

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 № 125 КІБЕРБЕЗПЕКА

галузі знань № 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Кваліфікація – Фахівець із організації захисту інформації з обмеженим
доступом



ЗАТВЕРДЖЕНО ВЧЕНОЮ
РАДОЮ

Голова вченої ради

/ О.М. Дубовий /

(протокол № 5 від "28" 05 2021 р.)

Освітня програма вводиться в дію з 01.09.2021 р.

/ Є.І. Трушляков

(наказ № 192 від "06" 07 2021 р.)

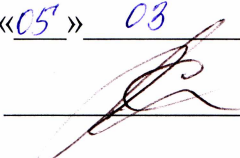


Миколаїв 2021 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

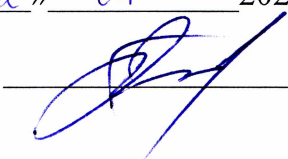
Проект освітньої програми «*Системи технічного захисту інформації, автоматизація її обробки*» розглянуто на засіданні кафедри комп'ютерних технологій та інформаційної безпеки.

Протокол № 4 від «05» 03 2021 р.

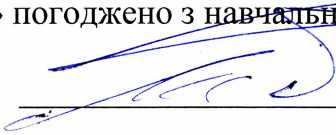
Завідувач кафедри  / С.М. Нужний /

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

Протокол № 09 від «22» 04 2021 р.

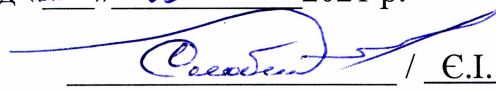
Голова ВР ННІАЕ  / Г.В. Павлов /

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

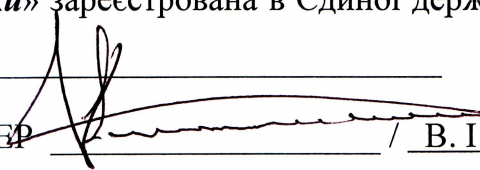
Начальник відділу  / А.В. Лабарткава /

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

Протокол № 5 від «26» 05 2021 р.

Голова НМР НУК  / Є.І. Трушляков /

Освітньо-професійна програма «*Системи технічного захисту інформації, автоматизація її обробки*» зареєстрована в Єдиної держаній базі з питань освіти ID програми 4975

Начальник відділу ВР  / В.І. Комишнік /

ПЕРЕДМОВА

Освітньо-професійна програма «Системи технічного захисту інформації, автоматизація її обробки» розроблена на підставі Стандарту вищої освіти першого (бакалаврського) рівня. Галузь знань: 12 Інформаційні технології. Спеціальність: 125 Кібербезпека. Затверджено і введено в дію наказом МОН України від 04 жовтня 2018р. № 1074.

Розроблено робочою групою у складі:

Гарант освітньо-професійної програми – Нужний Сергій Миколайович, доцент кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент (наказ ОП № 15 від 17 січня 2021 р.).

Науково-педагогічні працівники:

1. Турти Марина Валентинівна, доцент кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент,
2. Козирєв Сергій Сергійович, доцент кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент,

Працедавці:

1. Дмитриченко С. В., начальник Управління Держспецзв'язку в Миколаївській області
2. Григор'єв І.Ф., директор ТОВ Безпекаінфосервіс

Рецензії-відгуки зовнішніх стейкхолдерів:

1. Управління Держспецзв'язку в Миколаївській області
2. ТОВ Безпекаінфосервіс

Освітньо-професійна програма запроваджена з 2018 р.

Термін перегляду освітньої програми 1 раз на рік.

ЗМІСТ

1. Профіль освітньо-професійної програми зі спеціальності 125 «Кібербезпека» за спеціалізацією «Системи технічного захисту інформації, автоматизація її обробки»	5
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність	16
2.1. Перелік компонент ОПП	16
2.2. Структурно-логічна схема освітньо-професійної програми	19
3. Форма атестації здобувачів вищої освіти	20
4. Матриця відповідності програмних компетентностей компонентам освітньої програми	21
5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньо-професійної програми	22

**1. Профіль освітньо-професійної програми
зі спеціальності 125 «Кібербезпека» за спеціалізацією «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	Бакалавр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
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 Фахівець із організації захисту інформації з обмеженим доступом
Кваліфікація в дипломі	Ступінь вищої освіти – бакалавр Спеціальність 125 Кібербезпека Освітня програма Системи технічного захисту інформації, автоматизація її обробки
Тип диплому та обсяг освітньо програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців. 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)
Наявність акредитації	Акредитаційна комісія МОН України Україна Сертифікат – УД №15003125 Термін дії – 01.07.2023 р.
Цикл / рівень	НРК України – 6 рівень (бакалаврський), FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Без обмежень доступу до навчання. 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 01.07.2023 р.
Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://www.nuos.edu.ua/students/osvita/osvitni-programy.php
2 - Мета освітньої-професійної програми	
Мета: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки при здійсненні професійної діяльності або в процесі навчання, що передбачає застосування певних теорій та методів відповідних наук та характеризується невизначеністю умов. Методи, методики, технології забезпечення інформаційної та/або кібербезпеки, якими має оволодіти здобувач вищої освіти для застосовування на практиці: методами фундаментальних та	

прикладних наук, технологіями створення та супроводження систем інформаційної безпеки; методами автоматизованого проектування їх компонент з використанням програмно-технічних засобів, математичного та комп'ютерного моделювання, інформаційними технологіями, професійними прикладними програмами, сучасними мовами програмування; 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: об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси й інформаційні технології, інтерфейси та протоколи взаємодії їх компонентів універсального та спеціального призначення; об'єктів різного рівня (система, об'єкт системи, компонент об'єкта), що пов'язані з інформаційними, інформаційно-комунікаційними технологіями, що використовуються для забезпечення функціонування цих об'єктів; 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; методи та способи управління інформаційною і кібербезпекою на об'єкті інформаційної діяльності, створення, функціонування, моніторинг та удосконалення системи управління інформаційною безпекою.

Інструменти та обладнання: системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; загальне та спеціалізоване технічне та програмне забезпечення, контрольно-вимірювальні прилади, програмні та радіотехнічні засоби моніторингу і протидії витоку інформації

3 - Характеристика освітньо-професійної програми

Предметна область (галузь знань, спеціальність, спеціалізація)	Галузь знань 12 – Інформаційні технології Спеціальність 125 – Кібербезпека Спеціалізація – Системи технічного захисту інформації, автоматизація її обробки
Орієнтація освітньо-професійної програми	Практична прикладна професійна діяльність
Основний фокус освітньої програми та спеціалізації	Підготовка фахівців зі спеціалізації «Системи технічного захисту інформації, автоматизація її обробки» спеціальності 125 «Кібербезпека» галузі знань 12 «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-телекомунікаційних систем.
Особливості освітньо-професійної 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 управління інформаційною безпекою водно-транспортного комплексу України, захищених акваторій, судноплавних компаній, окремих суден (у т.ч. безпілотних надводних і підводних апаратів).

4 - Придатність випускників до працевлаштування та подальшого навчання

Придатність до працевлаштування	Фахівець може займати первинні посади (за ДК 003:2010): 3121 – фахівець з інформаційних технологій 3439 – фахівець із організації інформаційної безпеки,
--	--

	3439 – фахівець із організації захисту інформації з обмеженим доступом 3439 – фахівець з режиму секретності, 3439 – інспектор з організації захисту секретної інформації, 4112 – шифрувальник
Подальше навчання	Випускники першого (бакалаврського) рівня вищої освіти можуть продовжувати навчання на другому (магістерському) рівні вищої освіти у навчальних закладах відповідного рівня акредитації. Можливість підвищення кваліфікації та отримання додаткової післядипломної освіти.
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'язання комплексних проблем у професійній галузі. Індивідуальне наукове керівництво, підтримка і консультування науковим керівником.
Оцінювання	Екзамени, заліки, тестові завдання, курсовий проект, курсові роботи, лабораторні звіти, презентації, звіт з практики, захист кваліфікаційної роботи. Методи оцінювання: письмовий контроль, самоконтроль, тестовий контроль, усний контроль.
6 - Програмні компетентності	
Інтегральна компетентність (ІК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області та розуміння професії. ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК 5. Здатність до пошуку, оброблення та аналізу інформації. ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ЗК 7. 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

Фахові компетентності спеціальності (ФК)	ФК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
7 - Програмні результати навчання**	
	РН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

	RH6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; RH7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; RH8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; RH9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; RH10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; RH11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; RH12. Розробляти моделі загроз та порушника; RH13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; RH14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; RH15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; RH16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; RH17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; RH18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; RH19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; RH20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; RH21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; RH22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки; RH23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; RH24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-
--	---

	телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); RH25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в' інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; RH26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; RH27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; RH28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки; RH29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; RH30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; RH31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; RH32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; RH33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; RH34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; RH35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки; RH36. Виявляти небезпечні сигнали технічних засобів; RH37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоків технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; RH38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; RH39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
--	--

	RH40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; RH41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; RH42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; RH43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; RH44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; RH45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; RH46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; RH47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; RH48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; RH49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; RH50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); RH51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; RH52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; RH53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. RH54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
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 зв'язок теоретичної та практичної підготовки.

	Гарант освітньої програми та викладацький склад, який забезпечує її реалізацію, відповідає 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 роботизований комплексів і морської лабораторії «Дельта»: 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 системи та методи технічного захисту інформації; ННЛ організації та управління інформаційною безпекою; ННЛ електроніки та мікропроцесорної техніки 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 у бібліотеці та кафедрах університету, де наявне спеціалізоване програмне забезпечення та відкритий доступ 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 імені адмірала Макарова перевищує 768 тис. примірників, наукових видань – 94 тис. прим., навчальних – 400 тис. прим., біля 125 тис. прим. періодичних видань. Віртуальний сервіс бібліотеки складається з: електронного каталогу, баз даних (24), веб-сайту бібліотеки та Регіонального освітньо-інформаційного порталу бібліотек ВНЗ Миколаївщини, 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. Для студентів, аспірантів та викладачів НУК передплачується (щорічно з 2003 р.) доступ в режимі on-line до ресурсів інформаційної агенції EBSCO PUBLISHING. Доступ здійснюється через IP-ідентифікацію комп'ютерів в усіх корпусах університету за посиланням http://search.ebscohost.com. Вільний доступ через сайт НУК до баз даних періодичних фахових наукових видань (в тому числі, англійською мовою) забезпечується: • участю бібліотеки університету у консорціумі ElibUkr «Електронна бібліотека України: створення Центрів знань в університетах України», що об'єднує бібліотеки вищих навчальних закладів, національні бібліотеки та інші організації України. Учасникам консорціуму ElibUkr надається доступ до БД електронних журналів, електронних книг

	• найважливішого ядра світових інформаційних ресурсів, що покривають усі галузі знань (наука, техніка, медицина, соціальні та гуманітарні науки); • входженням бібліотеки університету в асоціацію «Інформаційно-Консорціум», що пропонує тестові (тріал) доступи для ознайомлення з новими можливостями відомих інформаційних електронних провайдерів та до нових ресурсів. У рамках нового консорціуму E-Verum в 2016 р. бібліотека НУК приєдналася до проекту «ТОРНАДО», що надає доступ до бібліографічних даних наукових статей з престижних періодичних видань, книг та матеріалів наукових конференцій із зазначенням реальної цитованості цих матеріалів, зокрема існує тріал-доступ до таких баз даних та он-лайн утиліт: • Web of Science Core Collection: Science Citation Index Expanded (1970-2018); Social Science Citation Index (1970-2018); Arts and Humanities Citation Index (1975-2018); Conference Proceedings Citation Index (1990-2018); Book Citation Index (2003-2018); • Russian Science Citation Index (2002-2018); • SciELO Citation Index (1980-2018); • Emerging Sources Citation Index (2015-2018); • Korean Journal Index (1980-2018); • Chinese Science Citation Database (1989-2018); • Journal Citation Reports (2004-2018); • Derwent Innovations Index (дані по патентах, 1963-2018); • Medline® (1950-2018).
9 - Академічна мобільність	
Національна кредитна мобільність	Національна кредитна мобільність забезпечується у рамках договорів про встановлення науково-освітніх 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 кредитна мобільність в рамках договорів про встановлення науково-освітніх відносин для задоволення потреб розвитку освіти і науки, укладених між НУК та навчальними закладами країн-партнерів. Допускаються індивідуальні угоди про академічну мобільність для навчання та проведення досліджень в університетах та наукових установах країн-партнерів. Кредити можуть бути перезараховані відповідно до довідки про академічну мобільність
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 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: – Вдосконалення методів та технологій аналізу інформаційної безпеки судових спеціалізованих інформаційно-комунікаційних систем, виявлення та локалізація їх вразливостей; – Вдосконалення методів та технологій аналізу на основі теорії однозначних нечітких систем та нейронних мереж для оцінки захищеності інформації; – Вдосконалення методів та технологій моніторингу та управління корпоративними мережами; – Вдосконалення методів та технологій побудови систем об'єктового захисту для об'єктів критичної інфраструктури водотранспортного комплексу; – Дослідження принципів побудови 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; – Розробка методів і технологій побудови систем захисту акваторії та виявлення порушників з використанням підводного охоронного робота та систем висвітлення підводної обстановки; – Створення та дослідження апаратних та апаратно-програмних засобів дослідження захисту мовної інформації, звукоізоляції та електроакустичних перетворювачів; – Створення та модернізація баз знань та систем підтримки прийняття рішень для захисту інформаційних ресурсів сучасної локальної обчислювальної мережі на об'єктах водотранспортного комплексу; – Створення та модернізація комплексних системи 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	В університеті розроблена, впроваджена в дію та сертифікована система управління якістю, що базується на вимогах міжнародного стандарту серії ISO 9001:2015 та Національного стандарту ДСТУ ISO 9001:2015. Впроваджена система сертифікована з 2015 року компанією «Бюро Верітас Сертифікейшн Україна» і підлягає щорічному аудиту. Сферою сертифікації внутрішньої системи забезпечення якості є: 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 науково-педагогічних 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.
--	--

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	2	3	4	5
I ОBOB'ЯЗКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ				
1. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ				
ЗП1	Історія України та української культури	3	Екзамен	1
ЗП2	Українська мова (за професійним спрямуванням)	3	Екзамен	1
ЗП3	Іноземна мова	6	Залік/ Залік/ Екзамен	1/2/3
ЗП4	Філософія	4	Екзамен	2
ЗП5	Фізичне виховання*		–/Залік/ –/Залік	1/2/3/4
ЗП6	Вища математика I, II, III	12	Залік/ Залік/ Екзамен	1/2/3
ЗП7	Фізика I, II	7	Екзамен/ Екзамен	1/2
ЗП8	Права людини та їх захист в сучасних реаліях	3	Залік	3
ЗП9	Охорона праці та навколишнього середовища, безпека життєдіяльності	3	Залік	7
ЗП10	Соціологія	3	Залік	4
Всього за цикл		44		
2. ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ				
ПП1	Виробнича практика	4	Залік	6
ПП2	Кваліфікаційна атестація (кваліфікаційна робота)	6	Екзамен	8
ПП3	Кваліфікаційний екзамен	3	Екзамен	8
ПП4	Технічна графіка в системах автоматизованої обробки і захисту інформації	4	Залік	1
ПП5	Технології програмування систем автоматизованої обробки і захисту інформації	7	Екзамен/ Екзамен	2/3
ПП6	Основи теорії кіл, сигналів та процесів в системах автоматизованої обробки і захисту інформації	10	Залік/ Екз + КР	3/4
ПП7	Метрологія та вимірювання в системах автоматизованої обробки і захисту інформації	3	Залік	1

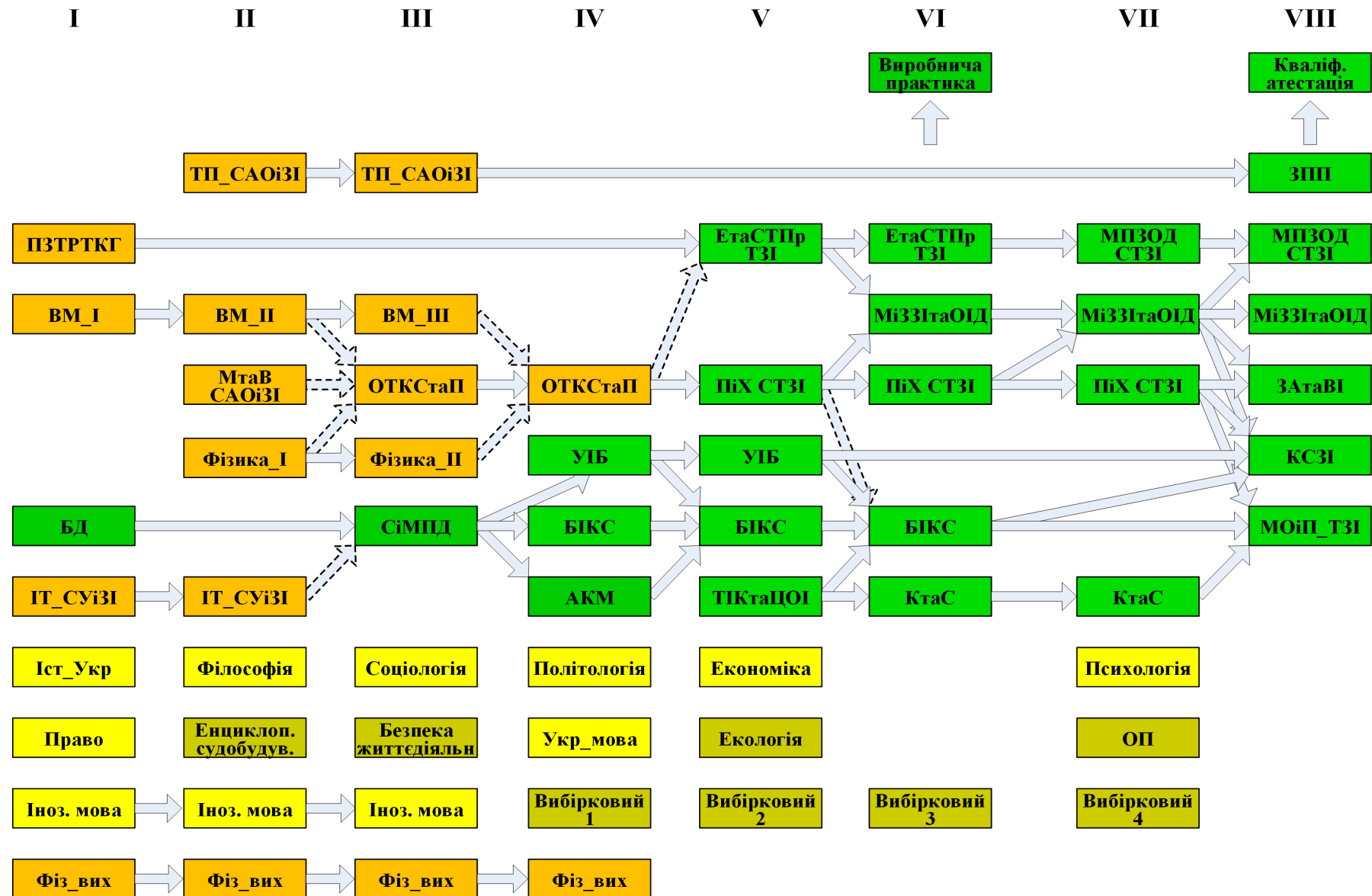
1	2	3	4	5
ПП8	Інформаційні технології систем управління та захисту інформації	7	Залік/ Екзамен	1/2
ПП9	Бази даних	4	Екзамен	1
ПП10	Системи і мережі передачі даних	4	Екзамен	3
ПП11	Адміністрування комп'ютерних мереж	4	Екзамен	4
ПП12	Управління інформаційною безпекою	9	Екзамен/ Екзамен	4/5
ПП13	Безпека інформаційних та комунікаційних систем	12	Екзамен/ Екзамен/ Екз.+КР	4/5/6
ПП14	Теорія інформації, кодування та цифрової обробки інформації	3	Екзамен	5
ПП15	Електроніка та схемотехніка пристроїв технічного захисту інформації	6	Екзамен/ Екзамен	5/6
ПП16	Поля і хвилі в системах технічного захисту інформації	12	Залік/ Залік/ Екз.+КР	5/6/7
ПП17	Криптографія та стеганографія	8	Екзамен/ Екзамен	6/7
ПП18	Мікропроцесорні засоби обробки даних в системах технічного захисту інформації та кібербезпеки	9	Екзамен/ Екз.+КР	7/8
ПП19	Методи і засоби захисту інформації	6	Екзамен/ Екзамен	6/7
ПП20	Технічні засоби охорони об'єктів	3	Залік	8
ПП21	Захист програмного продукту	3	Залік	8
ПП22	Комплексні системи захисту інформації	3	Екзамен	8
ПП23	Моделювання об'єктів і процесів технічного захисту інформації	3	Залік	8
ПП24	Захист аудіо- та відеоінформації	3	Залік	8
Всього за цикл:		136		
Загальний обсяг обов'язкових компонентів		180		
II ВИБРИКІВ 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 4	5	Залік	4
ВК6	Вибірковий курс 5	5	Залік	4

1	2	3	4	5
ВК7	Вибірковий курс економічного спрямування	5	Залік	5
ВК8	Вибірковий курс 6	5	Залік	5
ВК9	Вибірковий курс 7	5	Залік	6
ВК10	Вибірковий курс 8	5	Залік	6
ВК11	Вибірковий курс 9	5	Залік	7
ВК12	Вибірковий курс соціально-гуманітарного спрямування	5	Залік	7
Загальний обсяг вибірових компонентів		60		
Загальний обсяг освітньо-професійної програми		240		

* – вибірові компоненти програми обираються студентом згідно «Положення про вибірові 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 ОП



3. Форма атестації здобувачів вищої освіти.

Атестація випускників освітньої-професійної програми «Системи технічного захисту інформації, автоматизація її обробки» спеціальності 125 «Кібербезпека» проводиться у формі складання кваліфікаційного письмового тестового іспиту та захисту кваліфікаційної роботи бакалавра. Атестація випускників завершується видачою документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації: «Фахівець із організації захисту інформації з обмеженим доступом».

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 іспит.

Захист кваліфікаційної роботи бакалавра 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. 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. В роботі проводиться аналіз ефективності прийнятих рішень, охорону праці та навколишнього середовища.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	ЗП1	ЗП2	ЗП3	ЗП4	ЗП5	ЗП6	ЗП7	ЗП8	ЗП9	ЗП10	ПП1	ПП2	ПП3	ПП4	ПП5	ПП6	ПП7	ПП8	ПП9	ПП10	ПП11	ПП12	ПП13	ПП14	ПП15	ПП16	ПП17	ПП18	ПП19	ПП20	ПП21	ПП22	ПП23	ПП24	БК1	БК2	БК3	БК4	БК5	БК6	БК7	БК8	БК9	БК10	БК11	БК12			
ЗК1						+	+				+			+	+		+		+	+	+	+	+		+		+			+																			
ЗК2						+	+				+				+	+		+		+				+				+	+	+		+	+																
ЗК3		+	+								+																																						
ЗК4				+							+						+		+	+					+					+	+																		
ЗК5											+						+		+					+						+																			
ЗК6	+							+		+																																							
ЗК7				+			+	+	+																																								
ФК1											+			+				+	+	+		+							+	+		+																	
ФК2											+									+	+	+							+				+	+															
ФК3											+								+			+				+		+				+																	
ФК4											+										+					+			+																				
ФК5											+							+	+								+		+		+		+																
ФК6											+												+		+							+																	
ФК7											+																		+			+		+															
ФК8											+											+																											
ФК9											+											+	+																										
ФК10											+																+		+	+																			
ФК11											+												+											+	+														
ФК12											+											+	+									+	+	+															

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

	3П1	3П2	3П3	3П4	3П5	3П6	3П7	3П8	3П9	3П10	ПП1	ПП2	ПП3	ПП4	ПП5	ПП6	ПП7	ПП8	ПП9	ПП10	ПП11	ПП12	ПП13	ПП14	ПП15	ПП16	ПП17	ПП18	ПП19	ПП20	ПП21	ПП22	ПП23	ПП24	БК1	БК2	БК3	БК4	БК5	БК6	БК7	БК8	БК9	БК10	БК11	БК12	
PH1	+	+									+																																				
PH2															+																	+															
PH3											+							+																													
PH4											+																		+	+		+															
PH5																		+																													
PH6				+		+	+	+	+	+	+																																				
PH7											+											+																									
PH8											+											+																									
PH9											+											+										+															
PH10											+									+	+								+																		
PH11											+								+	+														+													
PH12											+																		+	+		+															
PH13											+										+																										
PH14											+								+													+															
PH15											+				+				+	+													+														
PH16											+																						+														
PH17											+									+			+											+													
PH18											+						+						+									+			+												
PH19											+												+	+																							
PH20											+																					+															
PH21											+										+																										
PH22											+											+																									
PH23											+												+																								
PH24											+										+																										
PH25											+										+																										
PH26											+												+																								
PH27											+												+	+																							
PH28											+												+																								
PH29											+												+																								
PH30											+												+																								

	ЗП1	ЗП2	ЗП3	ЗП4	ЗП5	ЗП6	ЗП7	ЗП8	ЗП9	ЗП10	ПП1	ПП2	ПП3	ПП4	ПП5	ПП6	ПП7	ПП8	ПП9	ПП10	ПП11	ПП12	ПП13	ПП14	ПП15	ПП16	ПП17	ПП18	ПП19	ПП20	ПП21	ПП22	ПП23	ПП24	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6	ВК7	ВК8	ВК9	ВК10	ВК11	ВК12
PH31											+											+																								
PH32											+										+		+																							
PH33											+											+																								
PH34											+											+											+													
PH35											+																						+													
PH36											+						+								+					+	+															
PH37											+						+													+	+															
PH38											+					+										+				+	+					+										
PH39											+						+										+						+													
PH40											+					+										+									+											
PH41											+											+	+																							
PH42											+											+																								
PH43											+											+																								
PH44											+											+																								
PH45											+												+																							
PH46											+												+																							
PH47											+													+			+																			
PH48											+																+		+	+																
PH49											+											+								+	+															
PH50											+											+	+																							
PH51											+										+	+	+																							
PH52											+										+	+	+																							
PH53											+																				+															
PH54	+	+	+	+				+	+	+																																				

Керівник робочої групи

доц., к.т.н. Нужний С.М.

Робоча група:

доц., к.т.н. Козирєв С.С.

доц., к.т.н. Турти М.В.