



Силабус освітнього компонента Програма навчальної дисципліни



Ігрове та системно-динамічне моделювання кіберконфліктів

Шифр та назва спеціальності

125 – Кібербезпека та захист інформації

Інститут

ІНІ комп'ютерних наук та інформаційних технологій

Освітня програма

Освітньо-наукова програма Кібербезпеки

Кафедра

Кібербезпеки (328)

Рівень освіти

Магістр

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. Студенти вивчатимуть основи стратегічного прийняття рішень у кіберпросторі та використання динамічних моделей для прогнозування результатів кіберконфліктів. Лабораторні роботи дозволять студентам застосувати вивчені методи на практиці, моделюючи взаємодію між кіберзагрозами та заходами кіберзахисту.

Мета та цілі дисципліни

Метою дисципліни є розвиток у студентів 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 – залік.

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

КЗ-2. Здатність проводити дослідження на відповідному рівні.

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

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.

КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в 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.

КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес/операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

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.
- РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
- РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів у сфері інформаційної та/або кібербезпеки 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.
- РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.
- 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 – 16 год., лабораторні роботи – 16 год., самостійна робота – 88 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Технології управління безпекою бізнес-процесів, Основи математичного моделювання систем безпеки

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. Еквілібрій 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 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. 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.lapropective.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=Ey58AAAIIAAJ&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;
- 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