Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки(№ 503)

ЗАТВЕРДЖУЮ

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ О.О. Ілляшенко
(підпис) (ініціали та прізвище)

« 31 » серпня 2023 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Прикладна криптологія (КП)
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: 125 "Кібербезпека та захист інформації"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2023 рік

Розробник: Карпенко А.С., асистент
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри «Комп'ютерних систем, мереж і кібербезпеки»
(назва кафедри)

Протокол № 1 від «30» 08 2022 р.

Завідувач кафедри д.т.н., професор _____ В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. **Опис навчальної дисципліни**

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни (денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 2</td><td rowspan="11">Галузь знань
12 «Інформаційні технології"
(шифр та найменування)

Спеціальність
125 «Кібербезпека та захист інформації"
(код та найменування)

Освітня програма
«Безпека інформаційних і комунікаційних систем,
(найменування)

Рівень вищої освіти:

перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 1</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 2</td><td>2023/ 2024</td></tr>
<tr><td>Індивідуальне завдання немає
(назва)</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 16/44</td><td>6-й</td></tr>
<tr><td>Лекції *</td></tr>
<tr><td rowspan="2">Тижневих годин для денної форми навчання:
аудиторних – 1
самостійної роботи студента – 3</td><td>0 годин</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td></td><td>16 годин</td></tr>
<tr><td></td><td>Лабораторні *</td></tr>
<tr><td></td><td>0 годин</td></tr>
<tr><td></td><td>Самостійна робота</td></tr>
<tr><td></td><td>44 годин</td></tr>
<tr><td></td><td>Вид контролю</td></tr>
<tr><td></td><td>Диференційований залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: *48/72*.

* Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: оволодіння студентом навичок для розв’язання комплексу сучасних наукових і прикладних завдань відповідно до захисту інформації в інформаційно -комунікаційних системах.

Завдання: систематизація, закріплення і розширення теоретичних знань; розвиток навичок самостійної роботи, оволодіння методикою досліджень і експериментування використання сучасних інформаційних технологій у процесі розв'язання задач, які передбачені завданням на курсове проектування.

Компетентності, які набуваються. Дисципліна має допомогти сформувати у здобувачів такі загальні та спеціальні компетентності:

– (КЗ 1) здатність застосовувати знання у практичних ситуаціях;
– (КЗ 2) знання та розуміння предметної області та розуміння професії;
– (КЗ 3) здатність до абстрактного мислення, аналізу та синтезу;
– (КЗ 4) вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;
– (КЗ 5) здатність до пошуку, оброблення та аналізу інформації.
– (КФ 1) здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки;
– (КФ 3) Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури;
– (КФ 10) здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності;
– (КФ 12) здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Очікувані результати навчання. В результаті вивчення дисципліни здобувачі мають досягти такі результати навчання:

– (ПРН 1) Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки;
– (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.

Пререквізити – дисципліна є обов'язковим компонентом освітній програми і базується на знаннях, отриманих під час вивчення дисциплін із циклу загальної підготовки, зокрема "Вища математика" (ОК1), "Фізика" (ОК5), "Дискретна математика " (ОК2), "Іноземна мова".

Кореквізити – є базою для дисциплін із циклу професійної підготовки, а саме "Захист інформації в інформаційно-комунікаційних системах" (ОК27), " Системи технічного захисту інформації" (ОК8), "Комплексні системи захисту інформації: проектування, впровадження, супровід" (ОК28), "Безпека операційних систем", для курсового та дипломного проектування. «Науково-педагогічне стажування».

3. Програма навчальної дисципліни

Модуль 1.

Змістовий модуль 1. Розроблення програми досліджень

Тема 1. Основи захисту інформації в інфокомунікаційних системах.

Тема 2. Аналіз існуючих криптографічних алгоритмів.

Тема 3. Постановка завдання на дослідження

Тема 4. Розроблення технічного завдання

Змістовий модуль 2.

Тема 5. Розробка алгоритму рішення поставленого завдання

Тема 6. Розробка програмного забезпечення.

Тема 7. Верифікація та тестування програмного продукту.

Тема 8. Розроблення пояснювальної записки.

Тема 9. Розроблення докладу та презентації.

Тема 10. Публічний захист курсового проекту.

9. Реалізація алгоритмів автентифікації і цифрового підпису

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	с. р.
Модуль 1					
Змістовий модуль 1					
Тема 1. Основи захисту інформації в інфокомунікаційних системах	3		1		2
Тема 2. Аналіз існуючих криптографічних алгоритмів.	3		1		2
Тема 3. Постановка завдання на дослідження	3		1		2
Тема 4. Розроблення технічного завдання	3		1		2
Разом	12		4		8

Змістовий модуль 2					
Тема 5. Розробка алгоритму рішення поставленого завдання	6		2		4
Тема 6. Розробка програмного забезпечення.	8		2		6
Тема 7. Верифікація та тестування програмного продукту.	6		2		4
Тема 8. Розроблення пояснювальної записки.	23		3		20
Тема 9. Розроблення докладу та презентації.	4		2		2
Тема 10. Публічний захист курсового проекту.	1		1		
Разом	48		12		36
Усього годин за дисципліною	60		16		44

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	*Не передбачено*	
	Разом	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Тема 1. Основи захисту інформації в інфокомунікаційних системах	1
2	Тема 2. Аналіз існуючих криптографічних алгоритмів.	1
3	Тема 3. Постановка завдання на дослідження	1
4	Тема 4. Розроблення технічного завдання	1
5	Тема 5. Розробка алгоритму рішення поставленого завдання	2
6	Тема 6. Розробка програмного забезпечення.	2
7	Тема 7. Верифікація та тестування програмного продукту.	2
8	Тема 8. Розроблення пояснювальної записки.	3
9	Тема 9. Розроблення докладу та презентації.	2
10	Тема 10. Публічний захист курсового проекту.	1
	Разом	**16**

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	*Не передбачено*	
	Разом	

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Тема 1. Основи захисту інформації в інфокомунікаційних системах	2
2	Тема 2. Аналіз існуючих криптографічних алгоритмів.	2
3	Тема 3. Постановка завдання на дослідження	2
4	Тема 4. Розроблення технічного завдання	2
5	Тема 5. Розробка алгоритму рішення поставленого завдання	4
6	Тема 6. Розробка програмного забезпечення.	6
7	Тема 7. Верифікація та тестування програмного продукту.	4
8	Тема 8. Розроблення пояснювальної записки.	16
9	Тема 9. Розроблення докладу та презентації.	2
10	Тема 10. Публічний захист курсового проекту.	4
	Разом	**44**

9. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин
1	*Не передбачено*	
	Разом	

10. Методи навчання

Проведення лабораторних занять, консультацій, а також самостійна робота студентів за відповідними матеріалами.

11. Методи контролю

Проведення поточного контролю, підсумковий контроль у вигляді публічного захисту.

12. Критерії оцінювання та розподіл балів, які отримують здобувачі

Поточний контроль передбачає контроль за роботою студента протягом семестру над курсовим проектом, надання йому допомоги та надання консультацій під час роботи над відповідними пунктами курсового проекту.

Підсумкова оцінка виставляється виходячи з якості пояснювальної записки, повноти викладеного матеріалу, відповідності ЄСКД та ЄСПД, якості та повноти доповіді, відповідей на питання членів комісії.

№ з/п	Показчик	Кількість балів
1	Якість пояснювальної записки	0 - 10
2	Повнота викладеного матеріалу	0 - 10
3	Відповідність ЄСКД та ЄСПД	0 - 10
4	Якість та повнота доповіді	0 - 30
5	Якість відповідей на питання	0 - 40
6	Разом	0 - 100

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою
	Диференційований залік
90 – 100	Відмінно
75 – 89	Добре
60 – 74	Задовільно
0 – 59	Незадовільно

13. Методичне забезпечення

1. Навчально-методичний комплекс дисципліни розміщений на кафедральному сервері у відповідному каталозі.

2. Дистанційний курс в системі дистанційного навчання Ментор, розташований за адресою: https://mentor.khai.edu/course/view.php?id=4835.

14. Рекомендована література

Базова

1. Горбенко Ю., Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації, Харків: Видавництво "Форт", 2015.

2. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.

3. Оглобліна О.І., Елементи теорії чисел: навч. посіб. / О. І. Оглобліна, Т.С. Сушко, Ю. В. Шрамко. – Суми: Сумський державний університет, 2015. – 186 с.

4. Корченко О.Г., Прикладана криптологія: системи шифрування: підручник О.Г. Корченко, В.П. Сіденко, Ю.О. Дрейс. – К.: ДУК, 2014.

5. Бабенко Т.В., Криптологія у прикладах, тестах і задачах: навч. посібник / Т.В. Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я. Фомичова. − Д.: Національний гірничий університет, 2013. − 318 с.

6. Горбенко І.Д., Гриненко Т.О. Захист інформації в інформаційно-комунікаційних системах. Част.1. Криптографічний захист інформації. Харків: ХНУРЕ, 2004. 367 с.

Допоміжна

7. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч. посібник / Г. Л. Козіна. – Запоріжжя: НУ «Запорізька політехніка», 2020. – 192 с.

8. Steinberg J., Beaver K., Winkler I., Coombs T. Cybersecurity All-in-One For Dummies. New York: Wiley, 2022. 700 p.

9. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition edition. New York: Wiley, 2015. 784 p.

10. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч. посібник / Г. Л. Козіна. – Запоріжжя: НУ «Запорізька політехніка», 2020. – 192 с.

11. Богуш В.М., Мухачов В.А. Криптографічні застосування елементарної теорії чисел. Навчальний посібник. – Київ: ДУІКТ, 2006. – 125 с.

12. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, затверджені наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22.

13. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу, затверджені наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22.

15. Інформаційні ресурси

14. http://www.dsszzi.gov.ua Державна служба спеціального зв'язку та захисту інформації України.

15. http://www.csn.khai.edu Кафедральний сайт

16. http://www.bezpeka.com/ru/lib/spec/cript.html Криптографічний захист інформації.