

1. Опис навчальної дисципліни

Показник	Значення показника
Курс	1,2
Семестр	2,3
Обсяг (<i>кредити ЄКТС/години</i>)	5 / 150
Кількість змістових модулів	2
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	10
семінарські заняття (СЗ)	4
практичні заняття (ПЗ)	2
лабораторні заняття (ЛЗ)	-
самостійна робота (СР)	134
форма підсумкового контролю (<i>семестр</i>)	екзамен (3)

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета: формування цілісного розуміння принципів побудови та функціонування комплексних систем захисту інформації (КСЗІ), опанування теоретичних основ, нормативно-правових вимог та практичних навичок із проектування, впровадження й експлуатації таких систем у різних сферах діяльності.

Завдання:

- засвоїти понятійний апарат і теоретичні основи побудови КСЗІ;
- вивчити принципи створення комплексного захисту з урахуванням організаційних, технічних, програмних та криптографічних складових;
- здобути навички використання методів та засобів контролю доступу, криптографічного захисту, моніторингу й аудиту інформаційних систем;
- опанувати нормативно-правові та стандартні вимоги до побудови КСЗІ (національні та міжнародні);
- сформуванати навички проектування КСЗІ для різних об'єктів інформаційної діяльності, у тому числі об'єктів критичної інфраструктури;
- навчитися використовувати сучасні програмні й апаратні засоби забезпечення комплексного захисту;
- розвинути компетентності з оцінки ефективності функціонування КСЗІ та підготовки рекомендацій щодо їх удосконалення;
- вивчити методи тестування, атестації та сертифікації КСЗІ.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Комплексні системи захисту інформації» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної програми «Організація захисту інформації з обмеженим доступом» (від 12.09.2024р. № 29/3/4-408/ві; зміни від 11.02.2025р. №29/3-30/ві)), а саме:

ПРН 7	Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.
ПРН 17	Створювати та документально оформлювати бази персональних даних на підприємствах, установах та організаціях різних формах власності.
ПРН 20	Організовувати та розробляти комплексну систему захисту інформації та формувати систему суб'єктів захисту інформації з обмеженим доступом установ, підприємств, організацій; здійснювати моніторинг, протидію загрозам конфіденційності, цілісності, доступності інформації з обмеженим доступом.

3. Програма та структура навчальної дисципліни

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>
2 семестр						
Змістовий модуль 1. Комплексний підхід до захисту інформації						
Тема 1. Вступ до дисципліни	22	2				20
Лекція 1. Основні поняття та визначення комплексного захисту інформації		2				
Самостійна робота 1. Основні поняття та визначення комплексного захисту інформації						20
Тема 2. Нормативно-правове регулювання у сфері КСЗІ	22	2				20
Лекція 1. Нормативно-правове регулювання у сфері КЗІ та ТЗІ в Україні		2				
Самостійна робота 1. Нормативно-правове регулювання у сфері КЗІ та ТЗІ в Україні						20
Тема 3. Методи, засоби і заходи захисту інформації на ОІД та в ІТС	28		4			24
Самостійна робота 1. Методи, засоби і заходи захисту інформації на ОІД та в ІТС						24
Семінарське заняття 1. Порядок створення, введення в експлуатацію та супроводження КСЗІ			2			
Семінарське заняття 2. Політика безпеки інформації в АС, розроблення технічного завдання на створення КСЗІ. Модульна контрольна робота 1			2			
Всього годин за модуль 1	72	4	4			64
Всього за 2 семестр	72	4	4			64

3 семестр					
Змістовний модуль 2. Проектування, введення в експлуатацію та супроводження КСЗІ					
Тема 4. Створення КСЗІ	54	6		2	46
Лекція 1. Порядок проведення робіт зі створення КСЗІ		2			
Практичне заняття 1. Порядок обстеження ОІД, документальне оформлення результатів			2		
Самостійна робота 1. Порядок проведення робіт зі створення КСЗІ					14
Лекція 2. Політика безпеки інформації в АС, розроблення технічного завдання на створення КСЗІ		2			
Самостійна робота 2. Політика безпеки інформації в АС, розроблення технічного завдання на створення КСЗІ					12
Лекція 3. Основні підходи та принципи розроблення плану захисту для АС класу 1		2			
Самостійна робота 3. Основні підходи та принципи розроблення плану захисту для АС класу 1					10
Самостійна робота 4. Введення КСЗІ в експлуатацію					10
Тема 5. Особливості проектування та створення КСЗІ для автоматизованих систем різних класів	24				24
Самостійна робота 1. Особливості проектування та створення КСЗІ для автоматизованих систем різних класів.					24
Всього годин за модуль 2	78	6		2	70
Всього годин за 3 семестр	78	6		2	70
Семестровий контроль (екзамен)					
Всього годин за навчальну дисципліну	150	10	4	2	134

Організаційно-методичні вказівки до проведення навчальних занять та контрольних заходів: *при проведенні в режимі офлайн планувати проведення практичних занять в центрі кібербезпеки.*

4. Основні методи навчання

Під час викладання навчальної дисципліни «Комплексні системи захисту інформації» використовуються такі методи навчання: індуктивний, дедуктивний, дослідницький та метод стимулювання.

Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить здобувачів вищої освіти до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Дослідницький метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню слухачів новою інформацією.

Теоретична підготовка здобувачів вищої освіти забезпечується шляхом вивчення вимог керівних документів з питань національної та інформаційної безпеки, політико-правових аспектів формування інформаційного суспільства держави, науково-методичних засад державного управління національними інформаційними ресурсами як необхідної складової системи інформаційної безпеки.

Основними видами занять є лекції, практичні, семінарські заняття та самостійна робота.

5. Оцінювання результатів навчання

5.1 Результати навчання здобувача вищої освіти з навчальної дисципліни оцінюються за 100-бальною шкалою як сума балів поточного та підсумкового контролю із застосуванням наступних вагових коефіцієнтів, загальна сума яких дорівнює 1:

Вид контролю	Ваговий коефіцієнт
Поточний контроль (К)	0,8
Підсумковий контроль (ПК)	0,2

Підсумкова семестрова оцінка (ПСО) обчислюється за формулою:
 $ПСО = К + ПК$

5.2. Складниками для обчислення балу поточного контролю здобувача вищої освіти є:

Види навчальної діяльності	Кількість балів (максимальна)
Робота на лекціях (ведення конспекту лекцій або інше)	10
Робота на практичних заняттях	20
Робота на семінарських заняттях	20
Виконання завдань для самостійної роботи	10
Виконання модульної контрольної роботи	10

Мінімальна кількість балів для допуску до підсумкового контролю 48 балів.

5.3. Шкала оцінювання здобувача вищої освіти

Оцінка за шкалою ЄКТС	Оцінка за 100-бальною шкалою	Значення оцінки
A	90-100	<i>Відмінно – відмінне виконання лише з незначною кількістю помилок.</i> Здобувач вищої освіти виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили.
B	84-89	<i>Дуже добре – вище середнього рівня, але з кількома помилками.</i> Здобувач вищої освіти вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна
C	75-83	<i>Добре – загалом правильна робота, але з певною кількістю помилок.</i> Здобувач вищої освіти вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок.
D	65-74	<i>Задовільно – непогано, але зі значною кількістю недоліків.</i> Здобувач вищої освіти відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих.
E	60-64	<i>Достатньо – виконання задовольняє мінімальні вимоги.</i> Здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.
FX	35-59	<i>Незадовільно – потрібна додаткова робота.</i> Здобувач вищої освіти володіє матеріалом на рівні

		окремих фрагментів, що становлять незначну частину навчального матеріалу
F	1-34	<i>Незадовільно – потрібна значна додаткова робота.</i> Здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів.

6. Ресурсне забезпечення навчальної дисципліни

Рекомендовані джерела інформації

Основна література:

1. Гулак Г.М., Жильцов О.Б., Киричок Р.В., Коршун Н.В., Складанний П.М. Інформаційна та кібернетична безпека підприємства: підручник. Київ: Вид-во КУБГ, 2024. – 396 с.
2. Інформаційна безпека: підручник / [В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.]; під ред. В. В. Остроухова. – К.: Ліра-К, 2021. – 412 с.
3. Організаційно-правові основи забезпечення кібербезпеки : Підручник / М. В. Гуцалюк, А. І. Марущак, Д. С. Мельник [та ін.] ; За заг. ред. Присяжнюка М.М. - Київ : Наук.-вид. відділ НА СБ України, 2023. - 320с.
4. Організація та управління служби захисту інформації : Практикум / О. В. Шепета. - Київ : НА СБУ, 2021. - 48с. - Видавництво НА СБУ

Допоміжна література:

1. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації: підручник/ - Вінниця: ВНТУ, 2011. - 199с.
2. Гуз А.М., Довгань О.Д., Марущак А.І.: Основи захисту інформації з обмеженим доступом: підручник/ К.: НА СБУ, 2011 р.
3. Гулак Г.М., Гринь А.К., Довгань О.Д., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2013. – 184 с.
4. Бурячок В.Л., Гулак Г.М., Толубко В.Л. Інформаційний та кібернетичний простори: проблеми безпеки, методи та засоби боротьби Підручник. – К.: ТОВ «СІК ГУП Україна», 2015. – 449 с.
5. Богуш В.М., Юдін О.К., Інформаційна безпека держави. –К.: «МК-Прес», 2005. – 432с.
6. Гайворонський М.В. БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ / М.В.Гайворонський, О.М.Новиков. - К.: Видавнича група ВНУ, 2009. - 608 с. [Режим доступу]: МЕТОД/СК-31/КСЗІ/Література

7. Богуш В.М. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ: ВСТУП ДО СПЕЦІАЛЬНОСТІ / В.М.Богуш, О.К.Юдін. – Харків: Консум, 2004. – 439 с.

Інформаційні ресурси

1. Національна бібліотека ім. В.І.Вернадського / [Електронний ресурс]. – Режим доступу: <http://www.nbuv.gov.ua/>
2. Цифровий репозитарій ХНУГХ ім. А.Н.Бекетова / [Електронний ресурс]. – Режим доступу: <http://eprints.kname.edu.ua/>
3. Цифровий репозитарій Харківського національного університету ім. В.Н.Каразіна / [Електронний ресурс]. – Режим доступу: <http://dspace.univer.kharkov.ua/handle/123456789/568>

Адреса розміщення робочої програми навчальної дисципліни:

<https://academy.ssu.gov.ua/>

(офіційний вебсайт НА СБУ / платформа дистанційного навчання / електронний ресурс навчально-наукового інституту, кафедри, бібліотеки тощо)

7. Дані про перегляд робочої програми навчальної дисципліни

№ п/п	Дата, номер протоколу засідання кафедри (спільного засідання кафедр)	Рішення за результатами перегляду	Підпис керівника кафедри