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 та захист інформації
СПЕЦІАЛІЗАЦІЯ	
КВАЛІФІКАЦІЯ	Магістр з кібербезпеки та захисту інформації, управління інформаційною безпекою

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Львівського державного університету
безпеки життєдіяльності
Голова Вченої ради

_____ Дмитро БОНДАР
(протокол № ___ від „___” _____ 20___ р.)

Освітньо-професійна програма
вводиться в дію
з „___” _____ 20___ р.
(наказ № ____ від „___” _____ 20___ р.)

Львів 2024

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

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

ВНЕСЕНО:

Кафедрою управління інформаційною безпекою

Протокол №_____ від «___»_____ 20__ р.

РЕКОМЕНДОВАНО:
Вченою радою навчально-наукового інституту цивільного захисту

Протокол №_____від «___»_____ 20__ р.

ПОГОДЖЕНО

Проректор з навчальної та методичної роботи

_____ Дмитро ЧАЛИЙ
“__-__”_____20___ р.

Начальник навчально-наукового інституту цивільного захисту

_____ Василь ПОПОВИЧ
“__-__”_____20___ р.

Начальник навчально-методичного центру

_____ Микола СИЧЕВСЬКИЙ
“_____”_____20___ р.

ПЕРЕДМОВА

Освітньо-професійна програма (далі – ОП) розроблена та оновлена на підставі Стандарту вищої освіти України за другим (магістерський) рівень, галузі знань 12 – Інформаційні технології, спеціальність 125 Кібербезпека. Стандарт затвердженого і введеного в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332 та внесеними доповненнями, відповідно до наказу Міністерства освіти і науки України від 13.01.2022 № 26 та Постанови Кабінету Міністрів України від 16.12.2022 № 1392.

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

Керівник робочої групи

Ростислав ТКАЧУК *(гарант освітньої програми)*	доктор технічних наук, професор, завідувач кафедри управління інформаційною безпекою.

Члени робочої групи:

Орест ПОЛОТАЙ	кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою;
Андрій ЛАГУН	кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою;
Тарас БРИЧ	кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою;
Андрій ІВАНУСА	кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою;
Валентина ЯЩУК	кандидат економічних наук, доцент, доцент кафедри управління інформаційною безпекою;
Валерія БАЛАЦЬКА	викладач кафедри управління інформаційною безпекою.

До розроблення програми залучено зовнішніх stakeholders:

Михайло КРОПИВА	InfoSec Director компанії SoftServe;
Роман КАРПЮК	CSOC Specialist at SoftServe;
Олег ЛЕСЬКІВ	менеджер освітніх проєктів Львівського IT Кластеру;
Михайло МАКСИМІВ	SOC Project Manager компанії UnderDefense;
Роман ЯРЕМЧУК	начальник Центру оперативного зв'язку, телекомунікаційних систем та інформаційних технологій ГУ ДСНС України у Львівській області;
Максим СМІЛЕВСЬКИЙ	начальник управління безпеки департаменту міської мобільності та вуличної інфраструктури Львівської міської ради;
Олена ГУНЬКО	начальник управління інформаційних технологій Львівської міської ради;
Юрій КОШЕЛЕНКО	випускник освітньої програми, начальник сектору технічного захисту інформації та радіотехнічного контролю центру оперативного зв'язку, телекомунікаційних систем та інформаційних технологій головного управління ДСНС України у Львівській області;
Ростислав ГРИНИК	випускник освітньої програми, expert center of excellence та Java Senior Engineer IT-компанії Intellias;
Юрій ДРАБ	здобувач освітньої програми другого освітнього ступеня «магістр» зі спеціальності 125 «Кібербезпека та захист інформації», інженер-програміст відділу інформаційних технологій та технічного захисту інформації Львівського державного університету безпеки життєдіяльності.

Рецензенти:

Олександр ПОТІЙ	заступник голови Державної служби спеціального зв'язку та захисту інформації України, д.т.н., професор

Іван ОПІРСЬКИЙ	завідувач кафедри захисту інформації Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка», д.т.н., професор
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 та захист інформації Освітня кваліфікація: магістр з кібербезпеки та захисту інформації, управління інформаційною безпекою
3.	*Офіційна назва освітньої програми*	Управління інформаційною безпекою
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 та захист інформації, 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 – 7 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. Вступ на основі освітнього ступеня бакалавра, магістра (освітньо-кваліфікаційного рівня спеціаліста).
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 та захист інформації, 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.		
3- Характеристика освітньої програми		
11	*Предметна область*	Галузь знань: 12 Інформаційні технології Спеціальність: 125 Кібербезпека та захист інформації 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 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 кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та кібербезпеки. <u>Цілі навчання:</u> Підготовка фахівців, здатних розв’язувати задачі дослідницького характеру у сфері інформаційної та кібербезпеки. <u>Теоретичний зміст предметної області:</u> 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 кібербезпеки. <u>Методи, методики та технології:</u> – 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 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. <u>Інструменти та обладнання:</u> – 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 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.
13	*Основний фокус освітньої програми*	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, лабораторних робіт, самостійної роботи в віртуальному навчальному середовищі, консультацій з викладачами, професійна практика; підготовка дослідницької кваліфікаційної роботи.
18	*Система оцінювання*	*Види контролю:* поточний, підсумковий (семестровий та підсумкова атестація). *Форми контролю:* Поточний контроль передбачає опитування в усній або письмові формі, тестування, захист виконання індивідуальних практичних завдань, реферати, захист звітів лабораторних робіт, презентацію проектів. Підсумковий (семестровий) контроль знань проводиться у вигляді диференційного заліку або екзамену (у письмовій формі, у письмовій формі з подальшою усною співбесідою, на базі електронного навчального середовища), захисту результатів проходження навчальної практики та захисту курсової роботи. Поточне та підсумкове оцінювання здійснюється за

		національною шкалою (відмінно/ добре/ задовільно/ незадовільно або зараховано/ не зараховано), а також 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F). Підсумкова атестація передбачає кваліфікаційну роботу.

	6-Програмні компетентності		
19	*Інтегральна*	Здатність особи розв'язувати задачі дослідницького характеру у сфері інформаційної безпеки та кібербезпеки.	
20	*Загальні*		*Компетентності відповідно до стандарту вищої освіти*
		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).
			Компетентності освітньої програми передбачені закладом вищої освіти
		ЗК6	Здатність усвідомлювати функції держави та їх форм реалізації, основи цивільного захисту; дотримуватись основних принципів здійснення цивільного захисту на об'єктах інформаційної діяльності.
21	*Фахові*		*Компетентності відповідно до стандарту вищої освіти*
		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 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 кібербезпеки.

		ФК3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
		ФК4	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та 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 кібербезпеки організації.
		ФК6	Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та 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 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 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 кібербезпеки.

			Програмні результати навчання освітньої програми
		ФК11	Здатність проведення ідентифікації, визначення умов виникнення і розвитку надзвичайних ситуацій та забезпечення скоординованих дій щодо безпеки та кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури відповідно до своїх професійних обов’язків.

7-Програмні результати навчання		
		Програмні результати навчання відповідно до стандарту вищої освіти
22	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 кібербезпеки.
	РН2	Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та кібербезпеки у широких або мультидисциплінарних контекстах.
	РН3	Провадити дослідницьку діяльність в сфері інформаційної безпеки та 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 кібербезпеки.
	РН5	Критично осмислювати проблеми інформаційної безпеки та 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 кібербезпеки.
	РН8	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
	РН9	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та 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 кібербезпеки організації.
	РН11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та 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 кібербезпеки в цілому.
	РН15	Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та 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 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 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 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 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 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 кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
		Програмні результати навчання передбачені закладом вищої освіти
	РН24	Розуміти завдання та організаційну структуру цивільного захисту України, й, зокрема організацію та управління системою цивільного захисту установ та організацій різної форми власності; знати алгоритм дій формувань цивільного захисту в умовах надзвичайних ситуацій, вміти забезпечувати стійкість роботи та збереження життя й здоров'я персоналу у сфері інформаційної діяльності.

	8 - Ресурсне забезпечення реалізації програми	
23	*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.
24	Матеріально-технічне забезпечення	Використання сучасних комп'ютерних засобів та ліцензійного програмного забезпечення (ПЗ з відкритою ліцензією) розподіленого між спеціалізованими лабораторіями та комп'ютерними класами, а також іншого аудиторного фонду Університету, кризового центру управління в надзвичайних ситуаціях, бібліотечним комплексом, читальними залами та соціально-побутовою інфраструктурою. Кількісні та якісні показники матеріально-технічного забезпечення відповідають вимогам Ліцензійних умов провадження освітньої діяльності закладів освіти.
25	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.

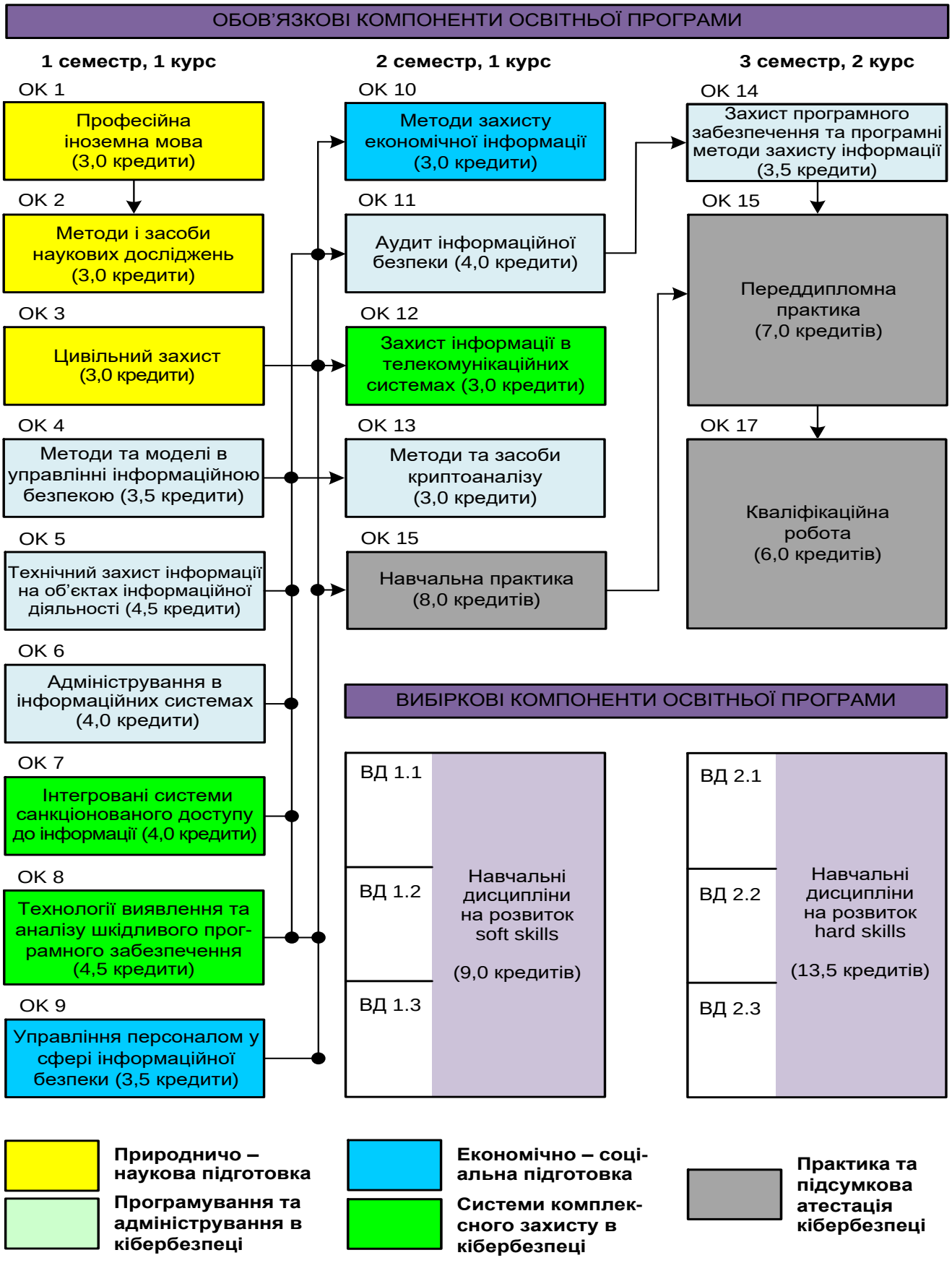
	9 - Академічна мобільність	
26	Національна кредитна мобільність	Може реалізуватись в рамках двосторонніх договорів між закладами вищої освіти про встановлення науково-освітянських відносин. Допускаються індивідуальні угоди про академічну мобільність для навчання (проходження практики) та проведення досліджень в університетах та наукових установах України.
27	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.
28	Навчання іноземних здобувачів вищої освіти	Можливе, після вивчення курсу української мови. Навчання іноземних громадян за кошти фізичних та юридичних осіб. 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			
1.1. Цикл загальної підготовки			
ОК 1	Професійна іноземна мова	3,0	екзамен
ОК 2	Методи і засоби наукових досліджень	3,0	диф. залік
ОК 3	Цивільний захист	3,0	диф. залік
Разом за циклом		***6,0***	
1.2. Цикл профільної підготовки			
ОК 4	Методи та моделі в управлінні інформаційною безпекою	3,0	екзамен
ОК 5	Технічний захист інформації на об'єктах інформаційної діяльності	4,0	диф. залік
ОК 6	Адміністрування в інформаційних системах	3,5	диф. залік
ОК 7	Інтегровані системи санкціонованого доступу до інформації	3,5	екзамен, курсова робота
ОК 8	Технології виявлення та аналізу шкідливого програмного забезпечення	4,0	диф. залік
ОК 9	Управління персоналом у сфері інформаційної безпеки	3,0	екзамен
ОК 10	Методи захисту економічної інформації	3,0	екзамен
ОК 11	Аудит інформаційної безпеки	4,0	екзамен
ОК 12	Захист інформації в телекомунікаційних системах	3,0	екзамен
ОК 13	Методи та засоби криптоаналізу	3,0	екзамен
ОК 14	Захист програмного забезпечення та програмні методи захисту інформації	3,5	екзамен, курсова робота
ОК 15	Навчальна практика	8,0	диф. залік
ОК 16	Переддипломна практика	7,0	диф. залік
Разом за циклом		***55,5***	
1.3. Атестація			
ОК 17	Кваліфікаційна робота	6,0	
Разом за циклом		***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	9,0	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



3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

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

Кваліфікаційна робота має розв’язувати складну задачу інформаційної безпеки та кібербезпеки і передбачати проведення досліджень та 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.

4. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

Програмні компетентності	Перелік нормативних компонент освітньої програми																
	Цикл загальної підготовки			Цикл профільної підготовки													
	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	ОК 17
ЗК 1	•				•				•	•				•	•	•	
ЗК 2		•						•			•						•
ЗК 3		•									•		•				•
ЗК 4					•	•		•	•								
ЗК 5	•					•			•		•				•	•	
ЗК 6			•						•								
ФК 1				•	•		•							•			•
ФК 2		•			•		•		•		•	•		•	•		
ФК 3				•				•					•			•	•
ФК 4		•							•			•			•	•	•
ФК 5						•		•		•						•	•
ФК 6					•		•							•	•	•	•
ФК 7				•		•		•				•			•		•
ФК 8					•		•					•	•				•
ФК 9						•				•	•	•					
ФК 10				•					•							•	•
ФК 11			•	•					•								

5. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

Програмні компетентності	Перелік нормативних компонент освітньої програми																
	Цикл загальної підготовки			Цикл профільної підготовки													
	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	ОК 17
РН 1	•								•						•	•	•
РН 2				•							•						•
РН 3		•					•	•					•				•
РН 4				•	•			•		•		•					•
РН 5					•		•							•			•
РН 6					•		•	•				•		•	•		•
РН 7		•								•							
РН 8					•		•					•			•	•	•
РН 9						•	•		•			•			•	•	•
РН 10					•	•	•	•				•			•		•
РН 11				•			•							•		•	
РН 12						•		•	•						•		•
РН 13					•					•			•			•	•
РН 14						•					•					•	•
РН 15	•								•						•	•	•
РН 16									•		•	•				•	•
РН 17		•							•						•	•	
РН 18			•						•						•	•	
РН 19				•	•												•
РН 20		•		•											•	•	•
РН 21		•		•											•	•	•
РН 22		•		•											•	•	•
РН 23		•						•						•			•
РН 24			•	•					•								

Розглянуто на засіданні кафедри управління інформаційною безпекою,
протокол № 5 від 08.12.2023 р.

Керівник групи забезпечення ОПП Ростислав ТКАЧУК

РОЗПОДІЛ КОМПЕТЕНЦІЙ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ

Шифр	Компетенції	Найменування освітніх компонентів
ЗК 1	Здатність застосовувати знання у практичних ситуаціях.	ОК 1 Професійна іноземна мова; ОК 5 Технічний захист інформації на об'єктах інформаційної діяльності; ОК 9 Управління персоналом у сфері інформаційної безпеки; ОК 10 Методи захисту економічної інформації; ОК 14 Захист програмного забезпечення та програмні методи захисту інформації; ОК 15 Навчальна практика; ОК 16 Переддипломна практика.
ЗК 2	Здатність проводити дослідження на відповідному рівні.	ОК 2 Методи і засоби наукових досліджень; ОК 8 Технології виявлення та аналізу шкідливого програмного забезпечення; ОК 11 Аудит інформаційної безпеки; ОК 17 Кваліфікаційна робота.
ЗК 3	Здатність до абстрактного мислення, аналізу та синтезу.	ОК 2 Методи і засоби наукових досліджень; ОК 11 Аудит інформаційної безпеки; ОК 13 Методи та засоби криптоаналізу; ОК 17 Кваліфікаційна робота.
ЗК 4	Здатність оцінювати та забезпечувати якість виконуваних робіт.	ОК 5 Технічний захист інформації на об'єктах інформаційної діяльності; ОК 6 Адміністрування в інформаційних системах; ОК 8 Технології виявлення та аналізу шкідливого програмного забезпечення; ОК 13 Інтегровані системи санкціонованого доступу до інформації.
ЗК 5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).	ОК 1 Професійна іноземна мова; ОК 6 Адміністрування в інформаційних системах; ОК 9 Управління персоналом у сфері інформаційної безпеки; ОК 11 Аудит інформаційної безпеки; ОК 15 Навчальна практика; ОК 16 Переддипломна практика.
ЗК 6	Здатність усвідомлювати функції держави та їх форм реалізації, основи цивільного захисту; дотримуватись основних принципів здійснення цивільного захисту на об'єктах інформаційної діяльності.	ОК 3 Цивільний захист; ОК 9 Управління персоналом у сфері інформаційної безпеки.
ФК 1	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і	ОК 4 Методи та моделі в управлінні інформаційною безпекою; ОК 5 Технічний захист інформації на об'єктах інформаційної діяльності; ОК 7 Інтегровані системи санкціонованого доступу до інформації;

Шифр	Компетенції	Найменування освітніх компонентів
	спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та кібербезпеки.	ОК 14 Захист програмного забезпечення та програмні методи захисту інформації; ОК 17 Кваліфікаційна робота.
ФК 2	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 кібербезпеки.	ОК 2 Методи і засоби наукових досліджень; ОК 5 Технічний захист інформації на об’єктах інформаційної діяльності; ОК 7 Інтегровані системи санкціонованого доступу до інформації; ОК 9 Управління персоналом у сфері інформаційної безпеки; ОК 11 Аудит інформаційної безпеки; ОК 12 Захист інформації в телекомунікаційних системах; ОК 14 Захист програмного забезпечення та програмні методи захисту інформації; ОК 15 Навчальна практика.
ФК 3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.	ОК 4 Методи та моделі в управлінні інформаційною безпекою; ОК 8 Технології виявлення та аналізу шкідливого програмного забезпечення; ОК 13 Методи та засоби криптоаналізу; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
ФК 4	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.	ОК 2 Методи і засоби наукових досліджень; ОК 9 Управління персоналом у сфері інформаційної безпеки; ОК 12 Захист інформації в телекомунікаційних системах; ОК 15 Навчальна практика; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
ФК 5	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 кібербезпеки організації.	ОК 6 Адміністрування в інформаційних системах; ОК 8 Технології виявлення та аналізу шкідливого програмного забезпечення; ОК 10 Методи захисту економічної інформації; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
ФК 6	Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та кібербезпеки організації.	ОК 5 Технічний захист інформації на об’єктах інформаційної діяльності; ОК 7 Інтегровані системи санкціонованого доступу до інформації; ОК 14 Захист програмного забезпечення та програмні методи захисту інформації;

Шифр	Компетенції	Найменування освітніх компонентів
		ОК 15 Навчальна практика; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
ФК 7	Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	ОК 4 Методи та моделі в управлінні інформаційною безпекою; ОК 6 Адміністрування в інформаційних системах; ОК 8 Технології виявлення та аналізу шкідливого програмного забезпечення; ОК 12 Захист інформації в телекомунікаційних системах; ОК 15 Навчальна практика; ОК 17 Кваліфікаційна робота.
ФК 8	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 кібербезпеки організації.	ОК 5 Технічний захист інформації на об’єктах інформаційної діяльності; ОК 7 Інтегровані системи санкціонованого доступу до інформації; ОК 11 Методи та засоби крипто аналізу; ОК 12 Захист інформації в телекомунікаційних системах; ОК 17 Кваліфікаційна робота.
ФК 9	Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та кібербезпеки організації в цілому.	ОК 6 Адміністрування в інформаційних системах; ОК 10 Методи захисту економічної інформації; ОК 11 Аудит інформаційної безпеки; ОК 12 Захист інформації в телекомунікаційних системах.
ФК 10	Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та кібербезпеки.	ОК 4 Методи та моделі в управлінні інформаційною безпекою; ОК 9 Управління персоналом у сфері інформаційної безпеки; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
ФК11	Здатність проведення ідентифікації, визначення умов виникнення і розвитку надзвичайних ситуацій та забезпечення скоординованих дій щодо безпеки та кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури відповідно до своїх професійних обов’язків.	ОК 3 Цивільний захист; ОК 4 Методи та моделі в управлінні інформаційною безпекою; ОК 9 Управління персоналом у сфері інформаційної безпеки.

РОЗПОДІЛ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ

Шифр	Результати навчання	Найменування освітніх компонентів
РН 1	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 кібербезпеки.	ОК 1 Професійна іноземна мова; ОК 9 Управління персоналом у сфері інформаційної безпеки; ОК 15 Навчальна практика; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
РН 2	Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та кібербезпеки у широких або мультидисциплінарних контекстах.	ОК 4 Методи та моделі в управлінні інформаційною безпекою; ОК 11 Аудит інформаційної безпеки; ОК 17 Кваліфікаційна робота.
РН 3	Провадити дослідницьку діяльність в сфері інформаційної безпеки та кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	ОК 2 Методи і засоби наукових досліджень; ОК 7 Інтегровані системи санкціонованого доступу до інформації; ОК 8 Технології виявлення та аналізу шкідливого програмного забезпечення; ОК 13 Методи та засоби криптоаналізу; ОК 17 Кваліфікаційна робота.
РН 4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та кібербезпеки.	ОК 4 Методи та моделі в управлінні інформаційною безпекою; ОК 5 Технічний захист інформації на об'єктах інформаційної діяльності; ОК 8 Технології виявлення та аналізу шкідливого програмного забезпечення; ОК 10 Методи захисту економічної інформації; ОК 12 Захист інформації в телекомунікаційних системах; ОК 17 Кваліфікаційна робота.
РН 5	Критично осмислювати проблеми інформаційної безпеки та 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.	ОК 5 Технічний захист інформації на об'єктах інформаційної діяльності; ОК 7 Інтегровані системи санкціонованого доступу до інформації; ОК 14 Захист програмного забезпечення та програмні методи захисту інформації; ОК 17 Кваліфікаційна робота.
РН 6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	ОК 5 Технічний захист інформації на об'єктах інформаційної діяльності; ОК 7 Інтегровані системи санкціонованого доступу до інформації; ОК 8 Технології виявлення та аналізу шкідливого програмного забезпечення;

Шифр	Результати навчання	Найменування освітніх компонентів
		ОК 12 Захист інформації в телекомунікаційних системах; ОК 14 Захист програмного забезпечення та програмні методи захисту інформації; ОК 15 Навчальна практика; ОК 17 Кваліфікаційна робота.
РН 7	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та кібербезпеки.	ОК 2 Методи і засоби наукових досліджень; ОК 10 Методи захисту економічної інформації.
РН 8	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	ОК 5 Технічний захист інформації на об'єктах інформаційної діяльності; ОК 7 Інтегровані системи санкціонованого доступу до інформації; ОК 12 Захист інформації в телекомунікаційних системах; ОК 15 Навчальна практика; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
РН 9	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	ОК 6 Адміністрування в інформаційних системах; ОК 7 Інтегровані системи санкціонованого доступу до інформації; ОК 9 Управління персоналом у сфері інформаційної безпеки; ОК 12 Захист інформації в телекомунікаційних системах; ОК 15 Навчальна практика; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
РН 10	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та кібербезпеки організації.	ОК 5 Технічний захист інформації на об'єктах інформаційної діяльності; ОК 6 Адміністрування в інформаційних системах; ОК 7 Інтегровані системи санкціонованого доступу до інформації; ОК 8 Технології виявлення та аналізу шкідливого програмного забезпечення; ОК 12 Захист інформації в телекомунікаційних системах; ОК 15 Навчальна практика; ОК 17 Кваліфікаційна робота.
РН 11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та кібербезпеки організації.	ОК 4 Методи та моделі в управлінні інформаційною безпекою; ОК 7 Інтегровані системи санкціонованого доступу до інформації; ОК 14 Захист програмного забезпечення та програмні методи захисту інформації; ОК 16 Переддипломна практика.

Шифр	Результати навчання	Найменування освітніх компонентів
РН 12	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.	ОК 6 Адміністрування в інформаційних системах; ОК 8 Технології виявлення та аналізу шкідливого програмного забезпечення; ОК 9 Управління персоналом у сфері інформаційної безпеки; ОК 15 Навчальна практика; ОК 17 Кваліфікаційна робота.
РН 13	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.	ОК 5 Технічний захист інформації на об’єктах інформаційної діяльності; ОК 10 Методи захисту економічної інформації; ОК 13 Методи та засоби криптоаналізу; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
РН 14	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.	ОК 6 Адміністрування в інформаційних системах; ОК 11 Аудит інформаційної безпеки; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
РН 15	Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	ОК 1 Професійна іноземна мова; ОК 9 Управління персоналом у сфері інформаційної безпеки; ОК 15 Навчальна практика; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
РН 16	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	ОК 9 Управління персоналом у сфері інформаційної безпеки; ОК 11 Аудит інформаційної безпеки; ОК 12 Захист інформації в телекомунікаційних системах; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
РН 17	Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.	ОК 2 Методи і засоби наукових досліджень; ОК 9 Управління персоналом у сфері інформаційної безпеки; ОК 15 Навчальна практика; ОК 16 Переддипломна практика.

Шифр	Результати навчання	Найменування освітніх компонентів
РН 18	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та кібербезпеки.	ОК 3 Цивільний захист; ОК 9 Управління персоналом у сфері інформаційної безпеки; ОК 15 Навчальна практика; ОК 16 Переддипломна практика.
РН 19	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.	ОК 4 Методи та моделі в управлінні інформаційною безпекою; ОК 5 Технічний захист інформації на об’єктах інформаційної діяльності; ОК 17 Кваліфікаційна робота.
РН 20	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	ОК 2 Методи та моделі в управлінні інформаційною безпекою; ОК 4 Методи і засоби наукових досліджень; ОК 15 Навчальна практика; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
РН 21	Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та кібербезпеки.	ОК 2 Методи та моделі в управлінні інформаційною безпекою; ОК 4 Методи і засоби наукових досліджень; ОК 15 Навчальна практика; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
РН 22	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.	ОК 2 Методи та моделі в управлінні інформаційною безпекою; ОК 4 Методи і засоби наукових досліджень; ОК 15 Навчальна практика; ОК 16 Переддипломна практика; ОК 17 ОК 15 Навчальна практика; ОК 16 Переддипломна практика; ОК 17 Кваліфікаційна робота.
РН 23	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	ОК 2 Методи і засоби наукових досліджень; ОК 8 Технології виявлення та аналізу шкідливого програмного забезпечення; ОК 14 Захист програмного забезпечення та програмні методи захисту інформації; ОК 17 Кваліфікаційна робота.
РН 24	Розуміти завдання та організаційну структуру цивільного захисту України, й, зокрема організацію та управління системою цивільного захисту установ та організацій різної форми власності; знати алгоритм дій	ОК 3 Цивільний захист; ОК 4 Методи та моделі в управлінні інформаційною безпекою; ОК 9 Управління персоналом у сфері інформаційної безпеки.

Шифр	Результати навчання	Найменування освітніх компонентів
	формувань цивільного захисту в умовах надзвичайних ситуацій, вміти забезпечувати стійкість роботи та збереження життя й здоров'я персоналу у сфері інформаційної діяльності.	

РОЗПОДІЛ КОМПЕТЕНЦІЙ ТА ПРОГРАМНИХ РЕЗУЛЬТАТІВ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ

ОК	Назва дисципліни	Компетенції	Програмні результати
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ			
1.1. Цикл загальної підготовки			
ОК 1	Професійна іноземна мова	ЗК1, ЗК5	РН1, РН15
ОК 2	Методи і засоби наукових досліджень	ЗК2, ЗК3, ФК2, ФК4	РН3, РН7, РН17, РН20, РН21, РН22, РН23
ОК 3	Цивільний захист	ЗК6, ФК11	РН18, РН24
1.2. Цикл профільної підготовки			
ОК 4	Методи та моделі в управлінні інформаційною безпекою	ФК1, ФК3, ФК7, ФК10	РН2, РН4, РН11, РН19, РН20, РН21, РН22
ОК 5	Технічний захист інформації на об'єктах інформаційної діяльності	ЗК1, ЗК4, ФК1, ФК2, ФК6, ФК8	РН4, РН5, РН6, РН8, РН10, РН13, РН19
ОК 6	Адміністрування в інформаційних системах	ЗК4, ЗК5, ФК5, ФК7, ФК9	РН9, РН10, РН12, РН14
ОК 7	Інтегровані системи санкціонованого доступу до інформації	ФК1, ФК2, ФК6, ФК8	РН3, РН5, РН6, РН8, РН9, РН10, РН11
ОК 8	Технології виявлення та аналізу шкідливого програмного забезпечення	ЗК2, ЗК4, ФК3, ФК5, ФК7	РН3, РН4, РН6, РН10, РН12, РН23
ОК 9	Управління персоналом у сфері інформаційної безпеки	ЗК1, ЗК4, ЗК5, ФК2, ФК4, ФК10	РН1, РН9, РН12, РН15, РН16, РН17, РН18
ОК 10	Методи захисту економічної інформації	ЗК1, ФК5, ФК9	РН4, РН7, РН13
ОК 11	Аудит інформаційної безпеки	ЗК2, ЗК3, ЗК5, ФК2, ФК9	РН2, РН14, РН16
ОК 12	Захист інформації в телекомунікаційних системах	ФК2, ФК4, ФК7, ФК8, ФК9	РН4, РН6, РН8, РН9, РН10, РН16
ОК 13	Методи та засоби криптоаналізу	ЗК3, ФК3, ФК8	РН3, РН13
ОК 14	Захист програмного забезпечення та програмні методи захисту інформації	ЗК1, ФК1, ФК2, ФК6	РН5, РН6, РН11, РН23

ОК	Назва дисципліни	Компетенції	Програмні результати
ОК 15	Навчальна практика	ЗК1, ЗК5, ФК2, ФК4, ФК6, ФК7	РН1, РН6, РН8, РН9, РН10, РН12, РН15, РН17, РН18, РН20, РН21, РН22
ОК 16	Переддипломна практика	ЗК1, ЗК5, ФК3, ФК4, ФК5, ФК6, ФК10	РН1, РН8, РН9, РН11, РН13, РН14, РН15, РН16, РН17, РН18, РН20, РН21, РН22
1.3. Атестація			
ОК 17	Кваліфікаційна робота	ЗК2, ЗК3, ФК1, ФК3, ФК4, ФК5, ФК6, ФК7, ФК8, ФК10	РН1, РН2, РН3, РН4, РН5, РН6, РН8, РН9, РН10, РН12, РН13, РН14, РН15, РН16, РН19, РН20, РН21, РН22, РН23

Керівник робочої групи **Ростислав ТКАЧУК**

ТАБЛИЦЯ ПРОПОЗИЦІЙ
ДО ПРОЄКТУ ОСВІТНЬОЇ ПРОГРАМИ ЗА РЕЗУЛЬТАТАМИ ГРОМАДСЬКОГО ОБГОВОРЕННЯ

Вид та назва освітньої програми освітньо-професійна програма «Управління інформаційною безпекою»

Рівень вищої освіти другий (магістерський)

Назва спеціальності 125 Кібербезпека та захист інформації

Керівник групи забезпечення ТКАЧУК Ростислав Львович

№ п/п	Автор пропозиції (прізвище, ініціали, належність до групиstakeholders)	Розділ, пункт, підпункт / позиція проєкту освітньої програми, до якого вноситься пропозиція. Зміст пропозиції, дата	Нова редакція відповідного розділу /пункту / підпункту / позиції освітньої програми з урахуванням пропозицій / змін	Зміни, що вносяться до змісту освітніх компонентів з метою забезпечення виконання пропозицій та їх обґрунтування / обґрунтування відмови
1.	Ткачук Ростислав – гарант освітньо-професійної програми, начальник кафедри УІБ ЛДУБЖД, внутрішній stakeholder	Внести зміни до розділу 2 «Перелік компонент освітньо-професійної програми та їх логічна послідовність», п. 2.1 «Перелік компонент освітньо-професійної програми» та п. 2.2. «Структурно-логічна схема», зокрема вилучити «Комплексний кваліфікаційний екзамен» (1,5 кредити). - забрати курсовий проєкт з дисципліни «Методи та моделі в управлінні інформаційною безпекою».	Внесені зміни: - вилучений «Комплексний кваліфікаційний екзамен» (1,5 кредити); - вилучений курсовий проєкт з дисципліни «Методи та моделі в управлінні інформаційною безпекою».	**Враховано повністю**
2.	Кропива Михайло - InfoSec Director, Softserve, Львів, зовнішній stakeholder	Внести зміни до розділу 2 «Перелік компонент освітньо-професійної програми та їх логічна послідовність», п. 2.1 «Перелік компонент освітньо-професійної програми» та п. 2.2. «Структурно-логічна схема». Збільшити кількість кредитів «Переддипломної	Внесені зміни: - «Переддипломна практика» (7,0 кредити)	**Враховано повністю**

№ п/п	Автор пропозиції (прізвище, ініціали, належність до групиstakeholders)	Розділ, пункт, підпункт / позиція проєкту освітньої програми, до якого вноситься пропозиція. Зміст пропозиції, дата	Нова редакція відповідного розділу /пункту / підпункту / позиції освітньої програми з урахуванням пропозицій / змін	Зміни, що вносяться до змісту освітніх компонентів з метою забезпечення виконання пропозицій та їх обґрунтування / обґрунтування відмови
		практики» (5,5 кредитів).		
3.	Лагун Андрій – доцент кафедри УІБ ЛДУБЖД, внутрішній stakeholder	Внести зміни до розділу 2 «Перелік компонент освітньо-професійної програми та їх логічна послідовність», п. 2.1 «Перелік компонент освітньо-професійної програми» та п. 2.2. «Структурно-логічна схема». Забрати курсовий проєкт з освітньої компоненти «Методи та моделі в управлінні інформаційною безпекою» без зміни кількості кредитів (3,5 кредити) для її вивчення.	Внесені зміни: - «Методи та моделі в управлінні інформаційною безпекою» (3,5 кредити)	**Враховано повністю**

Розглянуто на засіданні кафедри управління інформаційною безпекою,
протокол № 5 від 08.12.2023 р.

Керівник групи забезпечення ОПП Ростислав ТКАЧУК