Силабус освітнього компонента
Програма навчальної дисципліни

Ігрове та системно-динамічне моделювання кіберконфліктів

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

Семестр
3

Мова викладання
Українська

Викладачі, розробники

МІЛЕВСЬКИЙ Станіслав Валерійович

stanislav.milevskyi@khpi.edu.ua
Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 100 наукових та навчально-методичних праць. Гарант освітньо-наукової програми «Кібербезпека» 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 заняття, самостійна робота, консультації. Підсумковий контроль – диференційований 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. Провадити 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 напряму 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 – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Основи програмування, Основи математичного моделювання систем безпеки, Технології управління безпекою бізнес-процесів, Комплексні системи захисту інформації.

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

Навчальні заняття

Лекції

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

Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Побудова ігрової моделі кіберконфлікту. Моделювання взаємодії атакуючих і захисних сторін з використанням теорії ігор.	6	0,2
Тема 2. Системно-динамічне моделювання кіберконфліктів у Vensim. Побудова динамічних моделей кіберзагроз та стратегій захисту.	6	0,1
Тема 3. Аналіз кіберконфлікту за сценаріями з використанням теорії ігор. Визначення оптимальних стратегій для кожної сторони конфлікту.	6	0,1
Тема 4. Моделювання петлі зворотного зв'язку у динамічному розвитку кіберконфлікту. Розглядаються принципи побудови позитивних і негативних петель зворотного зв'язку у кіберконфліктах. Аналізується їхній вплив на стабільність системи, поширення атак та ефективність контрзаходів. Виконується моделювання взаємодії між атакуючими і захисними діями з урахуванням часових затримок і накопичувальних ефектів.	6	0,2
Тема 5. Симуляція ескалації кіберконфлікту та розробка стратегії його врегулювання. Вивчаються підходи до створення симуляцій, що відображають етапи ескалації кіберконфліктів. Аналізуються сценарії розвитку атак, реакції сторін та методи стабілізації ситуації. Розробляються стратегії управління кіберконфліктами, спрямовані на зниження ризиків і мінімізацію наслідків для кіберінфраструктури.	8	0,2
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Теоретичні основи ігрового моделювання кіберконфліктів. Робота присвячена вивченню основ теорії ігор та її застосуванню для моделювання кіберконфліктів. Розглядаються стратегічні взаємодії між атакуючими та захисними сторонами, поняття рівноваги Неша, нульові й ненульові ігри, а також дилема ув'язненого в контексті кібербезпеки.	0,1
Тема 2. Системно-динамічне моделювання процесів ескалації кіберконфліктів. У роботі аналізуються методи системно-динамічного моделювання кіберконфліктів. Вивчаються поняття зворотних зв'язків, сценарії розвитку та ескалації конфліктів, визначаються критичні точки системи. Розглядаються програмні засоби для побудови моделей — Vensim, PowerSim, AnyLogic.	0,1

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 та еволюція кіберконфліктів. Аналіз ключових подій і тенденцій розвитку кіберпротистоянь між державами, організаціями та окремими групами.	8
Тема 2. Типологія кіберзагроз і моделей поведінки порушників. Види атак, мотивація зловмисників, класифікація кіберзагроз у контексті ігрового моделювання.	8
Тема 3. Психологічні аспекти прийняття рішень у кіберконфліктах. Моделювання поведінки людини та групових стратегій під час протидії атакам.	7
Тема 4. Застосування теорії катастроф у кіберконфліктах. Моделі різких змін стану системи при перевищенні критичних параметрів.	7
Тема 5. Моделювання інформаційних впливів та кіберпропаганди. Аналіз ігрових сценаріїв, що враховують психологічні та соціотехнічні аспекти кібервійн.	7
Тема 6. Аналіз рівноваги у багатосторонніх кіберконфліктах. Застосування узагальненої рівноваги Неша для оцінювання стратегій у конфліктах із кількома гравцями.	7
Тема 7. Застосування агентного підходу до моделювання кіберконфліктів. Моделювання взаємодії кібер-агентів, що імітують поведінку атакуючих та захисних сторін.	7
Тема 8. Оцінювання ефективності стратегій захисту в ігрових моделях. Розрахунок показників успішності оборони, витрат на контрзаходи та ймовірності відновлення системи.	7
Тема 9. Системно-динамічні моделі управління кіберінцидентами. Моделювання процесів реагування, ліквідації наслідків і відновлення після атак.	7
Тема 10. Програмні засоби візуалізації результатів ігрових і динамічних моделей. Огляд сучасних інструментів (Vensim, AnyLogic, MATLAB, NetLogo) для представлення результатів моделювання кіберконфліктів.	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. 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

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:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

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

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

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

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

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	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Станіслав МІЛЕВСЬКИЙ