СИЛАБУС ДИСЦИПЛІНИ «ОСНОВИ КРИПТОГРАФІЧНОГО ТА СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

Ступінь вищої освіти – Бакалавр
Спеціальність 125 – КІБЕРБЕЗПЕКА
Освітня програма «Кібербезпека»
Рік навчання 3, семестр 5
Форма навчання денна
Кількість кредитів ЄКТС 4
Мова викладання українська

Лектор курсу	 **Сагун Андрій Вікторович, к.т.н., доцент (портфоліо)**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки корпус. 15, к. 207, тел. 5278724** **e-mail a.sagun@nubip.edu.ua** **ЕНК (1 семестр)**
Сторінка курсу в eLearn	https://elearn.nubip.edu.ua/course/view.php?id=4668

ОПИС ДИСЦИПЛІНИ

Навчальна дисципліна передбачає вивчення основ використання криптографічних та стеганографічних засобів та методів захисту інформації у комп'ютерних системах та мережах, дослідження проблем зберігання, опрацювання, пошуку, передачі, перетворення, закриття та відновлення інформації в організаціях і на підприємствах різних напрямків діяльності та різних форм власності, способів захисту від несанкціонованого доступу до інформаційних ресурсів.

Навчальна дисципліна забезпечує формування ряду фахових компетентностей:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професії.

ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК 8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

У результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме:

ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН 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;

ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки 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.

Неформальна on-line освіта на основі МВОК.

СТРУКТУРА КУРСУ

Тема	Години (лекції/ лабораторні)	Результати навчання	Завдання	Оцінювання
1 семестр				
Модуль 1. Симетричні та асиметричні криптоалгоритми та схеми шифрування				
Основні складові криптографічних систем. Задачі криптології та стеганографії в кібербезпеці.	2/-	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;	Опитування	-
Поняття шифрування. Шифри, ключі. Симетричні та асиметричні шифри та їх основні параметри.	2/2	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; 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	Захист лабораторної роботи	**4**
Модулярна арифметика для задач криптографії. Елементи теорії чисел. Алгоритм Евкліда. Теорема Ейлера та Ферма. Обчислення у скінченних полях	2/2		Здача лабораторної роботи.	**6**
Прості симетричні криптосистеми та шифри. Моно та поліалфавітні шифри. Шифри підстановок та перестановок, заміни (квадрат Полібія) Афінні криптоперетворення	2/2		Здача лабораторної роботи.	**4**
Операції в кільцях. Криптоперетворення XOR-шифруванням. Гамування. Композиційні шифри	2/2		Здача лабораторної роботи.	**5**
Симетричні блочні криптоалгоритми на базі мережі Фейстеля: DES, 3-DES, ДСТУ ГОСТ 28147-2009, алгоритм RC5.	2/2		Здача лабораторної роботи.	**6**
Симетричні блочні криптосистеми на базі SP-боксів: AES, ДСТУ 7624:2014. Потокові шифри. Шифри A5, RC4, «СТРУМОК».	2/2		Здача лабораторної роботи.	**6**
Асиметрична криптографія. Основні поняття та властивості асиметричних криптосхем. Односторонні криптоперетворення, хеш-функції	2/2		Здача лабораторної роботи	**6**
Криптосхема RSA. Реалізації RSA та алгоритму Ель Гамаля (EG). Робота з довгою арифметикою	2/2		Здача лабораторної роботи.	**5**

Асиметричні криптосистеми. Алгоритм DSA. Протоколи обміну ключами. Алгоритм Діфі-Хелмана. Еліптичні криві в криптографічних задачах.	2/4		Здача лабораторної роботи.	**6**
Модульний контроль			Модульний тест в ЕНК	**6**
Всього за 1 модуль	**20/20**			**54**
Модуль 2. Стеганографічні методи захисту властивостей інформації				
Розвиток і значення науки стеганографії. Основні терміни, означення в стеганографії. Задачі приховування інформації для стеганографічних перетворень.	2/2	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.	Тестування та опитування.	**2**
Стеганографічні методи приховування форматуванням тексту. Модель стеганосистеми. Вимоги до стеганосистем.	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;	Здача лабораторної роботи.	**4**
Стеганографічні контейнери та цифрові водяні знаки (Watermark). Метод найменшого значущого біта (LSB) при стеганографічних перетвореннях графічної інформації.	4/4		Здача лабораторної роботи.	**4**
Модульний контроль			Модульний тест в ЕНК	**6**
Всього за модуль 2	**10/10**			**16**
Екзамен			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 заліків**	
	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. О.В. Вербицький. Вступ до криптології. – Львів.: Видавництво науково – технічної літератури, 1998. – 247 с. ISBN 966-7148-03-3