



Силабус освітнього компонента

Програма навчальної дисципліни



Моделювання кіберфізичних дій

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

Магістр

Тип дисципліни

Профільна підготовка, Вибіркова

Семестр

1

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 шпіднаж», «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 дисципліна "Моделювання кіберфізичних дій" є вибірковою навчальною дисципліною. Дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця з кібербезпеки та дозволяють вирішувати професійні задачі, що базуються на організації та моделюванні дій в кризових ситуаціях пов'язаних з кібербезпекою.

Мета та цілі дисципліни

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

Формат занять

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

Компетентності

КФ3. Здатність досліджувати, розробляти і

супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

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.

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.

Результати навчання

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

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.

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.

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 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Математичні основи криптології, Основи криптографічного захисту, 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.

Цілі та завдання навчальної дисципліни «Моделювання кіберфізичних дій». 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, непротирічність моделі.

Постановка завдання ідентифікації, основні етапи його вирішення та їх взаємозв'язок. Поняття адекватності, чутливості та непротирічності 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. Соціальна інженерія.

Соціальна інженерія. Огляд проекту «Інструментарій соціальної інженерії».

Тема 9. Системно-динамічні моделі дій у кіберпросторі. 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 10. Системно-динамічні моделі дій у кіберпросторі. 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 (дебріфінг). Поліпшення моделі.

Тема 11. Теоретико-ігрові моделі дій у кіберпросторі.

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 12. Застосування теорії ігор для моделювання кіберфізичних дій.

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 13. Агентні моделі кіберфізичних дій.

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.

Тема 14. Планування дій у кібер-фізичних системах.

Планування дій. Планування при синтезі програм. Вчинки та поведінка.

Тема 15. Навчання у кіберфізичних системах.

Моделі навчання. Навчання за прикладами. Навчальні системи.

Тема 16. Розпізнавання у кібер-фізичних системах.

Проблема розпізнавання. Математична теорія розпізнавання образів. Розпізнавання атак. Розпізнавання зловмисників. Алгоритмічні основи знань.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Використання системи MATLAB для моделювання дій у кіберфізичних системах.

Тема 2. Використання системи SIMULINK для моделювання дій у кіберфізичних системах.

Тема 3. Моделювання кінцевих автоматів як прототипів агентів кіберпростору.

Тема 4. Моделювання кіберфізичних дій мережема 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».

Тема 7. Мультиагентна модель поведінки та взаємодії агентів в кіберфізичній системі.

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 заліку.

Література та навчальні матеріали

Основна література:

1. Томашевський В.М, Моделювання систем. – К. Видавнича група ВНУ, 2005. – 352 с.
2. Євсєєв С.П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів "Новий світ-2000", 2020. – 241 с.
3. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсєєв, О.В. Мілов, С.Е. Остапов, О.В. Северінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.
4. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0.

Додаткова література :

- 1 Жерновий Ю. В. Імітаційне моделювання систем масового обслуговування: Практикум. – Львів: Видавничий центр ЛНУ імені Івана Франка, 2007. – 307 с.
2. Shoham, Yoav, and Kevin Leyton-Brown, «Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations». Cambridge University Press, 2009.

3. Sun, Ron, Cognition and Multi-Agent Interaction: From Cognitive Modeling to Social Simulation. Cambridge University Press, 2006. <http://www.cambridge.org/uk/catalogue/catalogue.asp?isbn=0521839645>.
4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
5. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlov, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
6. 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.

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: 20% семестрової оцінки;
- залік: 30% 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

28.08.2023



Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2023



Гарант ОП
Олександр МІЛОВ