

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки
Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ



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

С.О. Слободян

_____ 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Program of the Discipline

**ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ
КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ ВОДНОГО ТРАНСПОРТУ**

**Information technologies for ensuring cyber resilience of water
transport facilities**

Рівень вищої освіти _____ другий (магістерський) _____

Тип дисципліни _____ обов'язкова _____

Мова викладання _____ українська _____

Робоча програма навчальної дисципліни «Інформаційні технології забезпечення кіберстійкості об'єктів водного транспорту» є однією із складових комплексної підготовки фахівців галузі знань «F - Інформаційні технології», спеціальності «F5 Кібербезпека та захист інформації», освітня програма «Системи технічного захисту інформації, автоматизація її обробки»

«24» 04 2025 р. – 23 с.

Розробник: Передерій В.І., професор кафедри Комп'ютерних технологій та інформаційної безпеки, док. техн. наук, доцент.

Проект робочої програми навчальної дисципліни «Інформаційні технології забезпечення кіберстійкості об'єктів водного транспорту» узгоджено з гарантом освітньої програми

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

Передерій В.І., д. т. н, доцент



Проект робочої програми навчальної дисципліни «Інформаційні технології забезпечення кіберстійкості об'єктів водного транспорту» розглянуто на засіданні кафедри КТІБ.

Протокол від «24» 04 2025 р. № 12.

Завідувач кафедри КТІБ, к.т.н., доцент



С.М. Нужний

Проект робочої програми навчальної дисципліни «Інформаційні технології забезпечення кіберстійкості об'єктів водного транспорту» розглянуто методичною радою Навчально-наукового інституту автоматики та електротехніки.

Протокол від «15» 05 2025 р. № 5.

Заступник голови МР ННІАЕ, к.т.н., доц.



С.М.Новогрецький

Проект робочої програми навчальної дисципліни «Інформаційні технології забезпечення кіберстійкості об'єктів водного транспорту» погоджено з навчальним відділом.

Начальник навчального відділу, к.т.н., доцент



А.В. Лабарткава

Робочу програму навчальної дисципліни «Інформаційні технології забезпечення кіберстійкості об'єктів водного транспорту» затверджено Навчально-методичною радою НУК ім. адм. Макарова.

Протокол від «21» 05 2025 р. № 5.

Голова Навчально-методичної ради НУК ім. адм. Макарова,

к.т.н., доцент



С.О.Слободян

ЗМІСТ

Вступ.....	4
1. Опис навчальної дисципліни	6
2. Мета навчальної дисципліни.....	7
3. Передумови для вивчення навчальної дисципліни	8
4. Очікувані результати навчання.....	9
5. Програма навчальної дисципліни.....	9
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування	15
7. Форми поточного та підсумкового контролю.....	16
8. Критерії оцінювання результатів навчання.....	18
9. Засоби навчання.....	19
10. Рекомендовані джерела інформації.....	21

ВСТУП

Анотація

Навчальна дисципліна «Інформаційні технології забезпечення кіберстійкості об'єктів водного транспорту» є обов'язковою навчальною дисципліною і забезпечує формування умінь використовувати сучасні інформаційні технології забезпечення кіберстійкості об'єктів водного транспорту при управлінні і забезпеченню інформаційної та кібернетичної безпеки об'єктів водного транспорту.

Головна мета курсу «Інформаційні технології забезпечення кіберстійкості об'єктів водного транспорту» – познайомити студентів з основними положеннями інтелектуальних та інформаційно-когнітивних технологій в системах підтримки прийняття рішень по забезпеченню кіберстійкості об'єктів водного транспорту, в умовах невизначеності та ризику, як сучасних міждисциплінарних методологій, що базуються на прикладних математичних методах і сучасних інформаційних технологіях для вирішення задач аналізу і синтезу технічних, економічних, соціальних, екологічних та інших складних систем.

Варто відзначити, що вивчення навчальної дисципліни «Інформаційні технології забезпечення кіберстійкості об'єктів водного транспорту» не тільки дає змогу здобувачу вищої освіти в перспективі застосовувати отримані знання в фаховій діяльності, а і формує фундамент для підвищення ефективності поточного навчального процесу. Використання сучасних Інтелектуальних та інформаційно-когнітивних технологій по забезпеченню кіберстійкості об'єктів водного транспорту дає можливість здобувачу вищої освіти самостійно формувати розв'язки задач, розширювати межі їх застосування та аналізувати виключення та окремі випадки, переконуватись в справедливості теоретичних тверджень, виконувати імітаційне моделювання процесів, що вивчаються, а також сприяє інтуїтивному розумінню вивченого матеріалу шляхом візуалізації результатів обчислень.

В даному курсі будуть використанні наукові матеріали результатів авторських досліджень.

Ключові слова: інформаційно-когнітивні технології підтримки прийняття рішень, об'єкти критичної інфраструктури, інформаційна та кібернетична безпека.

Abstract

The academic discipline "Information Technologies for Ensuring Cyber Resilience of Water Transport Facilities" is a mandatory academic discipline and provides the formation of the ability to use modern information technologies for ensuring cyber resilience of water transport facilities in the management and provision of information and cyber security of water transport facilities.

The main goal of the course "Information Technologies for Ensuring Cyber Resilience of Water Transport Facilities" is to introduce students to the basic principles of intellectual and information and cognitive technologies in decision-making support systems for ensuring cyber resilience of water transport facilities, in conditions of uncertainty and risk, as modern interdisciplinary methodologies based on applied mathematical methods and modern information technologies for solving problems of analysis and synthesis of technical, economic, social, environmental and other complex systems.

It is worth noting that studying the academic discipline "Information Technologies for Ensuring Cyber Resilience of Water Transport Facilities" not only allows a higher education student to apply the acquired knowledge in professional activities in the future, but also forms the foundation for increasing the efficiency of the current educational process. The use of modern Intellectual and information and cognitive technologies for ensuring cyber resilience of water transport facilities allows a higher education student to independently formulate solutions to problems, expand the boundaries of their application and analyze exceptions and individual cases, verify the validity of theoretical statements, perform simulation modeling of the processes being studied, and also contributes to an intuitive understanding of the studied material by visualizing the results of calculations.

This course will use scientific materials from the results of the author's research.

Keywords: information and cognitive technologies for decision support, critical infrastructure facilities, information and cyber security.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 3	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
		Семестр	
Загальна кількість годин – 90		2-ий	2-ий
Тижневих годин для денної форми навчання: Аудиторних – 2 Самостійної роботи: – 4.	Рівень вищої освіти: другий (магістерський)	Лекції, год	
		15 год.	4 год.
		Лабораторні роботи, год	
		15 год.	8 год.
		Практичні роботи, год	
		-	-
		Самостійна робота, год	
		60	78
		Вид контролю: Екзамен	
		Форма контролю: усна, письмова	

2. Мета навчальної дисципліни

Метою вивчення навчальної дисципліни «Інформаційні технології забезпечення кіберстійкості об'єктів водного транспорту» є формування у студентів відповідно до освітньо-професійної програми таких **компетентностей**:

Інтегральна компетентність:

– (ІК) Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту Інформації.

Загальні компетентності:

- (ЗК1) Здатність застосовувати знання у практичних ситуаціях;
- (ЗК2) Здатність проводити дослідження на відповідному рівні.
- (ЗК3) Здатність до абстрактного мислення, аналізу та синтезу;
- (ЗК4) Здатність оцінювати та забезпечувати якість виконуваних;
- (ЗК6) Здатність діяти соціально відповідально та громадсько свідомо.

Фахові компетентності:

- (КФ6) Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації;
- (КФ7) 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;
- (КФ8) 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;
- (КФ13) Здатність проводити спеціалізовані дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності;
- (КФ14) Здатність впроваджувати(активізувати) програмні та апаратні засоби захисту інформації в системах і на об'єктах.

3. Передумови для вивчення навчальної дисципліни

Передумовами для вивчення навчальної дисципліни «Інформаційні технології забезпечення кіберстійкості об'єктів водного транспорту» є наступні навчальні дисципліни:

- Вища математика,
- Моделювання об'єктів і процесів технічного захисту інформації,
- Комплексні системи захисту інформації,

- Інформаційні технології систем управління та захисту інформації,
- Безпека інформаційних та комунікаційних систем.

4. Очікувані результати навчання

Основними (програмними) результатами навчання з дисципліни «Інформаційні технології забезпечення кіберстійкості об'єктів водного транспорту» є:

- (РН 2) Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

- (РН 3) Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі

- (РН 4) Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

- (РН 5) 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) Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

- (РН 8) Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

- (РН 9) Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки

- (РН 10) 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 11) Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

- (РН 15) 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) 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) 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) Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки

– (РН 24) 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.

Відповідність результатів навчання Професійним стандартам

№ з/П	ОПП «Системи технічного захисту інформації, автоматизація її обробки»	ПС «Фахівець сфери захисту інформації»		Примітки
1	РН-2	A1.31,A2.34,B1.31,B1.31,B4.32 Г1.31,Д1.31	A1.Y2, B1.Y1, Г1.Y5 Г2.Y4	
2	РН-3	A2.36,A3.31,A3.32,A3.33,B2.35, Г1.31,Д1.31	A1.Y4,B1.Y3,B1.Y4, B2.Y1,Г1.Y4,Г2.Y3	
3	РН-4	A2.36,A3.31,A3.33,B2.36,B4.32, Г1.31,Д1.31	A1.Y2,A1.Y4,A3.Y4, B1.Y4,B2.Y3,B3.Y3,Г1.Y5	
4	РН-5	A2.34,A3.31,B2.35,B4.33,Г1.31	A1.Y4,A3.Y5,B1.Y4,B3.Y1 B4.Y2,B4.Y3	
5	РН-6	A2.34,B1.31,B1.35,B2.32,B2.34 Г1.31	A2.Y2,B1.Y1,B1.Y2,B2.Y1 B2.Y4,B3.Y1,B3.Y3,Г1.Y3	
6	РН-8	A2.36,B3.36,B4.32,B4.34,Г1.31, Г1.33,Г2.31,Д1.31	A1.Y4,B1.Y3,B3.Y1,B3.Y3, Г1.Y2,Г2.Y3,Г2.Y4,Д1.Y3 Д1.Y4	
7	РН-9	A1.34,B2.32,B1.31,B2.31,B4.31, Г1.35,Г2.35,Д1.34	A1.Y1,A2.Y2,B1.Y1,B1.Y3, B1.Y1,Г1.Y1,Г1.Y3,Г1.Y4,Г2.Y2 Д1.Y4	
8	РН-10	A1.35,A1.37,A2.31,B1.31,B1.34 B1.31,B2.31,B3.32,B3.35,Д1.32 Д2.31	A1.Y1,A1.Y4,B1.Y1,B1.Y1,B2.Y1 B3.Y1,B4.Y2,B5.Y3,Д2.Y1	
9	РН-11	A1.34,B1.35,B2.37,B1.32,B5.31 B5.32,Д1.34	A1.Y1,A1.Y4,A2.Y5,B1.Y1,B1.Y3 B1.Y1,B2.Y3,B5.Y3	
10	РН-15	A1.36,B2.33,Г2.31,Г2.34	A1.Y3,B4.Y5,Г1.Y1,Г1.Y2,Г1.Y3 Г2.Y2,Г2.Y3,Г2.Y4	
11	РН-16	A1.35,B1.31,B1.31,Г1.33,Д1.32 Д2.32	A1.Y1,B1.Y3,B1.Y1,B1.Y4,B3.Y1 B4.Y2,Д1.Y3,Д2.Y3	
12	РН-20	A2.34,A2.36,B1.31,B1.31,B4.32 Г1.31,Г1.36,Д1.31	A1.Y2,A2.Y2,B1.Y3,B3.Y1,B4.Y4 Д1.Y5	
13	РН-21	A2.34,B4.34	A1.Y2,A1.Y4,A2.Y2,B2.Y3,B4.Y2 B4.Y4,B2.Y7	
14	РН-24	A2.34,B1.31,B1.31,B4.31,Г1.33 Г1.36,Д1.32	A2.Y2,B1.Y1,B1.Y3,B1.Y1,B1.Y4 B4.Y2,Д2.Y4	

5. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Основні особливості забезпечення кіберстійкості об'єктів водного транспорту.

Тема 1. Аналіз та основні особливості забезпечення кіберстійкості об'єктів водного транспорту. Нормативні вимоги до комплексного підходу забезпечення кіберстійкості об'єктів водного транспорту [1,2,4,6-8].

Тема 2. Класифікація проблем оцінки та підтримки кіберстійкості об'єктів водного транспорту. Сучасні системи управління інформацією та подіями безпеки SIEM SPLUNK на об'єктах водного транспорту

Тема 3. Сучасні антивірусні технології на об'єктах водного транспорту.

Змістовий модуль 2. Сучасні інформаційні технології забезпечення інформаційної та кібер-безпеки на об'єктах водного транспорту.

Тема 4. Сучасні інформаційні технології та математичні методи і моделі в сфері інформаційної та кібербезпеки об'єктів водного транспорту

Тема 5. Особливості застосування інтелектуальних технологій оцінки та підтримки інформаційної та кібербезпеки на об'єктах водного транспорту [5].

Тема 6. Методи та моделі м'яких обчислень побудови адаптивних інформаційних технологій підтримки інформаційної та кібербезпеки на об'єктах водного транспорту. 4,5].

Тема 7. Застосування методів Інформаційної технології моніторингу та підтримки комплексу показників інформаційної та кібербезпеки на об'єктах водного транспорту [6].

Тема 8. Застосування методів та моделей Інформаційної технології визначення та контролю впливу показників людського фактору на функціональну стійкість об'єктів водного транспорту [4,5].

Тематичний план навчальної дисципліни

Назви змістових модулів і тем	Денна форма				Заочна форма			
	Кількість годин							
	усього	у тому числі			усього	у тому числі		
		л	лаб	с.р		л	лаб	с.р
Модуль 1								
Змістовий модуль 1. Основні особливості забезпечення кіберстійкості об'єктів водного транспорту								
Тема 1. Аналіз та	10	2	2	6	10	2	2	6

Назви змістових модулів і тем	Денна форма				Заочна форма			
	Кількість годин							
	усього	у тому числі			усього	у тому числі		
		л	лаб	с.р		л	лаб	с.р
основні особливості забезпечення кіберстійкості об'єктів водного транспорту. Нормативні вимоги до комплексного підходу забезпечення кіберстійкості об'єктів водного транспорту								
Тема 2. Класифікація проблем оцінки та підтримки кіберстійкості об'єктів водного транспорту. Сучасні системи управління інформацією та подіями безпеки SIEM SPLUNK на об'єктах водного транспорту	4	2	-	2	4		-	4
Тема 3. Сучасні антивірусні технології на об'єктах водного транспорту.	6	2	-	4	6		-	6
Тема 4. Сучасні інформаційні технології та математичні методи і моделі в сфері інформаційної та кібербезпеки об'єктів водного транспорту	10	2	2	6	10		-	10
Разом за змістовим модулем 1	30	8	4	18	30	2	2	26
Змістовий модуль 2. Сучасні інформаційні технології забезпечення інформаційної та кібер-безпеки на об'єктах водного транспорту								
Тема 5. Особливості застосування інтелектуальних технологій оцінки та	8	2	-	6	8	2	-	6

Назви змістових модулів і тем	Денна форма				Заочна форма			
	Кількість годин							
	усього	у тому числі			усього	у тому числі		
л		лаб	с.р	л		лаб	с.р	
підтримки інформаційної та кібербезпеки на об'єктах водного транспорту								
Тема 6. Методи та моделі м'яких обчислень побудови адаптивних інформаційних технологій підтримки інформаційної та кібербезпеки на об'єктах водного транспорту	14	2	2	10	14		2	12
Тема 7. Застосування методів Інформаційної технології моніторингу та підтримки комплексу показників інформаційної та кібербезпеки на об'єктах водного транспорту	30	2	8	20	30		4	22
Тема 8. Застосування методів та моделей Інформаційної технології визначення та контролю впливу показників людського фактору на функціональну стійкість об'єктів водного транспорту	8	1	1	6	8		-	12
Разом за змістовим модулем 2	60	7	11	42	60	2	6	52
Разом	90	15	15	60	90	4	8	78

Для студентів заочної форми навчання читаються оглядові лекції за

темами змістових модулів в обсягах відповідно до вищенаведеної таблиці.

Теми практичних занять

Практичні роботи програмою не передбачені

Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
Модуль 1		
Змістовий модуль 1		
1	Нормативні вимоги до комплексного підходу забезпечення кіберстійкості об'єктів водного транспорту	2
2	Застосування методів Інформаційної технології моніторингу та підтримки комплексу показників інформаційної та кібер-безпеки на об'єктах водного транспорту	2
Разом за змістовим модулем 1		4
Змістовий модуль 2		
3	Побудова реляційної когнітивної моделі взаємовпливу факторів інформаційної та кібер-безпеки на об'єктах водного транспорту.	2
4	Використанням імовірністних графо-аналітичних методів для оцінки інформаційної та кібербезпеки на об'єктах водного транспорту	2
5	Побудова типів мереж Байєса для визначення показників інформаційної та кібер-безпеки на об'єктах водного транспорту	2
6	Побудова та дослідження інформаційної моделі впливу основних факторів інформаційної та кібер-безпеки на об'єктах водного транспорту	2
7	Застосування інтелектуальних технологій підтримки прийняття рішень забезпечення інформаційної та кібер-безпеки на об'єктах водного транспорту.	2
8	Застосування інформаційно-когнітивних технологій підтримки прийняття рішень забезпечення інформаційної та кібер-безпеки на об'єктах водного транспорту	1
Разом за змістовим модулем 2		11
Разом		15

Студенти заочної форми виконують роботи № 1, 3, 4, 7,

За необхідністю можуть проводитись групові та індивідуальні консультації за розкладом кафедри в тому числі із застосуванням дистанційних технологій навчання. Це сприяє роз'ясненню найбільш складних питань дисципліни та підвищенню якості виконання завдань.

Лабораторні заняття проводяться в лабораторіях кафедри з використанням комп'ютерної техніки. Допускається виконання лабораторних завдань в дистанційному режимі із застосуванням персонального комп'ютера за межами лабораторій кафедри.

Самостійна робота.

Самостійна робота здобувача вищої освіти є однією з форм організації навчання, основною формою оволодіння навчального матеріалу в час, вільний від обов'язкових навчальних занять.

Метою самостійної роботи є повторення й осмислення студентом основних питань кожної теми, висвітлених на лекційних 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).

Навчальний матеріал дисципліни, передбачений для засвоєння здобувачем вищої освіти в процесі самостійної роботи, виноситься на підсумковий контроль поряд з навчальним матеріалом, який опрацьовувався при проведенні навчальних занять.

Розподіл годин самостійної роботи для денної форми навчання:

- підготовка до лекційних занять – 0,5 год. / 1 заняття (на 1 лекцію);
- самостійне опрацювання окремих тем навчальної дисципліни (які не викладаються на лекціях) – 2 год. / 1 заняття;
- підготовка до лабораторних занять – 1-2 год. / 1 заняття;
- підготовка до модульних контрольних робіт 5 год на 1 роботу
- підготовка до екзаменів – 22 год. на 1 захід.

Розподіл годин самостійної роботи для заочної форми навчання:

- підготовка до лекційних занять – 2 год. / 1 заняття (на 1 лекцію);
- самостійне опрацювання окремих тем навчальної дисципліни (які не викладаються на лекціях) – 4 год. / 1 заняття;
- підготовка до лабораторних занять – 2 год. / 1 заняття;
- підготовка до модульних контрольних робіт 5 год на 1 роботу
- підготовка до екзаменів – 22 год. на 1 захід.

Розподіл годин самостійного опрацювання окремих тем навчальної дисципліни

№ з/п	Назва теми	Кількість годин	
		Д.Ф.Н	З.Ф.Н.
Модуль 1			
1	До теми 1. Нормативні вимоги до комплексного підходу забезпечення кіберстійкості об'єктів водного транспорту	2	1

№ з/п	Назва теми	Кількість годин	
		Д.Ф.Н	З.Ф.Н.
2	До теми 2. Сучасні системи управління інформацією та подіями безпеки SIEM SPLUNK на об'єктах водного транспорту.	2	1
3	До теми 3. Сучасні антивірусні технології на об'єктах водного транспорту.	2	2
4	До теми 4. Сучасні інформаційні технології в сфері інформаційної та кібербезпеки об'єктів водного транспорту	2	3
5	До теми 5. Інтелектуальні технології оцінки та підтримки інформаційної та кібербезпеки на об'єктах водного транспорту.	2	2
6	До теми 6. Інформаційні технології оцінки основних факторів інформаційної та кібер-безпеки на об'єктах водного транспорту.	2	2
7	До теми 7.. Інтелектуальні технології підтримки прийняття рішень забезпечення інформаційної та кібер-безпеки на об'єктах водного транспорту	2	1
8	До теми 8. Інформаційно-когнітивні технології підтримки прийняття рішень забезпечення інформаційної та кібер-безпеки на об'єктах водного транспорту	2	1
Разом		16	41

Розподіл годин підготовки самостійної роботи

№	Вид роботи	Кількість годин	
		ДФН	ЗФН
Модуль 1			
1	Підготовка до лекцій	4	4
2	Підготовка до лабораторних робіт	8	8
3	Підготовка до модульних контрольних робіт	10	10
4	Самостійне опрацювання окремих тем навчальної дисципліни	16	16
5	Підготовка до екзамену	22	22
Разом за курсом		60	78

Індивідуальне науково-дослідне завдання

Індивідуальне навчально-дослідне програмою не передбачене.

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;
- робота з літературою;
- лабораторна робота;
- інструктаж (інструктаж з техніки безпеки та пожежної безпеки проводиться одноразово на першому занятті в лабораторії);
- репродуктивний метод;
- метод проблемного викладу.

При вивченні дисципліни використовуються 3 групи методів навчання:

I група методів - методи організації та здійснення навчально-пізнавальної діяльності:

- словесні: розповідь-пояснення, лекція;
- наочні: ілюстрація, презентація, демонстрація;
- практичні: лабораторні роботи;
- індуктивні методи: узагальнення, пов'язані із проведенням експериментів;
- дедуктивні методи: розвиток абстрактного мислення для засвоєння навчального матеріалу на основі узагальнень;
- репродуктивні методи: робота за готовими прикладами;
- творчі, проблемно-пошукові методи: самостійна, творча пізнавальна діяльність;
- навчальна робота студентів під керівництвом НПП;
- самостійна робота студентів.

II група методів - методи стимулювання й мотивації навчально-пізнавальної діяльності:

- методи стимулювання інтересу до навчання: створення ситуації інтересу при викладанні матеріалу; аналіз життєвих ситуацій;
- методи стимулювання обов'язку й відповідальності: роз'яснення мети навчального предмета; вимоги до вивчення предмета; заохочення та покарання в навчанні;

III група методів - методи контролю (самоконтролю, взаємоконтролю), корекції (самокорекції, взаємокорекції) за ефективністю навчально-пізнавальної діяльності:

Засобами оцінювання результатів навчання є:

- модульні контрольні роботи;
- звіти з лабораторних робіт;
- командні проекти;

- індивідуальні та групові завдання;
- завдання на лабораторному обладнанні;
- екзаменаційні роботи;
- 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 екзаменаційних робіт;
- 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 за змістом є об'єднаним представленням модульних контрольних робіт, які проводяться для здобувачів денної форми навчання, і має відповідати тим самим вимогам. Контрольна робота на заочній формі навчання 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 семестрову екзаменаційну роботу (проводиться у письмовій формі), до якої він допускається, якщо він має за виконання всіх передбачених елементів модулів не менше 35 балів. Максимальна кількість балів за семестрову підсумкову залікову роботу (екзамен) становить 40 балів. Студенти заочної форми навчання пишуть підсумкову залікову роботу обов'язково.

Підсумкова оцінка з дисципліни від 60 до 100 балів визначається як сума балів за змістовими модулями та семестрової залікової роботи (у разі її написання).

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.

8.1 Критерії оцінювання лабораторних робіт

При оцінюванні лабораторних робіт враховуються наступні критерії:

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

Максимальна оцінка за кожну лабораторну роботу для студентів ДФН становить 5 балів.

Максимальна оцінка за кожну лабораторну роботу для студентів ЗФН становить 8 балів.

Максимальна сумарна кількість балів за лабораторні роботи для студентів ДФН становить: $8 \times 5 = 40$ балів

Максимальна сумарна кількість балів за лабораторні роботи для студентів ЗФН становить: $4 \times 8 = 32$ бали.

Критерії оцінювання лабораторних робіт

Кількість балів (в дужках для ЗФН)	Критерії оцінювання
Модуль 1	
5 (8)	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 (6,4)	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 (4,8)	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 (3,2)	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.

Кількість балів (в дужках для ЗФН)	Критерії оцінювання
1 (1,6)	Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.
0 (0)	Робота не виконана.
	<i>Максимальна сумарна оцінка студента за даний компонент програми для ДФН – 40 балів (8 робіт по 5 балів). Максимальна сумарна оцінка студента за даний компонент програми для ЗФН – 32 балів (4 роботи по 8 балів). При незначних відхиленнях від вказаних критеріїв оцінка може доповнюватись знаками «-» або «+», що при підсумовуванні відповідає 0,5 бала.</i>

8.2 Критерії оцінювання модульних контрольних робіт

Для поточного модульного контролю студентами виконуються 2 (дві) модульні контрольні роботи (МКР) за матеріалами змістовних модулів.

Критерієм оцінювання МКР є відсоток правильних відповідей на питання модульної контрольної роботи.

Максимальна кількість балів за кожну МКР для студентів ДФН становить 10 балів.

Загальна сума балів за модульні контрольні роботи для студентів ДФН становить: $2 \times 10 = 20$ балів;

Максимальна кількість балів за кожну МКР для студентів ЗФН становить: 14 балів.

Загальна сума балів за модульні контрольні роботи для студентів ЗФН становить: $2 \times 14 = 28$ балів.

Критерії оцінювання задач та практичних завдань в МКР для ДФН

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

Критерії оцінювання задач та практичних завдань в МКР для ЗФН

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	14	12,6	11,2	9,8	8,4	7,0	5,6	4,2	2,8	1,4

8.3 Критерії оцінювання екзаменаційної роботи

Максимальна оцінка за екзаменаційні роботи – 40 балів.

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	40	36	32	28	24	20	16	12	8	4

Рівні підсумкової оцінки екзамену з дисципліни
(перерахунковий коефіцієнт – 0,4)

Оцінка за 100-бальною шкалою університету / Grade according to 100-points scale of University	Оцінка за шкалою ЄКТС / Grade according to ECTS scale
90-100 (творчий рівень)/(creative level)	A (відмінно) / (excellent)
82-89 (високий рівень)/(high level)	B (дуже добре) / (very good)
74-81 (добрий рівень)/(good level)	C (добре) / (good)
64-73 (середній рівень)/(average level)	D (посередньо) / (average)
60-63 (задовільний рівень)/(satisfactory level)	E (достатньо) / (satisfactory)
35-59 (низький рівень)/(low level)	FX (незадовільно з можливістю повторного складання) / (unsatisfactory with the possibility to repass the exam)
1-34 (незадовільний рівень)/(unsatisfactory level)	F (незадовільно з обов'язковим повторним вивченням) / (unsatisfactory with the compulsory repeating of the course)

8.5 Розподіл балів

Розподіл оцінки за змістовними модулями та видами контролю

		Денна форма		Заочна форма	
		Вид роботи	Кількість балів	Вид роботи	Кількість балів
Модуль 1					
ЗМ1	T1	Лабораторна робота 1	5	Лабораторна робота 1	8
	T4	Лабораторна робота 2	5	-	-
	МКР1	Тест	10	Тест	14
ЗМ2	T6	Лабораторна робота 3	5	Лабораторна робота 3	8
	T7	Лабораторні роботи 4, 5, 6	15	Лабораторна робота 4	8
	T8	Лабораторні роботи 7, 8	10	Лабораторна робота 7	8
	МКР2	Тест	10	Тест	14
Підсумковий семестровий контроль		екзамен	40	екзамен	40
Всього			100	100	

9. Засоби навчання

Апаратне забезпечення, необхідне для вивчення навчальної дисципліни, включає персональний комп'ютер (настільний або ноутбук) із доступом до Інтернет.

Програмне забезпечення, необхідне для вивчення навчальної дисципліни, включає:

- операційну систему Windows;
- текстовий процесор та редактор растрових зображень (для підготовки звітів з лабораторних робіт);
- pdf-, djv-переглядач (для ознайомлення з джерелами інформації, представленими в електронній формі);
- Power Point для ознайомлення з тематичними презентаціями;
- MS Excel та Mathcad для виконання розрахункових завдань.

Використовуються апаратні та програмні можливості лабораторій №129 і 130, 133 б кафедри КТІБ ННІАЕ НУК.

В процесі проведення лекцій і лабораторних робіт для демонстрації тематичних презентацій і прикладів використовується наявне в лабораторіях мультимедійне обладнання.

7. Рекомендовані джерела інформації

Основні:

1. Передерій В.І. Інтелектуальні та інформаційно-когнітивні технології підтримки прийняття рішень: навчально-методичний посібник / В.І. Передерій, С.М. Нужний – Миколаїв: НУК, 2024. – 132 с. (Затверджено Грифом Вченої ради НУК, протокол № 2 від 23.02.2024 року).

2. Castillo E. Expert systems and probabilistic network models / E. Castillo, J.M. Gutierrez, A.S. Hadi // Springer Science & Business Media, New York. – 2012. DOI: 10.1007/978-1-4612-2270-5

3. Штовба С.Д. Введення в теорію нечітких множин та нечітку логіку / http://matlab.exponenta.ru/fuzzylogic/book1/1_7_5_5.php

4. Perederiy V., Borchik E. Information technology for determination, assessment and correction of functional sustainability of the human-operator for the relevant decision-making in human-machine critical application systems / Theoretical and practical aspects of the development of modern science: the experience of countries of Europe and prospects for Ukraine: monograph. Riga, Latvia: «Baltija Publishing», 662 p, 2019. P. 490-509.

Допоміжна:

5. Advances in Fuzzy Decision Making Theory and Practice / I.Skalna, J.Duda, B.Rebiasz та ін.; Editor: Kacprzyk J. — Springer, 2015 .— 162 p.
6. Liao H. Hesitant Fuzzy Decision Making Methodologies and Applications / H.Liao, Z.Xu .— Singapore: Springer, 2017 .— 285 p
7. Коваленко І.І., Передерій В.І., Швед А.В. Концепція побудови системних інформаційних технологій для підтримки експертного аналізу сценаріїв. *Системні технології: регіональний міжвузівський збірник наукових праць*. Дніпропетровськ, 2010. № 6(71). С. 74-88
8. Копитчук М.Б., Передерій В.І. Визначення нечітких ситуацій впливу навколишнього середовища на когнітивний стан особи, що приймає рішення в ергатичних системах. Вісник Національного університету "Львівська політехніка". Комп'ютерні науки та інформаційні технології. 2014. № 800. С.244-250: веб-сайт. URL: http://nbuv.gov.ua/UJRN/VNULPKNIT_2014_800_35
9. Лавров Е.А., Волосюк Н.Б., Пасько В.П. та ін. Комп'ютерне моделювання дискретної взаємодії людини та машини для забезпечення надійності та кібербезпеки критичних систем. Третя міжнародна конференція з людського фактору у складних технічних системах та середовищах (ERGO). 2018. С. 67–70.
10. Передерій В.І., Бабічев С.О., Литвиненко В.І. Застосування мережі Байєса з оцінки ступеня значимості впливових факторів на оператора в автоматизованих системах прийняття релевантних рішень. Комп'ютерні науки та інформаційні технології. Вісник національного університету «Львівська політехніка». Львів, 2012. №733. С. 120-128.

Інформаційні ресурси мережі Інтернет:

1. Посібник користувача GeNIe 2.0 <https://www.bayesfusion.com/>
<https://www.bayesfusion.com/genie/>

Зміни та доповнення