

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
Кафедра комп'ютерних технологій та інформаційної безпеки

Код за ОПП:

ОК8

“ЗАТВЕРДЖУЮ”

Проректор з науково-педагогічної
роботи, к.т.н., доцент



С.О. Слободян

» 2025 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Program of the Discipline

**ІНФОРМАЦІЙНА І КІБЕРБЕЗПЕКА СПЕЦІАЛІЗОВАНИХ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ НА
ВОДНОМУ ТРАНСПОРТІ**

**The information and cyber security of information and
communication systems on water transport**

Рівень вищої освіти	<u>другий (магістерський)</u>
Тип дисципліни	<u>обов'язкова</u>
Мова викладання	<u>українська</u>

Миколаїв 2025 рік

Робоча програма навчальної дисципліни «Інформаційна і кібербезпека спеціалізованих інформаційно-комунікаційних систем на водному транспорті» є однією із складових підготовки студентів, що навчаються за освітньою програмою ОПП «Системи технічного захисту інформації, автоматизація її обробки», спеціальності «F5 Кібербезпека та захист інформації», галузі знань «F Інформаційні технології»

Розробник: Сірівчук А.С., доцент кафедри комп'ютерних технологій та інформаційної безпеки, канд. техн. наук, доцент

Проект робочої програми навчальної дисципліни «Інформаційна і кібербезпека спеціалізованих інформаційно-комунікаційних систем на водному транспорті» узгоджено з гарантом освітньої програми.

Гарант освітньої програми «Системи технічного захисту інформації, автоматизація її обробки»

Передерій В.І., д. т. н

Проект робочої програми навчальної дисципліни «Інформаційна і кібербезпека спеціалізованих інформаційно-комунікаційних систем на водному транспорті» розглянуто на засіданні кафедри КТІБ.

Протокол від « 24 » 04 2025 р. № 12

Завідувач кафедри КТБ, к.т.н., доцент Нужний С.М.

Проект робочої програми навчальної дисципліни «Інформаційна і кібербезпека спеціалізованих інформаційно-комунікаційних систем на водному транспорті» розглянуто методичною радою Навчально-наукового інституту автоматики та електротехніки.

Протокол від « 15 » 05 2025 р. № 5

Заступник голови МР ННІАЕ, к.т.н., доц. Новогрецький С.М.

Проект робочої програми навчальної дисципліни «Інформаційна і кібербезпека спеціалізованих інформаційно-комунікаційних систем на водному транспорті» погоджено з навчальним відділом

Начальник відділу к.т.н., доцент Лабарткава А.В.

Робоча програма навчальної дисципліни «Інформаційна і кібербезпека спеціалізованих інформаційно-комунікаційних систем на водному транспорті» затверджена Навчально-методичною радою НУК

Протокол № 5 від « 21 » 05 2025 року.

Голова Навчально-методичної ради НУК ім. адм. Макарова,
к.т.н., доцент Слободян С.О.

ЗМІСТ

Вступ	4
1. Опис навчальної дисципліни	5
2. Мета вивчення навчальної дисципліни	6
3. Передумови для вивчення дисципліни	7
4. Очікувані результати навчання	7
5. Програма навчальної дисципліни	9
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування	13
7. Форми поточного і підсумкового контролю	14
8. Критерії оцінювання результатів навчання	16
9. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна	18
10. Рекомендовані джерела інформації	18
Зміни та доповнення	22

ВСТУП

Анотація

Південний регіон України є її морськими воротами – транспортним вузлом, що забезпечує основну частину товарообігу держави. Порти Одеської, Миколаївської та Херсонської областей на Чорному морі за останнє десятиріччя збільшили об'єми переробки вантажів майже вдвічі. І це на тлі агресії Росії.

Другим важливим елементом економіки південного регіону є енергетична сфера – нафто-газові родовища на українському шельфі Чорного моря (родовища Дельфін, Одеське, Зміїне та інші).

Безпека водно-транспортного комплексу, критичних елементів його інфраструктури та інфраструктури енергетичного комплексу в значній мірі визначає економічну, енергетичну та військову безпеку держави.

Світовий досвід показує, що питання інформаційної та кібербезпеки для водно-транспортного та енергетичного комплексів є однією з найневищених задач. Програмою передбачається, за умови отримання студентами відповідної форми допуску до ІзОД, ознайомлення слухачів з документами категорії ДСК та «Т».

Ключові слова: комплексна система захисту інформації, модель загроз, модель каналу витоку інформації

Abstract

The southern region of Ukraine is its sea gate – a transport hub that provides the main part of the country's trade. Over the last decade, the ports of Odesa, Mykolaiv and Kherson regions on the Black Sea have almost doubled the volume of cargo processing. And this against the background of Russia's aggression.

The second important element of the economy of the southern region is the energy sphere – oil and gas fields on the Ukrainian shelf of the Black Sea (Delphin, Odeske, Zmiine and other).

The security of the water transport complex, critical elements of its infrastructure and the infrastructure of the energy complex largely determines the economic, energy and military security of the state.

World experience shows that the issue of information and cyber security for water transport and energy complexes is one of the most unresolved problems.

Keywords: complex information protection system, threat model, information leakage channel model, restricted information, object of information activity

1 Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 4	Галузь знань F Інформаційні технології Спеціальність: F5 Кібербезпека та захист інформації	Обов’язкова	
Модулів – 1	Освітня програма «Системи технічного захисту інформації, автоматизація її обробки»	Рік підготовки	
Змістових модулів – 2		1-й	1-й
Загальна кількість годин – 120		Семестр	
		1-й	1-й
Тижневих годин для денної форми навчання: Аудиторних – 3; Сам. роботи – 5.	Рівень вищої освіти: другий (магістерський)	Аудиторні:	
		Лекції, год	
		15	4
		Лабораторні роботи, год	
		15	4
		Практичні роботи, год	
		15	4
		Самостійна робота, год	
		75	104
		Види контролю: екзамен	
		Форма контролю: усна, письмова	

2. Мета та завдання навчальної дисципліни

Метою вивчення навчальної дисципліни «Інформаційна і кібербезпека спеціалізованих інформаційно-комунікаційних систем на водному транспорті» є ознайомлення з методами та засобами захисту інформації і відповідними нормативно-правовими актами в сфері спеціалізованих інформаційно-комунікаційних систем (ІКС) об'єктів морської інфраструктури, особливостями побудови і експлуатації ІКС воднотранспортного комплексу та основним напрямком проведення робіт по забезпеченню кібербезпеки як безпосередньо на об'єктах морської інфраструктури, так і на ІКС воднотранспортного комплексу в цілому, з урахуванням вимог українських та міжнародних нормативних документів.

Вивчення дисципліни повинно забезпечити набуття студентами наступних компетентностей:

Інтегральна компетентність:

Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності:

- ЗК-1 (ЗК.02) – здатність застосовувати знання у практичних ситуаціях;
- ЗК-2 – здатність проводити дослідження на відповідному рівні;
- ЗК-3 (ЗК.04) – здатність до абстрактного мислення, аналізу та синтезу;
- ЗК-4 (ЗК.03) – здатність оцінювати та забезпечувати якість виконуваних робіт;
- ЗК-6 (ЗК.01) – здатність діяти соціально відповідально та громадсько свідомо;

Фахові компетентності:

– КФ-1 (А1) – здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки;

– КФ-3 (А3) – здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури;

– КФ-5 (А2) – здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації;

– КФ-7 – здатність 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;

– КФ-8 (Б) – здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації;

– КФ-9 (В) – здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому;

– КФ-15 (А8) – здатність адмініструвати системи, мережі та системи безпеки інформації;

– КФ-16 (Г1) – здатність проводити оцінку відповідності (держану експертизу) програмних засобів технічного та криптографічного захисту інформації.

3. Передумови для вивчення навчальної дисципліни

Передумов для вивчення навчальної дисципліни «Інформаційна і кібербезпека спеціалізованих інформаційно-комунікаційних систем на водному транспорті» немає.

4. Очікувані результати навчання

Основними (програмними) результатами навчання з дисципліни «Інформаційна і кібербезпека спеціалізованих інформаційно-комунікаційних систем на водному транспорті» є:

– РН-4 (А2.36, А3.31, А3.33, Б2.36, В4.32, Г1.31, Д1.31, А1.У4, А3.У4, В3.У3, Г1.У5) – застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки;

– РН-5 (А2.34, А3.31, В4.33, Г1.31, А1.У4, А3.У5, В1.У4, В3.У1, В4.У3) – критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також

розвитку технологій створення та використання спеціалізованого програмного забезпечення;

- РН-6 (А2.34, Б1.31, Б1.35, Б2.34, Г1.31, А2.У2, Б2.У4, В3.У1, В3.У3, Г1.У3) – аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення;

- РН-7 (А3.35, А3.36, А6.37, В1.33, В4.34, В4.32, Б1.У2, Г2.У3) – обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки;

- РН-10 (А1.35, А1.37, А2.31, Б1.31, Б1.34, В1.31, В2.31, В3.35, Д1.32, А1.У1, А1.У4, В1.У1, В2.У1, В3.У1, В4.У2, В5.У3, Д2.У1) – забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації;

- РН-12 (А1.37, А2.36, В2.31, В2.32, В3.31, В4.33, А1.У4, А2.У2, Б3.У1, В2.У1, В3.У1, В4.У3, Г2.У2, В5.У3) – 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;

- РН-15 (А1.36, Б2.33, Г2.31, Г2.34, А1.У3, Г1.У2, Г1.У3, Г2.У2, Г2.У3, Г2.У4) – зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб;

- РН-16 (А1.35, Б1.31, В1.31, Г1.33, Д1.32, Д2.32, А1.У1, В1.У1, В3.У1, В4.У2, Д1.У3, Д2.У3) – приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень;

- РН-20 (А2.34, А2.36, Б1.31, В1.31, В4.32, Г1.31, Д1.31, А1.У2, А2.У2, В1.У3, В3.У1, В4.У4, Д1.У5) – ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик;

- РН-21 (А2.34, В4.34, А1.У4, А2.У2, В4.У2, В4.У4) – використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки;

- РН-24 (А2.34, Б1.31, В1.31, В4.31, Г1.33, Д1.32, А2.У2, В1.У1, В4.У2, Д2.У4) – приймати обґрунтовані рішення з виконання передпроектних робіт щодо систем та комплексів захисту інформації, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

5. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Безпека воднотранспортного комплексу України. Судно, як об'єкт інформаційної діяльності (ОІД) і загрози його функціонуванню

Тема 1. Безпека воднотранспортного комплексу України.. Основні поняття, визначення, міжнародні та національні вимоги. [1-31,32,34]

Тема 2. Технічний захист інформації на судні [1-31,32,34]

Тема 3. Захист інформації в ІКС на судні. Кібербезпека інформаційних і комунікаційних мереж судна. [1-31,32,34]

Тема 4. Управління інформаційною та кібербезпекою на судні [1-31,32,34]

Змістовий модуль 2. Інформаційна та кібербезпека воднотранспортних шляхів (ВТШ) та систем регулювання рухом суден (СРРС)

Тема 5. Структура ВТШ, характеристика інформаційних потоків, розробка моделі загроз [1-31,32,34]

Тема 6. Розробка моделі загроз, моделі порушника та моделі протидії загрозам, вибір засобів та методів захисту інформації [1-31,32,34]

Тема 7 СРРС як об'єкт інформаційної діяльності. Аналіз інформаційних потоків, аналіз загроз. [1-31,32,34,36]

Тема 8. Інформаційна та кібербезпека в портах. Сучасні тенденції розвитку в галузі інформаційної та кібербезпеки ВТШ [1-31,32,36,37,38]

Назви змістових модулів і тем	Денна форма					Заочна форма				
	Кількість годин									
	усього	у тому числі				усього	у тому числі			
		л	п	лаб	с.р		л	п	лаб	с.р
Модуль 1 (М1)										
Змістовий модуль 1. Архітектура комп'ютерних систем										
Тема 1. Безпека водотранспортного комплексу України.. Основні поняття, визначення, міжнародні та національні вимоги.	15	2	2	-	11	15	-	-	-	15
Тема 2. Технічний захист інформації на судні	15	2	2	3	8	15	2			13
Тема 3. Захист інформації в ІКС на судні. Кібербезпека інформаційних і комунікаційних мереж судна.	15	2	2	2	9	15	-	-	2	13
Тема 4. Управління інформаційною та кібербезпекою на судні	15	2	2	2	9	15	-	2	-	13
Разом за змістовим модулем 1	60	8	8	7	37	60	2	2	2	54
Змістовий модуль 2. Методи і засоби обробки інформації										
Тема 5. Структура ВТІШ, характеристика інформаційних потоків, розробка моделі загроз	15	2	2	2	9	15	2	-	-	13
Тема 6. Розробка моделі загроз, моделі порушника та моделі протидії загрозам, вибір засобів та методів захисту інформації	15	2	2	2	9	15	-	2	-	13
Тема 7 СРРС як об'єкт інформаційної діяльності. Аналіз інформаційних потоків, аналіз загроз.	15	2	2	2	9	15	-	-	1	14
Тема 8 Інформаційна та кібербезпека в портах. Сучасні тенденції розвитку в галузі інформаційної та кібербезпеки ВТІШ	15	1	1	2	11	15	-	-	1	14
	60	7	7	8	38	60	2	2	2	54
	120	15	15	15	75	120	4	4	4	104

Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Розробка моделі загроз інформації для судна	3
2	Розробка моделі порушника для судна	2
3	Розробка моделі порушника для ВТШ	2
4	Розробка моделі загроз інформації для ВТШ	2
5	Розробка моделі загроз інформації для морського порту	2
6	Розробка моделі порушника для морського порту	2
7	Розробка «Плану охорони судна»	2
Разом		15

Примітка. Студенти заочної форми виконують лабораторні роботи згідно індивідуального графіку бригади загальним об'ємом 4 години із переліку вказаних тем лабораторних робіт

Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Аналіз вимог МКУБ з питань безпеки ВТК	2
2	Аналіз вимог кваліфікаційних товариств з питань безпеки ВТК	2
3	Сфери компетенцій осіб командного складу, відповідальних за охорону на судні («Манільські поправки до Додатка до Міжнародної конвенції про підготовку і дипломування моряків...»)	2
4	Міжнародний Кодекс з охорони суден і портових засобів (ОСПЗ). Функціональні вимоги осіб командного складу в сфері інформаційної та кібербезпеки.	2
5	Міжнародний Кодекс з охорони суден і портових засобів. Рівні охорони. Вимоги. Задачі. Обов'язки осіб командного складу	2
6	Концепція розвитку ВТК України. Вимоги що до інформаційної та кібербезпеки	2
7	Аналіз інформаційних потоків і загроз інформації для СРРС	3
Разом		15

Самостійна робота

Метою самостійної роботи є повторення й осмислення студентом основних питань кожної теми, висвітлених на лекційних, практичних і лабораторних заняттях.

Самостійна робота проводиться в лабораторіях НУК, читальних залах, на об'єктах майбутньої діяльності і/або вдома. Результати цієї роботи фіксуються студентом в індивідуальному робочому зошиті (конспекті).

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1	Безпека водотранспортного комплексу України.. Основні поняття, визначення, міжнародні та національні вимоги.	11	15
2	Технічний захист інформації на судні	8	13
3	Захист інформації в ІКС на судні. Кібербезпека інформаційних і комунікаційних мереж судна.	9	13
4	Управління інформаційною та кібербезпекою на судні	9	13
5	Структура ВТШ, характеристика інформаційних потоків, розробка моделі загроз	9	13
6	Розробка моделі загроз, моделі порушника та моделі протидії загрозам, вибір засобів та методів захисту інформації	9	13
7	СРРС як об'єкт інформаційної діяльності. Аналіз інформаційних потоків, аналіз загроз.	9	14
8	Інформаційна та кібербезпека в портах. Сучасні тенденції розвитку в галузі інформаційної та кібербезпеки ВТШ	11	14
Разом		75	104

Навчальний матеріал дисципліни, передбачений для засвоєння здобувачем вищої освіти в процесі самостійної роботи, включається в завдання поточного контролю разом із навчальним матеріалом, який опрацьовувався при проведенні навчальних занять.

Денна форма навчання

Розподіл годин самостійної роботи для денної форми навчання:

- підготовка до лекційних занять – 0,6 год. / 1 год. занять;
- самостійне опрацювання лекційних матеріалів – 0,6 год. / 1 год. занять;
- підготовка до лабораторних робіт – 2,0 год. / 1 год. занять;
- підготовка до практичних робіт – 1,0 год. / 1 год. занять;
- підготовка до контрольних заходів – 6,0 год. на 1 захід.

Заочна форма навчання

Розподіл годин самостійної роботи для заочної форми навчання:

- підготовка до лекційних занять – 2 год. / 1 год. занять;
- самостійне опрацювання лекційних матеріалів – 2 год. / 1 год. занять;
- підготовка до лабораторних робіт – 9,0 год. / 1 год. занять;
- підготовка до практичних робіт – 4 год. / 1 год. заняття;
- підготовка до контрольних заходів – 14 год. на 1 захід.

Розподіл годин підготовки самостійної роботи

№	Вид роботи	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1	Підготовка до лекцій	9	12
2	Самостійне опрацювання окремих тем навчальної дисципліни	9	12
3	Підготовка до лабораторних робіт	30	36
4	Підготовка до практичних робіт	15	16
5	Підготовка до модульних контрольних робіт	12	28
Разом за курсом		75	104

6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування

Здобувач зобов'язаний вивчити теоретичний матеріал та здобути практичні навички у відповідності до тематичного плану навчальної дисципліни.

Методами навчання є:

- пояснення, демонстрування;
- лекція; відеометод;
- лабораторна робота, інструктаж;
- репродуктивний метод;
- проблемного викладу.

Засобами оцінювання результатів навчання є:

- модульні контрольні роботи;
- звіти з лабораторних робіт;
- індивідуальні та групові завдання;

- завдання на лабораторному обладнанні;
- комплексна контрольна робота (за необхідністю).

Методами демонстрування результатів навчання є:

- усні відповіді;
- письмові відповіді;
- виконання завдань із застосуванням комп'ютерної техніки;
- оформлення звітів з лабораторних робіт;
- презентації результатів виконаних завдань та досліджень.

Допускається застосування дистанційних технологій для діагностики результатів навчання.

7. Форми поточного та підсумкового контролю

Досягнення здобувача вищої освіти оцінюються за 100-бальною системою Університету.

Поточний контроль проводиться в межах навчальних занять і передбачає оцінювання теоретичної підготовки здобувачів вищої освіти із зазначених тем (у тому числі, самостійно опрацьованого матеріалу) та практичних навичок, набутих під час виконання лабораторних робіт.

Поточний контроль здійснюється протягом семестру в наступних формах:

- перевірка та захист звітів з лабораторних робіт;
- проведення та перевірка модульних контрольних робіт;
- контрольна робота на заочній формі навчання;
- семестрова атестація;
- перевірка конспекту лекцій;
- контроль відвідування занять.

Перевірка звіту з лабораторної роботи включає оцінювання правильності та повноти виконання завдання, правильності та повноти висновків, правильності оформлення звіту.

Процедура захисту звіту з лабораторної роботи включає один або декілька елементів:

- письмове викладення відповідей на запитання за тематикою роботи;
- усне опитування за тематикою роботи;
- виконання завдань із застосуванням комп'ютерної техніки.

При виконанні модульних контрольних робіт здобувач вищої освіти відтворює засвоєні знання шляхом надання письмових відповідей на поставлені запитання. На теоретичні запитання необхідно давати розгорнуті відповіді, супроводжуючи їх прикладами та ілюстраціями. Повнота відповідей оцінюється згідно з теоретичним матеріалом, наведеним у джерелах інформації для кожної теми. На тестові запитання потрібно вказати номер правильної відповіді та її формулювання.

Контрольна робота на заочній формі навчання має ті ж вимоги, виконується протягом семестру і здається до проведення підсумкового контролю.

Поточний модульний контроль проводиться з урахуванням даних поточного контролю за відповідний змістовний модуль і має на меті оцінку результатів знань студента після вивчення матеріалу з логічно-завершеної частини дисципліни – змістового модуля.

Семестрова атестація дає змогу здійснити проміжну оцінку досягнень здобувача вищої освіти. В період семестрової атестації викладач оцінює результати поточного контролю та атестує чи не атестує здобувача вищої освіти.

За рішенням кафедри студентам, які брали участь у науково-дослідній роботі – роботі конференцій, студентських наукових гуртків, підготовці публікацій, а також були учасниками олімпіад, конкурсів, тощо можуть присуджуватися додаткові бали. Додаткові бали також можуть присуджуватися за результатами перевірки конспекту лекцій, контролю відвідування занять та за активність на лекціях і практичних заняттях.

За всі поточні контрольні заходи протягом семестру, з урахуванням додаткових балів, студент сумарно може отримати від 0 до 100 балів.

Умовою допуску студента до семестрового підсумкового контролю є мінімальна сума у 60 балів, яку студент повинен набрати у разі виконання всіх елементів модулів.

Семестровий підсумковий контроль з дисципліни проводиться відповідно до навчального плану у вигляді **екзамену** в терміни, встановлені графіком навчального процесу, та в обсязі навчального матеріалу, визначеному робочою програмою навчальної дисципліни.

Студент, який набрав за всі поточні контрольні заходи менше 60 балів або хоче отримати додаткові бали, пише додаткову семестрову залікову роботу (проводиться у письмовій формі), до якої він допускається, якщо має за виконання всіх передбачених елементів модулів не менше 40 балів. Максимальна кількість балів за залікову роботу становить 20 балів.

Зарахування кредитів навчального курсу можливо тільки після досягнення результатів, запланованих РПНД, що виражається в одній з позитивних оцінок, передбачених чинним законодавством.

8. Критерії оцінювання результатів навчання

При оцінюванні лабораторних та практичних робіт враховуються наступні критерії:

- виконання роботи та правильність виконання;
- наявність звіту, вчасність подачі та якість звіту;
- захист звіту.

Максимальна оцінка за кожну лабораторну роботу – 5 балів.

Максимальна сумарна кількість балів за лабораторні роботи для:

- ДФН – $5 \times 7 = 35$ балів;
- ЗФН – $5 \times 3 = 15$ балів.

Критерії оцінювання лабораторних робіт

Кількість балів	Критерії оцінювання
5	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.
4	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).
3	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.
2	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.
1	Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.
0	Робота не виконана.

Максимальна оцінка за кожну лабораторну роботу – 3 балів.

Максимальна сумарна кількість балів за лабораторні роботи для:

- ДФН – $3 \times 7 = 21$ бал;
- ЗФН – $3 \times 2 = 6$ балів.

Критерії оцінювання практичних робіт

Кількість балів	Критерії оцінювання
3	Робота виконана у встановлений термін. Студент самостійно визначає тип задачі і раціонально розв'язує її. Може розв'язувати комбіновані задачі. Звіт відповідає встановленим вимогам
2	Робота виконана з порушенням встановлених термінів. Студент наводить потрібні формули. Розв'язує задачу користуючись алгоритмом. Складений звіт містить неточності у висновках та помилки
1	Студент складає скорочену умову задачі, робить обчислення лише за готовою формулою.
0	Робота не виконана.

Для поточного модульного контролю студентами виконуються по 2 (дві) модульних контрольних роботи за матеріалами змістовних модулів за Модулем. Максимальний бал за кожне питання (тему) МКР – 5 балів. Загальна сума балів за модульні контрольні роботи для кожного модуля:

Контрольні роботи	МКР1	МКР2	Разом за модуль
Кількість балів	2 x 5 = 6	3 x 5 = 10	20

За заочною формою навчання в кінці семестру виконується підсумкова залікова робота. Максимальна оцінка за підсумкову залікову роботу – 29 балів.

Критерії оцінювання задач та практичних завдань в МКР

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
бал	3	2,7	2,4	2,1	1,8	1,5	1,2	0,9	0,6	0,3

Розподіл оцінки за змістовними модулями та видами контролю

Модуль 1	Денне форма		Заочна форма	
	Вид роботи	Кількість балів	Вид роботи	Кількість балів
ЗМ 1	Лабораторні роботи	15	Лабораторні роботи	5
	Практичні роботи	9	Практичні роботи	3
	МКР 1	10	–	0
ЗМ 2	Лабораторні роботи	20	Лабораторні роботи	10
	Практичні роботи	12	Практичні роботи	3
	МКР 2	10	–	0
А	Атестація	4	–	0

КР	–	0	Контрольна робота	30
Конспект лекцій	Конспект	0	Конспект	29
Екзамен	Екзамен	20	Екзамен	20
Сума		100		100

9. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

Апаратне забезпечення, необхідне для вивчення навчальної дисципліни, включає персональний комп'ютер (настільний або ноутбук) та спеціалізовані лабораторні стенди.

Програмне забезпечення, необхідне для вивчення навчальної дисципліни, включає операційну систему, спеціалізоване програмне забезпечення для інженерних розрахунків та моделювання технічних засобів, текстовий процесор та редактор растрових зображень (для підготовки звітів з практичних робіт); pdf-, djv-переглядач (для ознайомлення з джерелами інформації, представленими в електронному виді).

10. Рекомендовані джерела інформації

1. Закон України. Про перевезення небезпечних вантажів. Закон України від 06.04.2000 № 1644-III. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/1644-14#Text>
2. Закон України. Про страхування. Закон України від 18.11.2021 № 1909-IX. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/1909-20#Text>
3. Закон України. Про транспорт. Закон України від 10.11.1994 № 232/94-BPR. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/232/94-%D0%B2%D1%80#Text>
4. Кодекс України. Водний кодекс України. Кодекс від 06.06.1995 № 213/95-BP. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/213/95-%D0%B2%D1%80#Text>
5. Кодекс України. Кодекс торговельного мореплавства України. Кодекс від 23.05.1995 № 176/95-BP. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/176/95-%D0%B2%D1%80#Text>
6. Кодекс України. Кодекс торговельного мореплавства України. Кодекс від 23.05.1995 № 176/95-BP [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/176/95-%D0%B2%D1%80#Text>

7. Міжнародна конвенція по запобіганню забрудненню з суден (з поправками). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/896_009#Text
8. Міжнародна конвенція про безпечні контейнери [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_013#Text
9. Міжнародна конвенція про вантажну марку (з поправками). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/896_007#Text
10. Міжнародна конвенція про охорону людського життя на морі 1974 року (СОЛАС-74). <https://marad.gov.ua/ua/npa/mizhnarodna-konvenciya-pro-ohoronu-lyudskogo-zhittya-na-mori-1974-roku-solas-74>
11. Міжнародна конвенція про підготовку і дипломування моряків та несення вахти (з поправками). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_053#Text
12. Міжнародна конвенція про пошук і рятування на морі. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_138#Text
13. Міжнародна конвенція щодо втручання у відкритому морі у випадках аварій, які призводять до забруднення нафтою (з поправками). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_049#Text
14. Міжнародна конвенція. Експлуатаційна угода Міжнародної організації морського супутникового зв'язку (ІНМАРСАТ). [Електронний ресурс]. – Режим доступу: <http://consultant.parus.ua/?doc=00VYA2BF2F&abz=1LG29>
15. Міжнародна конвенція. Конвенція про боротьбу з незаконними актами, спрямованими проти безпеки морського судноплавства. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_220#Text
16. Міжнародна конвенція. Конвенція про Міжнародну організацію морського супутникового зв'язку (ІНМАРСАТ) [Електронний ресурс]. – Режим доступу: <http://consultant.parus.ua/?doc=00VY976843>
17. Міжнародна конвенція. Поправки до Міжнародної конвенції про пошук і рятування на морі 1979 року, які були прийняті Комітетом з безпеки на морі Міжнародної морської організації 18 травня 1998 року (Резолюція КБМ.70 (69)). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/896_001-98#Text
18. Міжнародні правила запобігання зіткненню суден у морі. https://zakon.rada.gov.ua/laws/show/995_220#Text
19. Наказ Мінінфраструктури. Про затвердження Змін до Положення про порядок підготовки та подання інформації про вантаж для його безпечного морського перевезення. Наказ від 26.06.2013 № 425. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z1177-13#Text>
20. Наказ Мінінфраструктури. Про затвердження Положення про морських лоцманів. Наказ, Положення, Форма типового документа від 08.05.2013 № 292. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0920-13#Text>

21. Наказ Мінітрансу України Про затвердження Положення про систему управління безпекою судноплавства на морському і річковому транспорті. Положення, від 20.11.2003 № 904. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z1193-03#Text>

22. Наказ Мінітрансу України. Про Головну державну інспекцію України з безпеки судноплавства. Наказ від 21.03.2002 № 185 [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/rada/show/v0185361-02#Text>

23. Наказ Мінітрансу України. Про Головну державну інспекцію України з безпеки судноплавства. Наказ від 21.03.2002 № 185. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/rada/show/v0185361-02#Text>

24. Наказ Мінітрансу України. Про затвердження Інструкції про огляд суден, які здійснюють плавання (експлуатуються) на внутрішніх водних шляхах України. Інструкція від 19.04.2001 № 225. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0400-01#Text>

25. Наказ Мінітрансу України. Про затвердження Положення про державних річкових лоцманів. Наказ, Положення, Форма типового документа від 14.01.2002 № 11. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0091-02#Text>

26. Наказ Мінітрансу України. Про затвердження Положення про порядок підготовки та подання інформації про вантаж для його безпечного морського перевезення. Наказ, Положення, Форма типового документа від 14.12.1998 № 497. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0848-98#Text>

27. Наказ Мінітрансу України. Про затвердження Правил безпечної експлуатації баз для стоянки маломірних (малих) суден. Наказ, Правила, Форма типового документа від 16.07.2004 № 642. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0915-04#Text>

28. Постанова Кабінету Міністрів України. Про вдосконалення технічного, класифікаційного і судноплавного нагляду на морському і внутрішньому водному транспорті. Положення від 08.06.1998 № 814. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/814-98-%D0%BF#Text>

29. Постанова Кабінету Міністрів України. Про внесення зміни до Порядку здійснення нагляду за забезпеченням безпеки руху на транспорті та визнання такими, що втратили чинність, деяких постанов Кабінету. Перелік від 29.02.2012 № 159. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/159-2012-%D0%BF#Text>

30. Розпорядження Кабінету Міністрів України Про схвалення Національної транспортної стратегії України на період до 2030 року Стратегія від 30.05.2018 № 430-р. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/430-2018-%D1%80#Text>

31. Стан безпеки судноплавства та аварійності на водному транспорті в Україні (у тому числі і за її межами, але із українськими суднами), включаючи маломірні (малі) судна, за січень – червень 2022 року з наростаючим підсумком

[Електронний ресурс]. – Режим доступу: https://marad.gov.ua/storage/app/sites/1/uploaded-files/Zvit_2022.pdf

32. Балобанов А.О. Діяльність Європейського Союзу з правового забезпечення безпеки мореплавання. – Одеса: Вид-во ОНМУ, 2003. – 227с.

33. Іванов Д.А. Історія правового регулювання використання радіозв'язку для пошуку та рятування на морі // Актуальні проблеми держави і права: Зб. наук. пр. – Одеса: Юрид. л-ра, 2005. – Вип. 26. – С. 246-254.

34. Україна в міжнародних відносинах. Боротьба із злочинністю та взаємна правова допомога (Книга перша) / Зб. докум. (укр.. і рос. мовами). – Юрінком. – Київ, 1996.

35. Липинский В.Н., Качан В.Д., Аксенов Н.Ф. Глобальна морська система зв'язку під час лиха та для забезпечення безпеки За заг. ред.. В.В. Пономаренко. - Одеса: Морський тренажерний центр. - – 2002. – 525 с.

36. Лукшин І.В. Протиправні дії, що посягають на свободу мореплавання // Право і політика. - 2000. - № 6.

37. Ромашев Ю.С., Корбут Л.В. Основи боротьби з актами тероризму та піратства на морі. // Альманах "Організована злочинність, тероризм та корупція". - 2003. - № 2.

38. Блінцов В.С. Підводно-технічні засоби і технології обстеження морських кабелів зв'язку.// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні К.,1998 . – С. 109-110

Зміни та доповнення