

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА
СТРАТЕГІЧНИХ КОМУНІКАЦІЙ
ЦЕНТР КІБЕРБЕЗПЕКИ
кафедра безпеки інформаційно-комунікаційних систем

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Безпека розподілених інформаційних ресурсів та хмарні технології»

Освітня програма	Кіберзахист у сфері інформаційних технологій та кіберпросторі
Рівень вищої освіти	другий (магістерський)
Форма здобуття вищої освіти	очна (денна)
Статус навчальної дисципліни	обов'язкова
Мова викладання	українська

Робочу програму навчальної дисципліни розглянуто та схвалено на засіданні кафедри безпеки інформаційно-комунікаційних систем від 15.11.2025 року, протокол № 11.

1. Опис навчальної дисципліни

Показник	Значення показника
Курс	2
Семестр	4
Обсяг (<i>кредити ЄКТС/години</i>)	4 / 120
Кількість змістових модулів	4
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	20
практичні заняття (ПЗ)	20
семінарські заняття (СЗ)	-
самостійна робота (СР)	80
Форма підсумкового контролю (<i>семестр</i>)	<i>Екзамен (4)</i>

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета: підготовка фахівців, які володіють методами побудови розподілених інформаційно-комунікаційних систем і середовищ та принципами утворення обчислювальних систем прикладного значення, а також підходами до роботи з хмарними сервісами

Завдання:

- ознайомлення здобувачі вищої освіти із основним положенням побудови розподілених систем та середовищ;
- формування навичок реалізації та супроводу розподілених систем та хмарних сервісів;
- оволодіння протоколами захисту при організації зв'язку;
- оволодіння методами забезпечення синхронізації в системах;
- оволодіння теорією та методами організації обчислювальних процесів.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Безпека розподілених інформаційних ресурсів та хмарні технології» спрямована на досягнення результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної програми «Кіберзахист у сфері інформаційних технологій та кіберпросторі» (від 11.09.2024 №29/3/1/1-1276/ві), а саме:

ПРН-01	Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.
ПРН-07	Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.
ПРН-09	Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов'язаних з викликами глобальній, європейській та регіональній безпеці.
ПРН-18	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізикоматематичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

ПРН-21	Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
ПРН-23	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
ПРН-24	Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

3. Програма та структура навчальної дисципліни

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>
Семестр 4						
Змістовий модуль №1. БЕЗПЕКА РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ РЕСУРСИ						
Тема 1. Вступ до розподілених інформаційних систем	24	4	-	4	-	16
Лекція 1. Поняття, класифікація, моделі побудови та роль розподілених інформаційних систем в сучасних інформаційних технологіях.	2	2				
Самостійна робота 1. Поняття розподіленого середовища	4					4
Практичне заняття 1. Порівняльна характеристика технологій побудови розподілених систем	2			2		
Самостійна робота 2. Взаємодія компонентів розподіленої системи	4					4
Лекція 2. Архітектурні підходи в розподілених системах	2	2				
Самостійна робота 3. Клієнт–сервер, багаторівнева архітектура, мікросервіси, P2P	4					4
Практичне заняття 2. Дослідження роботи мережевих протоколів у розподіленому середовищі	2			2		
Самостійна робота 4. Мережеві протоколи у розподіленому середовищі	4					4
Тема 2. Безпека розподілених інформаційних систем	36	6	-	6	-	24
Лекція 3. Основи безпеки розподілених інформаційних ресурсів	2	2				
Самостійна робота 5. Класифікація загроз, моделі атак, базові методи захисту	4					4
Практичне заняття 3. Побудова базової моделі загроз для розподіленої системи	2			2		
Самостійна робота 6. Відмовостійкість, балансування навантаження, точки відмови, затримки.	4					4
Лекція 4. Розробка механізмів захисту	2	2				
Самостійна робота 7. Керування захистом в розподілених системах.	4					4
Практичне заняття 4. Багаторівнева організація механізмів захисту	2			2		
Самостійна робота 8. Фокус-керування та розподіл механізмів захисту	4					4

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>
Лекція 5. Керування ризиками та оцінка надійності розподілених систем	2	2				
Самостійна робота 9. Ризики та оцінки надійності розподілених систем	4					4
Самостійна робота 10. Підготовка до модульної контрольної роботи №1	2			2		
Практичне заняття 5. Модульна контрольна робота №1	4					4
Всього годин за змістовий модуль 1	60	10	-	10	-	40
Змістовий модуль №2. ХМАРНІ ТЕХНОЛОГІЇ ТА БЕЗПЕКА ХМАРНИХ СЕРЕДОВИЩ						
Тема 3. Хмарні технології	36	6	-	6	-	24
Лекція 6. Архітектура хмарних платформ	2	2				
Самостійна робота 11. Принципи, сервіси та моделі взаємодії хмарних платформ	4					4
Практичне заняття 6. Правові та нормативні вимоги до захисту даних у хмарі.	2			2		
Самостійна робота 12. Загрози порушення конфіденційності, доступності, цілісності	4					4
Лекція 7. Організація обчислень в хмарних середовищах	2	2				
Самостійна робота 13. Хмарні обчислення	4					4
Практичне заняття 7. Програмні рішення та забезпечення безпеки в Грід	2			2		
Самостійна робота 14. Програмування і особливості планування хмарних технологій	4					4
Лекція 8. Інструменти розробки та керування хмарними сервісами	2	2				
Самостійна робота 15. Платформа Windows Azure	4					4
Практичне заняття 8. Сумісність проміжного програмного забезпечення хмарних технологій	2			2		
Самостійна робота 16. Архітектура та стандарти побудови хмарних технологій	4					4
Тема 4. Безпека хмарних середовищ	24	4	-	4	-	16
Лекція 9. Засоби безпеки хмарних середовищ від мережеских атак	2	2				
Самостійна робота 17. Аналіз мережевого трафіку	4					4
Практичне заняття 9. Відкриті систем виявлення та запобігання вторгненням вторгнень	2			2		
Самостійна робота 18. Системи виявлення та запобігання вторгненням вторгнень	4					4
Лекція 10. Вразливості хмарних обчислень та SDN	2	2				
Самостійна робота 19. Вразливості хмарних обчислень та SDN	4					4
Самостійна робота 20. Підготовка до модульної контрольної роботи №2	4					4
Практичне заняття 10. Модульна контрольна робота №2	2			2		
Всього годин за змістовий модуль 2	60	10	-	10	-	40
Підсумковий контроль – <i>екзамен</i>						
Всього годин за навчальну дисципліну	120	20	-	20	-	80

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 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. 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 здобувачів вищої освіти новою інформацією.

Методи активізації навчального процесу:

- мозкові атаки – метод розв'язання невідкладних завдань, сутність якого полягає в тому, щоб висловити якомога більшу кількість ідей за дуже обмежений проміжок часу, обговорити і здійснити їх селекцію;

- кейс-метод – розгляд, аналіз конкретних ситуацій, який дає змогу наблизити процес навчання до реальної практичної діяльності;

- презентації – виступи перед аудиторією, що використовуються для представлення певних досягнень, результатів роботи групи, звіту про виконання індивідуальних завдань тощо.

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 К
Робота на лекціях	1	10	10
Виконання завдань під час практичних занять	5	8	40
Виконання модульної контрольної роботи	10	2	20
Максимальна кількість балів			70

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. Дорогий Я.Ю. Захист розподілених баз даних та інформаційних систем: навч.-наук. посіб. ДонНТУ, 2024, 312с.
2. Смирнов С А. Хмарні технології обробки даних : навч.-метод. посібник КПІ ім. Ігоря Сікорського, 2022. 168 с.
3. Кавун С.В., Носов В.В., Манжай О.В. Інформаційна безпека: навчальний посібник ХНЕУ, 2023, 369с.
4. Кожевніков Г. К. Хмарні технології: Навч. посібник. – Харків: Нац. техн. ун-т "Харків. політехн. ін-т"., 2023. 113 с.

Додаткова література:

5. Юрчишин В.Я. Хмарні та грид технології: підручник. – КПІ ім. Ігоря Сікорського, 2019. 263с.
6. Дорогий Я.Ю. Безпека та захист операційних систем: навч.-наоч. посіб. ДонНТУ, 2023, 262с.
7. Єфіменко А.А. Основи побудови локальних комп'ютерних мереж: навч.-наук. посіб. Житомирська політехніка, 2024, 113с.
8. Бурячок В.Л., Киричок Р. В.Складаний П. М. Основи інформаційної та кібернетичної безпеки: Київ КУ ім. Грінченка, 2025, 256с.
9. Гапак О. М., Захист інформації в комп'ютерних системах: Ужгород УНУ, 2023, 187с.

Адреса розміщення робочої програми навчальної дисципліни:

<https://moodle.nasbu.edu.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
1.			
2.			
3.			
4.			
5.			
...			