МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

(повна назва освітньої програми)

магістр

(рівень вищої освіти)

ГАЛУЗІ ЗНАНЬ	12 Інформаційні технології
ЗА СПЕЦІАЛЬНІСТЮ	125 Кібербезпека
СПЕЦІАЛІЗАЦІЯ	Управління інформаційною безпекою
КВАЛІФІКАЦІЯ	Магістр з кібербезпеки, управління інформаційною безпекою

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Львівського державного університету
безпеки життєдіяльності
Голова Вченої ради
_____ Мирослав КОВАЛЬ
(протокол № 13 від „13” 07 2022 р.)

Освітньо-професійна програма вводиться в дію
з „14” 07 2022 р.
(наказ № 1400д від „14” 07 2022 р.)

Львів 2022

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Рівень вищої освіти	другий (магістерський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Спеціалізація	Управління інформаційною безпекою
Кваліфікація	Магістр з кібербезпеки, управління інформаційною безпекою

ВНЕСЕНО:

Кафедрою управління інформаційною безпекою

Протокол № 9 від «27» квітня 2022 р.

РЕКОМЕНДОВАНО:
Вченою радою навчально-наукового інституту цивільного захисту

Протокол № 1 від «12» липня 2022р.

ПОГОДЖЕНО

Проректор з навчальної та методичної роботи

Дмитро ЧАЛИЙ
"12" 07 2022 р.

Начальник навчально-наукового інституту цивільного захисту

Василь ПОПОВИЧ
"12" 07 2022 р.

Начальник навчально-методичного центру

Микола СИЧЕВСЬКИЙ
"12" 07 2022 р.

ПЕРЕДМОВА

Освітньо-професійна програма (далі – ОП) розроблена на підставі стандарту вищої освіти України за другим (магістерський) рівень, галузі знань 12 – Інформаційні технології, спеціальність 125 Кібербезпека, затвердженого і введеного в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.

Освітньо-професійна програма розроблена та оновлена робочою групою Львівського державного університету безпеки життєдіяльності у складі:

Керівник робочої групи

Ростислав Ткачук	– доктор технічних наук, доцент, завідувач кафедри управління інформаційною безпекою.

Члени робочої групи:

Орест Полотай	кандидат технічних наук, доцент кафедри управління інформаційною безпекою;
Андрій Лагун	кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою;
Оксана Чмир	кандидат фізико-математичних наук, доцент кафедри прикладної математики та механіки

До розроблення програми залучено зовнішніх стейкголдерів:

Роман Карпюк	– SecOps Analyst компанії SoftServe
Михайло Кропива	– InfoSec Director компанії SoftServe
Олег Леськів	– менеджер освітніх проєктів Львівського IT Кластеру
Роман Яремчук	– Начальник Центру оперативного зв'язку, телекомунікаційних систем та інформаційних технологій ГУ ДСНС України у Львівській області

Рецензенти:

Володимир Ромака	професор, д.т.н., професор кафедри захисту інформації Національного університету «Львівська політехніка»
Ігор Гайдар	керівник проекту компанії Uniservice Ltd

Відгуки представників професійних асоціацій / роботодавців:

Перегляд освітньо-професійної програми відбувається за результатами її моніторингу, але не рідше ніж один раз на 2 роки.

Актуалізовано:

Дата перегляду ОП/ внесення змін до ОП			
Підпис			
Прізвище, ініціали гаранта			

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

	1-Загальна інформація	
1.	*Повна назва закладу вищої освіти та структурного підрозділу*	Львівський державний університет безпеки життєдіяльності Навчально-науковий інститут цивільного захисту Кафедра управління інформаційною безпекою
2.	*Ступінь вищої освіти та назва кваліфікації мовою оригіналу*	Ступінь вищої освіти: магістр Спеціальність: 125 – Кібербезпека Освітня кваліфікація: магістр з кібербезпеки, управління інформаційною безпекою
3.	*Офіційна назва освітньої програми*	Кібербезпека
4.	*Тип диплому та обсяг освітньо-професійної програми*	Диплом магістра, одиничний Обсяг: 90 кредитів ЄКТС, термін навчання 1рік 6 місяців
5.	*Наявність акредитації*	Підготовка здобувачів освіти за даною освітньою програмою здійснюється на основі сертифікату про акредитацію спеціальності 125 – Кібербезпека, серія НД №1487337 / рішення Акредитаційної комісії від 30 червня 2015 року, протокол № 117 (наказ МОН України від 19.12.2016 № 1565) Термін дії сертифікату до 1 липня 2025 р. Термін подання програми на акредитацію – 1 липня 2024 р.
6.	*Рівень програми*	НРК України – 8 рівень; FQ-EHEA – другий цикл, EQF-LLL – 7 рівень.
7.	*Передумови*	Умови вступу визначаються «Правилами прийому до Львівського державного університету безпеки життєдіяльності», затвердженими Вченою радою університету. На базі диплому бакалавра (спеціаліста або магістра з іншої спеціальності).
8.	*Мова викладання*	Українська
9.	*Термін дії освітньої програми*	До наступного планового оновлення програми, але не перевищуючи періоду акредитації
10.	*Інтернет-адреса постійного розміщення опису освітньої програми*	https://ldubgd.edu.ua/content/upravlinnya-informaciynoyu-bezpekoyu-0

2-Мета освітньої програми
Забезпечити підготовку висококваліфікованих фахівців в галузі інформаційних технологій зі спеціальності 125 – Кібербезпека, а саме формування у здобувачів вищої освіти комплексу знань, умінь та навичок для застосування в професійній діяльності у сфері інформаційної безпеки та кібербезпеки через теоретичне та практичне навчання. А також підготувати здобувачів освіти для подальшого працевлаштування за обраною спеціальністю.

	3- Характеристика освітньої програми	
11	*Предметна область*	Галузь знань: 12 Інформаційні технології Спеціальність: 125 Кібербезпека Об'єкти вивчення: – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах

		інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. Цілі навчання: Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. Теоретичний зміст предметної області: Знання: Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. Методи, методики та технології: – методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. – технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. Інструменти та обладнання: – засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення; – автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних

		потоків); – методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
12	*Орієнтація освітньої програми*	Освітньо-професійна програма. Професійний акцент на готовність працювати й набувати навички знань з кібербезпеки, задач прогнозування, проектування, оптимізації, системного аналізу та прийняття рішень, аналізу і синтезу даних і знань пов'язаних з кібербезпекою. Наукова орієнтація є професійно-орієнтована.
13	*Основний фокус освітньої програми*	Загальна освіта в області кібербезпеки. Програма спрямована на підготовку аналітиків-професіоналів, здатних застосувати математичні основи, алгоритмічні принципи в моделюванні, проектуванні, розробці, впровадженні та супроводі інформаційних, інтелектуальних систем задля забезпечення конфіденційності, забезпечення процесів управління інформаційною безпекою.
14	*Особливості програми*	Програма розвиває перспективні напрями кібербезпеки, пов'язані з адміністративним менеджментом систем захисту інформації.

4 - Придатність випускників до працевлаштування та подальшого навчання		
15	*Придатність до працевлаштування*	Робочі місця в державному та приватному секторах у сфері інформаційних технологій, комп'ютерних систем та телекомунікацій, розробка і обслуговування систем інформаційної безпеки.
16	*Академічні права випускників*	Можливість продовження навчання за третім освітньо-науковим рівнем з отриманням ступеня доктора філософії (PhD), а також підвищення кваліфікації та отримання додаткової післядипломної освіти.

5 - Стиль викладання та оцінювання		
17	*Підходи до викладання та навчання*	Комбінація лекцій, практичних занять, виконання проектів, дослідницьких лабораторних робіт, самостійної роботи в віртуальному навчальному середовищі, консультацій з викладачами, професійна практика; підготовка дипломної роботи.
18	*Система оцінювання*	Письмові та усні екзамени, реферати, лабораторні звіти, презентації проектів, захист дипломної роботи.
19	*Форми атестації здобувачів вищої освіти*	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
20	*Вимоги до кваліфікаційної роботи*	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному

		сайті (або у репозитарії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

		6-Програмні компетентності	
21	*Інтегральна*	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.	
22	*Загальні*	ЗК1	Здатність застосовувати знання у практичних ситуаціях.
		ЗК2	Здатність проводити дослідження на відповідному рівні.
		ЗК3	Здатність до абстрактного мислення, аналізу та синтезу.
		ЗК4	Здатність оцінювати та забезпечувати якість виконуваних робіт.
		ЗК5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
23	*Фахові*	ФК1	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.
		ФК2	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.
		ФК3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
		ФК4	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.

		ФК5	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.
		ФК6	Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
		ФК7	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.
		ФК8	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.
		ФК9	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.
		ФК10	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.

7-Програмні результати навчання		
24	РН1	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.
	РН2	Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
	РН3	Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

	РН4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
	РН5	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.
	РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
	РН7	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
	РН8	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
	РН9	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
	РН10	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
	РН11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
	РН12	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.
	РН13	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.
	РН14	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.
	РН15	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.
	РН16	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.
	РН17	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.

	РН18	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
	РН19	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.
	РН20	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
	РН21	Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
	РН22	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.
	РН23	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 знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

	8 - Ресурсне забезпечення реалізації програми	
25	Кадрове забезпечення	Кадрове забезпечення освітньої програми складається з науково-педагогічних працівників кафедри Управління інформаційною безпекою Навально-наукового інституту цивільного захисту. До викладання окремих дисциплін відповідно до їх компетенцій та досвіду залучені науково-педагогічні працівників навчально-наукових інститутів Цивільного захисту, Психології і соціального захисту. Практично – орієнтований характер освітньої програми передбачає широку участь фахівців-практиків, які відповідають напряму програми, що підсилює синергетичний зв'язок теоретичної та практичної підготовки. Керівник та члени проектної групи, а також викладацький склад, який забезпечує реалізацію освітньої програми, відповідають вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності закладів освіти.
26	Матеріально-технічне забезпечення	Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає потребі. Використання сучасних комп'ютерних засобів та програмного забезпечення розподілено між центром інтелектуального моделювання безпечного майбутнього який обладнаний чотирма сучасними комп'ютерними аудиторіями на 62 робочих місця, та комплексом з чотирьох лабораторій інформаційних систем і технологій у галузі цифрової безпеки технічне оснащення яких дозволяє на високому рівні здійснювати навчання як у контактній, так і у дистанційній формі. Зокрема лабораторія соціальних

		комунікацій та інформаційної діяльності, лабораторія проектування та забезпечення безпеки інформаційних систем, лабораторія інформаційних систем та технологій програмування, лабораторія цифрових методів обробки та захисту інформації. Загалом, комплекс лабораторій обладнано 70-ма робочими місцями із сучасною комп'ютерною технікою. Також в навчальній діяльності використовується і інший аудиторний фонд Університету. Наявна вся необхідна соціально-побутова інфраструктура, кількість місць в гуртожитках відповідає вимогам. Користування мережею Інтернет безлімітне.
27	Інформаційне та навчально-методичне забезпечення	Використання віртуального навчального середовища Львівського державного університету безпеки життєдіяльності; авторських розробок працівників; підручників на навчальних посібників з грифом Вченої ради Університету; іншим навчальних та методичних матеріалів розміщених на відкритих он-лайн платформах.

	9 - Академічна мобільність	
28	Національна кредитна мобільність	Може реалізуватись в рамках двосторонніх договорів між закладами вищої освіти про встановлення науково-освітянських відносин. Допускаються індивідуальні угоди про академічну мобільність для навчання (проходження практики) та проведення досліджень в університетах та наукових установах України.
29	Міжнародна кредитна мобільність	Індивідуальна у рамках програми Erasmus+ та на основі підписаних двосторонніх угод між Львівським державним університетом безпеки життєдіяльності та вищими навчальними закладами країн-партнерів.
30	Навчання іноземних здобувачів вищої освіти	Підготовка іноземних громадян за акредитованими напрямами (спеціальностями), наказ МОН України від 04.06.2013 № 2070 л. Мова викладання – українська.

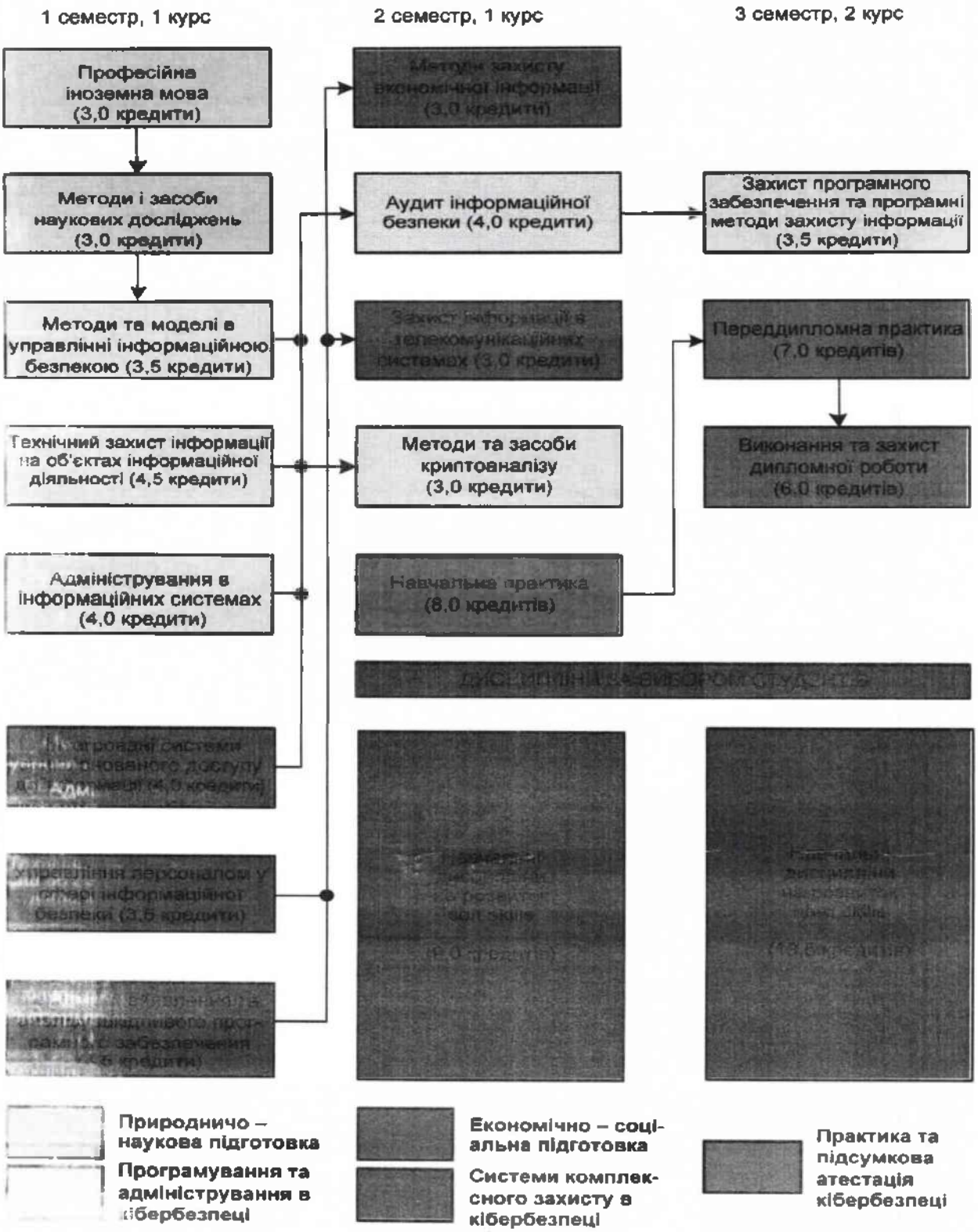
2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1. Перелік компонент освітньої програми

Код	Компоненти освітньої програми	Кількість кредитів	Форма підсумкового контролю
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ			
ОК 1	Професійна іноземна мова	3,0	екзамен
ОК 2	Методи і засоби наукових досліджень	3,0	диф. залік
ОК 3	Методи та моделі в управлінні інформаційною безпекою	3,5	екзамен
ОК 4	Методи захисту економічної інформації	3,0	екзамен
ОК 5	Технічний захист інформації на об'єктах інформаційної діяльності	4,5	диф. залік
ОК 6	Аудит інформаційної безпеки	4,0	екзамен
ОК 7	Захист програмного забезпечення та програмні методи захисту інформації	3,5	екзамен
ОК 8	Адміністрування в інформаційних системах	4,0	диф. залік
ОК 9	Захист інформації в телекомунікаційних системах	3,0	екзамен
ОК 10	Методи та засоби криптоаналізу	3,0	екзамен
ОК 11	Інтегровані системи санкціонованого доступу до інформації	4,0	екзамен
ОК 12	Управління персоналом у сфері інформаційної безпеки	3,5	екзамен
ОК 13	Технології виявлення та аналізу шкідливого програмного забезпечення	4,5	диф. залік
ОК 14	Навчальна практика	8,0	диф. залік
ОК 15	Переддипломна практика	7,0	диф. залік
ОК 16	Дипломна робота	6,0	
Загальний обсяг обов'язкових компонент: 67,5			
ВИБІРКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ			
ВД 1.1 ВД 1.2 ВД 1.3	Навчальні дисципліни на розвиток soft skills	9	диф. залік
ВД 2.1 ВД 2.2 ВД 2.3	Навчальні дисципліни на розвиток hard skills	13,5	диф. залік
Загальний обсяг вибіркових компонент: 22,5			
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ: 90			

2.2. Структурно-логічна схема

Структурно-логічна схема підготовки магістра за спеціальністю 125 Кібербезпека



3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників освітньої програми спеціальності 125 «Кібербезпека» проводиться у формі захисту кваліфікаційної роботи магістра, та завершується видачею документу встановленого зразка про присудження йому ступеня магістра із присвоєнням кваліфікації: Магістр з кібербезпеки, управління інформаційною безпекою.

Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.

4. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

Програмні компетентності	Перелік нормативних компонент освітньої програми															
	Обов'язкові компоненти освітньої програми															
	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16
ЗК 1	•			•	•		•					•		•	•	
ЗК 2		•				•							•			•
ЗК 3		•				•				•						•
ЗК 4					•			•				•	•			
ЗК 5	•					•		•				•		•	•	
ФК 1			•		•		•				•					•
ФК 2		•			•	•	•		•		•	•		•		
ФК 3			•							•			•		•	•
ФК 4		•							•			•		•	•	•
ФК 5				•				•					•		•	•
ФК 6					•		•				•			•	•	•
ФК 7			•					•	•				•	•		•
ФК 8					•				•	•	•					•
ФК 9				•		•		•	•							
ФК 10			•									•			•	•

5. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

Програмні компетентності	Перелік нормативних компонент освітньої програми															
	Обов'язкові компоненти освітньої програми															
	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16
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		•					•						•			•

Керівник робочої групи **Ростислав ТКАЧУК**