковий)

Тип дисципліни
Профільна підготовка, Вибіркова

Семестр
3

Мова викладання
Українська

Викладачі, розробники

МІЛЕВСЬКИЙ Станіслав Валерійович
stanislav.milevskyi@khpi.edu.ua
кандидат економічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Автор понад 100 наукових та навчально-методичних праць. Науковий Гарант освітньо-професійної програми другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Основи математичного моделювання систем безпеки», «Англійська мова в академічних застосунках», «Моделювання кіберфізичних дій» у студентів бакалавріата та магістратури.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна програма дисципліни "Ігрове та системно-динамічне моделювання кіберконфліктів" охоплює сучасні методи аналізу та моделювання кіберконфліктів з використанням системної динаміки та теорії ігор. Аспіранти вивчатимуть основи стратегічного прийняття рішень у кіберпросторі та використання динамічних моделей для прогнозування результатів кіберконфліктів. Лабораторні роботи дозволять аспірантам застосувати вивчені методи на практиці, моделюючи взаємодію між кіберзагрозами та заходами кіберзахисту.

Мета та цілі дисципліни

Метою дисципліни є розвиток у аспірантів навичок стратегічного планування та моделювання кіберконфліктів з використанням теорії ігор та системної динаміки для прогнозування розвитку кіберзагроз і визначення оптимальних стратегій кіберзахисту.

Формат занять

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

Компетентності

ЗК-1.Здатність до професійного спілкування іноземною мовою.
ЗК-2. Здатність до абстрактного мислення, аналізу та синтезу, проведення самостійних досліджень.
ЗК-3. Здатність до виявлення, генерування нових ідей, дослідження та вирішення проблем за професійним спрямуванням.
СК-1. Здатність до застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації, створення комплексних систем захисту інформації.
СК-4. Здатність систематизувати професійні знання в інформаційно-комунікаційних технологіях, моделювання механізмів кібербезпеки.
СК-7. Здатність критично переосмислювати наявні інформаційні технології та відстежувати тенденції їх розвитку.

Результати навчання

РН-1. Вміння формувати і аргументовано відстоювати власну думку з різних проблем філософії науки та методології наукового пізнання, бути критичним і самокритичним.
РН-2. Вміння вести дискусії, здійснювати публічні промови, робити повідомлення і доповіді з питань дисертаційного дослідження, аргументовано викладати власну точку зору державною та іноземною мовами.
РН-3. Вміння читати оригінальну наукову літературу на іноземній мові, опрацьовувати та оформляти інформацію. Вміння та навики працювати з сучасними бібліографічними і реферативними базами даних, а також наукометричними платформами (наприклад, Scopus, Web of Science, Web of Knowledge та ін.).
РН-4. Знання, розуміння, вміння та навички використання правил цитування та посилання на використані джерела, правил оформлення бібліографічного списку, розуміння змісту і порядку розрахунків основних кількісних наукометричних показників ефективності наукової діяльності (індекс цитування, індекс Гірша (h-індекс), імпакт-фактор (ІФ, або IF)).
РН-5. Вміння та навички критично сприймати та аналізувати існуючі наукові теорії та ідеї, шукати власні шляхи вирішення проблеми та завдань, проводити критичний аналіз власних матеріалів, генерувати власні нові ідеї, приймати обґрунтовані рішення.
РН-9. Вміння та навички спілкуватися в діалоговому режимі з широкою науковою спільнотою та громадськістю в галузі наукової та/або професійної діяльності з метою обговорення дискусійних питань, результатів досліджень, узгодження дій і спільної роботи на конференціях, симпозіумах, наукових семінарах, доводити результати досліджень та інновацій до колег, публічно представляти, захищати результати своїх досліджень, обговорювати їх і дискутувати з науково-професійною спільнотою, використовувати сучасні засоби візуальної презентації результатів дослідження..
РН-10. Володіння предметною базою знань та сучасними техніками дослідження, здатність створювати та інтерпретувати нові знання.
РН-11. Вміння розробляти проекти наукових досліджень та моделювати їх структуру, застосовуючи різні способи подання статистичної інформації та результатів.
РН-14. Вміння приймати обґрунтовані рішення, бути здатним їх оцінювати та забезпечувати якість виконуваних робіт.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 20 год., лабораторні роботи – 20 год., самостійна робота – 80 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Технології управління безпекою бізнес-процесів, Основи математичного моделювання систем безпеки. Моделювання механізмів кібербезпеки.

Особливості дисципліни, методи та технології навчання

Викладання дисципліни передбачає використання пояснювально-ілюстративного та репродуктивного методів, а також активізацію навчально-пізнавальної діяльності через презентації, індивідуальні та групові проекти, моделювання систем, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Вступ до моделювання кіберконфліктів.
Основні концепції кіберконфліктів. Системно-динамічні та ігрові моделі у кіберпросторі.
Тема 2. Теорія ігор для моделювання кіберконфліктів.
Основи теорії ігор. Нульові та ненульові ігри. Дилема ув'язненого в контексті кібербезпеки.
Тема 3. Моделі системної динаміки у кіберконфліктах.
Використання системної динаміки для аналізу кіберконфліктів. Побудова моделей кіберзагроз та кіберзахисту.
Тема 4. Кіберконфлікти як стратегічні ігри.
Взаємодія атакуючих і захисних сторін у кіберконфліктах. Ігрові стратегії для вибору найкращого сценарію.
Тема 5. Аналіз рішень у кіберконфліктах за допомогою теорії ігор.
Домінантні стратегії. Еквілюбрій Неша. Моделювання поведінки кіберсистем на основі ігрових моделей.
Тема 6. Системні петлі зворотного зв'язку у моделюванні кіберконфліктів.
Позитивні та негативні петлі зворотного зв'язку. Вплив на динаміку кіберконфліктів.
Тема 7. Моделювання сценаріїв ескалації кіберконфліктів.
Створення моделей динамічної ескалації та керування кіберконфліктами. Визначення "точок перелому".
Тема 8. Використання програмних інструментів для ігрового та динамічного моделювання.
Інструменти для моделювання кіберконфліктів: AnyLogic, Vensim, MATLAB.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Побудова ігрової моделі кіберконфлікту.
Моделювання взаємодії атакуючих і захисних сторін з використанням теорії ігор.
Тема 2. Системно-динамічне моделювання кіберконфліктів у Vensim.
Побудова динамічних моделей кіберзагроз та стратегій захисту.
Тема 3. Аналіз кіберконфлікту за сценаріями з використанням теорії ігор.
Визначення оптимальних стратегій для кожної сторони конфлікту.
Тема 4. Моделювання петлі зворотного зв'язку у динамічному розвитку кіберконфлікту.
Тема 5. Симуляція ескалації кіберконфлікту та розробка стратегії його врегулювання.

Самостійна робота

Самостійна робота аспіранта є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи аспіранти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Аспірантам 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. Axelrod, Robert. The Evolution of Cooperation. Basic Books, 1984. URL: https://books.google.com.ua/books/about/The_Evolution_of_Cooperation.html?id=NJZBCGbNs98C&redir_esc=y
2. Sterman, John. Business Dynamics: Systems Thinking and Modeling for a Complex World. McGraw-Hill Education, 2000. URL: https://books.google.com.ua/books/about/Business_Dynamics.html?id=CCKCQgAACAAJ&redir_esc=y
3. Myerson, Roger B. Game Theory: Analysis of Conflict. Harvard University Press, 1991. URL: https://books.google.com.ua/books/about/Game_Theory.html?id=E8WQFRCsNr0C&redir_esc=y

Додаткова література

4. Forrester, Jay W. Industrial Dynamics. MIT Press, 1961. URL: http://www.laprospective.fr/dyn/francais/memoire/autres_textes_de_la_prospective/autres_ouvrages_numerises/industrial-dynamics-forrester-1961.pdf
5. Richardson, George P. Feedback Thought in Social Science and Systems Theory. University of Pennsylvania Press, 1991. URL: https://books.google.com.ua/books/about/Feedback_Thought_in_Social_Science_and_S.html?id=Ey58AAAAIAAJ&redir_esc=y
6. Vensim User's Guide. Ventana Systems, 2020. URL: https://vensim.com
7. AnyLogic in Practice: Model Development and Simulation. AnyLogic Software, 2018. URL: https://www.anylogic.com/

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;
•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

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	28.08.2024		Завідувач кафедри Сергій ЄВСЕЄВ
	28.08.2024		Гарант ОП Олександр МІЛОВ