Силабус освітнього компонента
Програма навчальної дисципліни

Основи стеганографічного захисту інформації

Шифр та назва спеціальності
113 – Прикладна математика

Інститут
ННІ Комп`ютерних наук та інформаційних технологій

Освітня програма
Інтелектуальний аналіз даних

Кафедра
Кібербезпеки

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Вибіркова

Семестр
7

Мова викладання
Українська

Викладачі, розробники

Корольов Роман Володимирович
roman.korolev@khpi.edu.ua
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 40, з яких 1 навчальний посібник, 23 статті у закордонних виданнях та фахових виданнях України, 10 патентів на корисну модель. Провідний лектор з дисциплін: «Фізичні основи технічних засобів розвідки», «Основи стеганографічного захисту інформації», «Корпоративні мережі та системи доступу» , «Безпека та аудит бездротових та рухомих мереж».

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Основи стеганографічного захисту інформації" є обов'язковою навчальною дисципліною. Дисципліна спрямована на придбання студентами навичок та принципів побудови, реалізації та застосування стеганографічних систем та протоколів, вміння застосовувати методи, алгоритми та засоби оцінки стеганостійкості та інших якісних показників стеганосистем та стеганографічних протоколів.

Мета та цілі дисципліни

Отримання студентами необхідних базових знань з цифрової стеганографії, яка використовується для приховування факту існування інформації та створення водяних знаків. Особливу увагу в курсі приділяють вивченню проблематики використання цифрової стеганографії у сучасному інформаційному просторі, аналізу атак на стеганограмми та оцінки стійкості.

Формат занять

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

Компетентності

ЗК 1. Здатність учитися й оволодівати сучасними знаннями.
ЗК 2. Здатність застосовувати знання у практичних ситуаціях.
ЗК 7. Здатність до пошуку, оброблення й аналізу інформації з різноманітних джерел.
ЗК 8. Знання і розуміння предметної області та розуміння професійної діяльності.
ЗК 10. Навички у використанні інформаційних і комунікаційних технологій.
СК 7. Здатність розв'язувати професійні задачі за допомогою комп'ютерної техніки, комп'ютерних мереж та Інтернету, в середовищі сучасних операційних систем, із використанням стандартних офісних додатків.
СК 8. Здатність експлуатувати та обслуговувати програмне забезпечення автоматизованих та інформаційних систем різного призначення.
СК 14. Здатність зрозуміти постановку завдання, сформульовану мовою певної предметної галузі, здійснювати пошук та збір необхідних вихідних даних.

Результати навчання

РН 7. Вміти проводити практичні дослідження та знаходити розв'язок некоректних задач.
РН 8. Поєднувати методи математичного та комп'ютерного моделювання з неформальними процедурами експертного аналізу для пошуку оптимальних рішень.
РН 10. Володіти методиками вибору раціональних методів та алгоритмів розв'язання математичних задач оптимізації, дослідження операцій, оптимального керування і прийняття рішень, аналізу даних.
РН 14. Виявляти здатність до самонавчання та продовження професійного розвитку.
РН 15. Уміти організувати власну діяльність та одержувати результат у рамках обмеженого часу.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 30 год., лабораторні роботи – 30 год., самостійна робота – 60 год.

Передумови вивчення дисципліни (пререквізити)

«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

Теми лекційних занять

Тема 1. Цифрова стеганографія.
Структура та зміст дисципліни, її зв'язок з іншими дисциплінами навчального плану. Предмет, термінологія, галузь використання.
Тема 2. Математична модель стеганосистем.
Стеганографічні протоколи. Практичні аспекти вбудування даних.
Тема 3. Основні напрямки практичного використання стеганографічніх методів захисту інформації.
Класифікація стеганографічних систем та стегоконтейнерів.
Тема 4. Особливості зорової системи людини.
Основні властивості зорової системи людини, що використовуються при приховуванні даних в зображеннях.
Тема 5. Цифрові формати нерухомих зображень.
Формати BMP, GIF, TIFF, JPEG. Особливості комп'ютерної обробки зображень.
Тема 6. Приховування даних у просторої області зображень.

Метод приховування в найменш значущому біті даних.
Тема 7. Приховування даних у частотній області зображень. Метод Коха та Жао.
Приховання конфіденційної інформації в частотній множині зображення.
Тема 8. Особливості слухової системи людини.
Основні властивості слухової системи людини, що використовуються при приховуванні даних в аудіо сигналах. Цифрові формати аудіосигналів (формати WAV, WMA, MP3, AAC, OGG Vorbis). Особливості комп'ютерної обробки аудіо сигналів.
Тема 9. Цифрові водяні знаки.
Узагальнена модель системи цифрових водяних знаків. Класифікація системи цифрових водяних знаків.
Тема 10. Цифрові відбитки.
Термінологія й основні положення. Статистична реєстрація відбитка. Схема асиметричної реєстрації відбитка.
Тема 11. Приховані канали в комп'ютерних системах і мережах.
Приховані канали в операційних системах. Приховування даних у виконуваних файлах. Поняття клептрографії.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Програмні засоби стеганографічного захисту інформації.
Тема 2. Работа з програмою стеганографічного захисту інформації Steganos Security Suite.
Тема 3. Приховування даних в просторової області зображень методом найменш значимого біта.
Тема 4. Приховування даних в просторової області зображень методом перестановок.

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 іспиту.

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. – Режим доступу:
http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
2. Кузнецов О.О. Стеганографія: навчальний посібник / О.О.Кузнецов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2015. – 232 с.
http://www.repository.hneu.edu.ua/jspui/bitstream/123456789/2289/1/%d0%a1%d1%82%d0%b5%d0%b3%d0%b0%d0%bd%d0%be%d0%b3%d1%80%d0%b0%d1%84%d0%b8%d1%8f.pdf
3. Хорошко В.О. Комп'ютерна стеганографія: навчальний посібник / В.О. Хорошко, Ю.Є. Яремчук, В.В. Карпінець – Вінниця : ВНТУ, 2017. – 155 с.
https://learn.ztu.edu.ua/pluginfile.php/272322/mod_resource/content/1/Xoroshko_Komputer_2017_155.pdf
4. Козюра В.Д. Захист інформації в комп'ютерних системах :підручник / В.Д.Козюра, В.О.Хорошко, М.Є.Шелест – Ніжин : ФОП Лукяненко В.В., ТПК «Орхідея», 2020. – 236 с.
http://ir.stu.cn.ua/bitstream/handle/123456789/19248/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC.%20%D0%B2%20%D0%BA%D0%BE%D0%BC%D0%BF.%20%D1%81%D0%B8%D1%81.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
5. Конахович Г.Ф. Компютерна стеганографічна обробка й аналіз мультимедійних даних : підручник /Г.Ф. Конафович, Д.О.Прогонов, О.Ю. Пузиренко. – К. – «Alex Print Centre», 2018/ – 558 с.

https://books.google.com.ua/books?id=-clcDwAAQBAJ&printsec=frontcover&hl=uk&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Додаткова література :

6. Євсеєв С. П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів "Новий світ-2000", 2020. – 241 с. – Режим доступу: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
7. Євсеєв С.П. Кібербезпека: Криптографія з Python: навчальний посібник. – Львів "Новий світ-2000", 2021. – 120 с. – Режим доступу: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
8. Євсеєв 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. – Режим доступу: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. 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
10. 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. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
11. 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. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

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;
- іспит: 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 28.08.2023		Завідувач кафедри Сергій ЄВСЕЄВ
	Дата погодження, підпис 31.08.2023 р.		Гарант ОП Олена АХІЄЗЕР