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

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

ЗАТВЕРДЖУЮ

Голова НМК

_____ Д .М. Крицький
(підпис) (ініціали та прізвище)

« 31 » серпня 2023 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в інформаційно-комунікаційних системах (КП)
(назва навчальної дисципліни)

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

Спеціальність: 125 "Кібербезпека"
(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: Пєвнєв В. Я., доцент, д.т.н., доцент
(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 2023 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"
(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>7-й</td></tr>
<tr><td>Лекції *</td></tr>
<tr><td rowspan="4">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>0 годин</td></tr>
<tr><td>Лабораторні *</td></tr>
<tr><td>16 годин</td><td>Самостійна робота</td></tr>
<tr><td>44 годин</td><td>Вид контролю</td></tr>
<tr><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: визначення рівня підготовленості студента до 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:

– здатність застосовувати знання у практичних ситуаціях;

– знання та розуміння предметної області та розуміння професії;

– здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово;

– вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;

– здатність до пошуку, оброблення та аналізу інформації;

– 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;

– здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;

– 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:

– ПРН 1 Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

– ПРН 8 Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

– ПРН 14 Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

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

– ПРН 30 Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

– ПРН 31 Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

– ПРН 34 Приймати участь у розробці та впровадженні стратегії

інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

– ПРН 50 Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

– ПРН 51 Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень 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", "Фізика", "Теорія електричних кіл і мікроелектроніка", " Дискретна математика " "Іноземна мова".

Кореквізити – є базою для дисциплін із циклу професійної підготовки, а саме "Захист інформації в інформаційно-комунікаційних системах ", " Системи технічного захисту інформації ", "Комплексні системи захисту інформації: проектування, впровадження, супровід", " 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.

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		
2		
	Разом	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1		
2		
	Разом	

7. Теми лабораторних 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**

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.	20
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		
2		
	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 І.Д., Гриненко Т.О. Захист інформації в інформаційно-комунікаційних системах. Част.1. Криптографічний захист інформації. Харків: ХНУРЕ, 2004. 367 с.
2. Задірака В., Олесик О. Комп'ютерна криптологія. К.: «Політехніка», 2002. 502 с.

Допоміжна

1. Барич С.Г., Гончаров В. В., Сєров Р. Є. Основи сучасної криптографії.-М.: Гаряча лінія-Телеком, 2001.-120 с.
2. Романець Ю. І., Тимофєєв П. А., Шаньгін В.Ф. Захист інформації в комп'ютерних системах та мережах.-М.: Радіо та зв'язок, 1999.-328 с.
3. Ельтанов Б.А. Розвиток методу решета. М.: Статистика, 1986. - 157с.
4. Василенко О. Н. Теоретико-числові алгоритми у криптографії. М: МЦНМО. 2003. 328 с.

15. Інформаційні ресурси

1. http://www.kernel.org
2. http://fedoraproject.org
3. http://www.ubuntu.com
4. http://www.csn.khai.edu