

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
ІМЕНІ АДМІРАЛА МАКАРОВА**

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

**«СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ,
АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ»**

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

Освітня кваліфікація – Бакалавр з кібербезпеки та захисту інформації,

Професійна кваліфікація – Фахівець з технічного захисту інформації

/ Фахівець сфери захисту інформації

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

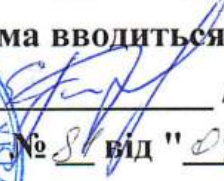
Голова вченої ради

 / **О.М. Дубовий** /

(протокол № 2 від "28" 02 2025 р.)

Освітня програма вводиться в дію з ____ 2025 р.

Ректор / **Є.І. Трушляков** /

 (наказ № 8 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 «10» 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

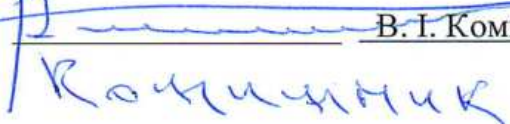
Протокол № 2 від «16» 02 2025 р.

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 Єдиній держаній базі 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** першого рівня вищої освіти розроблена у зв'язку імплементацією 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 – Нужний Сергій Миколайович, завідувач кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент (наказ № 228 від 23.09.2024 р.)

Науково-педагогічні працівники:

1. Передерій Віктор Іванович, професор кафедри КТІБ, д.т.н., доцент, член проектної групи
2. Сірівчук Андрій Сергійович, доцент кафедри КТІБ, к.т.н., член проектної групи
3. Козирєв Сергій Сергійович, доцент кафедри КТІБ, к.т.н., доцент, член проектної групи
4. Божаткін Сергій Михайлович, старший викладач кафедри КТІБ, магістр, 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 першого рівня вищої освіти за ОПП «Системи технічного захисту інформації, автоматизація її обробки»	5
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність	15
2.1. Перелік компонент ОПП	15
2.2. Структурно-логічна схема освітньо-професійної програми	18
3. Форма атестації здобувачів вищої освіти	19
4. Матриця відповідності програмних компетентностей компонентам освітньої програми	20
5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньо-професійної програми	21
6 Перелік професійних стандартів, вимоги яких враховані в ОП	22

**1. Профіль освітньо-професійної програми зі спеціальності
F5 «Кібербезпека та захист інформації» першого 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 освіти	Бакалавр
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	Бакалавр з кібербезпеки та захисту інформації
Професійна кваліфікація	Фахівець з технічного захисту інформації / Фахівець сфери захисту інформації
Кваліфікація в дипломі	Освітня програма – «Системи технічного захисту інформації, автоматизація її обробки» Ступінь вищої освіти – бакалавр Спеціальність – F5 Кібербезпека та захист інформації Галузь знань – F Інформаційні технології
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців.
Наявність акредитації	Акредитаційна комісія МОН України Україна Сертифікат – УД №15003125 Термін дії – 01.07.2025 р. (продовжений у зв'язку з військовим станом)
Цикл / рівень	НРК України – 6 рівень (бакалаврський), EQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Без обмежень доступу до навчання. На основі ступеня молодшого бакалавра (освітньо-кваліфікаційного рівня молодшого спеціаліста) перезараховується не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста). 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	4 роки.
Інтернет-адреса постійного розміщення опису освітньо-професійної програми	https://nuos.edu.ua/studentu/polozhennya-nuk/opis-opp/

2 - Мета освітньої програми

Мета: підготовка висококваліфікованих фахівців, здатних виконувати і впроваджувати технології кібербезпеки та захисту інформації, розв'язувати складні задачі у галузі кібербезпеки та захисту інформації, в тому числі забезпечення захищеності інформації, що обробляється в інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних системах від несанкціонованих дій з інформацією, витоку технічними каналами та спеціальних впливів на засоби обробки інформації, а також інформації, що озвучується на об'єктах інформаційної діяльності, витоку технічними каналами, для об'єктів критичної інформаційної інфраструктури водотранспортного комплексу України та електроенергетичних систем України (південний регіон).

Теоретичний зміст предметної області

Принципи, концепції, теорії захисту життєво важливих Інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Методи, методики, технології методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації.

Об'єкти вивчення:

- технології кібербезпеки та захисту інформації;
- процеси управління кібербезпекою та захистом інформації;
- об'єкти інформаційної діяльності, в тому числі інформаційні (автоматизованих), електронних комунікаційних та інформаційно-комунікаційні системи, інформаційні ресурси і технології;
- системи технічного захисту інформації, технології, методи, способи та системи автоматизованого та автоматичного проектування;
- налагодження, виробництва й експлуатації, проектна документація, стандарти, процедури та засоби підтримки керування життєвим систем технічного захисту інформації.

Інструменти та обладнання: засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків):

- системи розробки, забезпечення, моніторингу та контролю процесів захисту інформації та кібербезпеки;
- засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне і програмно-апаратне забезпечення інформаційно-комунікаційних комплексів;
- інформаційні системи та комплекси проектування, моделювання та експлуатації систем захисту інформації та кібербезпеки;
- системи контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків);
- загальне та спеціалізоване технічне, програмне та апаратно-програмне забезпечення контрольно-вимірювальних систем та комплексів, 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
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	Акцент робиться на набутті студентами компетентностей, отриманні комплексу знань, умінь і навичок за рахунок ґрунтовної підготовки з базових курсів та спеціалізованих дисциплін, в тому числі таких, що мають специфіку південного регіону України. Значна увага приділяється набуттю компетентностей в сфері захисту інформації та кібербезпеки об'єктів критичної інфраструктури, а саме водно-транспортного комплексу (захищені акваторії, судноплавні компанії, окремі судна (у т.ч. безпілотні надводні і підводні апарати)) та енергетичного комплексу півдня України. Метою є підготовка студентів до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації «бакалавр з кібербезпеки та захисту інформації» та професійної кваліфікації «фахівець сфери захисту інформації» або «фахівець з технічного захисту інформації» (визначається темою кваліфікаційної роботи)
4 - Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	На посади у структурних підрозділах установ/ підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності F5 Кібербезпека та захист інформації. 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 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 Фахівець з технічного захисту інформації
Подальше навчання	Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки 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 екзамен, захист кваліфікаційної роботи. Методи оцінювання: письмовий контроль, самоконтроль, тестовий контроль, усний контроль.

6 - Програмні компетентності					
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту Інформації.				
Загальні компетентності (ЗК)	За ОПП	За ОПС¹	За ПС²	За ПС³	Опис компетенції
	ЗК-1		ЗК.02	–	Здатність застосовувати знання у практичних ситуаціях.
	ЗК-2		ЗК.03	–	Знання та розуміння предметної області і розуміння професійної діяльності
	ЗК-3		ЗК.07	–	Здатність спілкування рідною мовою як усно, так і письмово,
	ЗК-4		ЗК.07	–	Здатність спілкування спілкуватися іноземною мовою
	ЗК-5		ЗК.04	–	Здатність вчитися і оволодівати сучасними знаннями
	ЗК-6		ЗК.01	–	Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.
	ЗК-7		ЗК.01	–	Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.
	ЗК-8		ЗК.01	–	Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
	ЗК-9	–	ЗК.05	–	Здатність до адаптації та дії у новій ситуації
	ЗК-10	–	ЗК.06	–	Здатність до вибору стратегії спілкування, працюючи в команді
Примітки: ¹ – компетенції та результати навчання за Стандартом вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» для першого (бакалаврського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 29.10.2024 року №1347 ² – компетенції та результати навчання («знання» – «З» і «уміння та навички» – «У») за Професійним стандартом «Фахівець сфери захисту інформації» (професійна кваліфікація – фахівець сфери захисту інформації), затвердженого наказом Адміністрації Держспецзв'язку від 25.11.2022 року №715 ³ – компетенції та результати навчання («знання» – «З» і «уміння та навички» – «У») за Професійним стандартом «Фахівець з технічного захисту інформації» (професійна кваліфікація – фахівець з технічного захисту інформації), затвердженого наказом Адміністрації Держспецзв'язку від 23.01.2024 року № 38					
Фахові компетентності (ФК)	ФК-1	СК1	A9	B5	Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.
	ФК-2	СК2	A2	A2	Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.
	ФК-3	СК3	A3*	A3	Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

ФК-4	СК4	A1	A1	Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.
ФК-5	СК5	B3* B3	B1	Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.
ФК-6	СК6	A5 A7 B1 B2	B2 B4 B5 B1 B2	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)
ФК-7	СК7	A4* B3*	B1 B2 Г3	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
ФК-8	СК8	B4* Г1 Г2	Г1 Г2	Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
ФК-9	СК9	A6 B2* Г1 Г2	B3 Г1 Г2	Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.
ФК-10	СК10	B1* B5 B6	B1 B2	Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
ФК-11	–	A8	B4	Здатність адмініструвати системи, мережі та системи безпеки інформації
ФК-12	–	–	B6	Здатність виявляти закладні пристрої на об'єктах інформаційної діяльності

Примітки:

* – в частині професійних компетентностей А3, А4, А8, В1, В2, В3, В4 бере участь як член команди - в відповідності до п.1.5 Професійного стандарту «Фахівець сфери захисту інформації» (професійна кваліфікація – фахівець сфери захисту інформації), затвердженого наказом Адміністрації Держспецзв'язку від 25.11.2022 року №715

7 - Результати навчання

Знання та розуміння	РН-1	–	–	Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
	РН-2	–	–	Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
	РН-3	–	–	Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
	РН-4	–	–	Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

PH-5	–	–	Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
PH-6	–	–	Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
PH-7	–	–	Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
PH-8	–	–	Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
PH-9	A9	B5	Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
PH-10	A2	A2	Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
PH-11	A3*	A3	Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.
PH-12	A1	A1	Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
PH-13	A1	A1	Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому
PH-14	B3* B3	B1	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

	РН-15	Б3* В3	Б1	Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
	РН-16	А5 А7 В1 В2	Б2 Б4 Б5 В1 В2	Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
	РН-17	А4* Б3*	Б1 В2 Г3	Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
	РН-18	В4* Г1 Г2	Г1 Г2	Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
	РН-19	В4* Г1 Г2	Г1 Г2	Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
	РН-20	А6 Б1* В5 В6	В1 В2	Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
	РН-21	Б1* В5 В6	Б3 В1 В2	Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.
	РН-22	А8	–	Здатність адмініструвати системи, мережі та системи безпеки інформації
	РН-23	–	Б6	Здатність виявляти закладні пристрої на об'єктах інформаційної діяльності
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 напрямку 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., більше 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	Міжнародна наукова мобільність забезпечена договорами про наукову і

кредитна мобільність	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 екзамену (тестова форма) та публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	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. 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

	воднотранспортного 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	Історія України та української культури	3	Екзамен	1
OK2	Українська мова (за професійним спрямуванням)	3	Екзамен	3
OK3	Іноземна мова	6	Залік Екзамен	1,2 3
OK4	Філософія	4	Екзамен	2
OK5	Фізичне виховання*	—	Залік	2,4
OK6	Права людини та їх захист в сучасних реаліях	3	Залік	4
OK7	Соціологія	3	Залік	3
OK8	Вища математика I	4	Екзамен	1
OK9	Вища математика II	4	Екзамен	2
OK10	Вища математика III	4	Екзамен	3
OK11	Фізика I	3	Екзамен	1
OK12	Фізика II	3	Екзамен	2
OK13	Охорона праці та навколишнього середовища, безпека життєдіяльності	3	Залік	7
Всього за цикл		43		
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ				
OK14	Практика	4	Залік	6
OK15	Кваліфікаційна атестація	6	Екзамен	8
OK16	Кваліфікаційний екзамен (ЄДКІ)	3	Екзамен	8
OK17	Законодавча та нормативно-правова база України з кібербезпеки та захисту інформації	4	Залік	1
OK18	Технології програмування систем автоматизованої обробки і захисту інформації	7	Екзамен	12

OK19	Основи теорії кіл, сигналів та процесів в системах автоматизованої обробки і захисту інформації	10	Залік Екзамен КР	3 4 4
OK20	Метрологія та вимірювання в системах автоматизованої обробки і захисту інформації	3	Залік	1
OK21	Інформаційні технології в захисті інформації та кібербезпеці	7	Залік Екзамен	1 2
OK22	Розробка та застосування захищених баз даних	4	Екзамен	1
OK23	Структура, моніторинг та механізми безпеки систем та мереж передачі даних	8	Екзамен	34
OK24	Захист аудіо- та відеоінформації	3	Залік	8
OK25	Управління інформаційною безпекою	9	Екзамен КР	45 5
OK26	Безпека інформаційних та комунікаційних систем	14	Екзамен КР	456 6
OK27	Теорія інформації, кодування та цифрової обробки інформації	3	Екзамен	5
OK28	Електроніка та схемотехніка пристроїв технічного захисту інформації	6	Екзамен	56
OK29	Поля і хвилі в системах технічного захисту інформації	12	Залік Екзамен КР	56 7 7
OK30	Криптографія та стеганографія	7	Залік Екзамен	6 7
OK31	Мікропроцесорні засоби обробки даних в системах технічного захисту інформації та кібербезпеки	9	Залік Екзамен КР	7 8 8
OK32	Методи і засоби захисту інформації	6	Залік Екзамен	6 7
OK33	Технічні засоби охорони об'єктів	3	Залік	8
OK34	Захист програмного продукту	3	Залік	8
OK35	Комплексні системи захисту інформації	3	Екзамен	8
OK36	Моделювання об'єктів і процесів технічного захисту інформації	3	Залік	8
Всього за цикл:		137		
Загальний обсяг обов'язкових компонентів		180		
2. Вибіркові компоненти загальної та професійної підготовки освітньої програми				
ВК1	Вибірковий курс загальнотехнічного спрямування	5	Залік	2
ВК2	Вибірковий курс 1	5	Залік	2
ВК3	Вибірковий курс 2	5	Залік	3
ВК4	Вибірковий курс 3	5	Залік	3

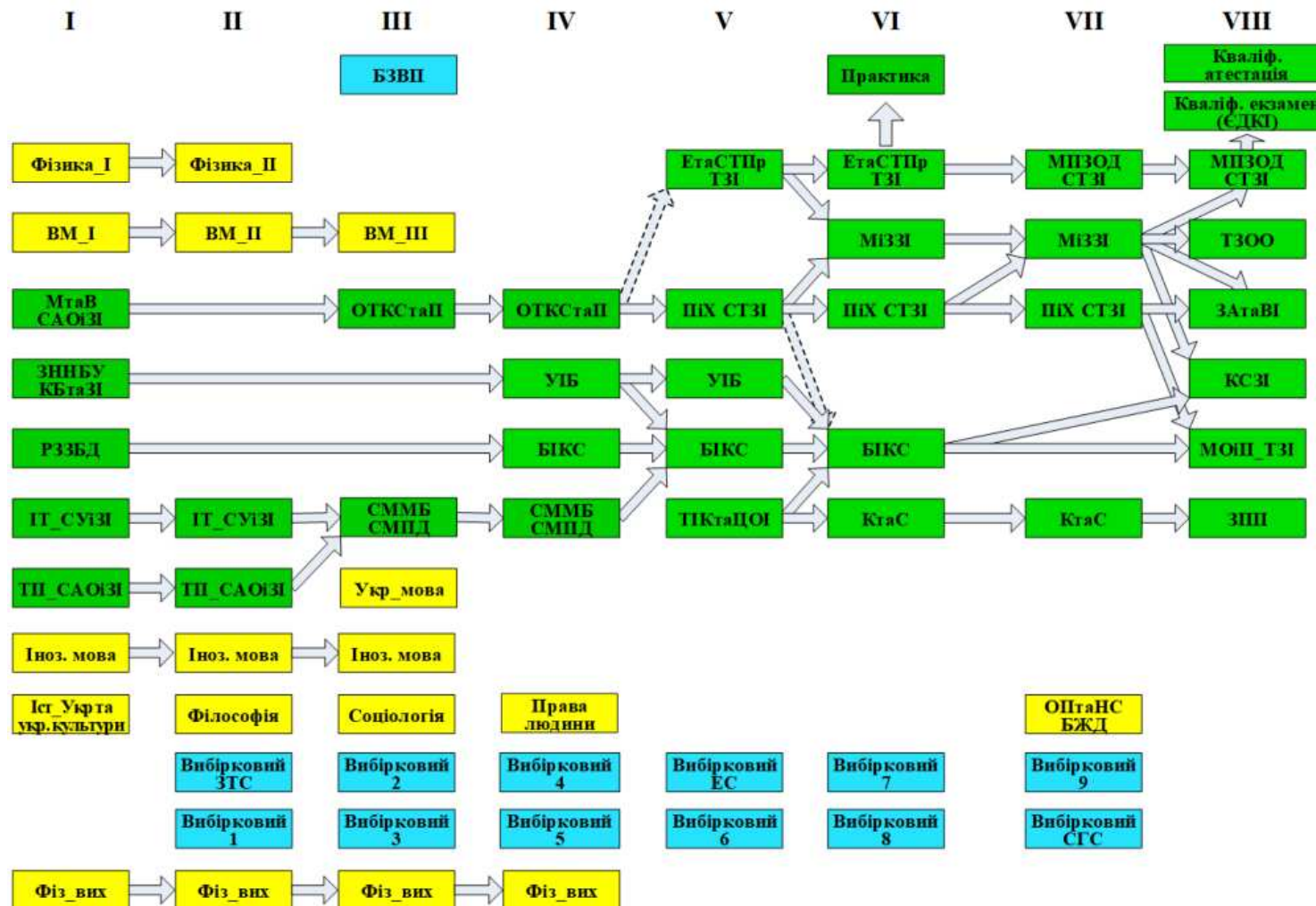
ВК5	Вибірковий курс соціально-гуманітарного спрямування	5	Залік	4
ВК6	Вибірковий курс 4	5	Залік	4
ВК7	Вибірковий курс економічного спрямування	5	Залік	5
ВК8	Вибірковий курс 5	5	Залік	5
ВК9	Вибірковий курс 6	5	Залік	6
ВК10	Вибірковий курс 7	5	Залік	6
ВК11	Вибірковий курс 8	5	Залік	7
ВК12	Вибірковий курс 9	5	Залік	7
ВК13	Базова загальновійськова підготовка**	3	Залік	3
Загальний обсяг вибірових компонентів		60 / 63		
Загальний обсяг освітньо-професійної програми		240 / 243		

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

** – компонент «Базова загальновійськова підготовка» введена в відповідності до статті 10¹ Закону України «Про військовий обов’язок і військову службу, постанови Кабінету Міністрів України № 734 від 21.06.2024 р. та Наказів Ректора НУК № 28 від 28.01.2025 р. зі змінами (Наказ №83 від 08.03.2025 р.) і №82 від 04.03.2025 р. Компонента є обов’язковою умовою опанування освітньої програми першого (бакалаврського) рівня для здобувачів чоловічої статі (жіночої статі – за бажанням)

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 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 (ЄДКІ) і захисту кваліфікаційної роботи. Атестація випускників завершується видачою документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням освітньої кваліфікації – «Бакалавр з кібербезпеки та захисту інформації», та професійної кваліфікації – «Фахівець з технічного захисту інформації»

До складання кваліфікаційного іспиту допускаються студенти, які успішно та повною мірою виконали навчальний план. До захисту кваліфікаційної роботи бакалавра допускаються студенти, які успішно склали кваліфікаційний екзамен (ЄДКІ).

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

	Інтегральна компетентність	Компетентності																					
		Загальні компетентності										Спеціальні (фахові) компетентності											
		ЗК-1	ЗК-2	ЗК-3	ЗК-4	ЗК-5	ЗК-6	ЗК-7	ЗК-8	ЗК-9	ЗК-10	ФК-1	ФК-2	ФК-3	ФК-4	ФК-5	ФК-6	ФК-7	ФК-8	ФК-9	ФК-10	ФК-11	ФК-12
PH-1	+			+																			
PH-2	+				+																		
PH-3	+						+	+															
PH-4	+	+	+																				
PH-5	+	+	+								+												
PH-6	+		+						+	+	+												
PH-7	+	+				+			+				+						+	+			
PH-8	+					+													+	+			
PH-9	+						+					+											
PH-10	+	+	+			+							+						+	+			
PH-11	+													+									
PH-12	+														+								
PH-13	+	+	+			+							+		+						+		
PH-14	+															+							
PH-15	+															+							
PH-16	+																+						
PH-17	+																	+					
PH-18	+																		+				
PH-19	+																		+				
PH-20	+	+	+													+			+	+	+		
PH-21	+																				+		
PH-22	+																					+	
PH-23	*																						+

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

	OK1	OK2	OK3	OK4	OK6	OK7	OK8	OK9	OK10	OK11	OK12	OK13	OK14	OK15	OK16	OK17	OK18	OK19	OK20	OK21	OK22	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	OK33	OK34	OK35	OK36	
PH-1		+											+	+	+																					
PH-2			+										+	+	+																					
PH-3	+			+	+	+							+	+	+	+																				
PH-4					+							+	+	+	+		+	+	+			+		+	+				+			+			+	
PH-5				+									+	+	+					+			+	+	+				+						+	
PH-6						+							+	+	+		+			+		+		+	+										+	
PH-7							+	+	+				+	+	+			+					+			+	+	+	+							
PH-8							+	+	+	+	+		+	+	+			+											+						+	
PH-9					+								+	+	+	+							+	+							+	+				
PH-10													+	+	+		+			+	+	+		+	+		+		+	+	+	+		+	+	
PH-11													+	+	+						+			+												
PH-12													+	+	+							+	+	+	+				+				+			
PH-13													+	+	+		+					+			+		+				+					
PH-14													+	+	+									+	+									+		
PH-15													+	+	+					+	+				+											
PH-16													+	+	+																+		+		+	
PH-17													+	+	+										+											
PH-18													+	+	+						+									+	+					
PH-19													+	+	+	+														+						
PH-20													+	+	+			+	+				+			+	+	+	+			+			+	
PH-21													+	+	+								+					+				+			+	
PH-22													+	+	+					+		+			+					+						
PH-23													+	+	+				+				+								+					

6 Перелік професійних стандартів, вимоги яких враховані в ОП

№	Назва професійного стандарту та код згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»	Мета діяльності за професією
ПС 1	Фахівець з технічного захисту інформації 2139.2	Забезпечення інженерно-технічними та організаційно-технічними заходами та засобами порядку доступу, конфіденційності, цілісності й доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави. Захист інформації та безпосередньо її властивостей, спрямований на забезпечення за допомогою нормативно-правових, організаційних та інженерно-технічних заходів та/або програмно-технічних засобів унеможливлення витoku, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації. Супроводження робіт зі створення, впровадження та забезпечення функціонування систем технічного захисту інформації на етапах життєвого циклу інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем (далі – автоматизовані системи).
ПС 2	Фахівець сфери захисту інформації 2139.2	Забезпечення захищеності (конфіденційності, цілісності, доступності) інформації, що обробляється (передається) в інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних системах від несанкціонованих дій з інформацією (включаючи комп'ютерні віруси), від витoku технічними каналами та від спеціальних впливів на засоби обробки інформації, а також інформації, що озвучується на об'єктах інформаційної діяльності, - від витoku технічними каналами.

Керівник робочої групи

к.т.н., доц., Нужний С.М.

Робоча група:

д.т.н., доц., Передерій В.І.

к.т.н., доц., Козирев С.С.

к.т.н., Сірівчук А.С

Божаткін С.М.