СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Основи криптографічного та стеганографічного захисту інформації – частина 1»

Ступінь вищої освіти - Бакалавр
Спеціальність «125-Кібербезпека»
Освітня програма «Кібербезпека»
Рік навчання 3, семестр 6
Форма здобуття вищої освіти - денна
Кількість кредитів ЄКТС 4
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 (5 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=4668

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення дисципліни «Основи криптографічного та стеганографічного захисту інформації – частина 1» є ознайомлення з математичними основами криптографічних перетворень, основними поняттями криптографії та алгоритмами і стандартами криптографічних симетричних схем та алгоритмів.

Вивчаються **наступні питання**: основи спеціальних розділів математики для задач криптографічного захисту інформації, характеристику та будову криптографічних алгоритмів, основні поняття і методи криптоперетворень. Основи побудови та використання симетричної криптографії та методів захисту інформації на її основі в комп'ютерних системах та мережах.

Компетентності навчальної дисципліни:

Загальні компетенції:

- здатність застосовувати знання у практичних ситуаціях.
- здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові) компетентності:

- здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
- здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем захисту інформації.

Програмні результати навчання навчальної дисципліни:

- аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
- застосовувати теорії, методи та засоби захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

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. Спеціальні розділи математики в крипотографії				
Тема 1. Основні складові криптографічних систем. Задачі криптології та стеганографії в кібербезпеці.	2/-	аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;	Опитування	-
Тема 2. Поняття шифрування. Шифри, ключі. Симетричні та асиметричні шифри та їх основні параметри.	2/-	виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.	Опитування	-
Тема 3. Модулярна арифметика для задач криптографії. Елементи теорії чисел. Алгоритм Евкліда. Теорема Ейлера та Ферма. Обчислення у скінченних полях	4/4		Здача лабораторної роботи.	**8**
Тема 4. Операції в кільцях. Криптоперетворення XOR-шифруванням. Гамування. Композиційні шифри	2/4		Здача лабораторної роботи.	**6**
Тема 5. Математичний апарат еліптичних кривих в криптографічних задачах. Види еліптичних кривих та їх властивостію	2/4		Здача лабораторної роботи.	**8**
Тема 6. Великі числа та довга арифметика в криптографічних задачах	2/2		Здача лабораторної роботи.	**7**

Модульний контроль			Модульний тест в ЕНК	**6**
Всього за 1 модуль	**14/14**			**35**
Модуль 2. Симетричні криптосистеми та алгоритми шифрування				
Тема 7. Прості симетричні криптосистеми та шифри. Моно та поліалфавітні шифри. Шифри підстановок та перестановок, заміни (квадрат Полібія). Афінні криптоперетворення.	4/4	аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. застосовувати теорії, методи та засоби захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;	Здача лабораторної роботи.	**6**
Тема 8. Симетричні блочні криптоалгоритми на базі мережі Фейстеля. Конструювання симетричних шифрів на базі мереж Фейстеля, їх теоретичниа криптостійкість	4/4		Здача лабораторної роботи.	**8**
Тема 9. Шифри DES, 3-DES, ДСТУ ГОСТ 28147-2009, алгоритм RC5.	2/-		Опитування	**-**
Тема 10. Симетричні блочні криптосистеми на базі SP-боксів: AES, ДСТУ 7624:2014	2/4		Здача лабораторної роботи.	**7**
Тема 11. Потокові шифри. Шифри A5, RC4, «СТРУМОК».	4/4		Здача лабораторної роботи.	**8**
Модульний контроль			Модульний тест в ЕНК	**6**
Всього за модуль 2	**16/16**			**16**
Залік			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. Франчук В.М. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних. Посібник для викладачів, вчителів та студентів інформатичних спеціальностей. – К.: НПУ імені М.П. Драгоманова, 2012. – 120 с. Режим доступу: https://vfranchuk.fi.npu.edu.ua/images/files/statty/32_ZIR_cript.pdf

2. Основи криптографічного та стеганографічного захисту інформації. Криптографічний захист інформації: навчальний посібник. Сагун А.В., Кулініч О.М., Хайдуров В.В. – Київ : НУБіП України, 2023. – 285.