Силабус освітнього компонента
Програма навчальної дисципліни

Основи математичного моделювання систем безпеки

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
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна, заочна

Семестр
5

Мова викладання
Українська, англійська

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», «Основи машинного навчання для кібербезпеки», «Англійська мова в академічних застосунках», «Моделювання кіберфізичних дій», «Математичні моделі управління ІТ-проєктами» у студентів бакалавріата та магістратури, «Моделювання механізмів кібербезпеки», «Математичні методи, моделі та інформаційні технології у наукових дослідженнях» у аспірантів .

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Основи математичного моделювання систем безпеки" є обов`язковою навчальною дисципліною. Дисципліна спрямована на придбання навичок в галузі моделювання систем, оволодіння методами імітаційного моделювання із застосуванням пакета (PowerSim).

Мета та цілі дисципліни

Формування у студентів теоретичних знань з основ моделювання систем безпеки, засвоєння студентами основних підходів і принципів побудови моделей та надбання навичок їх застосування для вирішення задач моделювання, що виникають при розробці інформаційних систем та систем безпеки.

Формат занять

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

Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
СК2. Здатність використовувати інформаційні технологій, сучасні методи і моделей кібербезпеки та систем захисту інформації.
СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Результати навчання

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН17. Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

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 побудови та захисту сучасних операційних систем, Математичні основи криптології.

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. Моделювання. Основні поняття. Види моделей, їх класифікація. Вимоги до моделей. Основні види моделювання. Формальні методи побудови моделей. Поняття моделювання, поняття системи та моделі, основні типи моделей, види моделей та їх класифікація за різними критеріями, вимоги до моделей. Основні види моделювання (аналітичне, імітаційне, статистичне), їх характеристики та відношення між собою. Формальні методи побудови моделей: кібернетичний підхід, системна динаміка, теоретично-множинний підхід.	2
Тема 2. 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.	2
Тема 3. 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.	2
Тема 4. Основні поняття і визначення, що використовуються при описі моделей безпеки комп'ютерних систем. Моделі комп'ютерних систем з дискреційним управлінням доступом. 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. Основні поняття. Поняття автомата. Елементи теорії графів. Алгоритмічно розв'язні і алгоритмічно нерозв'язні проблеми. Модель решітки. Основні види формальних моделей безпеки. Проблема адекватності реалізації моделі безпеки в реальному комп'ютерній системі. Модель матриці доступів Харрісона-Руззо-Ульмана. Опис моделі. Аналіз безпеки систем ХРУ. Модель типізованої матриці доступів. Модель поширення прав доступу Take-Grant. Основні положення класичної моделі Take-Grant. Розширена модель Take-Grant. Подання систем Take-Grant системами ХРУ. Дискреційні ДП-моделі. Базова ДП-модель. ДП-модель без кооперації довірених і недовірених суб'єктів.	2

Тема 5. Моделі ізольованого програмного середовища. Суб'єктно-орієнтована модель ізольованого програмного середовища. Коректність суб'єктів в ДП-моделях КС з дискреційним управлінням доступом. ДП-модель з функціонально асоційованими з суб'єктами сутностями. ДП-модель для політики безпечного адміністрування. ДП-модель для політики абсолютного поділу адміністративних і призначених для користувача повноважень. ДП-модель з функціонально або параметрично асоційованими з суб'єктами сутностями. Застосування ФАС ДП-моделі для аналізу безпеки веб-систем. Методи запобігання витоку прав доступу і реалізації заборонених інформаційних потоків. Метод запобігання можливості отримання права доступу володіння недовірених суб'єктом до довіреній суб'єкту. Метод реалізації політики безпечного адміністрування. Метод реалізації політики абсолютного поділу адміністративних і призначених для користувача повноважень.	2
Тема 6. Моделі комп'ютерних систем з мандатним управлінням доступом. Модель Бела-ЛаПадули. Класична модель Бела-ЛаПадули. Приклад некоректного визначення властивостей безпеки. Політика low-watermark в моделі Бела-ЛаПадули. Приклади реалізації заборонених інформаційних потоків. Безпека переходів. Модель мандатної політики цілісності інформації Віба. Модель систем військових сполучень. Загальні положення та основні поняття. Неформальне опис моделі СВС. Формальний опис моделі СВС. Мандатна ДП-модель. Правила перетворення станів мандатної ДП-моделі. Безпека в сенсі Бела-ЛаПадули. Умови підвищення суб'єктом рівня доступу.	2
Тема 7. Моделі безпеки інформаційних потоків. Автоматна модель безпеки інформаційних потоків. Програмна модель контролю інформаційних потоків. Імовірнісна модель безпеки інформаційних потоків. ДП-моделі безпеки інформаційних потоків за часом. ДП-модель з блокуючими доступами довірених суб'єктів. Мандатна ДП-модель з блокуючими доступами довірених суб'єктів. Мандатна ДП-модель з ототожненням породжених суб'єктів. Мандатна ДП-модель КС, що реалізують політику суворого мандатної управління доступом.	2
Тема 8. Моделі комп'ютерних систем з рольовим управлінням доступом. Моделі взаємодії в кібербезпеці. Поняття рольового управління доступом. Базова модель рольового управління доступом. Модель адміністрування рольового управління доступом. Основні положення. Адміністрування множин авторизованих ролей користувачів. Адміністрування множин прав доступу, якими володіють ролі. Адміністрування ієрархії ролей. Модель мандатної рольового управління доступом. Захист від загрози конфіденційності інформації. Захист від загроз конфіденційності та цілісності інформації. Мандатна сутнісно-рольова ДП-модель управління доступом та інформаційними потоками в операційних системах сімейства Linux. Стан системи. Функціонально або параметрично асоційовані суті. Доступи і права доступу. Завдання мандатної управління доступом для станів системи. Завдання мандатної контролю цілісності для станів системи. Фактичне володіння. Правила перетворення станів. Модель Лотка-Вольтерра. Класифікація типів взаємодій. Конкуренція. Хижак-жертва. Модель Колмогорова.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість	Вагові

	годин	коефіцієнти a
Тема 1. Автоматні моделі. Модель мережі Петрі. Поняття та класифікація автоматів. Методи побудови автоматних моделей. Мережі Петрі: структура та основні елементи. Використання мереж Петрі для моделювання процесів безпеки.	3	0,34
Тема 2. Моделі системної динаміки. Основи системної динаміки. Диференціальні рівняння у моделюванні. Побудова моделей зворотного зв'язку. Аналіз стійкості систем безпеки.	3	0,34
Тема 3. Дискретно-часові моделі. Принцип дискретизації часу. Рекурентні співвідношення. Марковські процеси в моделюванні безпеки. Приклади використання дискретно-часових моделей у практиці.	3	0,34
Тема 4. Структурні моделі безпеки. Поняття структурної моделі. Дерево відмов та дерево подій. Ієрархічні моделі складних систем. Аналіз ризиків за допомогою структурних моделей.	3	0,34
Тема 5. Імітаційні моделі. Види імітаційного моделювання. Алгоритми та методи реалізації. Використання комп'ютерних імітацій у сфері безпеки. Оцінка достовірності результатів імітаційного експерименту.	3	0,34
Тема 6. Моделювання комп'ютерних систем з дискреційним управлінням доступом. Основні принципи дискреційного управління доступом. Формалізація політики доступу. Моделювання потоків доступу користувачів. Оцінка ефективності дискреційного контролю.	3	0,34
Тема 7. Моделі ізольованого програмного середовища. Концепція «пісочниці» та ізольованого середовища. Формальні моделі ізоляції процесів. Методи запобігання витоку інформації. Аналіз захищеності ізольованих середовищ.	3	0,34
Тема 8. Моделі комп'ютерних систем з мандатним управлінням доступом. Принципи мандатного управління доступом. Модель Белла–ЛаПадули. Модель Біба. Практичне використання мандатних моделей у системах захисту.	3	0,34
Тема 9. Моделі безпеки інформаційних потоків. Поняття інформаційного потоку. Методи моделювання потоків у системах. Захист від несанкціонованих каналів передачі інформації. Аналіз загроз через побічні канали.	3	0,34
Тема 10. Моделі комп'ютерних систем з рольовим управлінням доступом. Основні принципи RBAC (Role-Based Access Control). Формалізація ролей і політик доступу. Ієрархія ролей та делегування прав. Приклади реалізації RBAC у сучасних системах.	3	0,47
Тема 11. Моделі систем взаємодії. Формалізація процесів взаємодії в системах. Моделі клієнт–сервер та однорангових систем. Протоколи взаємодії та їхнє моделювання. Безпекові аспекти у взаємодіючих системах.	2	0,47

Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 4$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Методи та підходи математичного моделювання систем безпеки. Класифікація моделей (детерміновані, стохастичні, імітаційні). Порівняння автоматних моделей, мереж Петрі та системної динаміки. Приклади застосування моделей у сфері інформаційної безпеки.	0,1
Тема 2. Математичні моделі управління доступом у комп'ютерних системах. Особливості дискреційних, мандатних та рольових моделей доступу. Формалізація політик безпеки. Аналіз переваг та недоліків різних моделей управління доступом.	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. Класифікація математичних моделей систем безпеки. Основні підходи, типи моделей, їх порівняльна характеристика.	13
Тема 2. Мережі Петрі як інструмент моделювання безпеки. Структура, властивості, приклади використання в інформаційній безпеці.	13
Тема 3. Дискретно-часові моделі у дослідженні систем захисту. Математичні апарати, застосування у моделюванні процесів безпеки.	12
Тема 4. Імітаційне моделювання в безпеці інформаційних систем. Методика побудови, приклади практичного використання.	12
Тема 5. Математичні моделі управління доступом. Дискреційна, мандатна та рольова моделі: переваги, обмеження та області застосування.	12
Тема 6. Моделі інформаційних потоків у комп'ютерних системах. Контроль і захист інформаційних потоків, методи їх аналізу.	12
Тема 7. Аналіз та оцінювання надійності систем безпеки методами математичного моделювання. Показники ефективності, методи оцінки ризиків та вразливостей.	12
Загальна кількість годин	**86**

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. Бахрушин В.Є. Математичне моделювання: навчальний посібник [Текст] – Запоріжжя: ГУ "ЗІДМУ", 2004. – 140 с.
http://moodle.nati.org.ua/mod/resource/view.php?id=7442
2. Жерновий Ю. В. Імітаційне моделювання систем масового обслуговування : Практикум / Ю. В. Жерновий. — Львів : Вид. центр ЛНУ ім. І. Франка, 2007. — 307 с.
https://new.mmf.lnu.edu.ua/wp-content/uploads/2018/02/Imit_model.pdf
3. Математичне моделювання систем і процесів: навч. посібник / П. М. Павленко, С. Ф. Філоненко, О. М. Чередніков, В. В. Трейтяк. – К. : НАУ, 2017. – 392 с.
https://pdf.lib.vntu.edu.ua/books/2020/Pavlenko_2017_392.pdf
4. Математичне моделювання телекомунікаційних систем та мереж: навчальний посібник [Текст] / Є.М. Чернихівський. – Львів: Видавництво Львівської політехніки, 2011. – 272 с.
https://vlp.com.ua/node/7158
5. Махней О. В. Математичне моделювання : навчальний посібник / О. В. Махней. — Івано-Франківськ : Супрун В. П., 2015. — 372 с.
https://kdrpm.pnu.edu.ua/wp-content/uploads/sites/55/2018/03/matmod_content.pdf
6. Томашевський В.М. Моделювання систем / В.М. Томашевський. — К. : Видавнича група BHV, 2005. — 352 с.
https://pdf.lib.vntu.edu.ua/books/2016/Tomashev_2005_352.pdf
7. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL: 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. URL: 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. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Додаткова література

10. Махней О. В. Математичне забезпечення автоматизації прикладних досліджень / О. В. Махней, Т. П. Гой. — Івано-Франківськ : Сімик, 2013. — 304 с.
https://kdrpm.pnu.edu.ua/wp-content/uploads/sites/55/2018/03/Maple_content.pdf
11. Павленко П. М. Основи математичного моделювання систем і процесів:навч. посіб. – К.: Книжкове вид-во НАУ, 2013. – 201 с.
https://er.nau.edu.ua/bitstream/NAU/24750/1/%D0%A2_%D0%9F%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9F.%D0%9C._%D0%9D%D0%B0%D0%B2%D1%87.pdf

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
0,4	0,2		0,4

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:

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

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** Сергій ЄВСЕЄВ