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 КРИПТОГРАФІЧНОГО ТА СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

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 КРИПТОГРАФІЧНОГО ТА СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

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

Київ – 2023

Опис навчальної дисципліни

«ОСНОВИ КРИПТОГРАФІЧНОГО ТА СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

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	120	
Кількість кредитів ECTS	4	
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	5	
Лекційні заняття, год.	30	
Практичні, семінарські заняття	-	
Лабораторні заняття, год.	30	
Самостійна робота, год.	60	
Індивідуальні завдання	-	
Кількість тижневих аудиторних годин для денної форми навчання	4 (15 тижнів)	

1. Мета, завдання та компетентності навчальної дисципліни

Мета: ознайомлення студентів з основними методами та засобами використанням криптографічних та стеганографічних перетворень в задачах захисту інформації.

Завдання навчальної дисципліни: сформувати базисні теоретичні поняття та практичні навички щодо проведення криптоперетворень з використанням класичних шифрів, блочних шифрів, асиметричних криптосистем та методів стеганографічного перетворення.

В результаті вивчення навчальної дисципліни студент повинен

знати:

- принципи роботи основних видів симетричних та асиметричних криптоалгоритмів;
- основні методи за галузі застосування стеганографічних перетворень в задачах захисту інформації.

вміти:

- реалізувати програмно асиметричний або симетричний криптоалгоритмі;
- визначати базові параметри криптографічого алгоритму
- використовувати засоби стеганографії для захисту конфіденційності або цілісності інформації.

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.

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

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 криптографічного та сгенанографічного захисту інформації» є курси «Методи та засоби захисту інформації», «Вища математика», «Теорія інформації та кодування» ОПП першого (бакалаврського) рівня вищої освіти спеціальності 125 - Кібербезпка.

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	всього	у тому числі					всього	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 та асиметричні криптоалгоритми та схеми шифрування													
Тема 1. Основні складові криптографічних систем. Задачі криптології та стеганографії в кібербезпеці.	1	2	2		-		-						
Тема 2. Поняття шифрування. Шифри, ключі. Симетричні та асиметричні шифри та їх основні параметри.	2	12	2		2		8						
Тема 3. Модулярна арифметика для задач криптографії. Елементи теорії чисел. Алгоритм Евкліда. Теорема Ейлера та Ферма. Обчислення у скінченних полях	3	4	2		2		-						
Тема 4. Прості симетричні криптосистеми та шифри. Моно та поліалфавітні шифри. Шифри підстановок та перестановок, заміни (квадрат Полібія) Афінні криптоперетворення	4	12	2		2		8						
Тема 5. Операції в кільцях. Криптоперетворення XOR-шифруванням. Гамування. Композиційні шифри	4	10	2		2		6						
Тема 6. Симетричні блочні криптоалгоритми на базі мережі Фейстеля: DES, 3-DES, ДСТУ ГОСТ 28147-2009, алгоритм RC5.	5	14	2		4		8						
Тема 7. Симетричні блочні криптосистеми на базі SP-боксів: AES, ДСТУ 7624:2014. Потокові шифри. Шифри A5, RC4, «СТРУМОК».	7	18	2		2		14						
Тема 8. Асиметрична криптографія. Основні поняття та властивості асиметричних криптосхем. Односторонні криптоперетворення, хеш-функції	9	16	2		2		12						
Тема 9. Криптосхема RSA. Реалізації RSA та	10	4	2		2		-						

алгоритму Ель Гамаля (EG). Робота з довгою арифметикою													
Тема 10. Асиметричні криптосистеми. Алгоритм DSA. Протоколи обміну ключами. Алгоритм Діфі-Хелмана. Еліптичні криві в криптографічних задачах.	11	6	2		4		-						
Разом за змістовим модулем 1		**96**	**20**		**20**		**56**						
Змістовий модуль 2. Стеганографічні методи захисту властивостей інформації													
Тема 11. Розвиток і значення науки стеганографії. Основні терміни, означення в стеганографії. Задачі приховування інформації для стеганографічних перетворень.	12	2	2		-		-						
Тема 12. Комп'ютерна стеганографія. Стеганографічні методи приховування форматуванням тексту. Модель стеганосистеми. Вимоги до стеганосистем.	13	12	4		4		4						
Тема 13. Стеганографічні контейнери та цифрові водяні знаки (Watermark). Метод найменшого значущого біта (LSB) при стеганографічних перетвореннях графічної інформації.	14	10	4		6		-						
Разом за змістовим модулем 2		**24**	**10**		**10**		**4**						
Всього годин		**120**	**30**		**30**		**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	Основи криптографічних перетворень. Прості шифри перестановки та заміни	2
2	Теорія чисел. Та її прикладне застосування в криптографії. Модулярна арифметика	4
3	Модулярна арифметика в криптографії. Афінні криптоперетворення	2
4	Симетричні криптосистеми. Шифри гамування,	4
5	Симетричні криптосистеми. XOR-шифрування.	2
6	Симетричне блочне шифрування. Алгоритм DES, 3-DES.	4
7	Симетричний криптоалгоритм AES	4
8	Асиметричні криптосистеми. Алгоритм RSA.	4
9	Односторонній криптоперетворення. Хеш-функції	4
10	Асиметричні криптосистеми. Алгоритм DSA. Протоколи обміну ключами. Алгоритм Діфі-Хелмана	
11	Стеганографічні методи приховування інформації форматуванням тексту	
12	Метод найменшого значущого біта при стеганографічних перетвореннях графічної інформації	
	Разом	**30**

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.

6.1 Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Шифри простої заміни. Квадрат Полібія	8
2	Абсолютно стійкі шифри. Шифр Вернама (одноразовий блокнот)	8
3	Шифри Фейстеля і Фейстель-сумісні (DES, S-DES, RC5)	8
4	Парні шифри	6
5	Блокові шифри. Принципи побудови та модифікація блокових ширфів	8
6	Хеш-функції. Принцип формування згортки.	6
7	Реалізація функції MD5.	6
8	Хеш – функція Blake.	6
9	Аудіостеганографія. Реалізація аудіостеганографії на базі цифрових методів обробки сигналів дискретними перетвореннями	4

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

7.1. Питання для перевірки знань студентів:

1. Симетричне шифрування. Принцип Керкгофса.

2. Приклади застосування криптографії. Класи атак.

3. Підстановлювальний шифр і його злом.

4. Шифр Віженера, роторна машина.

5. Визначення шифру. Шифр Вернама і досконала таємність.

6. Імовірнісні переформулювання абсолютної секретності.

7. Експеримент по злому. Довжина ключа в разі абсолютної секретності.

8. Псевдовипадковий генератор і його передбачуваність. Лінійний конгруентний генератор в шифрах гамування.

9. Атаки на потокові шифри.

10. Статистичні тести, перевага. Надійність псевдовипадкового генератора.

11. Непередбачуваність надійного генератора. Обчислювальна непомітність.

12. Визначення схеми шифрування із закритим ключем. Обчислювальна стійкість.

13. Стійкість потокового шифру. Шифрування кількох повідомлень.

14. Стійкість щодо chosen plaintext-атак. Функції з ключем і псевдовипадкові функції.

15. Шифрування за допомогою псевдовипадкової функції і його стійкість.

16. Псевдовипадкові перестановки. Методи роботи блокових шифрів.

17. Конструкції псевдовипадкових перестановок. Мережа Фейстеля.

18. Автентифікація повідомлень. Код автентифікації повідомлень і його надійність.

19. Конструкція коду автентифікації повідомлень з псевдовипадкової функції.

20. Протокол інтерактивного обміну ключами, його надійність. Опис протоколу Діфі-Хелмана.

21. Завдання DDH і надійність протоколу Діфі-Хеллмана.

22. Схема шифрування з відкритим ключем, її надійність щодо підслуховування щодо chosen plaintext-атак.

23. Шифрування кількох повідомлень, його надійність. Гібридне шифрування.

24. Наївна схема шифрування RSA. Прискорення дешифрування, маленький показник.

25. RSA з набиванням, завдання RSA і надійність схеми шифрування RSA з набиванням.

26. Схема Ель-Гамаля і її надійність.

27. Квадратичні відрахування і символ Якобі.

28. Завдання визначення квадратичних лишків і схема шифрування Гольдвасер-Мікалі.

29. Витяг квадратних коренів і схема шифрування Рабіна.

30. Залишки по модулю N2 і схема шифрування Пайє.

31. Схема цифрового підпису, її надійність. Наївна схема RSA.

32. RSA з хешем. Схема одноразової підписи Лемпорта.

33. Докази з нульовим розголошенням.

34. Сертифікати. Схеми поділу секрету.

35. Потокові шифри. Шифр А5. Шифр «СТРУМОК», режими шифрування «СТРУМОК-256», «СТРУМОК-512».

7.2. Приклади тестових питань з дисципліни:

ОКР бакалавр напрям підготовки/ спеціальність – 125 «Кібербезпека»	Кафедра комп'ютерних систем, мереж та кібербезпеки 2022-2023 навч.рік	ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ № 1 з дисципліни **«Основи криптогафічного та стеганографічного захисту інформації»**	Затверджую Зав.кафедри _____ доц.Касаткін Д.Ю. 2023 р.
Теоретичні (максимальна оцінка від 5 до 10 балів за відповідь на кожне запитання)			
1. Квадрат Полібія. Алгоритм шифрування та сфери застосування квадрату Полібія. Приклад шифрування на квадраті полібія для фрази «I like NULeS and my Ukraine» (10 балів)			
2. Охарактеризуйте і класифікуйте шифр AES. Наведіть приклади будови s,p блоків (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)			

_____*(доц. Сагун А.В.)*

8. Методи навчання

Виконання лабораторних робіт з використанням Linux Ubuntu, он-лайн засоби для обчислень модулярної арифметики та в скінчених числових полів; виконання індивідуальних навчально-дослідних завдань.

9. 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.

10. 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): $R_{дис}=R_{НР}+R_{АТ}$.

11. Методичне забезпечення

1. Конспект лекцій з курсу "Основи криптографічного та стеганографічного захисту інформації". - Київ, НУБіП, 2021 (elearn.nubip.edu.ua/course/view.php?id)

12. 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

13. Інформаційні ресурси

1. https://elearn.nubip.edu.ua/course/view.php?id=4668
2. https://www.convertstring.com/uk/Hash