СИЛАБУС ДИСЦИПЛІНИ «ОСНОВИ КРИПТОАНАЛІЗУ»

Ступінь вищої освіти – Бакалавр
Спеціальність 125 – КІБЕРБЕЗПЕКА
Освітня програма «Кібербезпека»
Рік навчання 3, семестр 6
Форма навчання денна
Кількість кредитів ЄКТС 5
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 (3 семестр)**
Сторінка курсу в eLearn	https://elearn.nubip.edu.ua/course/view.php?id=4936

ОПИС ДИСЦИПЛІНИ

Метою вивчення дисципліни «Основи криптоаналізу» є ознайомлення з основними теорії чисел, числових полів та аналітичної алгебри, надання студентам знань з основ криптоаналізу, принципів, методів та засобів проведення різних видів криптоаналізу, а також створення систем компрометації шифрованих повідомлень. Вивчаються наступні питання: лінійний та диференційний криптоаналіз; положення достовірності відстані, допоміжні методи та алгоритми криптоаналізу (алгоритм Евкліда, алгоритм Ферма та ін.); базові принципи та методи проведення криптоаналізу в система симетричного блочного та асиметричних двоключових схемах шифрування, системах з електронним цифровим підписом.

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.

СК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

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

ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно - телекомунікаційних системах.

ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;

ПРН 48. 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/ Лаборат-орні,)	Результати навчання	Завдання	Оціню-вання
3 семестр				
Модуль 1. Симетричні криптосистеми та методи їх криптоаналіз				
Вступ до курсу. Задачі криптоаналізу. Основні терміни і формулювання.	**2/-**	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.	Опитування	
Види та системи криптоаналізу. Криптоаналіз симетричних шифрів. Частотний статистичний криптоаналіз.	**4/5**		Здача лабораторної роботи.	**5**
Методи статистичного (частотного) та повного перебору шифрограми Цезаря та Віженера. Криптоаналіз шифрів простої заміни методом статистичних властивостей тексту	**4/6**		Здача лабораторної роботи.	**5**
Методи криптоаналізу шифрів підстановки та перестановки. Криптоаналіз шифрів підстановки (афінних).	**4/6**		Здача лабораторної роботи.	**5**
Методи криптоаналізу симетричних блокових шифрів. Побудова криптографічних алгоритмів. Принципи Керкхофа.	**4/-**		Опитування	**-**
Лінійний криптоаналіз. Криптоаналіз симетричних шифрів аналітичним методом.	**4/4**		Здача лабораторної роботи	**7**
Модульний контроль			Підсумковий тест в ЕНК	**6**
Всього за модуль	**22/21**			**35**
Модуль 2. Методи криптоаналізу асиметричних криптосистем				
Криптоаналіз асиметричних криптоалгоритмів. Основні методи показники криптостійкості	**2/-**	Застосовувати теорії та методи 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.	Опитування	**-**
Методи криптоаналізу асиметричних криптосистем. Проблеми факторизація алгоритму RSA. Обчислювальна складність факторизації	**3/6**		Здача лабораторної роботи	**8**
Тести простоти для параметрів асиметричних криптосистем. Проблема генерування простих чисел для криптосхеми DSA. Тест Мілера-Рабіна. Тест простоти Люка	**4/6**		Здача лабораторної роботи.	**9**
Оцінка параметрів хеш-функції для застосування в задачах криптології (обчислювальна складність, сумісність, цілісність).	**4/6**		Здача лабораторної роботи.	**10**
Проблема колізій та боротьба з ними в хеш-функціях. Криптографічна сіль.	**4/-**		Опитування	**-**
Потокові шифри. Шифри сімейства А5. Шифр «СТРУМОК». Криптоаналіз та стійкість потокових шифрів.	**6/6**		Здача лабораторної роботи	**9**
Модульний контроль			Підсумковий тест в ЕНК	**6**

Всього за семестр	**23/24**			**35**
Екзамен			**Тест, теоретичні питання, задача**	**30**
Всього за курс	**45/45**			**100**

Неформальна on-line освіта на основі МВОК.

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 несвоєчасної здачі передбачено зниження оцінки
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. Остапов С. Е. Технології захисту інформації: навч. посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2013. – 476 с. – URL: http://kist.ntu.edu.ua/textPhD/tzi.pdf

2. Прикладна криптологія: системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с. – URL: https://er.nau.edu.ua/handle/NAU/32583

3. Dooley F. John History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms – Springer, 2018. – URL: https://books.google.com.ua/books?id=q61qDwAAQBAJ&printsec =frontcover&hl=uk#v=onepage&q&f=false

4. Фільштінський В. А. Математичні основи криптографії: конспект лекцій для студ. спец. 7.080202 "Прикладна математика" денної форми навчання / В. А. Фільштінський, А. В. Бережний.– Суми: СумДУ, 2011. – 138 с.