

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Безпека інформації в інформаційно-комунікаційних системах»

Освітня програма	<i>Кіберзахист інформаційних ресурсів</i>
Рівень вищої освіти	<i>перший (бакалаврський)</i>
Форма навчання	<i>денна</i>
Статус навчальної дисципліни	<i>обов'язкова</i>
Мова викладання	<i>українська</i>

Робочу програму навчальної дисципліни розглянуто та схвалено на засіданні кафедри Безпеки інформаційно-комунікаційних систем від 01.09.2024 року, протокол № 1.

1. Опис навчальної дисципліни

Показник	Значення показника
Курс	3
Семестр	6
Обсяг (<i>кредити ЄКТС/години</i>)	6 / 180
Кількість змістових модулів	4
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	38
семінарських занять (СЗ)	18
практичні заняття (ПЗ)	38
самостійна робота (СР)	86
Форма підсумкового контролю (<i>семестр</i>)	<i>Екзамен</i>

Передумови для вивчення навчальної дисципліни:

1. *Мережеві технології та протоколи.*
2. *Операційні системи та віртуалізація.*
3. *Програмні засоби захисту інформації.*

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

допомогти здобувачам вищої освіти опанувати знання та навички щодо питання забезпечення безпеки інформації в інформаційно-комунікаційних системах, ознайомити з особливостями їх майбутньої професії.

Завдання:

- здатність застосовувати методи теорії систем і системного аналізу при моделюванні, побудові та дослідженні інформаційно-комунікаційних систем;
- здатність обґрунтовувати застосування методів та засобів забезпечення безпеки інформації в інформаційно-комунікаційних системах;
- здатність обґрунтовувати застосування методів та засобів забезпечення безпеки та захисту інформації в інформаційно-комунікаційних системах, пов'язаних з проектуванням, впровадженням і використанням мереж всередині організації, між організаціями, між організаціями і користувачами;
- здатність обґрунтовувати, впроваджувати та забезпечувати функціонування систем інформаційних ресурсів організації.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Безпека інформації в інформаційно-комунікаційних системах» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної / освітньо-наукової програми «Кіберзахист інформаційних ресурсів» (від 11.09.2024 № 29/3/1/3-1277/ві), а саме:

ПРН 5.	Адаптуватись до нових викликів та дій у певних ситуаціях, застосовувати знання державної та іноземних мов, інформаційно – комунікаційних технологій, комп'ютерної техніки для забезпечення професійної комунікації.
ПРН 7.	Обґрунтовувати та визначати основні напрями створення та експлуатації системи та основних підсистем управління інформаційною безпекою та кібербезпекою, використовуючи інформаційні та комунікаційні технології для формування ефективної системи інформаційно-аналітичного забезпечення, підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.
ПРН 12.	Планувати та організовувати особисту діяльність в умовах протиборства в інформаційній сфері та кіберпросторі для забезпечення інформаційної безпеки та кібербезпеки держави та організації.
ПРН 13.	Оцінювати стан безпеки особистості, суспільства та держави за окремими сферами забезпечення і видами діяльності на основі положень теорії безпеки окремих сфер забезпечення національної безпеки і видів діяльності
ПРН 16.	Розробляти основні положення методів та заходів забезпечення інформаційної безпеки та кібербезпеки держави у різноманітних сферах життєдіяльності.
ПРН 22.	Обґрунтовувати застосування методів та засобів захисту програмних засобів, оцінки забезпечення якості програмного забезпечення а також інформаційно-програмних ресурсів і процесів, що беруть участь в життєвому циклі застосунків.
ПРН 24.	Забезпечувати процеси захисту та функціонування інформаційно-комунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурнологічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент

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>
Семестр 6						
Змістовий модуль 1. ФОРМУВАННЯ ПОЛІТИКИ БЕЗПЕКИ ТА РОЗГЛЯД ЗАХОДІВ ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ						
Тема 1. Формування політики безпеки в інформаційно-комунікаційних системах	18	4	2	4	-	8
Лекція 1. Основні визначення та положення. Характеристика загроз безпеці інформації.		2				
Самостійна робота 1. Характеристика загроз безпеці інформації.						2
Практичне заняття 1. Визначення вихідних даних щодо створення умов захисту інформаційно-комунікаційних систем.				2		
Самостійна робота 2. Умови для захисту інформаційно-комунікаційних систем.						2
Лекція 2. Формування політики безпеки інформаційно-		2				

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
<i>I</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>
комунікаційних систем.						
Самостійна робота 3. Політика безпеки інформаційно-комунікаційних систем.						2
Практичне заняття 2. Визначення політики безпеки для інформаційно-комунікаційних систем.				2		
Самостійна робота 4. Застосування політики безпеки для захисту інформаційно-комунікаційних систем.						2
Семінарське заняття 1. Визначення загроз та формування політики безпеки на прикладах.			2			
Тема 2. Заходи захисту цілісності інформації в інформаційно-комунікаційних системах.	30	6	4	6	-	14
Лекція 3. Несанкціонований доступ. Моделі порушників інформаційної безпеки. Протоколи ідентифікації та аутентифікації.		2				
Самостійна робота 5. Цілісність інформації в інформаційно-комунікаційних системах						2
Практичне заняття 3. Безпечна ідентифікація та аутентифікація користувачів.				2		
Семінарське заняття 2. Несанкціонований доступ. Безпечна аутентифікація та ідентифікація.			2			
Самостійна робота 6. Безпечна ідентифікація та аутентифікація						2
Лекція 4. Криптографічні методи захисту інформації.		2				
Самостійна робота 7. Криптографічні методи захисту інформації.						2
Практичне заняття 4. Захист інформації за допомогою асинхронного симетричного шифрування.				2		
Самостійна робота 8. Електронний цифровий підпис.						2
Лекція 5. Алгоритми шифрування.		2				
Самостійна робота 9. Алгоритми шифрування. Методи простої заміни та перестановки.						2
Семінарське заняття 3. Види алгоритмів шифрування			2			
Самостійна робота 10. Алгоритми шифрування. Методи складної заміни						2
Самостійна робота 11. Підготовка до проходження модульної контрольної роботи 1.						2
Практичне заняття 5. Модульна контрольна робота 1.				2		
Всього годин за змістовий модуль 1.	48	10	6	10	-	22
Змістовий модуль 2. АСПЕКТИ ПОБУДОВИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ						
Тема 3. Сегментний підхід в побудові мереж	18	4	2	4	-	8
Лекція 6. Побудова сегментів фізичного, каналного та мережевого рівня. Поєднання сегментів мережі.		2				
Самостійна робота 12. Поєднання сегментів мережі.						2
Практичне заняття 6. Синтез інформаційно-комунікаційних систем.				2		
Самостійна робота 13. Синтез інформаційно-комунікаційних систем.						2
Лекція 7. Математичні моделі та методи аналізу інформаційно-комунікаційних систем.		2				
Самостійна робота 14. Математичні моделі та методи аналізу інформаційно-комунікаційних систем						2
Практичне заняття 7. Проведення аналізу інформаційно-комунікаційних систем та мереж.				2		

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
<i>I</i>	2	3	4	5	6	7
Семінарське заняття 4. Синтез та аналіз інформаційно-комунікаційних систем.			2			
Самостійна робота 15. Аналіз інформаційно-комунікаційних систем.						2
Тема 4. Структуровані кабельні системи	24	6	-	6	-	12
Лекція 8. Структуровані кабельні системи.		2				
Самостійна робота 16. Загальні поняття структурованих кабельних систем.						2
Практичне заняття 8. Побудова структурованої кабельної системи.				2		
Самостійна робота 17. Основні аспекти побудови структурованої кабельної системи.						2
Лекція 9. Захист структурованих кабельних систем		2				
Самостійна робота 18. Способи захисту структурованих кабельних систем.						2
Практичне заняття 9. Побудова системи відеонагляду.				2		
Самостійна робота 19. Системи відеонагляду.						2
Лекція 10. Фізичні аспекти побудови захищених інформаційно-комунікаційних систем		2				
Самостійна робота 20. Фізичні аспекти побудови захищених інформаційно-комунікаційних систем.						2
Самостійна робота 21. Підготовка до проходження модульної контрольної роботи 2.						2
Практичне заняття 10. Модульна контрольна робота 2.				2		
Всього годин за змістовий модуль 2.	42	10	2	10	-	20
Змістовий модуль 3. ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ						
Тема 5. Програмні засоби захисту інформації	26	4	4	4	-	14
Лекція 11. Основні принципи та методи забезпечення безпеки інформації в інформаційно-комунікаційних системах.		2				
Самостійна робота 22. Безпека інформації в інформаційно-комунікаційних системах.						2
Практичне заняття 11. Захист інформації засобами операційних систем. Резервне копіювання даних.				2		
Самостійна робота 23. Хмарні сервіси для резервного зберігання даних.						2
Семінарське заняття 5. Порівняльний аналіз деяких систем виявлення вторгнень			2			
Самостійна робота 24. Системи виявлення вторгнень.						2
Самостійна робота 25. Способи захисту інформації в інформаційно-комунікаційних системах.						2
Лекція 12. Огляд вірусів та їх основні способи виявлення.		2				
Самостійна робота 26. Віруси: історія виникнення, типи та вплив на роботу інформаційно-комунікаційних систем.						2
Практичне заняття 12. Робота з антивірусним програмним забезпеченням ОС комп'ютерів.				2		
Самостійна робота 27. Хмарні технології в антивірусному програмному забезпеченні						2
Семінарське заняття 6. Антивіруси: історія виникнення, класифікація.			2			
Самостійна робота 28. Антивірусне програмне забезпечення						2
Тема 6. Розбиття мережі на виокремлені сегменти,	28	6	4	6	-	12

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>
налаштування кінцевих пристроїв та маршрутизації						
Лекція 13. Ідентифікація вузлів глобальних систем обробки та обміну інформацією на базі IP адрес		2				
Самостійна робота 29. Ідентифікація вузлів мережі.						2
Практичне заняття 13. Розрахунок підмереж IPv4 та розбиття IP мереж на підмережі				2		
Самостійна робота 30. Розбиття мережі на виокремлені сегменти.						2
Лекція 14. Базові налаштування комутаторів та кінцевих пристроїв		2				
Самостійна робота 31. Налаштування кінцевих пристроїв						2
Практичне заняття 14. Налаштування мережевих сервісів DNS, DHCP та Web				2		
Самостійна робота 32. Мережеві сервіси						2
Лекція 15. Маршрутизація в мережі		2				
Самостійна робота 33. Маршрутизація в мережах: види, відмінності, переваги та недоліки						2
Семінарське заняття 7. Налаштування статичної маршрутизації			2			
Семінарське заняття 8. Налаштування динамічної маршрутизації			2			
Самостійна робота 34. Підготовка до проходження модульної контрольної роботи 3.						2
Практичне заняття 15. Модульна контрольна робота 3.				2		
Всього годин за змістовий модуль 3.	54	10	8	10	-	26
Змістовий модуль 4. МЕХАНІЗМИ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ						
Тема 7. Механізми безпеки інформаційно-комунікаційних систем.	36	8	2	8	-	18
Лекція 16. Протоколи формування захищених каналів на каналному рівні.		2				
Самостійна робота 35. Захист каналів на каналному рівні.						2
Практичне заняття 16. Використання технології NAT та застосування технології VLAN.				2		
Самостійна робота 36. Огляд технології NAT та VLAN.						2
Лекція 17. Захист на мережевому рівні - протокол IPSec.		2				
Самостійна робота 37. Мережевий рівень.						2
Практичне заняття 17. Налаштування протоколу IPSec.				2		
Самостійна робота 38. Протокол IPSec.						2
Лекція 18. Протоколи безпеки на сеансовому рівні (SSL/TLS).		2				
Самостійна робота 39. Протокол SSL/TLS.						2
Практичне заняття 18. SSL/TLS тунелювання з'єднань захищеної доставки пошти.				2		
Самостійна робота 40. Протоколи налаштування електронної пошти						2
Семінарське заняття 9. Налаштування безпечного WI-FI.			2			
Самостійна робота 41. Безпека WI-FI.						2
Лекція 19. Віртуальні приватні мережі (VPN)		2				
Самостійна робота 42. Віртуальні приватні мережі (VPN)						2
Самостійна робота 43. Підготовка до проходження модульної контрольної роботи 4.						2
Практичне заняття 19. Модульна контрольна робота 4.				2		
Всього годин за змістовий модуль 4.	36	8	2	8	-	18

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
<i>I</i>	2	3	4	5	6	7
Підсумковий контроль (екзамен)						
Всього годин за навчальну дисципліну	150	38	-	38	-	74

4. Основні методи навчання

Під час викладання навчальної дисципліни використовуються такі методи навчання як індуктивний, дедуктивний, продуктивний, дослідницький та метод стимулювання.

Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить слухачів 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. Продуктивний 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.

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)	0,7
Підсумковий контроль (ПК)	0,3

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 за одиницю)	Кількість одиниць	Максимальна кількість балів
Виконання завдань під час практичних занять	5	15	75
Робота під час семінарських занять	2	9	18
Робота під час лекційних занять	2	19	38
Ведення конспекту лекцій	0,5	19	9
Виконання модульної контрольної роботи	10	4	40
Максимальна кількість балів (середнє арифметичне)			180

Мінімальна кількість балів для допуску до підсумкового контролю 80

Для переведення балів поточного контролю в 100 бальну систему необхідно набрані бали поділити на 2,5

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. Жураковський Б.Ю., Зенів І.О. Комп'ютерні мережі – Київ: КПІ ім. Ігоря Сікорського, 2020. – 336 с.

2. Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А. Комп'ютерні мережі - К.: Компрінт, 2017.- 821с.

3. Захарченко М.В. Інформаційна безпека інформаційно-комунікаційних систем. Захист інформації від НСД у каналах зв'язку: навч. посіб. / М.В. Захарченко, В.В. Топалов, М.С. Русляченко // За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2014. – 228 с.

4. Кібербезпека: сучасні технології захисту. Навчальний посібник для вищих навчальних закладів. / Остапов С.Е., Євсєєв С.П., Король О.Г. – Львів: «Новий світ-2000», 2019. – 678 с.

5. Грайворонський М. В., Новіков О. М. Безпека Інформаційно-комунікаційних систем. – К.: Видавнича група ВНУ, 2009. – 608 с.: іл.

Допоміжна література:

6. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсєєв С. П., Король О. Г.,

Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С.Кузнеця, 2016. – 1013 Мб. ISBN 978-966-676-624-6.

7. Царьов Р.Ю. Структуровані кабельні системи: навч. посіб. для студентів вищих навчальних закладів. / Царьов Р.Ю., Нікітюк Л. А., Резніченко П. І. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 260 с.: іл.

8. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.: іл.

9. С. П. Євсєєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с.

10. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с.

11. Безрук В.М. Інформаційні мережі зв'язку. Ч.1. Математичні основи інформаційних мереж зв'язку. [Текст] / В.М. Безрук, Ю.М. Бідний А.В. Омельченко, під ред. В.М. Безрука, – Харків: ХНУРЕ, 2011. – 292 с.

12. Жураковський Ю.П., Полторац В.П. Теорія інформації та кодування.- К.:ВШ, 2001.-255с.

13. Організація комп'ютерних мереж / Л.М.Олещенко – Київ: КПІ ім.Ігоря Сікорського, 2018. – 225с.

14. Блавацька Н.М. Програмне забезпечення систем захисту інформації: підручник / Н.М.Блавацька, В.Д.Козюра, В.О.Хорошко. – К.: Вид. ДУІКТ, 2011. – 330 с. [Електронний ресурс].

15. Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2014. – 251 с.

16. Буров Є. В. Комп'ютерні мережі: підручник / Євген Вікторович Буров. - Львів: «Магнолія 2006», 2010

17. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. - Львів: «Магнолія 2006», 2013

Адреса розміщення робочої програми навчальної дисципліни:

(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
1.			
2.			

29/31/12 - 1721/01
25.10.24