СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Основи криптографічного та стеганографічного захисту інформації – частина 2»

Ступінь вищої освіти - Бакалавр
Спеціальність «125-Кібербезпека»
Освітня програма «Кібербезпека»
Рік навчання 3, семестр 6
Форма здобуття вищої освіти - денна
Кількість кредитів ЄКТС 3
Мова викладання українська/англійська

Лектор навчальної дисципліни	**Сагун Андрій Вікторович, к.т.н., доцент**  **(портфоліо)**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем і мереж,** **корпус. 15, к. 207, тел. 5278724** **e-mail a.sagun@nubip.edu.ua**
URL ЕНК на навчальному порталі НУБіП України	**ЕНК (6 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=4668

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення дисципліни «Основи криптографічного та стеганографічного захисту інформації – частина 2» є ознайомлення з математичними основами симетричних криптографічних перетворень, принципами створення та функціонування односторонніх (геш-) функцій та стандартами криптографічних асиметричних схем та алгоритмів, принципами роботи та конструювання стеганографічних методів та засобів захисту інформації.

Вивчаються **наступні питання**: принципи роботи асиметричної схем та алгоритмів в криптографії, конструювання та практичне застосування односторонніх функціях в системах захисту інформації та методів алгоритми і методи стеганографічного захисту інформації.

Компетентності навчальної дисципліни:
Загальні компетенції:
- здатність застосовувати знання у практичних ситуаціях.
- здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові) компетентності:
- здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
- здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп’ютерних систем захисту інформації.

Програмні результати навчання навчальної дисципліни:

- використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
- вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

Зробимо курс корисним для вас. Якщо ви будете наполегливо працювати і докладати особливих зусиль, щоб не відставати від матеріалу, ви отримаєте винагороду – як в короткостроковій перспективі, так і в набутті фахових компетентностей. Будь-ласка, широко використовуйте аудиторні заняття, відеоінструкції, вебінари, щоб переконатися, що рухаєтесь за графіком навчання.

СТРУКТУРА КУРСУ

Тема	Години (лекції/ лабораторні)	Результати навчання	Завдання	Оцінювання
1 семестр				
Модуль 1. Асиметричні криптосистеми та алгоритми				
Тема 1. Асиметрична криптографія. Основні поняття та властивості асиметричних криптосхем. Теоретична та практична криптостійкість асиметричних криптоалгоритмів.	2/-	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації	Здача лабораторної роботи	-
Тема 2. Односторонні криптоперетворення. Геш-функції та їх параметри. Принципи конструювання геш-функцій.	4/4		Здача лабораторної роботи.	**8**
Тема 3. Криптосхема RSA. Реалізації RSA та алгоритму Ель Гамаля (EG).	4/4		Здача лабораторної роботи.	**7**
Тема 4. Асиметричні криптосистеми. Алгоритм DSA.	2/4		Здача лабораторної роботи.	**7**
Тема 5. Протоколи обміну ключами. Алгоритм Діфі-Хелмана	2/2		Здача лабораторної роботи	**6**
Модульний контроль			Модульний тест в ЕНК	**7**
Всього за 1 модуль	**14/14**			**35**
Модуль 2. Стеганографічні методи захисту інформації				
Тема 6. Розвиток і значення науки стеганографії. Основні терміни, означення в стеганографії. Задачі приховування інформації для стеганографічних перетворень.	4/-	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації	Опитування	-
Тема 7. Стеганографічні методи приховування форматуванням тексту. Модель стеганосистеми. Вимоги до стеганосистем.	4/6		Здача лабораторної роботи.	**9**

Тема 8. Стеганографічні контейнери та цифрові водяні знаки (Watermark). Метод найменшого значущого біта (LSB) при стеганографічних перетвореннях графічної інформації.	4/6		Здача лабораторної роботи.	**10**
Тема 9. Принципи дискретних перетворень аналогових сигналів в стеганографії. Приховування інформації в звукових файлах.	4/4		Здача лабораторної роботи.	**8**
Модульний контроль			Модульний тест в ЕНК	**8**
Всього за 2 модуль	**16/16**			**35**
Іспит			Підсумковий тест в ЕНК	**30**
Всього за курс	**30/30**			**100**

ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо дедлайнів та перескладання:	Дедлайни визначені в ЕНК. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний, стажування або відрядження). В разі здачі лабораторних робіт пізніше запланованих термінів без поважної причини оцінка може бути знижена
Політика щодо академічної доброчесності:	Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).
Політика щодо відвідування:	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній on-line формі за погодженням із деканом факультету)

ШКАЛА ОЦІНЮВАННЯ СТУДЕНТІВ

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів**	
	Екзаменів	**Заліків**
90-100	Відмінно	-
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	-

Рекомендована література

1. Основи криптографічного та стеганографічного захисту інформації. Стеганографічний захист інформації: навчальний посібник/ Сагун А.В., Кулініч О.М., Хайдуров В.В. – Київ : НУБіП України, 2023. – 146 с.
2. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.
3. Конахович Г. Ф., Прогонов Д. О., Пузиренко О. Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних [підручник]. — К. : «Центр навчальної літератури», 2018. — 558 с.

4. Конахович Г. Ф., Пузиренко О. Ю. Комп'ютерна стеганографія. Теорія і практика. — К.: «МК-Пресс», 2006. — 288 с., іл.

5. Стеганографічні методи захисту документів / Б. В. Дурняк, Д. В. Музика, В. І. Сабат. — Львів : Укр. акад. друкарства, 2014. — 159 с. : іл., портр. ; 21 см. — На паліт.: Інформ. технології. — Частина тексту парал. укр., англ. — Бібліогр.: с. 149—159 (118 назв). — 300 пр. — ISBN 978-966-322-401-5