МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ «РІВНЕНСЬКИЙ ФАХОВИЙ КОЛЕДЖ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ»
Циклова комісія *програмування та інформаційних дисциплін*

ЗАТВЕРДЖУЮ
Заступник директора з навчальної роботи
29 серпня 2025 р.
Людмила БАЛДИЧ

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЛІЦЕНЗУВАННЯ І СЕРТИФІКАЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

освітньо-професійна програма — *Кібербезпека та захист інформацій*
(назва освітньо-професійної програми)

галузь знань — *12 Інформаційні технології*
(шифр і назва напряму підготовки)

спеціальність — *125 Кібербезпека та захист інформацій*
(шифр і назва спеціальності)

відділення — *Інформаційних технологій*
(назва відділення)

Рівне – 2025 рік

Програму навчальної дисципліни *Ліцензування і сертифікація програмного забезпечення* розроблено на основі освітньо-професійної програми «Кібербезпека та захист інформацій » для здобувачів освіти освітньо-професійного ступеня «Фаховий молодший бакалавр» галузі знань *12 Інформаційні технології*, спеціальності *125 Кібербезпека та захист інформацій*, затвердженої Вченою радою НУБіП України від 26.04.2023 р. № 10.

Розробник: Черняк Вадим Андрійович, викладач програмування та інформаційних дисциплін, спеціаліст.

Програма навчальної дисципліни затверджена на засіданні циклової комісії *програмування та інформаційних дисциплін*

Протокол від *29 серпня* 2025 року № *1*

Голова циклової комісії *програмування та інформаційних дисциплін*

29 серпня 2025 року _____ *Павло СТРИК*
(підпис) (ім'я та прізвище)

Погоджено методичною радою ВСП «РФК НУБіП України»

Протокол від *29 серпня* 2025 року № *1*

29 серпня 2025 року Голова _____ *Людмила БАЛДИЧ*
(підпис) (ім'я та прізвище)

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Галузь знань, напрям підготовки, спеціальність, освітньо-професійний ступінь		
Освітньо-професійний ступінь	Фаховий молодший бакалавр	
Галузь знань	12 Інформаційні технології	
Спеціальність	125 Кібербезпека та захист інформацій	
Характеристика навчальної дисципліни		
Вид	обов'язкова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
Мова викладання, навчання та оцінювання	українська	
Форма контролю	залік	
Показники навчальної дисципліни для денної та заочної форм навчання		
Форма навчання	денна	
Рік підготовки, навчальний рік	IV, 2025-2026	
Семестр	8	
Аудиторні години:	44	
лекційні	34	
практичні	10	
семінарські	-	
Самостійна робота	76	
Кількість тижневих годин для денної форми навчання	2,5	

1. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни «Ліцензування і сертифікація програмного забезпечення» є формування у здобувачів освіти знань, умінь і навичок щодо організації, проведення, нормативно-правового забезпечення та практичної реалізації процесів ліцензування і сертифікації засобів технічного, програмного та криптографічного захисту інформації.

Студенти повинні оволодіти принципами, методами й інструментами, що забезпечують відповідність засобів захисту інформації чинним державним, галузевим та міжнародним стандартам, а також навчитися застосовувати їх у професійній діяльності в галузі інформаційної та кібербезпеки.

Основними завданнями вивчення дисципліни «Ліцензування та сертифікація програмного забезпечення» є формування у здобувачів освіти знань і практичних навичок щодо: застосування нормативно-правових актів та державних стандартів у сфері ліцензування і сертифікації засобів технічного, програмного та криптографічного захисту інформації; розуміння етапів і процедур проведення сертифікації засобів захисту інформації, включаючи підготовку технічної документації та проведення випробувань; ознайомлення з порядком ліцензування господарської діяльності, пов’язаної із захистом інформації, відповідно до законодавства України; застосування сертифікованих засобів у комплексних системах захисту інформації з урахуванням чинної політики інформаційної та кібербезпеки.

Згідно з вимогами освітньо-професійної програми студенти повинні:

Знати:

- законодавчу та нормативно-правову базу України у сфері ліцензування і сертифікації засобів технічного, програмного та криптографічного захисту інформації;
- порядок та умови ліцензування господарської діяльності, пов’язаної із захистом інформації;
- етапи, процедури та учасників процесу сертифікації засобів захисту інформації, а також вимоги до них;
- державні стандарти (ДСТУ), нормативні документи системи технічного захисту інформації (НД ТЗІ), міжнародні стандарти (ISO/IEC серій 27000, 15408 *Common Criteria*, 17065 тощо);
- вимоги до технічної, експлуатаційної та супровідної документації на засоби захисту інформації;
- структуру та функції органів сертифікації, випробувальних лабораторій і регуляторних органів у сфері інформаційної безпеки;
- принципи оцінювання відповідності, аудиту та перевірки сертифікованих засобів захисту;

- значення сертифікації для забезпечення надійності, стійкості та безперервності інформаційних систем;
- основи управління життєвим циклом сертифікованих засобів і порядок оновлення сертифікатів відповідності.

Вміти:

- аналізувати нормативно-правові документи, що регулюють процеси ліцензування і сертифікації у сфері інформаційної безпеки;
- визначати вимоги до засобів захисту інформації згідно з національними та міжнародними стандартами;
- готувати пакет документів для проходження процедур ліцензування та сертифікації;
- розробляти технічні завдання, програми та методики випробувань засобів захисту інформації;
- оцінювати відповідність засобів захисту інформації нормативним вимогам і критеріям безпеки;
- складати протоколи, звіти та експертні висновки за результатами випробувань і перевірок;
- використовувати сертифіковані засоби технічного, програмного та криптографічного захисту при розробці або модернізації систем інформаційної безпеки;
- проводити аудит відповідності засобів і систем вимогам безпеки;
- здійснювати оцінку ризиків і визначати доцільність сертифікації засобів у конкретних інформаційних системах;
- впроваджувати рекомендації аудиту з метою підтримання сертифікованого статусу системи захисту інформації.

Очікувані результати навчання.

Після вивчення дисципліни «Ліцензування і сертифікація засобів захисту інформації» у здобувачів освіти формуються такі **компетентності:**

Фахові:

ФК01. 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.

ФК04. Здатність забезпечувати неперервність бізнесу згідно зі встановленої політики інформаційної та/або кібербезпеки.

ФК09. Здатність здійснювати професійну діяльність та впроваджувати системи управління інформаційною та/або кібербезпекою.

Програмні результати навчання.

ПР02. Знати національні та міжнародні стандарти, регулюючі акти виявлення, ідентифікації, аналізу та реагування на інциденти в сфері інформаційної безпеки та/ або кібербезпеки.

ПР16. Вміти вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків.

ПР17. Вміти вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

1. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1. ЛІЦЕНЗУВАННЯ ТА ПРАВОВА ОХОРОНА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Тема 1. Вступ. Основні поняття та визначення

Предмет і завдання дисципліни. Поняття ліцензування і сертифікації у сфері інформаційної безпеки. Якість програмних засобів протягом життєвого циклу. Ключові поняття: ліцензія, сертифікат, експертиза, відповідність. Законодавчі акти України у сфері захисту інформації.

Тема 2. Комп'ютерна програма як об'єкт авторського права

Комп'ютерна програма як об'єкт правової охорони. Реєстрація авторського права. Поняття службового твору. Трудовий договір і питання авторства, співавторства. Майнові та немайнові авторські права. Механізм захисту прав розробників програмного забезпечення.

Тема 3. Авторські договори та вільне використання програмного забезпечення

Види авторських договорів. Передача майнових прав. Використання програмного забезпечення без згоди автора: випадки, межі, відповідальність. Особливості вільного використання програм у навчальних, наукових і службових цілях.

Тема 4. Ліцензування програмного забезпечення та моделі відкритості

Правова охорона програмного забезпечення. Види ліцензій на програмні продукти. Моделі відкритості програмного забезпечення (Open Source, Freeware, Shareware). Ознаки, що визначають ліцензійне програмне забезпечення. Програми ліцензування і засоби перевірки легальності використання ПЗ.

Змістовий модуль 2. СЕРТИФІКАЦІЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

Тема 5. Основи сертифікації у сфері інформаційної безпеки

Поняття, сутність і мета сертифікації. Нормативна база України щодо сертифікації. Основні організаційно-методичні документи, що регламентують вимоги до сертифікації засобів захисту інформації. Порядок проведення сертифікаційних робіт.

Тема 6. Документація для сертифікації програмних засобів

Переліки, форми та зміст документів, необхідних для сертифікації. Каталоги нормативних документів. Вимоги до технічної, експлуатаційної та супровідної документації. Підготовка документів до подання на сертифікацію.

Тема 7. Суб'єкти експертизи та процедура оцінки відповідності

Учасники процесу сертифікації: заявник, орган сертифікації, випробувальна лабораторія, експерт. Поняття експертного висновку. Сертифікати відповідності та якості. Декларація про відповідність. Технічні регламенти та їх роль у сертифікації інформаційних систем.

Тема 8. Порядок сертифікації програмних засобів та інформаційних ресурсів

Покроковий процес сертифікації: подання заявки, перевірка, експертиза, тестування, видача сертифіката. Оцінка об'єктів інтелектуальної власності під час сертифікації. Особливості сертифікації засобів технічного, криптографічного та програмного захисту інформації.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№	Назви змістових модулів і тем	Кількість годин			
		денна форма			
		всього	лекційні	практичні	самостійне вивчення
Змістовий модуль 1. ЛІЦЕНЗУВАННЯ ТА ПРАВОВА ОХОРОНА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ					
Тема 1	Вступ. Основні поняття та визначення	12	4	-	8
Тема 2	Комп'ютерна програма як об'єкт авторського права	14	4	-	10
Тема 3	Авторські договори та вільне використання програмного забезпечення	16	4	2	10
Тема 4	Ліцензування програмного забезпечення та моделі відкритості	20	6	2	12
	Разом за змістовим модулем 1	**62**	**18**	**4**	**40**
Змістовий модуль 2. СЕРТИФІКАЦІЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ					
Тема 5	Основи сертифікації у сфері інформаційної безпеки	14	4	2	8
Тема 6	Документація для сертифікації програмних засобів	14	4		10
Тема 7	Суб'єкти експертизи та процедура оцінки відповідності	14	4	2	8
Тема 8	Порядок сертифікації програмних засобів та інформаційних ресурсів	16	4	2	10
	Разом за змістовим модулем 2	**58**	**16**	**6**	**36**
Всього годин		**120**	**34**	**10**	**76**

5. ТЕМИ ЛЕКЦІЙНИХ, ПРАКТИЧНИХ ЗАНЯТЬ ТА ЗМІСТ САМОСТІЙНОГО ВИВЧЕННЯ

№ теми	№ занят-тя	Вид навчальної діяльності	Назва теми	Кількість годин
IIIV семестр				**120** 34/10/76
Змістовий модуль 1. ЛІЦЕНЗУВАННЯ ТА ПРАВОВА ОХОРОНА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ				**62**
1	***Вступ. Основні поняття та визначення***			**12**
	1	лекція 1	Вступ до дисципліни. Предмет вивчення та завдання дисципліни. Поняття ліцензування і сертифікації у сфері інформаційної безпеки.	2
		самостійне вивчення	Законодавчі акти України у сфері захисту інформації.	4
		лекція 2	Якість програмних засобів протягом життєвого циклу. Ключові поняття: ліцензія, сертифікат, експертиза, відповідність.	2
		самостійне вивчення	Ознайомитись із Законом України «Про захист інформації в інформаційно-телекомунікаційних системах», Законом України «Про авторське право і суміжні права», Законом України «Про технічні регламенти та оцінку відповідності».	4
2	***Комп'ютерна програма як об'єкт авторського права***			**14**
	2	лекція 3	Комп'ютерна програма як об'єкт правової охорони.	2
		самостійне вивчення	Реєстрація авторського права. Поняття службового твору.	6
		лекція 4	Трудовий договір і питання авторства, співавторства. Майнові та немайнові авторські права.	2
		самостійне вивчення	Механізм захисту прав розробників програмного забезпечення.	4
3	***Авторські договори та вільне використання програмного забезпечення***			**4**
	3	лекція 5	Види авторських договорів. Передача майнових прав.	2
		самостійне вивчення	Об'єкти інтелектуальної власності у сфері інформаційних технологій та інформаційної безпеки, правові механізми передачі майнових прав	2
	4	практична робота 1	Порядок реєстрації авторського права на комп'ютерну програму. Підготовка та заповнення основних документів для подання заявки.	
	5	лекція 6	Використання програмного забезпечення без згоди автора: випадки, межі, відповідальність.	
		самостійне вивчення	Особливості вільного використання програм у навчальних, наукових і службових цілях.	
4	***Ліцензування програмного забезпечення та моделі відкритості***			**20**
	6	лекція 7	Правова охорона програмного забезпечення. Види ліцензій на програмні продукти	2
		самостійне	Механізмами захисту прав розробників та	6

№ теми	№ занят-тя	Вид навчальної діяльності	Назва теми	Кількість годин
		вивчення	користувачів ПЗ.	
	7	лекція 8	Моделі відкритості програмного забезпечення (Open Source, Freeware, Shareware). Ознаки, що визначають ліцензійне програмне забезпечення.	2
	8	практична робота 2	Дослідження видів ліцензій на програмні продукти. Аналіз умов використання відкритого та комерційного ПЗ.	2
	9	лекція 9	Програми ліцензування і засоби перевірки легальності використання ПЗ.	2
		самостійне вивчення	Особливостей українського та міжнародного законодавства у сфері правової охорони ПЗ.	6
Змістовий модуль 2. СЕРТИФІКАЦІЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ				**22**
5	***Основи сертифікації у сфері інформаційної безпеки***			**14**
	10	лекція 10	Поняття, сутність і мета сертифікації. Нормативна база України щодо сертифікації.	2
		самостійне вивчення	основні принципи сертифікації у сфері інформаційної безпеки, законодавча та нормативна бази України.	4
	11	лекція 11	Основні організаційно-методичні документи, що регламентують вимоги до сертифікації засобів захисту інформації.	2
	12	практична робота 3	Підготовка пакета документів для сертифікації програмного продукту. Створення заяви, технічного опису, декларації про відповідність.	2
		самостійне вивчення	Порядок проведення сертифікаційних робіт.	4
6	***Документація для сертифікації програмних засобів***			**14**
	13	лекція 12	Переліки, форми та зміст документів, необхідних для сертифікації.	2
		самостійне вивчення	Каталоги нормативних документів.	4
		лекція	Підготовка документів до подання на сертифікацію.	2
		самостійне вивчення	Вимоги до технічної, експлуатаційної та супровідної документації.	4
7	***Суб'єкти експертизи та процедура оцінки відповідності***			**14**
	14	лекція 13	Учасники процесу сертифікації: заявник, орган сертифікації, випробувальна лабораторія, експерт.	2
		самостійне вивчення	Поняття експертного висновку	4
		лекція 14	Сертифікати відповідності та якості. Декларація про відповідність.	2
	9	самостійне вивчення	Технічні регламенти та їх роль у сертифікації інформаційних систем.	4
	15	практична робота 4	Аналіз документів сертифікації: сертифікати відповідності, декларації про відповідність та технічні регламенти у сфері захисту інформації	2
8	***Порядок сертифікації програмних засобів та інформаційних ресурсів***			**16**

№ теми	№ занят-тя	Вид навчальної діяльності	Назва теми	Кількість годин
		лекція15	Покроковий процес сертифікації: подання заявки, перевірка, експертиза, тестування, видача сертифіката.	2
		самостійне вивчення	Оцінка об’єктів інтелектуальної власності під час сертифікації.	5
		лекція16	Особливості сертифікації засобів технічного, криптографічного та програмного захисту інформації.	2
		самостійне вивчення	порядок проведення сертифікації у сфері технічного, криптографічного та програмного захисту інформації; основні вимоги, процедури та органи, що здійснюють сертифікацію відповідних засобів.	5
	16	практична робота 5	Оцінка результатів експертизи програмного засобу та складання сертифіката відповідності. Аналіз прикладів сертифікованих засобів захисту інформації.	2
			Всього	**120**

6. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Індивідуально-консультативна робота виконується за графіком у таких формах: індивідуальні заняття, консультації, перевірка виконання курсової роботи та індивідуальних завдань і захист результатів їх виконання тощо.

Формами організації індивідуально-консультативної роботи є:

а) консультації з теоретичного матеріалу:

- інтерактивне спілкування (питання-відповідь);
- групові (розгляд типових завдань);
- диспути (обговорення вирішення типових питань);

б) індивідуальні та групові консультації з освоєння практичного матеріалу;

в) індивідуальна здача та захист виконаних курсових робіт для комплексної оцінки ступеня оволодіння програмним матеріалом.

7. ПЕРЕЛІК ПИТАНЬ НА ЗАЛІК

1. Предмет і завдання навчальної дисципліни «Ліцензування і сертифікація засобів захисту інформації».
2. Поняття ліцензування у сфері інформаційної безпеки.
3. Поняття сертифікації у сфері інформаційної безпеки.
4. Мета і завдання ліцензування засобів захисту інформації.
5. Основні етапи процесу ліцензування програмного забезпечення.
6. Законодавча база України у сфері ліцензування діяльності з технічного захисту інформації.
7. Роль Державної служби спеціального зв’язку та захисту інформації України (ДССЗЗІ) у сфері ліцензування.
8. Види ліцензій на програмні продукти.
9. Поняття авторського права на програмне забезпечення.
10. Майнові та немайнові права автора програмного продукту.
11. Види авторських договорів у сфері розроблення програмного забезпечення.
12. Умови передачі майнових прав на програмне забезпечення.
13. Поняття легального та неліцензованого програмного забезпечення.
14. Ознаки, що визначають ліцензійне програмне забезпечення.
15. Програми ліцензування і засоби перевірки легальності використання ПЗ.
16. Поняття і роль сертифікації у забезпеченні інформаційної безпеки.
17. Основні етапи проведення сертифікації засобів захисту інформації.
18. Види сертифікації в Україні.
19. Суб’єкти процесу сертифікації та їх повноваження.
20. Нормативна база України щодо сертифікації засобів захисту інформації.
21. Технічні регламенти та їх роль у сертифікації інформаційних систем.
22. Поняття «сертифікат відповідності» та «декларація про відповідність».
23. Вимоги до документації, що подається на сертифікацію.
24. Порядок оформлення сертифіката відповідності.

25. Права та обов’язки заявника при проведенні сертифікації.
26. Відмінності між обов’язковою та добровільною сертифікацією.
27. Особливості сертифікації засобів технічного захисту інформації.
28. Поняття технічних каналів витоку інформації.
29. Сертифікація засобів криптографічного захисту інформації.
30. Порядок проведення експертизи засобів криптографічного захисту.
31. Особливості сертифікації програмних засобів захисту інформації.
32. Вимоги до програмних засобів захисту при сертифікації.
33. Роль акредитованих лабораторій у процесі сертифікації.
34. Структура сертифікаційного випробування.
35. Поняття «експертний висновок» у процесі сертифікації.
36. Контроль за дотриманням вимог після отримання сертифіката відповідності.
37. Підстави для анулювання сертифіката відповідності.
38. Взаємозв’язок між ліцензуванням і сертифікацією засобів захисту інформації.
39. Роль стандартів ДСТУ та ISO/IEC у сертифікації засобів захисту інформації.
40. Міжнародна система сертифікації Common Criteria (ISO/IEC 15408).
41. Поняття рівня довіри до засобів захисту інформації (EAL).
42. Міжнародна практика сертифікації програмного забезпечення.
43. Відповідальність за порушення законодавства у сфері ліцензування і сертифікації.
44. Захист авторських прав на програмні продукти в Україні.
45. Відмінність між відкритими та закритими моделями програмного забезпечення (Open Source, Freeware, Shareware).
46. Сутність концепції відкритого коду (Open Source License).
47. Особливості використання вільного програмного забезпечення у сфері інформаційної безпеки.
48. Етапи життєвого циклу програмного забезпечення та його якість.
49. Вимоги до забезпечення якості програмних засобів протягом життєвого циклу.
50. Значення ліцензування і сертифікації у побудові комплексної системи захисту інформації.

8. МЕТОДИ НАВЧАННЯ

Під час вивчення дисципліни «Ліцензування і сертифікація засобів захисту інформації» у навчальному процесі застосовуються такі методи навчання: розповідь, бесіда, проблемні лекції, пояснення, демонстрація, ілюстрація, навчальна дискусія, диспут, мозкові атаки, робота в малих групах, кейс-метод, самостійне виконання практичних завдань, розв’язування задач, виконання вправ.

9. КОНТРОЛЬ РЕЗУЛЬТАТІВ НАВЧАННЯ

9.1. Форми та засоби поточного і підсумкового контролю

Контроль знань студентів здійснюється за модульно-рейтинговою системою.

Засобами діагностики та методами демонстрування результатів навчання здобувачів освіти з дисципліни є:

- індивідуальне опитування, фронтальне опитування;
- модульні контрольні робот у формі тестування;
- презентація дослідження за темою курсової роботи;
- звіти з виконання практичних робіт;
- комплексна контрольна робота;
- залік
- екзамен.

Зміст курсу дисципліни «Ліцензування і сертифікація програмного забезпечення» поділений на 2 змістових модулів. Кожний модуль включає в себе лекції, практичні заняття та самостійну роботу студентів і завершуються рейтинговим контролем рівня засвоєння знань програмного матеріалу відповідної частини курсу.

У змістовий модуль 1 (ЗМ1) входять теми 1-4, у змістовий модуль 2 (ЗМ2) – теми 5-8.

Після завершення відповідно змістового модуля проводяться ***модульні контрольні роботи*** **(МК)**. До модульної контрольної роботи допускаються студенти, які опрацювали весь обсяг теоретичного матеріалу в т. ч і матеріал самостійно, виконали практичні (практичні, графічні, розрахункові) роботи, відпрацювали семінарські заняття.

Рейтингову кількість балів студента формують бали, отримані за модульні контрольні роботи, які проводяться у формі тестування, та середній рейтинг виконання практичних (практичні, графічні, розрахункові) робіт і відпрацювання семінарських занять.

Участь студентів в контрольних заходах обов'язкова. МК проводиться у письмовій тестовій формі, тестові завдання обов’язково включають матеріал, який передбачено до самостійного опрацювання студентами. Студент, який не виконав вимоги щодо самостійної роботи чи будь якого іншого виду навчальної діяльності, не допускається до складання МК і даний модуль йому не зараховується.

Семестрові бали (семестровий рейтинг) студент отримує як середнє арифметичне балів змістових модулів з усіх тем п’ятьох змістових модулів:

Оцінка навчальної успішності студентів здійснюється під час семестрового оцінювання у формі екзамену, який передбачає виконання тестових завдань та вирішення практичного завдання.

9.2. Критерії оцінювання результатів начиння

Критерії оцінювання модульної контрольної роботи, директорської контрольної роботи, усних і письмових відповідей на питання, виконання практичних занять доповідей на семінарських заняттях, (виконання курсових робіт) – від 0 до 50 балів:

- глибоке, теоретично обґрунтоване розкриття питання; розрахунки, зроблені без помилок, проведено повний аналіз, відображена власна позиція – **48-50 балів**;
- обґрунтоване розкриття питання чи/та розрахунки, зроблені з незначними неточностями, які істотно не впливають на правильність відповіді – **45-47 балів**;
- відповідь не дає повного розкриття питання, не проведено повний аналіз результатів розрахунків, немає власної позиції – **42-44 балів**;
- неповне розкриття питання, доведені до завершення розрахунки але не зроблено їх аналіз; загалом наявні достатні знання – **38-41 балів**;
- питання розкрите фрагментарно, наявні фактологічні помилки під час викладу чи/та помилки під час проведення розрахунків – **34-37 балів**;
- відповідь неповна, наявні суттєві помилки при викладі та проведенні розрахунків **– 30-33 балів**;
- відповідь має значні помилки елементарного рівня – **1-30 бали**;
- відсутність відповіді на питання – **0 балів**.

Оцінювання за формами контролю

Шкала оцінювання

	Заліковий модуль 1	**Заліковий модуль 2**	**Разом**
%	50	50	100
Мінімум	0	0	0
Максимум	50	50	50

Відсоток формування компетентностей та набуття програмних результатів навчання	**Рейтинг за п'ятдесятибальною шкалою**	**Оцінка за п'ятибальною шкалою**	**Запис у заліковій книжці студента та відомості**
96-100	48, 49, 50	5	відмінно
90-95	45, 46, 47	5	відмінно
84-89	42, 43, 44	4	добре
75-83	38, 39, 40, 41	4	добре
67-74	34, 35, 36, 37	3	задовільно
60-66	30, 31, 32, 33	3	задовільно
менше 60	0-29	2	незадовільно

10. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

1. Витяг з навчального плану
2. Програма навчальної дисципліни
3. Плани занять

4. Конспект лекцій з дисципліни
5. Питання до модульних контрольних робіт
6. Питання до заліку
7. Залікові білети
8. Навчальний посібник
9. Роздавальний матеріал
10. Презентації до тем

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Гребенюк А. М., Рибальченко Л. В. *Основи управління інформаційною безпекою: навч. посібник* – Дніпро: Дніпроп. держ. ун-т внутр. справ, 2020. – 144 с. er.dduvs.edu.ua
2. Рибальський О. В., Хахановський В. Г., Кудінов В. А. *Основи інформаційної безпеки та технічного захисту інформації: посібник для курсантів ВНЗ МВС України* – Київ: Нац. акад. внутр. справ, 2012. – 104 с. nnipd.navs.edu.ua
3. Вишняков В. М. *Захист інформації в комп'ютерних системах: навч. посібник* – Київ: КНУБА, 2022. – 120 с. Repositary KNUBA
4. Лужецький В. А., Северин Л. І., Гульчак Ю. П., Кожухівський А. Д. *Основи організаційного захисту інформації: навч. посібник* – Вінниця: ВНТУ, 2005. – 148 с. VNTU Repository+1
5. Тарнавський Ю. А. *Технології захисту інформації: підручник* – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с. ELAKPI
6. Кавун С. В. *Інформаційна безпека: навч. посібник* – Харків: (вид-во), 2008. – (кількість с. не вказано) HNEU Repository
7. Ахрамович В. М., Чегренець В. М., Котенко А. М. *Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності: навч. посібник* – Київ: ДУТ, 2018. – 412 с.