

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
ІМЕНІ АДМІРАЛА МАКАРОВА

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ,
АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ»

Другого рівня вищої освіти
за спеціальністю «F5 Кібербезпека та захист інформації»
галузі знань «F Інформаційні технології»

Освітня кваліфікація – Магістр з кібербезпеки та захисту інформації,
Професійна кваліфікація – Провідний фахівець сфери захисту інформації

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Голова вченої ради
/ О.М. Дубовий /
(протокол № 2 від "18" 02 2025 р.)
Освітня програма вводиться в дію з ____ 2025 р.
Ректор / Є.І. Трушляков /
(наказ № 1 від "04" 03 2025 р.)



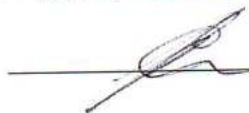
Миколаїв 2025 р.

ЛИСТ ПОГОДЖЕННЯ освітньо-професійної програми

Проект Освітньо-професійної програми «*Системи технічного захисту інформації, автоматизація її обробки*» розглянута на засіданні кафедри комп'ютерних технологій та інформаційної безпеки.

Протокол № 10 від «12» 02 2025 р.

Завідувач кафедри

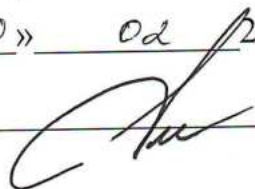


С.М. Нужний

Проект Освітньо-професійної програми «*Системи технічного захисту інформації, автоматизація її обробки*» розглянуто Методичною радою Навчально-наукового інституту автоматики та електротехніки

Протокол № 2 від «20» 02 2025 р.

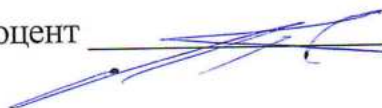
В.о голови, к.т.н., доц.



Д.О. Жук

Проект Освітньо-професійної програми «*Системи технічного захисту інформації, автоматизація її обробки*» погоджено з навчальним відділом

Начальник навчального, к.т.н., доцент



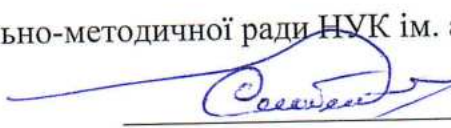
А.В. Лабарткава

Проект Освітньо-професійної програми «*Системи технічного захисту інформації, автоматизація її обробки*» розглянуто Навчально-методичною радою НУК ім. адм. Макарова

Протокол № 2 від «26» 02 2025 р.

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

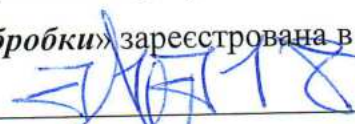
К.т.н., доцент



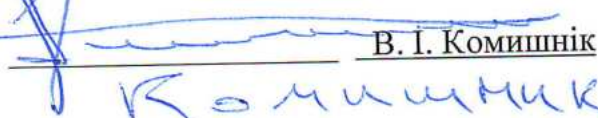
/ С.О. Слободян /

Освітньо-професійна програма «*Системи технічного захисту інформації, автоматизація її обробки*» зареєстрована в Єдиної державної бази з питань освіти.

ID програми



Керівник ННЦЦК



В.І. Комишнік

ПЕРЕДМОВА

Освітньо-професійна програма «Системи технічного захисту інформації, автоматизація її обробки» зі спеціальності **F5 Кібербезпека та захист інформації** другого рівня вищої освіти розроблена у зв'язку з метою імплементації постанови Кабінету Міністрів України від 30 серпня 2024 року № 1021 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти» та наказом Міністерства освіти та науки України від 19.листопада 2024 року №1625 «Про особливості запровадження змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти, затверджених постановою Кабінету Міністрів України від 30 серпня 2024 року № 1021» (Із змінами і доповненнями, внесеними наказом Міністерства освіти і науки України від 5 грудня 2024 року N 1709)

Розроблено робочою групою у складі:

Гарант освітньо-професійної програми – Передерій Віктор Іванович, професор кафедри комп'ютерних технологій та інформаційної безпеки, д.т.н., (наказ №228 від 29.09.2024)

Науково-педагогічні працівники:

1. Нужний Сергій Миколайович, завідувач кафедри КТІБ, к.т.н., доцент, член проектної групи
2. Козирев Сергій Сергійович, доцент кафедри КТІБ, к.т.н., доцент, член проектної групи
3. Сірівчук Андрій Сергійович, доцент кафедри КТІБ, к.т.н., член проектної групи

Працедавці:

1. Деменюк О. А., начальник Управління Держспецзв'язку в Миколаївській області
2. Григор'єв І. Ф., директор ТОВ Безпекаінфосервіс
3. Богаченко Є. В., директор КП «Міський інформаційно-обчислювальний центр»

Освітньо-професійна програма запроваджена з 01.09.2025 р.

Термін перегляду освітньої програми 1 раз на 2 роки.

ЗМІСТ

1. Профіль освітньо-професійної програми зі спеціальності F5 Кібербезпека та захисту інформації другого рівня вищої освіти за ОПП «Системи технічного захисту інформації, автоматизація її обробки»	5
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність	14
2.1. Перелік компонент ОПП	14
2.2. Структурно-логічна схема освітньо-професійної програми	16
3. Форма атестації здобувачів вищої освіти	17
4. Матриця відповідності програмних компетентностей компонентам освітньої програми	18
5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньо-професійної програми	19

**1. Профіль освітньо-професійної програми зі спеціальності
F5 «Кібербезпека та захист інформації» другого рівня вищої освіти за ОПП
«Системи технічного захисту інформації, автоматизація її обробки»**

1 - Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, проспект Героїв України, 9, 54025. Навчально-науковий інститут автоматики і електротехніки Кафедра комп'ютерних технологій та інформаційної безпеки
Ступінь вищої	Магістр
Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Офіційна назва освітньо-професійної програми	Системи технічного захисту інформації, автоматизація її обробки <i>Systems of technical information security, automation of its processing</i>
Форми навчання	Денна, заочна
Освітня кваліфікація	Магістр з кібербезпеки та захисту інформації Провідний фахівець сфери захисту інформації
Кваліфікація в дипломі	Освітня програма – «Системи технічного захисту інформації, автоматизація її обробки» Ступінь вищої освіти – магістр Спеціальність – F5 Кібербезпека та захист інформації Галузь знань – F Інформаційні технології
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 роки 4 місяців.
Наявність акредитації	Не має (первина)
Цикл / рівень	НРК України – 7 рівень (магістерський), EQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра. Умови вступу визначаються «Правилами прийому до Національного університету кораблебудування імені адмірала Макарова», затвердженими Вченою радою НУК.
Мова(и) викладання	Українська мова. Окремі дисципліни викладаються англійською мовою.
Термін дії освітньо-професійної програми	до 01.07.2029 р.
Інтернет-адреса постійного розміщення опису освітньо-професійної програми	https://nuos.edu.ua/studentu/polozhennya-nuk/opis-opp/
2 - Мета освітньої програми	
Мета: підготовка висококваліфікованих (провідних) фахівців з технічного захисту інформації, які володіють сучасними аналітичним мисленням, теоретичними знаннями і прикладними навичками, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки критичної інформаційної інфраструктури воднотранспортного комплексу України та електроенергетичних систем Теоретичний зміст предметної області Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії	

ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, регресійного аналізу, методів технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки.

Методи, методики, технології забезпечення інформаційної безпеки, якими має оволодіти здобувач другого рівня вищої освіти для застосовування на практиці: методами фундаментальних та прикладних наук, технологіями створення та супроводження систем інформаційної безпеки; методами системного аналізу досліджувати їх компоненти з використанням програмно-технічних засобів, математичного та комп'ютерного моделювання, інформаційних технологій та професійних прикладних програм; методами та технологіями налагодження, виробництва й експлуатації програмно-технічних засобів комп'ютерних систем та мереж, стандартами, процедурами та засобами підтримки керування життєвим циклом систем захисту інформації; методами проектної, організаційної та управлінської діяльності.

Об'єкти вивчення:

– сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій на об'єктах інформаційної діяльності та критичних інфраструктур водотранспортного комплексу України та електроенергетичних систем в сфері інформаційної та кібербезпеки;

– інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології обробки інформації, в тому числі й з обмеженим доступом;

– інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур водотранспортного комплексу України та електроенергетичних систем;

– системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків) для водотранспортного комплексу України та електроенергетичних систем;

– інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси) ;

– програмне та програмно-апаратне забезпечення (засоби) інформаційного та кіберзахисту;

– системи управління інформаційною безпекою та/або кібербезпекою в водотранспортному комплексі України та в електроенергетичних системах;

– технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки .

Інструменти та обладнання: системи розробки, забезпечення, моніторингу та контролю процесів інформаційної безпеки; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; засоби, пристрої, мережне устаткування та середовище; загальне та спеціалізоване технічне та програмне забезпечення, контрольовано-вимірювальні прилади, програмні та радіотехнічні засоби моніторингу і протидії витоку інформації.

3 - Характеристика освітньої програми

Предметна область (галузь знань, спеціальність, спеціалізація)	Галузь знань – F Інформаційні технології Спеціальність – F5 Кібербезпека та захист інформації Спеціалізація – Системи технічного захисту інформації, автоматизація її обробки
Орієнтація освітньої програми	Практична прикладна професійна діяльність
Основний фокус освітньої програми та спеціалізації	Підготовка фахівців зі спеціалізації «Системи технічного захисту інформації, автоматизація її обробки» спеціальності F5 «Кібербезпека та захист інформації», галузі знань F «Інформаційні технології», спрямована на набуття знань, умінь, інших компетентностей для роботи у галузі інформаційної безпеки, технічного захисту інформації, автоматизації її обробки. Ключові слова: інформаційна безпека, захист інформації, управління безпекою, безпека інформаційно-комунікаційних систем.
Особливості програми	Вивчення особливостей проектування та експлуатації систем технічного захисту інформації та кібербезпеки критичних інформаційних інфраструктур водно-транспортного комплексу України (в т.ч. захищених акваторій, судноплавних компаній та окремих суден,

	з використанням безпілотних надводних і підводних апаратів) та електроенергетичних систем України (південний регіон), з метою підготовки студентів до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації «магістр з кібербезпеки та захисту інформації» та професійної кваліфікації «провідний фахівець сфери захисту інформації»
4 - Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець може займати первинні посади (За ДК 003:2010): – Згідно до освітньо-професійної підготовки: 2139.2 Експерт з управління інформаційними технологіями; 2139.2 Аудитор інформаційних технологій (з кібербезпеки); 2139.2 Аналітик мереж і систем 2139.2 Аналітик загроз безпеки. 2139.2 Аналітик з безпеки інформаційно-комунікаційних систем 2139.2 Фахівець з технічного захисту інформації 2149.2 Професіонал із організації захисту інформації з обмеженим доступом; 2433.2 Професіонали в галузі інформації та інформаційного аналізу. – Згідно до професійної підготовки: 2139.2 Фахівець сфери захисту інформації 2139.2 Провідний фахівець сфери захисту інформації* 2139.2 Системний фахівець сфери захисту інформації* Примітка: * в відповідності до Додатку В «Похідні від професій (професійні назви робіт)» до ДК 003:2010
Подальше навчання	Можливість здобуття освіти на третьому (освітньо-науковому) рівні вищої освіти у навчальних закладах відповідного рівня акредитації. Можливість підвищення кваліфікації та отримання додаткової післядипломної освіти (в системі освіти дорослих)
5 - Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, технологія проблемного і диференційованого навчання, технологія інтенсифікації та індивідуалізації навчання, технологія програмованого навчання, інформаційна технологія, технологія розвивального навчання, кредитно-трансферна система організації навчання, самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді: лекцій, мультимедійних лекцій, інтерактивних лекцій, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, консультацій з викладачами, навчання через практику та курсове проектування. Проблемно-орієнтоване навчання з набуттям компетентностей, достатніх для продукування нових ідей, розв'язування комплексних проблем у професійній галузі. Індивідуальне наукове керівництво, підтримка і консультування науковим керівником.
Оцінювання	Екзамени, заліки, тестові завдання, курсові роботи, презентації, звіти з лабораторних та практичних робіт, кваліфікаційний екзамєн, захист кваліфікаційної роботи. Методи оцінювання: письмовий контроль, самоконтроль, тестовий контроль, усний контроль.
6 - Програмні компетентності	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки

Загальні компетентності (ЗК)	За ОПП	За ОПС ¹	За ПС ²	Опис компетенції
	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-5		–	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
	ЗК-6	–	ЗК.01	Здатність діяти соціально відповідально та громадсько свідомо
	ЗК-7	–	ЗК.05	Здатність до адаптації та дії у новій ситуації
	ЗК-8	–	ЗК.06	Здатність до вибору стратегії спілкування, праці в команді
	ЗК-9	–	ЗК.07	Здатність спілкування рідною мовою як усно, так і письмово, спілкуватися іноземною мовою (переважно англійською) на рівні, що забезпечує ефективну професійну діяльність

Примітки:

¹ – компетенції та результати навчання за Стандартом вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» для другого (магістерського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 18.03.2021 року №332

² – компетенції та результати навчання («знання» – «З» і «уміння та навички» – «У») за Професійним стандартом «Фахівець сфери захисту інформації» (професійна кваліфікація – провідний фахівець сфери захисту інформації), затвердженого наказом Адміністрації Держспецзв'язку від 25.11.2022 року №715

Фахові компетентності (КФ)	КФ-1		A1	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-2		A9	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
	КФ-3		A3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
	КФ-4		A4	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
	КФ-5		A2	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-6	–	Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно 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-10	Д	Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки
КФ-11	A10	Здатність виявляти закладні пристрої на об'єктах інформаційної діяльності (як члени команди)
КФ-12	A5	Здатність виконувати передпроектні роботи щодо систем та комплексів захисту інформації
КФ-13	A6	Здатність проводити спеціалізовані дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності
КФ-14	A7	Здатність впроваджувати(активізувати) програмні та апаратні засоби захисту інформації в системах і на об'єктах
КФ-15	A8	Здатність адмініструвати системи, мережі та системи безпеки інформації
КФ-16	Г1	Здатність проводити оцінку відповідності (держану експертизу) програмних засобів технічного та криптографічного захисту інформації

	КФ-17	Г2	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимог технічного та організаційного спрямування щодо системи технічного криптографічного захисту інформації
7 - Результати навчання			
Знання та розуміння	РН-1	A1.36 A2.35 B2.33 Г2.31	Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
		Г1.Y1. Г1.Y2. Г2.Y3. Г2.Y4	
	РН-2	A1.31 A2.34 B1.31 B1.31 B4.32 Г1.31 Д1.31	Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
		A1.Y2 B1.Y1 Г1.Y5 Г2.Y4	
	РН-3	A2.36 A3.31 A3.32 A3.33 B2.35 Г1.31 Д1.31	Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
		A1.Y4 B1.Y3 B1.Y4 B2.Y1 Г1.Y4 Г2.Y3	
	РН-4	A2.36 A3.31 A3.33 B2.36 B4.32 Г1.31 Д1.31	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
		A1.Y2 A1.Y4 A3.Y4 B1.Y4 B2.Y3 B3.Y3 Г1.Y5	
	РН-5	A2.34 A3.31 B2.35 B4.33 Г1.31	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.
		A1.Y4 A3.Y5 B1.Y4 B3.Y1 B4.Y2 B4.Y3	

PH-6	A2.34 Б1.31 Б1.35 Б2.32 Б2.34 Г1.31	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
	A2.Y2 Б1.Y1 Б1.Y2 Б2.Y1 Б2.Y4 В3.Y1 В3.Y3 Г1.Y3	
PH-7	A3.35 A3.36 A6.37 Б1.33 Б1.33 В4.34 Г1.36 Г2.37 В4.32	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
	Б1.Y2 Г1.Y5 Г2.Y3	
PH-8	A2.36 В3.36 В4.32 В4.34 Г1.31 Г1.33 Г2.31 Д1.31	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
	A1.Y4 В1.Y3 В3.Y1 В3.Y3 Г1.Y2 Г2.Y3 Г2.Y4 Д1.Y3 Д1.Y4	
PH-9	A1.34 Б2.32 В1.31 В2.31 В4.31 Г1.35 Г2.35 Д1.34	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
	A1.Y1 A2.Y2 Б1.Y1 Б1.Y3 В1.Y1 Г1.Y1 Г1.Y3 Г1.Y4 Г2.Y2 Д1.Y4	
PH-10	A1.35 A1.37 A2.31 Б1.31 Б1.34	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для

	B1.31 B2.31 B3.32 B3.35 Д1.32 Д2.31 A1.Y1 A1.Y4 Б1.Y1 B1.Y1 B2.Y1 B3.Y1 B4.Y2 B5.Y3 Д2.Y1	інформаційної безпеки та/або кібербезпеки організації.
РН-11	A1.34 Б1.35 Б2.37 B1.32 B5.31 B5.32 Д1.34 A1.Y1 A1.Y4 A2.Y5 Б1.Y1 Б1.Y3 B1.Y1 B2.Y3 B5.Y3	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-12	A1.37 A2.36 Б2.35 B2.31 B2.32 B3.31 B4.33 A1.Y4 A2.Y2 Б3.Y1 B2.Y1 B3.Y1 B4.Y3 Г1.Y1 Г2.Y2 B5.Y3	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-13	A3.31 A3.32 A3.33 A3.36 Б2.36 B3.36 Д1.31 Г2.31 Г2.34 A1.Y4 A2.Y2 A3.Y4 A3.Y5 Б1.Y1 Б2.Y1 Б3.Y1 B3.Y3 Y2.Y2 Г2.Y3	Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

	PH-14	A1.35 A2.31 Б1.34 B4.31 Г1.33	Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
		A1.Y1 A1.Y4 A2.Y2 A3.Y1 Б3.Y1 B2.Y5 B3.Y1 B4.Y3 Г1.Y1 Г2.Y2 Г2.Y5	
		A1.36 B2.33 Г2.31 Г2.34	
		A1.Y3 B4.Y5 Г1.Y1 Г1.Y2 Г1.Y3 Г2.Y2 Г2.Y3 Г2.Y4	
		A1.35 Б1.31 B1.31 Г1.33 Д1.32 Д2.32	
	PH-15	A1.Y1 Б1.Y3 B1.Y1 B1.Y4 B3.Y1 B4.Y2 Д1.Y3 Д2.Y3	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.
		A1.35 Б1.31 B1.31 Г1.33 Д1.32 Д2.32	
		A1.Y1 Б1.Y3 B1.Y1 B1.Y4 B3.Y1 B4.Y2 Д1.Y3 Д2.Y3	
		A1.35 Б1.31 B1.31 Г1.33 Д1.32 Д2.32	
		A1.Y1 Б1.Y3 B1.Y1 B1.Y4 B3.Y1 B4.Y2 Д1.Y3 Д2.Y3	
	PH-16	Г1.31 Г2.33 Д1.31	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.
		A3.Y5 B1.Y3 Г1.Y3 Г2.Y4	
		A1.36 E1.33 Д1.33 Д2.33	
		A1.Y3 A3.Y5 Б1.Y3 Г1.Y1 Г1.Y3 Г2.Y4 E1.Y3 Д2.Y5	
		A1.36 E1.33 Д1.33 Д2.33	
	PH-17	A1.Y3 A3.Y5 Б1.Y3 Г1.Y1 Г1.Y3 Г2.Y4 E1.Y3 Д2.Y5	Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та\або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
		A1.36 E1.33 Д1.33 Д2.33	
		A1.Y3 A3.Y5 Б1.Y3 Г1.Y1 Г1.Y3 Г2.Y4 E1.Y3 Д2.Y5	
		A1.36 E1.33 Д1.33 Д2.33	
		A1.Y3 A3.Y5 Б1.Y3 Г1.Y1 Г1.Y3 Г2.Y4 E1.Y3 Д2.Y5	
	PH-18	A1.36 E1.33 Д1.33 Д2.33	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та\або кібербезпеки.
		A1.Y3 A3.Y5 Б1.Y3 Г1.Y1 Г1.Y3 Г2.Y4 E1.Y3 Д2.Y5	
		A1.36 E1.33 Д1.33 Д2.33	
		A1.Y3 A3.Y5 Б1.Y3 Г1.Y1 Г1.Y3 Г2.Y4 E1.Y3 Д2.Y5	
		A1.36 E1.33 Д1.33 Д2.33	

PH-19	A2.34 A2.36 Б1.31 Б2.33 Б2.35 В3.36 В4.32 Г1.31 Д1.31	Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
	A1.Y2 A2.Y2 A3.Y5 В1.Y3 В2.Y1 В4.Y4 Г1.Y2 Г1.Y2 Г1.Y3 Г2.Y3	
PH-20	A2.34 A2.36 Б1.31 В1.31 В4.32 Г1.31 Г1.36 Д1.31	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
	A1.Y2 A2.Y2 В1.Y3 В3.Y1 В4.Y4 Д1.Y5	
PH-21	A2.34 В4.34	Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
	A1.Y2 A1.Y4 A2.Y2 Б2.Y3 В4.Y2 В4.Y4 В2.Y7	
PH-22	A2.34 Б1.31 В4.32 Г1.31 Д1.31	Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
	A1.Y5 A3.Y5 В1.Y2 В1.Y3 В2.Y1 В4.Y2 Г1.Y1 Г2.Y2	
PH-23	A1.31 A2.34 Б2.31 Г1.31 Г1.36 Д1.31	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних

	A2.Y2 A3.Y5 B1.Y1 B1.Y4 B2.Y2 B2.Y1 B3.Y1 Г1.Y2 знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
	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 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.
8-Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Кадрове забезпечення освітньої програми «Системи технічного захисту інформації, автоматизація її обробки» складається з професорсько-викладацького складу кафедр Навчально-наукового інституту автоматики і електротехніки. До викладання окремих дисциплін відповідно до їх компетенції та досвіду залучений професорсько-викладацький склад кафедр Навчально-науково гуманітарного інституту. Практико-орієнтовний характер освітньої програми передбачає участь фахівців-практиків, які відповідають наряду програми, що підсилює синергетичний ефект комплексу теоретичної та практичної підготовки. Гарант освітньої програми та викладацький склад, який забезпечує її реалізацію, відповідають вимогам, визначеним Ліцензійними вимогами провадження освітньої діяльності
Матеріально-технічне забезпечення	Навчально-лабораторна база структурних підрозділів ННІ автоматики та електротехніки Національного університету кораблебудування імені адмірала Макарова дозволяє організовувати та проводити заняття з усіх навчальних дисциплін на достатньому рівні. Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає встановленим вимогам. Наявна вся необхідна соціально-побутова інфраструктура, кількість місць у гуртожитках відповідає потребам. Наукові дослідження проводяться у спеціалізованих навчально-наукових лабораторіях (ННЛ) кафедри комп'ютерних технологій та інформаційної безпеки, кафедри електричної інженерії суден та роботизованих комплексів та на базі морської лабораторії «Дельта». На кафедрі наявні: ННЛ захисту аудіо- і відеоінформації та комп'ютерних технологій в інформаційних мережах; ННЛ безпеки інформаційних телекомунікаційних систем і мереж; ННЛ електромагнітних полів та хвиль в системах ТЗІ; ННЛ систем та методів технічного захисту інформації; ННЛ інформаційної та кібербезпеки інформаційно-телекомунікаційних систем; СННЛ технічних систем засобів інформації (з обмеженим доступом): ННЛ електроніки та мікропроцесорної і ННЛ електрообладнання та автоматики підводних апаратів В НУК є 4 локальні комп'ютерні мережі з повним покриттям навчально-наукових приміщень бездротовим доступом мережі Інтернет. Користування Інтернет-мережею безлімітне. Для проведення інформаційного пошуку та обробки результатів є спеціалізовані

	комп'ютерні класи в бібліотеці та на кафедрах університету із спеціалізованим програмним забезпеченням та відкритим доступом до локальних ресурсів університету та Інтернет.
Інформаційне та навчально-методичне забезпечення	Офіційний веб-сайт http://www.nuos.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Матеріали навчально-методичного забезпечення освітньо-професійної програми викладені на освітньому порталі http://education.nuos.edu.ua/. Фонд бібліотеки НУК перевищує 756 тис. примірників, наукових видань – 95 тис. прим., навчальних – 379 тис. прим., біліше 123 тис. прим. періодичних видань. Віртуальний сервіс бібліотеки складається з: електронного каталогу, баз даних, web-сайту бібліотеки, спробами впровадження ЕДД та віртуальної довідки. Читальний зал забезпечений бездротовим доступом до мережі Інтернет. Всі ресурси бібліотеки доступні через сайт університету: http://lib.nuos.edu.ua. Інституційний репозитарій (http://eir.nuos.edu.ua/) є одним із найважливіших шляхів розповсюдження результатів досліджень науковців університету. На 01.01.2025 р. в репозитарії налічувалось 8194 документи. Якісній підтримці освітнього процесу в університеті сприяє наявність доступу до наукометричних і навчальних БД, наукових платформ, електронних бібліотек, в першу чергу: Scopus та Web of Science; БД ScienceDirect; БД Springer, Research4Life.
9 - Академічна мобільність	
Національна кредитна мобільність	Національна кредитна мобільність забезпечується у рамках договорів про встановлення науково-освітнянських відносин для задоволення потреб розвитку освіти і науки, укладених між НУК та національними ВНЗ. Допускаються індивідуальні угоди про академічну мобільність для навчання та проведення досліджень в університетах та наукових установах України. Кредити, отримані в інших університетах України, можуть бути перезараховані відповідно до довідки про академічну мобільність.
Міжнародна кредитна мобільність	Міжнародна наукова мобільність забезпечена договорами про наукову і академічну співпрацю з Auburn University (USA), Stord/Haugesund University college (Norway), Хайкоуським економічним інститутом (Китай). Всі фахівців, залучені до професійної і наукової підготовки, пройшли стажування у провідних європейських університетах: в Університеті подвійної вищої освіти Баден Вюнтенберга (Duale Hochschule Baden-Württemberg Heilbronn Universitat, Німеччина); в Фундації Central European Academy Studies and Certification (CEASC, Польща) у співпраці з Університетом Інформатики (WSInf, м. Лодзь, Польща) та Центром Європейських фондів (BFE); в Морській академії Естонії (м. Таллін, Естонія); в Варшавському університетом наук про життя; в Польському національному комітеті у справах ЮНЕСКО; в Університеті науки та технологій провінції Цзянсу (КНР); Ягелонському університеті (м. Краків, Польща), мають міжнародний досвід освітньої і наукової діяльності Університету подвійної вищої освіти Баден Вюнтенберга (м. Хальброн, Німеччина).
Навчання іноземних здобувачів вищої освіти	Навчання іноземних студентів проводиться на загальних умовах або за індивідуальним графіком
10 – Форми атестації здобувачів вищої освіти	
Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі кваліфікаційного екзамєну (тестова форма) та публічного захисту кваліфікаційної роботи.
Вимоги до	Структура та правила виконання кваліфікаційної роботи визначаються

кваліфікаційної роботи	випускаючою кафедрою. Склад кваліфікаційної роботи повинен відповідати системі компетентностей та системі змістовних модулів відповідно до переліку навчальних дисциплін за спеціалізацією. Тематика кваліфікаційної роботи за спеціалізацією «Системи технічного захисту інформації, автоматизація її обробки» передбачає участь студента у науковій діяльності кафедри комп'ютерних технологій та захисту інформації за тематикою: – Побудова та дослідження моделей інформаційної безпеки судових спеціалізованих інформаційно-комунікаційних систем, виявлення та локалізація їх вразливостей; – Побудова та дослідження моделей на основі теорії однозначних нечітких систем та нейронних мереж для оцінки захищеності інформації; – Побудова та дослідження моделей моніторингу та управління корпоративними мережами; – Побудова та дослідження моделей побудови систем об'єктового захисту для об'єктів критичної інфраструктури водотранспортного комплексу; – Моделювання та дослідження систем контролю доступу на об'єкти критичної інфраструктури водотранспортного комплексу за атрибутними та біометричними ознаками суб'єкта; – Криптографія, криптологія та стеганографія для спеціалізованих систем захисту інформації в водотранспортному комплексі; – Розробка апаратних та апаратно-програмних засобів для захисту віброакустичної інформації; – Моделювання та дослідження систем захисту акваторії та виявлення порушників з використанням підводного охоронного робота та систем висвітлення підводної обстановки; – Програмно-інструментальних засобів дослідження захисту мовної інформації, звукоізоляції та електроакустичних перетворювачів; – Побудова систем підтримки прийняття рішень захисту інформаційних ресурсів сучасної локальної обчислювальної мережі на об'єктах водотранспортного комплексу; – Розробка комплексних систем захисту мережного інформаційного ресурсу; та інші. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації та фальсифікації. Кваліфікаційна робота має бути оприлюднена на офіційному сайті закладу вищої освіти або його підрозділу, або у репозитарії закладу вищої освіти. Оприлюднення кваліфікаційних робіт, що містять інформацію з обмеженим доступом, здійснювати у відповідності до вимог чинного законодавства
11 – Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти	
Наявність системи внутрішнього забезпечення якості вищої освіти	У Національному університеті кораблебудування імені адмірала Макарова розроблена, впроваджена і сертифікована система управління якістю за міжнародним стандартом ISO 9001:2015, що підтверджується відповідними сертифікатами за номером UA231286 та ДСТУ ISO 9001:2015 за номером UA231286 з терміном дії до 8 лютого 2027 року. Оцінку щорічно здійснює незалежна компанія «Bureau veritas certification». Система управління якістю НУК включає в себе наступні процедури і заходи: 1) визначення принципів та процедур забезпечення якості вищої освіти; 2) здійснення моніторингу та періодичного перегляду освітньої

	програми; 3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників вищого навчального закладу та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті вищого навчального закладу, на інформаційних стендах та в будь-який інший спосіб; 4) забезпечення підвищення кваліфікації педагогічних, наукових і науковопедагогічних працівників; 5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, в тому числі самостійної роботи студентів, за освітньою програмою; 6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом; 7) забезпечення публічності інформації про освітню програму, ступені вищої освіти та кваліфікації; 8) забезпечення ефективної системи запобігання та виявлення академічного плагіату в наукових працях працівників вищих навчальних закладів і здобувачів вищої освіти; 9) інші процедури і заходи. Сфера сертифікації: «Надання вищої освіти на рівні кваліфікаційних вимог до підготовки молодших спеціалістів, молодших бакалаврів, магістрів, докторів філософії; підготовка науково-педагогічного персоналу; проведення наукових досліджень та здійснення науково-технічних розробок, готових для подальшого впровадження та виробництва».
--	--

2. Перелік компонентів освітньо-професійної програми та їх логічна послідовність

2.1 Перелік компонентів ОПП

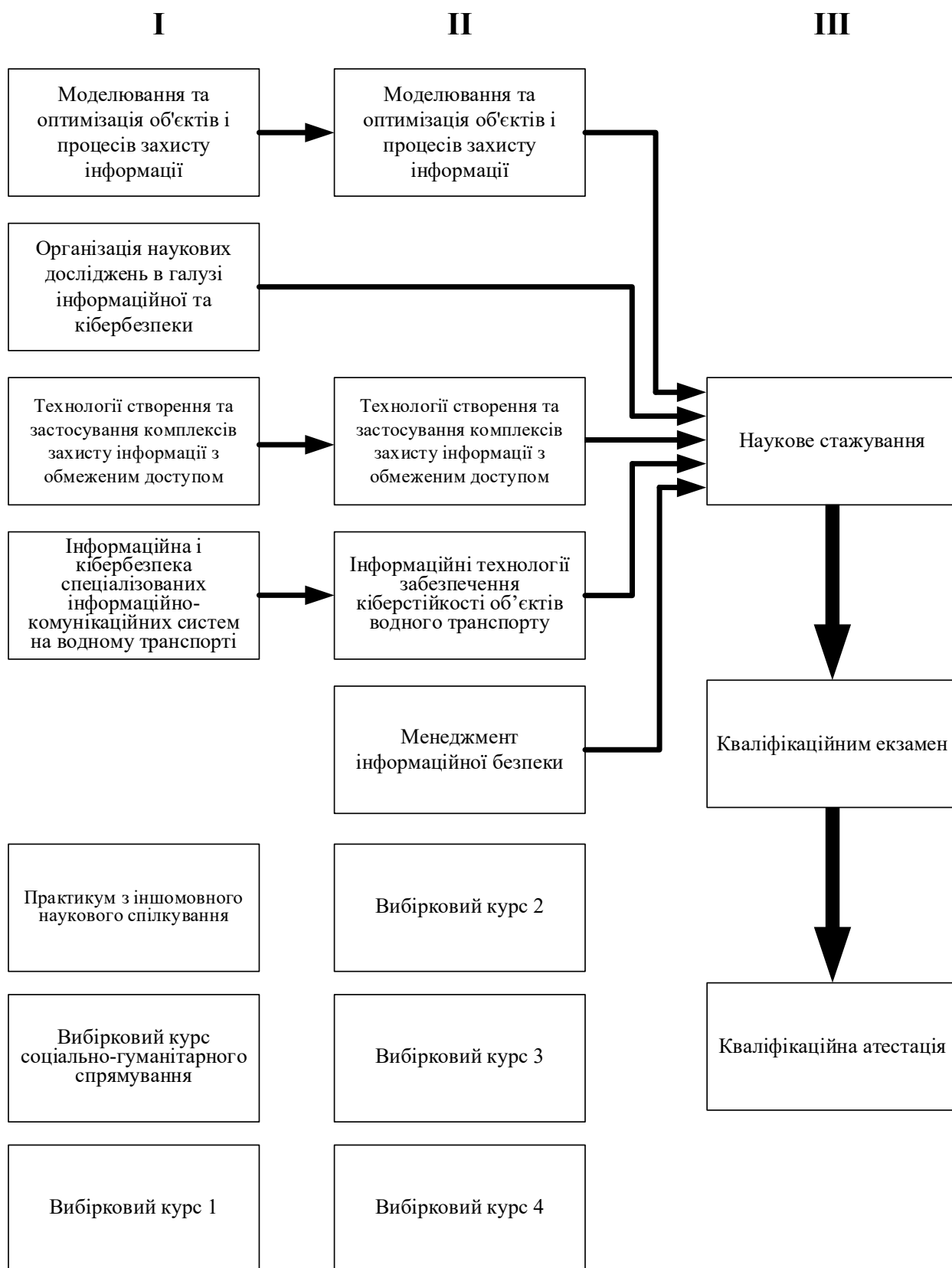
Код за ОПП	Компоненти освітньої-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ECTS	Форма підсумк. контролю	Семестр
1. Обов'язкові компоненти освітньої програми				
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ				
OK1	Практикум з іншомовного наукового спілкування	3	Залік	1
OK2	Моделювання та оптимізація об'єктів і процесів захисту інформації	9	Екзамен / Екзамен, КР	1,2
OK3	Організація наукових досліджень в галузі інформаційної та кібербезпеки	6	Екзамен, КР	1
Всього за цикл		18		
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ				
OK4	Практика	9	Залік	3
OK5	Кваліфікаційна атестація	18	Екзамен	3
OK6	Кваліфікаційний екзамен	3	Екзамен	3
OK7	Технології створення та застосування комплексів захисту інформації з обмеженим доступом	8	Екзамен / Екзамен	1,2
OK8	Інформаційна і кібербезпека спеціалізованих інформаційно-комунікаційних систем на водному транспорті	4	Екзамен	1
OK9	Інформаційні технології забезпечення кіберстійкості об'єктів водного транспорту	3	Екзамен	2
OK10	Менеджмент інформаційної безпеки	3	Екзамен	2
Всього за цикл:		48		
Загальний обсяг обов'язкових компонентів		66		
2. Вибіркові компоненти загальної та професійної підготовки освітньої програми				
ВК1	Вибірковий курс соціально-гуманітарного спрямування*	4	Залік	1
ВК2	Вибірковий курс 1*	5	Залік	1
ВК3	Вибірковий курс 2*	5	Залік	2

ВК4	Вибірковий курс 3*	5	Залік	2
ВК5	Вибірковий курс 4*	5	Залік	2
Загальний обсяг вибірових компонентів		24		
Загальний обсяг освітньо-професійної програми		90		

* – вибіркові компоненти програми обираються студентом згідно «Положення про вибіркові дисципліни у Національному університеті кораблебудування імені адмірала Макарова».

Згідно із Законом України «Про вищу освіту» студенти мають право на «вибір навчальних дисциплін у межах, передбачених відповідною освітньою програмою та робочим навчальним планом, в обсязі, що становить не менш як 25 відсотків загальної кількості кредитів ЄКТС, передбачених для даного рівня вищої освіти. При цьому здобувачі певного рівня вищої освіти мають право вибирати навчальні дисципліни, що пропонуються для інших рівнів вищої освіти, за погодженням з керівником відповідного факультету чи підрозділу».

2.2. Структурно-логічна схема ОПП



Примітка: перехресні зв'язки між дисциплінами 1 та 2 семестру умовно не показані

3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої-професійної програми «Системи технічного захисту інформації, автоматизація її обробки» спеціальності F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології» проводиться у формі кваліфікаційного екзамену і захисту кваліфікаційної роботи. Атестація випускників завершується видачею документу встановленого зразка про присудження йому ступеня магістра із присвоєнням освітньої кваліфікації – «Магістр з кібербезпеки та захисту інформації», та професійної кваліфікації – «Провідний фахівець сфери захисту інформації»

До складання кваліфікаційного іспиту допускаються студенти, які успішно та повною мірою виконали навчальний план. До захисту кваліфікаційної роботи магістра допускаються студенти, які успішно склали кваліфікаційний іспит.

Захист кваліфікаційної роботи магістра відбувається прилюдно на засіданні екзаменаційної комісії, склад якої затверджується у встановленому порядку.

Структура та правила виконання кваліфікаційної роботи визначаються випускаючою кафедрою. Склад кваліфікаційної роботи повинен відповідати системі компетентностей та системі змістовних модулів відповідно до переліку навчальних дисциплін за спеціалізацією. Кваліфікаційна робота за спеціалізацією «Системи технічного захисту інформації, автоматизація її обробки» передбачає комплексний аналіз стану захисту інформаційних ресурсів на досліджуваному об'єкті інформаційної діяльності, розробку моделі технічних каналів витоку інформації, моделі загроз та моделі зловмисника, аналіз інцидентів в системі безпеки об'єкта та автоматизованих системах обробки інформації, тощо. В рамках кваліфікаційної роботи студент повинен вибрати та обґрунтувати методи та технології дослідження, запропонувати алгоритми роботи та структуру системи проведення дослідження, провести верифікацію отриманих даних та Результати дослідження обробляються аналітично, з використанням сучасних методів цифрової обробки інформації/сигналів, спектрально-кореляційних та інших, за необхідності застосовуються методи нечіткої логіки та нейромережеве моделювання. Результати досліджень представляються в графічному та аналітичних виглядах.

**4. Матриця відповідності програмних компетентностей
компонентам освітньо-професійної програми**

	ОК-1	ОК-2	ОК-3	ОК-4	ОК-5	ОК-6	ОК-7	ОК-8	ОК-9	ОК-10
ЗК-1			+	+				+	+	+
ЗК-2		+	+	+				+	+	+
ЗК-3		+	+	+	+	+		+	+	
ЗК-4		+	+	+				+	+	+
ЗК-5	+									
ЗК-6					+		+	+	+	
ЗК-7				+						+
ЗК-8	+		+	+						
ЗК-9	+				+					
КФ-1		+	+					+		+
КФ-2					+	+	+			+
КФ-3			+		+	+	+	+		
КФ-4					+	+	+			+
КФ-5		+	+		+			+		+
КФ-6					+		+		+	
КФ-7					+	+	+	+	+	
КФ-8					+	+	+	+	+	
КФ-9				+	+			+		+
КФ-10	+	+	+							
КФ-11				+	+	+	+			
КФ-12				+	+	+	+			
КФ-13				+		+	+		+	
КФ-14				+		+	+		+	
КФ-15		+					+	+		+
КФ-16							+	+		
КФ-17						+	+			+

**5. Матриця забезпечення програмних результатів навчання (РН)
відповідними компонентами освітньої програми**

	ОК-1	ОК-2	ОК-3	ОК-4	ОК-5	ОК-6	ОК-7	ОК-8	ОК-9	ОК-10
РН-1	+			+	+	+				
РН-2		+		+	+	+	+		+	
РН-3		+	+	+	+	+	+		+	
РН-4		+		+	+	+		+	+	
РН-5						+	+	+	+	+
РН-6			+	+	+	+	+	+	+	
РН-7	+					+	+	+		+
РН-8			+	+	+	+	+		+	+
РН-9				+	+	+	+		+	+
РН-10				+	+	+	+	+	+	+
РН-11			+	+		+	+		+	+
РН-12				+	+	+	+	+		+
РН-13			+	+		+				+
РН-14		+			+	+	+			+
РН-15	+			+	+	+		+	+	
РН-16		+	+	+		+		+	+	+
РН-17		+		+	+	+				
РН-18				+	+	+				+
РН-19		+	+		+	+	+			
РН-20			+	+	+	+	+	+	+	
РН-21		+	+	+	+	+		+	+	
РН-22		+	+	+	+	+				
РН-23				+	+	+	+			
РН-24		+	+	+	+	+	+	+	+	

Керівник робочої групи

д.т.н., Передерій В.І.

Робоча група:

к.т.н., доц. Нужний С.М.

к.т.н., доц. Козирєв С.С.

к.т.н., Сірівчук А.С.