Силабус освітнього компонента
Програма навчальної дисципліни

Моделювання соціокіберфізичних систем

Шифр та назва спеціальності
113 – Прикладна математика

Інститут
ННІ Комп`ютерних наук та інформаційних технологій

Освітня програма
Інтелектуальний аналіз даних

Кафедра
Кібербезпеки

Рівень освіти
Бакалаврї

Тип дисципліни
Спеціальна (фахова), Вибіркова

Семестр
5

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

Мілевський Станіслав Валерійович

Stanislav.Milevskyi@khpi.edu.ua
Кандидат економічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 60, з них 5 патентів на корисну модель, 11 колективних монографій, 3 навчальних посібники, з яких 1 з грифом Міністерства освіти і науки України, понад 40 статей у закордонних виданнях та фахових виданнях України, з них 8 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Організація і безпека баз даних», «Основи планування та адміністрування служб доступу до інформаційних ресурсів», «Бази даних для корпоративних інформаційних систем», «Основи математичного моделювання систем безпеки», «Системи та методи прийняття рішень», «Ризик-менеджмент» , «Управління ІТ-проектами та їх безпека» у студентів бакалавріата та магістратури.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Моделювання соціокіберфізичних систем" є вибірковою навчальною дисципліною. Навчальна дисципліна присвячена фундаментальним основам теорії математичного та комп'ютерного моделювання соціокіберфізичних систем , принципам побудови та дослідження математичних моделей соціокіберфізичних систем.

Мета та цілі дисципліни

Підготовка фахівців, в області інформаційної безпеки, безпеки телекомунікаційного забезпечення, і мобільних пристроїв, а також фахівців з моделювання соціокіберфізичних систем, на базі освоєння принципів та методів збору цифрової інформації для дослідження поведінки агентів систем безпеки, проведення статичного аналізу індивідуальної та групової поведінки учасників соціокіберфізичних систем, використовуючи інструменти та методи різноманітних напрямків кібербезпеки.

Формат занять

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

Компетентності

ЗК 1. Здатність учитися й оволодівати сучасними знаннями.
ЗК 2. Здатність застосовувати знання у практичних ситуаціях.
ЗК 7. Здатність до пошуку, оброблення й аналізу інформації з різноманітних джерел.
ЗК 8. Знання і розуміння предметної області та розуміння професійної діяльності.
ЗК 10. Навички у використанні інформаційних і комунікаційних технологій.
СК 5. Здатність розробляти алгоритми та структури даних, програмні засоби та програмну документацію.
СК 6. Здатність проєктувати бази даних, інформаційні системи та ресурси.

Результати навчання

РН 11. Вміти застосовувати сучасні технології програмування та розроблення програмного забезпечення, програмної реалізації чисельних і символьних алгоритмів.
РН 12. Розв'язувати окремі інженерні задачі та/або задачі, що виникають принаймні в одній предметній галузі: в соціології, економіці, екології та медицині.
РН 13. Використовувати в практичній роботі спеціалізовані програмні продукти та програмні системи комп'ютерної математики.
РН 14. Виявляти здатність до самонавчання та продовження професійного розвитку.
РН 15. Уміти організувати власну діяльність та одержувати результат у рамках обмеженого часу.
РН 16. Демонструвати навички взаємодії з іншими людьми, уміння працювати в команді.
РН 18. Ефективно спілкуватися з питань інформації, ідей, проблем та рішень зі спеціалістами та суспільством загалом.

Обсяг дисципліни

Загальний обсяг дисципліни 180 год. (6 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 116 год.

Передумови вивчення дисципліни (пререквізити)

«Математичний аналіз», «Лінійна алгебра», «Аналітична геометрія», «Комп'ютерна дискретна математика», «Основи криптології», «Алгоритмізація та 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.
Цілі та завдання навчальної дисципліни “Моделювання соціокіберфізичних систем”. Місце дисципліни у навчальному процесі підготовки спеціаліста з кібербезпеки. Структура, зміст тематичного плану вивчення дисципліни; навчально-методична література. Особливості вивчення дисципліни; форми контролю знань, умінь та навичок учнів. Напрями науково-дослідної роботи студентів.
Тема 2. Моделювання.
Основні поняття моделювання, поняття системи та моделі, основні типи моделей, види моделей та їх класифікація за різними критеріями, вимоги до моделей.
Тема 3. Основні види моделювання. Формальні методи побудови моделей.
Основні види моделювання (аналітичне, імітаційне, статистичне), їх характеристики та відношення між собою. Формальні методи побудови моделей: кібернетичний підхід, системна динаміка, теоретично-множинний підхід.
Тема 4. Принципи побудови моделей. Технологія моделювання.
Основні принципи побудови моделей: інформаційної достатності, доцільності, здійсненності, множинності моделей, агрегації, параметризації, застосування методології ітераційного багаторівневого моделювання. Технологія моделювання: основні етапи, їх взаємозв'язок та характеристики.
Тема 5. Ідентифікація параметрів математичної моделі. Адекватність, чутливість, несуперечність моделі.
Постановка завдання ідентифікації, основні етапи його вирішення та їх взаємозв’язок. Поняття адекватності, чутливості та несуперечність моделі, формальні способи їх перевірки.
Тема 6. Структуровані підходи до збирання інформації.
Методи розвідки із відкритим вихідним кодом. Огляд методів структурованого аналізу. Типи інформації, що збирається: ділова інформація (фінансова, клієнти, постачальники, партнери). Інформація про IT-інфраструктуру. Виявлення джерел інформації.
Тема 7. Основні поняття і визначення, що використовуються при описі моделей безпеки комп'ютерних систем.
Елементи теорії комп'ютерної безпеки. Сутність, суб'єкт, доступ, інформаційний потік. Класична класифікація загроз безпеки інформації. Види інформаційних потоків. Види політик управління доступом та інформаційними потоками. Витік права доступу і порушення безпеки КС. Математичні основи моделей безпеки.
Тема 8. Системно-динамічні моделі у соціо-кіберфізичних системах. Мова системної динаміки.
Концепція системної динаміки. Класифікація систем. Методи вивчення складних систем. Системний аналіз та системна динаміка. Понятійний апарат. Основні поняття. Типи зв'язків між елементами системи. Класифікація та позначення елементів моделі.
Тема 9. Системно-динамічні моделі у соціо-кіберфізичних системах. Побудова імітаційних моделей.
Формування цілей дослідження. Збір інформації про систему та процеси (етап референції). Побудова концептуальної моделі. Побудова машинної моделі. Проведення імітаційних експериментів та верифікація моделі. Обговорення моделі (дебрифінг). Поліпшення моделі.
Тема 10. Теоретико-ігрові моделі поведінки у соціо-кіберфізичних системах.
Елементи теорії ігор. Ігри та їх класифікація. Чисті стратегії гравців. Змішана стратегія гравців. Матричні ігри. Мінімаксні стратегії. Гра з сідловою точкою. Гра без сідловою точкою. Вирішення матричної гри. Критерії оптимальності стратегії адміністратора. Методи розв'язання матричних ігор. Домінування. Використання лінійного програмування. Біматричні ігри. Рівноваги Неша у кінцевій грі N осіб. Дилема ув'язненого. Програмне забезпечення знаходження рішення ігор. Нескінченні ігри.
Тема 11. Застосування теорії ігор для моделювання соціо-кіберфізичних систем.

Приклад матричної гри "зловмисник - адміністратор". Програмне застосування для вибору оптимального набору засобів захисту. Відображення атак у кіберпросторі. Вибір засобу ефективного захисту від DoS/DDoS-атак. Моделювання поведінки азартного зловмисника.
Тема 12. Агентні моделі соціо-кіберфізичних систем.
Об'єкти та агенти. Класифікація агентів кіберфізичних систем. Мультиагентні системи. Взаємодія агентів у кіберпросторі. Комунікація та координація кіберфізичних агентів. Кооперація та конфронтація агентів. Моделі конфліктних ситуацій у кіберпросторі.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Використання системи MATLAB для моделювання соціо-кіберфізичних систем.
Тема 2. Використання системи SIMULINK для моделювання соціо-кіберфізичніх систем.
Тема 3. Моделювання кінцевих автоматів як прототипів агентів кіберпростору.
Тема 4. Моделювання соціо-кіберфізичних систем мережами Петрі.
Тема 5. Основи побудови системно-динамічних моделей за допомогою PowerSim. Побудова імітаційної моделі взаємодії «зловмисник-захисник».
Тема 6. Побудова та використання ігрової моделі «Відбиття атак у кіберпросторі»

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 та іспиту.

Література та навчальні матеріали

Основна література

1. Cyber-Physical Systems / ed. by G. M. Siddesh et al. Chapman and Hall/CRC, 2015. URL: https://doi.org/10.1201/b19206 (date of access: 31.01.2023).
2. Industrial Cloud-Based Cyber-Physical Systems / ed. by A. W. Colombo et al. Cham : Springer International Publishing, 2014. URL: https://doi.org/10.1007/9783-319-05624-1 (date of access: 31.01.2023).
3. Євсеєв С. П. Кібербезпека: сучасні технології захисту. / Євсеєв С. П, Остапов С. Е., Король О. Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: “Новий Світ- 2000”, 2019. – 678 с.
http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.
4. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.
https://lira-k.com.ua/preview/12867.pdf
5. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. – Львів : Видавництво Львівської політехніки, 2019. – 580 с. – ISBN 978-966-941-339-0.
http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf
6. Nardelli P. H. J. Cyber-Physical Systems: Theory, Methodology, and Applications. Wiley & Sons, Incorporated, John, 2022
https://content.e-bookshelf.de/media/reading/L-18316928-9cb3bd7865.pdf

Додаткова література

7. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
8. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.

https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022.–196 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
10. Євсеєв С. П. Кібербезпека: Лабораторний практикум з основ крипографічного захисту / С. П. Євсеєв, О. В. Мілов, О. Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
11. Євсєев С. П. Кібербезпека: основи кодування та криптографії/ С. П. Євсеєв, О. В. Мілов, С. Е. Остапов, О. В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

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

Дата погодження, підпис
28.08.2023 р.

Завідувач кафедри
Сергій ЄВСЕЄВ

Дата погодження, підпис
31.08.2023 р.

Гарант ОП
Олена АХІЄЗЕР