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

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

ЗАТВЕРДЖУЮ

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

" 31" 08 2024 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»
(шифр і назва галузі знань)

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

Освітня програма «Кібербезпека»
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2024 рік

Розробник: Пєвнєв В.Я., професор, 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 2024 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 rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>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 та 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 змістових модулів – 3</td><td>2024/ 2025</td></tr>
<tr><td>Індивідуальне завдання КП</td><td>Семестр</td></tr>
<tr><td>Загальна кількість годин
денна – 16 / 60</td><td>7-й</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання:
аудиторних – 1
самостійної роботи студента – 2,75</td><td>Лекції</td></tr>
<tr><td></td></tr>
<tr><td>Практичні, семінарські</td></tr>
<tr><td>16 годин</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td></td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>44 години</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>Диференційований залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: для денної форми навчання – 16/44

.

2. Мета та завдання навчальної дисципліни

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

Завдання:

– оволодіти практичними навичками знаходження та аналізу вразливостей інформації під час її передавання та збереження в інформаційно-комунікаційних системах.

Компетентності, які набуваються.

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

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

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості 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 27 Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) 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 – "Архітектура комп'ютерів", "Моделі та структури даних", "Апаратні та програмні засоби захисту інформації", "Інформаційно-комунікаційні системи", "Операційні системи".

Кореквізити –"Кваліфікаційна робота бакалавра".

3. Програма навчальної дисципліни

Модуль 1.

Змістовий модуль 1

Тема 1. Постановка задачи на курсове проектування

Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення. Місце дисципліни у навчальному процесі. Вимоги до знань та вмінь тих, хто навчається.

Тема 2. Основні вимоги до курсового проекту

Зміст та структура курсового проекту. Загальні положення. Основна частина. Список використаних джерел.

Змістовий модуль 2

Тема 3. Організація та проведення досліджень

Методологія дослідження: мета та предмет вивчення. Метод дослідження: поняття, його функція та ознаки. Типологія методів наукового дослідження. Методи, які використовуються на емпіричному рівні дослідження. Методи, які використовуються на теоретичному рівні дослідження.

Змістовий модуль 3

Тема 4. Підготовка та захист курсового проекту

Оформлення курсового проекту. Загальні вимоги до оформлення. .
Ілюстрації, таблиці, формули. Оформлення списку використаних джерел.
Порядок захисту курсового проекту. Оформлення презентації. Доповідь.

4. Структура навчальної дисципліни

Назви модулів і тем	Кількість годин				
	усього	у тому числі			
		л	п	лаб.	с.р.
Модуль 1					
Змістовий модуль 1.					
Тема 1. Постановка задачи на курсове проектування	6	-	2	-	4
Тема 2. Основні вимоги до курсового проекту	6	-	2	-	4
Разом за змістовим модулем1	**12**	**-**	**4**	**-**	**8**
Змістовий модуль 2					
Тема 3. Організація та проведення досліджень	14	-	2	-	12
Разом за змістовим модулем 2	**26**	**-**	**6**	**-**	**20**
Змістовий модуль 3					
Тема 4. Підготовка та захист курсового проекту	22	-	6	-	16
Разом за змістовим модулем 3	**22**	**-**	**6**	**-**	**16**
Разом за модулем 1	**60**	**-**	**16**	**-**	**44**
Усього годин	**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
		Денна форма навчання
1	Постановка задачи на курсове проектування	2
2	Основні вимоги до курсового проекту	2
3	Організація та проведення досліджень	6
4	Підготовка та захист курсового проекту	6
	Разом	16

7. Теми лабораторних занять

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

8. Самостійна робота

№ теми	Назва теми	Кількість годин
		Денна форма навчання
1	Постановка задачи на курсове проектування. Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення. Місце дисципліни у навчальному процесі. Вимоги до знань та вмінь тих, хто навчається.	2
2	Основні вимоги до курсового проекту. Зміст та структура курсового проекту. Загальні положення. Основна частина. Список використаних джерел.	2
3	Організація та проведення досліджень. Методологія дослідження: мета та предмет вивчення. Метод дослідження: поняття, його функція та ознаки. Типологія методів наукового дослідження. Методи, які використовуються на емпіричному рівні дослідження. Методи, які використовуються на теоретичному рівні дослідження.	6
4	Підготовка та захист курсового проекту. Оформлення курсового проекту. Загальні вимоги до оформлення. . Ілюстрації, таблиці, формули. Оформлення списку використаних джерел. Порядок захисту курсового проекту. Оформлення презентації. Доповідь. Захист.	6
	Разом	**16**

9. Індивідуальні завдання

Виконання КП. Теми КП обираються індивідуально кожному студенту.

10. Методи навчання

Проведення практичних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, підсумковий контроль у вигляді публічного захисту.

12. Критерії оцінювання знань студента під час іспиту

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. Важинський С. Е., Щербак Т. І. Методика та організація наукових досліджень навч. пос. Суми: СумДПУ ім. А. С. Макаренка, 2016. – 260 с.
2. Рассоха І. М. «Методологія та організація наукових досліджень» Харк. нац. акад. міськ. госп-ва. – Х.: ХНАМГ, 2011. – 76 с.
3. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем._ К.: Вид.група BHV, 2009.-608 с.
4. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С.Кузнеця, 2016. – 1013 Мб.

5. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с.
6. Захист інформації в автоматизованих системах управління: навч. посіб. /Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.
7. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ 2000», 2020. – 678 с

Допоміжна

1. Jeremiah Grossman. XSS Attacks CROSS SITE SCRIPTING EXPLOITS AND DEFENSE. – USA.: Amazon DS, 2018 – 630 с.
2. Holistic Info-Sec for Web Developers. [Electronic resource]. – Access mode: https://holisticinfosecforwebdevelopers.com/ 4
3. OWASP Web Security Testing Guide. [Electronic resource]. – Access mode : https://owasp.org/www-project-web-security-testing-guide/
4. Open Web Application Security Project [Електронний ресурс]. Режим доступу: a. www.owasp.org 6. Когут Ю.І. Кібербезпека

Інформаційні ресурси

1. Кваліфікаційний центр інформаційних технологій та кібербезпеки ДержНДІ технологій кібербезпеки [Електронний ресурс]. – http://dstszi.gov.ua/
2. Офіційний сайт Google, на якому розміщена документація по работі із Google App Engine. [Електронний ресурс]. – Режим доступу: https://cloud.google.com/products/appengine
3. Офіційний сайт Microsoft, на якому розміщена документація по роботі із платформою Microsoft Azure. [Електронний ресурс].