НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"___" _____ 2023 р.

НАВЧАЛЬНО-МЕТОДИЧНИЙ КОМПЛЕКС

з дисципліни

«ОСНОВИ КРИПТОАНАЛІЗУ»

для підготовки бакалаврів за спеціальністю 125 «Кібербезпека»

КИЇВ-2023

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"___" _____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем, мереж та кібербезпеки
Протокол №10 від "17" травня 2023 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП
«Кібербезпека»
_____
Гарант ОП
_____ (проф. Лахно В.А.)

«ОСНОВИ КРИПТОАНАЛІЗУ»

Спеціальність	125 - Кібербезпека
Освітня програма	Кібербезпека
Факультет	інформаційних технологій
Розробник:	Сагун А.В., к.т.н., доцент

Київ – 2023

Опис навчальної дисципліни

«ОСНОВИ КРИПТОАНАЛІЗУ»

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	Бакалавр	
Галузь знань	12 – Інформаційні технології	
Спеціальність	125 – Кібербезпека	
Освітня програма	Кібербезпека	
Характеристика навчальної дисципліни		
Вид	обов’язкова	
Загальна кількість годин	150	
Кількість кредитів ECTS	5	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	екзамен	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	3	
Семестр	6	
Лекційні заняття, год.	45	
Практичні, семінарські заняття	-	
Лабораторні заняття, год.	45	
Самостійна робота, год.	60	
Індивідуальні завдання	-	
Кількість тижневих аудиторних годин для денної форми навчання	6 (15 тижнів)	

1. Мета, завдання та компетентності навчальної дисципліни

Мета: 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

Завдання навчальної дисципліни: вивчення та застосування лінійного та диференційного криптоаналізу; положень достовірності відстані, допоміжних методів та алгоритмів криптоаналізу (алгоритм Евкліда, алгоритм Ферма та ін.); базових принципів та методів проведення криптоаналізу в система симетричного блочного та асиметричних двоключових схемах шифрування, системах з електронним цифровим підписом.

В результаті вивчення навчальної дисципліни студент повинен

знати:

- основні методи криптоаналізу симетричних і асиметричних криптосистем та криптофункцій;
- методи оцінки криптостійкості та криптосистем та криптоалгоритмів.

вміти:

- застосовувати математичні методи описання і дослідження криптосистем;
- аналізувати криптосистеми, оцінювати їх стійкість,
- застосовувати основні методи криптоаналізу для компроментації шифрограм.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

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.

Спеціальні (фахові, предметні) компетентності (СК):

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

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати (РН), 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.

В контексті зазначених вище компетентностей та програмних результатів навчання задачі викладання дисципліни визначають необхідний комплекс знань і вмінь, що отримують студенти під час вивчення дисципліни.

Навчальна програма розрахована на студентів, які навчаються за освітньою програмою підготовки бакалавра за спеціальністю «Кібербезпека».

Програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Робоча навчальна програма з курсу є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни розроблена на підставі наступних документів:

- освітня програма підготовки бакалаврів за спеціальністю 125 «Кібербезпека»;
- навчальний план підготовки бакалаврів за спеціальністю 125 «Кібербезпека».
- освітньо-професійної програми «Кібербезпека» першого (бакалаврського)рівня вищої освіти за спеціальністю 125 «Кібербезпека».

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчання курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Теоретичною базою для вивчення курсу «Основи криптоаналізу» є курси «Основи криптографічного та стеганографічного захисту інформації" ОПП першого (бакалаврського) рівня вищої освіти.

2. Програма та структура навчальної дисципліни

– повного терміну денної (заочної) форми навчання;

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тиж-ні	всьо-го	у тому числі					всьо-го	у тому числі				
			л	п	лр	інд	с.р.		л	п	лр	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Змістовий модуль 1. Симетричні криптосистеми та методи їх криптоаналіз													
Тема 1. Вступ до курсу. Задачі криптоаналізу. Основні терміни і формулювання.	1	2	2		-		-						
Тема 2. Види та системи криптоаналізу. Криптоаналіз симетричних шифрів. Частотний статистичний криптоаналіз.	2	17	4		5		8						
Тема 3. Методи статистичного (частотного) та повного перебору шифрограми Цезаря та Віженера. Криптоаналіз шифрів простої заміни методом статистичних властивостей тексту	3	20	4		6		10						
Тема 4. Методи криптоаналізу шифрів підстановки та перестановки. Криптоаналіз шифрів підстановки (афінних).	4	10	4		6		-						
Тема 5. Методи криптоаналізу симетричних блокових шифрів. Побудова криптографічних алгоритмів. Принципи Керкхофа.	5	4	4		-		-						
Тема 6. Лінійний криптоаналіз. Криптоаналіз симетричних шифрів аналітичним методом.	6	8	4		4		-						
Разом за змістовим модулем 1		**62**	**22**		**21**		**18**						
Змістовий модуль 2. Методи криптоаналізу асиметричних криптосистем													
Тема 7. Криптоаналіз асиметричних криптоалгоритмів. Основні методи показники криптостійкості	8	14	2		4		8						
Тема 8. Методи криптоаналізу асиметричних криптосистем. Проблеми факторизація алгоритму RSA. Обчислювальна складність факторизації	9	8	3		5		-						

Тема 9. Тести простоти для параметрів асиметричних криптосистем. Проблема генерування простих чисел для криптосхеми DSA. Тест Мілера-Рабіна. Тест простоти Люка	10	16	4		4		8						
Тема 10. Оцінка параметрів хеш-функції для застосування в задачах криптології (обчислювальна складність, сумісність, цілісність).	11	12	4				8						
Тема 11. Проблема колізій та боротьба з ними в хеш-функціях. Криптографічна сіль.	12	18	4		6		8						
Тема 12. Потокові шифри. Шифри сімейства A5. Шифр «СТРУМОК». Криптоаналіз та стійкість потокових шифрів.	13	20	6		4		10						
Разом за змістовим модулем 2		**88**	**23**		**24**		**42**						
Всього годин		**150**	**45**		**45**		**60**						

3. Теми практичних занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

4. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Частотний аналіз інформаційних повідомлень	5
2	Криптоаналіз шифрів простої заміни методом статистичних властивостей тексту	6
3	Криптоаналіз шифрів підстановки (афінних)	6
4	Лінійний криптоаналіз. Криптоаналіз симетричних шифрів аналітичним методом	4
5	Методи криптоаналізу асиметричних криптосистем. Факторизація алгоритму RSA	6
6	Криптоаналіз асиметричних криптоалгоритмів. Тести простоти. Тест Мілера-Рабіна. Тест простоти Люка	6

7	Елементи криптоаналізу хеш-функцій.	6
8	Будова та характеристики потокових шифрів. Особливості генератора ключів. Методи криптоаналізу потокових шифрів на базі лінійних регістрів зсуву	6
	Разом	**45**

Курсове проектування - Не передбачено робочим навчальним планом

6. САМОСТІЙНА РОБОТА СТУДЕНТІВ

Самостійна робота студентів передбачає:

– систематичне відвідання усіх видів аудиторних занять і ведення конспекту лекцій;

– систематичне вивчення лекційного матеріалу і навчальної літератури, що рекомендуються;

– сумлінну підготовку до лабораторних занять;

– вчасне і якісне оформлення звітів про лабораторні роботи.

6.1Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Методи імовірнісно - статистичного аналізу повідомлень	8
2	Індекс відповідності та його критерії в криптоаналізі. Методи криптоаналізу поліалфавітного шифра Віженера	10
3	Тести простоти параметрів асиметричних криптосистем. Сертифікат простоти Прата	8
4	Тест простоти AKS	8
5	Криптографічна сіль та її реалізація в схемах авторизації даних	8
6	Криптографічна хеш-функція Blake. Криптоаналіз алгоритма DSA на базі хеш-функції Blake	8
7	Крипостійкість алгоритму «СТРУМОК». Методи диференційного криптоаналізу потокових шифрів	10

7. Контрольні питання, комплекти тестів для визначення рівня засвоєння знань студентами

7.1. Питання для перевірки знань студентів

1. Задачі криптоаналізу. Основні терміни і формулювання.
2. Види та системи криптоаналізу.
3. Криптоаналіз симетричних шифрів. Методи лінійного криптоаналізу.
4. Методи статистичного (частотного) та повного перебору шифрограми Цезаря

5. Криптоаналіз шифрів табличної перестановки. Використання решітки Кардано для аналізу перестановочних шифрів.

6. Криптоаналіз поліалфавітних шифрів. Криптоаналіз поліалфавітних підстановок. Індекс відповідності.

7. Криптоаналіз асиметричних криптосистем. Проблема факторизації великих чисел.

8. Проблема генерування простих чисел для криптосхеми DSA. Тест Мілера-Рабіна. Тест простоти Люка.

9. Методи оцінки та прогнозування криптостійкості шифрів. Парадокс днів народження.

10. Проблема дискретного логарифмування. Незвідні поліноми

11. Проблема стійкості ключів в алгоритмі Ель-Гамаля

12. Криптоаналіз схеми Діфі-Хелмана.

13. Проблема існування та пошуку базової точки для криптоалгоритмів на базі еліптичних кривих в задачах ЕЦП.

14. Оцінка параметрів хеш-функції для застосування в задачах криптології (обчислювальна складність, сумісність, цілісність).

15. Криптоаналіз асиметричних криптосистем методом повного перебору.

7.2. Приклади тестових питань з дисципліни:

Теоретичні (максимальна оцінка від 5 до 10 балів за відповідь на кожне запитання)
1. Опишіть алгоритм криптоаналізу типу «атака грубою силою». Наведіть приклад роботи даного алгоритму (10 балів)
2. Охарактеризуйте шифр Квадрат Полібія. Наведіть можливий метод криптоаналізу (5 балів)
Тестові завдання (В системі дистанційної освіти elearn)
1. Студент відповідає на 15 випадково відібраних питань з 40 існуючих в системі elearn (15 балів)

8. Форми контролю

Систематичний контроль за самостійною роботою студентів і якістю засвоєння ними поточного навчального матеріалу:

– на лабораторних роботах шляхом перевірки підготовки до виконання роботи;

– роботу над індивідуальними завданнями до лабораторних робіт;

– вивчення літератури, що рекомендувалася, та конспекту лекцій;

– оформлення звітів про виконання лабораторним роботам.

Поточний контроль знань студентів проводиться:

– на лабораторних роботах оцінюється підготовка до роботи, обсяг її виконання, результати захисту звіту;

– на лекційних заняттях виконується вибіркове опитування студентів;

– шляхом проведення модульних контролів знань студентів та виставлення рейтингових оцінок знань студентів по усім видам занять.

9. Розподіл балів, які отримують студенти.

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «ПОЛОЖЕННЯ про екзамени та заліки у НУБіП України» (наказ про уведення в дію від «26» квітня 2023 р. протокол № 10):

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Для визначення рейтингу студента із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації $R_{АТ}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис}=R_{НР}+R_{АТ}$.

10. Методичне забезпечення

1. Конспект лекцій з курсу "основи криптоаналізу". - Київ, НУБіП, 2021 (elearn.nubip.edu.ua/course/view.php?id=4936)

11. Рекомендована література

Основна

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

Допоміжна

1. 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.

2. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. – John Wiley & Sons, 2015. – 784 p. – URL: https://books.google.com.ua/books?id=VjC9BgAAQBAJ&printsec =frontcover&hl=uk#v=onepage&q&f=false

3. Swenson C. Modern Cryptanalysis: Techniques for Advanced Code Breaking. – Wiley Publishing, Inc., 2008. – 264 p. – URL: https://books.google.com.ua/books?id=BuceBTs4ZwC&printsec=frontcover&hl=uk#v=onepage &q&f=false

Інформаційні ресурси

1. https://elearn.nubip.edu.ua/course/view.php?id=4936