Силабус освітнього компонента
Програма навчальної дисципліни

Основи стеганографічного захисту інформації

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

КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net
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». Гарант освітньо-професійної програми «Управління інформаційною безпекою» першого (бакалаврського) рівня вищої освіти.

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 – диференційований залік.

Компетентності

ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
СК2. Здатність використовувати інформаційні технологій, сучасні методи і моделей кібербезпеки та систем захисту інформації.

Результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
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.
РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

Обсяг дисципліни

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Основи криптографічного захисту, 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. Цифрова стеганографія. Структура та зміст дисципліни, її зв'язок з іншими дисциплінами навчального плану. Предмет, термінологія, галузь використання.	2
Тема 2. Математична модель стеганосистем. Стеганографічні протоколи. Практичні аспекти вбудування даних.	2
Тема 3. Основні напрямки практичного використання стеганографічних методів захисту інформації. Класифікація стеганографічних систем та стегоконтейнерів.	2
Тема 4. Особливості зорової системи людини. Основні властивості зорової системи людини, що використовуються при приховуванні даних в зображеннях	2
Тема 5. Цифрові формати нерухомих зображень. Формати BMP, GIF, TIFF, JPEG. Особливості комп'ютерної обробки зображень.	2
Тема 6. Приховування даних у просторої області зображень. Метод приховування в найменш значущому біті даних. Метод псевдовипадкової перестановки.	6
Тема 7. Приховування даних у частотній області зображень. Метод Коха та Жао. Приховання конфіденційної інформації в частотній множині зображення.	2
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.	4
Тема 9. Цифрові водяні знаки. Узагальнена модель системи цифрових водяних знаків. Класифікація системи цифрових водяних знаків.	2
Тема 10. Цифрові відбитки. Термінологія й основні положення. Статистична реєстрація відбитка. Схема асиметричної реєстрації відбитка.	2
Тема 11. Приховані канали в комп'ютерних системах і мережах. Приховані канали в операційних системах. Приховування даних у виконуваних файлах. Поняття клептрографії.	2
Тема 12. Методи текстової стеганографії. Аналіз реалізації методів. Синтаксичні методи текстової стеганографії. Лінгвістичні методи текстової стеганографії.	4
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a

Тема 1. Програмні засоби стеганографічного захисту інформації. Ознайомлення з поняттям стеганографії, її базовими принципами, використовуваними форматами контейнерів, способами упаковки приховується, найбільш популярними програмами стеганографії.	8	0,1
Тема 2. Робота з програмою стеганографічного захисту інформації Steganos Security Suite. Робота з програмою Steganos Security Suite.	8	0,1
Тема 3. Приховування даних в просторової області зображень методом найменш значимого біта. Розробка програмного продукту для приховування даних в просторової області зображень методом найменш значимого біта.	8	0,1
Тема 4. Приховування даних в просторової області зображень методом псевдовипадкової перестановки. Розробка програмного продукту для приховування даних в просторовій області зображень методом псевдовипадкової перестановки за рахунок використання генераторів псевдовипадкових чисел.	8	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}4$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Відпрацювання лекційних питань. Стеганографічні протоколи. Практичні аспекти вбудування даних. Методи приховування данних в зображеннях.	0,6
Загалом	$\sum_{i=1}^{m} b_i = 0{,}6$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Вступ до стеганографії як методу захисту інформації Основні визначення стеганографії та її відмінності від криптографії в контексті захисту інформації. Ключові принципи стеганографії (невидимість, стійкість, місткість) та їх значення для інформаційної безпеки.	9
Тема 2. Історія розвитку стеганографічних методів Опишіть еволюцію стеганографії від античних часів до цифрової ери. Які історичні приклади стеганографічних технік (наприклад, мікрописемність) вплинули на сучасні методи?	9
Тема 3. Класифікація стеганографічних методів Як класифікуються стеганографічні методи за типом носія (текст, зображення, аудіо)? Назвіть основні категорії стеганографії (просторова, частотна, адаптивна) та їх характеристики.	9

Тема 4. Стеганографія в цифрових зображеннях Метод LSB (Least Significant Bit) для вбудовування даних у растрові зображення. Алгоритми стеганографії для JPEG-формату (наприклад, Jsteg) та їх переваги.	9
Тема 5. Аудіостеганографія та приховування в звукових файлах Як застосовується стеганографія в WAV-файлах за допомогою фазової модуляції? Методи стеганографії для MP3 (спектральна стеганографія) та ризики виявлення.	9
Тема 6. Текстова стеганографія Методи приховування інформації в текстових документах (синтаксична, семантична стеганографія). Інструменти для текстової стеганографії (наприклад, на основі пробілів чи шрифтів).	9
Тема 7. Мережева стеганографія Як відбувається приховування даних у мережевому трафіку (наприклад, у TCP/IP-заголовках)? Приклади стеганографії в VoIP та протоколи для її реалізації.	8
Тема 8. Стеганаліз: методи виявлення прихованих даних Статистичні методи стеганалізу (хі-квадрат тест) для виявлення аномалій у носіях. Які машинно-навчальні підходи використовуються для стеганалізу зображень.	8
Тема 9. Інструменти та програмне забезпечення для стеганографії Назвіть популярні інструменти (Steghide, OpenStego) та їх функціональність. Як оцінюється безпека стеганографічних інструментів (місткість vs. стійкість до атак)?	8
Тема 10. Застосування та обмеження стеганографічного захисту Сфери застосування стеганографії (водяні знаки, цифрові права) в інформаційній безпеці. Основні обмеження стеганографії (втрата даних, вразливість до стеганалізу) та способи їх подолання.	8
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. 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

2. 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
3. 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
4. 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.
5. 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

Додаткова література

1. 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
2. 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
3. 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
4. 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

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	0,6		

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** Сергій ЄВСЕЄВ