Силабус освітнього компонента
Програма навчальної дисципліни

Методи захисту інформації та кібербезпека

Шифр та назва спеціальності
113 – Прикладна математика

Інститут
ННІ Комп`ютерних наук та інформаційних технологій

Освітня програма
Інтелектуальний аналіз даних

Кафедра
Кібербезпеки

Рівень освіти
Магістр

Тип дисципліни
Профільна, Вибіркова

Семестр
3

Мова викладання
Українська

Викладачі, розробники

Король Ольга Григорівна

olha.korol@khpi.edu.ua
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 161, з них патентів на корисну модель 18, 11 монографій, з яких 6 колективних монографій, 18 навчальних посібників, 66 статті у закордонних виданнях та фахових виданнях України, у тому числі у наукометричній базі Scopus. Провідний лектор з дисциплін: «Основи соціальної інженерії», «Інформаційна безпека держави», «Менеджмент інформаційної безпеки», «Організація документообігу з обмеженим доступом», «Безпека в соціальних мережах».
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна «Методи захисту інформації та кібербезпека» є вибірковою навчальною дисципліною. Дисципліна спрямована на вивчення симетричних та асиметричних методів шифрування інформації, їх використання; видів криптоаналізу та можливість його застосування.

Мета та цілі дисципліни

Ознайомлення з теоретичними основами криптології; придбання навичок в практичному використанні, постановці і вирішенні задач шифрування інформації; розуміння суті інформаційних процесів в криптографічних системах; застосування комп'ютерів для вирішення завдань шифрування і дешифрування; розробка і використання математичних і обчислювальних моделей процесів шифрування інформації, їх оптимізація та вироблення напрямків вдосконалення.

Формат занять

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

Компетентності

ЗК 3. Здатність до безперервного навчання, придбання нових знань і умінь, у тому числі в галузі, відмінній від професійної.
ЗК 4. Здатність виявляти, ставити та вирішувати проблеми у професійній діяльності.
ЗК 7. Здатність працювати з інформацією: знаходити і використовувати інформацію з різних джерел, потрібну для розв'язання професійних завдань.
СК 1. Здатність формулювати математичну постановку задачі, спираючись на постановку мовою предметної галузі, перевіряти коректність постановки, у тому числі в умовах невизначеності.
СК 2. Здатність обирати, розробляти та досліджувати математичний аналітичний або чисельний метод розв'язання практичних задач, що забезпечує потрібні точність і надійність результату.
СК 3. Здатність обирати, розробляти, досліджувати та застосовувати математичні методи для розв'язання практичних задач моделювання, проектування, керування, прогнозування, прийняття рішень.
СК 5. Здатність до проведення математичного і комп'ютерного моделювання та обчислювального експерименту, збору, візуалізації, аналізу та обробки отриманих даних, розв'язання формалізованих задач за допомогою спеціалізованих програмних засобів.
СК 7. Здатність до пошуку, вивчення та аналізу науково-технічної інформації, вітчизняного і закордонного досвіду, пов'язаного із застосуванням математичних методів для дослідження процесів та систем.
СК 10. Здатність обирати, розробляти, досліджувати та застосовувати математичні моделі і методи для інтелектуального аналізу даних в умовах невизначеності.
СК 11. Здатність розробляти, досліджувати та застосовувати математичні методи й алгоритми машинного навчання, м'яких обчислень і обчислювального інтелекту для аналізу невизначених даних, прогнозування та прийняття рішень.
СК 14. Здатність до використання сучасних інформаційних технологій інтелектуального аналізу даних, прогнозування, прийняття рішень, інформаційного пошуку і видобування знань.
СК 16. Здатність до постановки прикладних задач та обґрунтування досліджень і проектів по створенню математичного та програмного забезпечення для обробки та інтелектуального аналізу великих даних.

Результати навчання

РН 1. Демонструвати знання і розуміння основних концепцій, принципів, теорій фундаментальної та прикладної математики і використовувати їх на практиці.
РН 2. Уміти формалізувати задачі, сформульовані мовою певної предметної галузі й обирати раціональний метод вирішення; розв'язувати задачі аналітичними або чисельними методами, оцінювати точність і достовірність отриманих результатів та виконувати їхню інтерпретацію.
РН 3. Володіти методами розробки, дослідження та застосування математичних моделей складних об'єктів і процесів, у тому числі із застосуванням методів обчислювального інтелекту.
РН 5. Будувати ефективні щодо точності обчислень, стійкості, швидкодії і витрат системних та обчислювальних ресурсів алгоритми для чисельного дослідження математичних моделей і аналізу даних, прийняття рішень.
РН 6. Уміти вибирати, розробляти та досліджувати методи й алгоритми розв'язання математичних задач оптимізації систем, дослідження операцій, оптимального керування і прийняття рішень.
РН 8. Уміти застосовувати у практичній роботі спеціалізовані програмні продукти і програмні системи комп'ютерної математики, аналізу великих даних тощо.
РН 14. Уміти застосовувати наявні існуючі і розробляти нові алгоритми та програмні засоби для статистичного й інтелектуального аналізу невизначених даних.
РН 17. Вміти планувати і виконувати наукові дослідження у сфері прикладної математики, формулювати і перевіряти гіпотези, обирати методики та інструменти, аналізувати результати, обґрунтовувати висновки.

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)

Для успішного проходження курсу необхідно мати знання та практичні навички з дисциплін: «Некоректні задачі обробки даних», «Математичні методи машинного навчання 2», «Метаевристичні методи оптимізації».

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. Теоретичні основи захисту інформації.
Основні поняття. Моделі секретних систем. Основні завдання системи безпеки. Симетричні та несиметричні криптосистеми. Режими роботи симетричних криптосистем.
Тема 2. Протоколи автентичності. Цифровий підпис.
Механізми автентичності. Класифікація цифрового підпису. Методи гешування. Механізми автентифікації на основі використання програмно-апаратних засобів. Автентифікація Kerberos.
Тема 3. Протоколи суворої автентифікації.
Класифікація методів 2 FA. Рівні достовірності автентифікації. Загрози на 2 FA. Двофакторна автентифікація в Linux.
Тема 4. Система PGP.
Основні функції системи. Класифікація ключів. Механізми забезпечення автентичності та конфіденційності. Система довіри.
Тема 5. Основи технології PKI.
Основні функції та склад технології. Фізична та логічна топологія. Криптоперіод. Основні механізми технології на основі симетричних та несиметричних криптосистем.
Тема 6. Протоколи цілісності SSL, TLS.
Взаємозв'язок об'єктів критичної інфраструктури з кіберфізичними системами. Структура протоколів SSL, TLS. Функції протоколу SSL. АТАКИ НА SSL/TLS.
Тема 7. Основи постквантової криптографії.
Основні поняття. Основа квантових обчислень. Основні алгоритми квантового криптоаналізу.
Тема 8. Основи теорій інформації та кодування.
Загальна структура системи зв`язку. Моделі двійкового симетричного каналу без пам`яті. Ефективне кодування Хаффмана. Корекція та винахід помилок. Класифікація двійкових кодів. Основні поняття теорії перешкодостійкого кодування. Поля Галуа. Структура кінцевих полів їх властивості. Коди Боуза-Чоудхурі-Хоквінгему.
Тема 9. Основи розкодування.
Алгоритм Берлекемпа-Месі. Приклад.
Тема 10. Постквантові алгоритми на основі крипто-кодових конструкцій Мак-Еліса і Нідеррайтера. Гібридні системи захисту на збиткових кодах.
Класифікація крипто-кодових конструкцій. Еліптичні криві. Основи побудови (формування ключових матриць, формування криптограми). Оцінка стійкості. Шляхи зменшення ємності ключових даних. Формування крипто-кодових конструкцій на алгеброгеометричних (еліптичних) кодах. Основи криптографії на збиткових кодах. Формування гібридних крипто-кодових конструкцій.
Тема 11. Потокові симетричні криптосистеми.
Симетричні криптосистеми. Потоковий шифр RC-4. Стійкість. Ініціалізація S-блоку. Потоковий шифр PRC-4A. Потоковий шифр STRUMOK. Потоковий шифр SNOW2.0.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Найпростіші шифри.
Тема 2. Дослідження властивостей режимів роботи блокових шифрів.
Тема 3. Дослідження протоколів автентичності та конфіденційності за допомогою RSA.
Тема 4. Дослідження протоколів цифрового підпису.
Тема 5. Дослідження протоколів системи PGP.
Тема 6. Стеганографічні методи захисту інформації.
Тема 7. Методика NIST STS оцінки статистичних властивостей криптографічних алгоритмів.
Тема 8. Побудова циклічних кодів.
Тема 9. Робота з кубітами. Емуляція вимірювань.

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. 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.
2. 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
3. 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
4. Кібербезпека в сучасному світі : матеріали III Всеукраїнської науковопрактичної конференції (м. Одеса, 19 листопада 2021 р.) / за ред. О. В. Дикого ;уклад.: С. А. Горбаченко, Н. І. Логінова. – Одеса, 2020. – 148 с.
http://dspace.onua.edu.ua/handle/11300/15973
5. Лісовська Ю. Кібербезпека. Ризики та заходи. – К.: Кондор, 2019. – 272 с.
http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf

Додаткова література :

6. 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
7. Edited by Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. 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. Криптоаналіз. КриптографічніI протоколи / О. М. Гапак // Навчальний посібник з курсу «Комп'ютерна криптографія» для студентів інженерно-технічного факультету спеціальності 123-«Комп’ютерна інженерія». Ужгород: видавництво ПП «АУТДОР-ШАРК», 2021р. – 96 с.
https://dspace.uzhnu.edu.ua/jspui/handle/lib/36505

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

Дата погодження, підпис
31.08.2023 р.

Завідувач кафедри
Сергій ЄВСЕЄВ

Дата погодження, підпис
31.08.2023 р.

Гарант ОП
Олексій ГАЛУЗА