МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

(повна назва освітньої програми)

бакалавр

(рівень вищої освіти)

ГАЛУЗІ ЗНАНЬ	12 Інформаційні технології
ЗА СПЕЦІАЛЬНІСТЮ	125 Кібербезпека та захист інформації
СПЕЦІАЛІЗАЦІЯ	
КВАЛІФІКАЦІЯ	Бакалавр з кібербезпеки, управління інформаційною безпекою

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Львівського державного університету
безпеки життєдіяльності
Голова Вченої ради

_____ Мирослав КОВАЛЬ
(протокол № 10 від „ 14 ” 06 2023 р.)

Освітньо-професійна програма вводиться в дію
з „ 16 ” червня 2023 р.
(наказ № НС-56 від „ 16 ” 06 2023 р.)

Львів 2023

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Рівень вищої освіти	перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Спеціалізація	
Кваліфікація	Бакалавр з кібербезпеки, 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
„ 12” 05 2023 р.

ПЕРЕДМОВА

Освітньо-професійна програма розроблена та оновлена на підставі Стандарту вищої освіти за першим (бакалаврським) рівнем вищої освіти в галузі знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека.

Стандарт затверджено і введено в дію наказом Міністерства освіти і науки України від 04.10.2018 № 1074 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	
Орест ПОЛОТАЙ *(гарант освітньої програми)*	кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою.
Члени робочої групи:	
Ростислав ТКАЧУК	доктор технічних наук, професор, завідувач 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;
Віталій РУДИК	випускник освітньої програми, спеціаліст першої категорії відділу оперативно-технічних заходів 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;
Юрій ДРАБ	випускник освітньої програми, інженер-програміст відділу інформаційних технологій та технічного захисту інформації Львівського державного університету безпеки життєдіяльності;
Ростислав ГРИНИК	випускник освітньої програми, expert center of excellence та Java Senior Engineer IT-компанії Intellias;
Михайло ДОВГАНИЧ	здобувач освітньої програми освітнього ступеня «бакалавр» зі спеціальності 125 «Кібербезпека та захист інформації» (Penetration Tester and Ethical Hacker компанії UnderDefense);
Богдан ФІЛІПЧУК	здобувач освітньої програми освітнього ступеня «бакалавр» зі спеціальності 125 «Кібербезпека та захист інформації».

Рецензенти:

Василь ЯЦКІВ	професор, д.т.н., професор завідувач кафедри кібербезпеки Західноукраїнського національного університету
Володимир РОМАКА	професор, д.т.н., професор кафедри захисту інформації Національного університету «Львівська політехніка»
Орест ШОПСЬКИЙ	заступник начальник центру оперативного зв'язку, телекомунікаційних систем та інформаційних технологій Головного управління Державної служби України з надзвичайних ситуацій у Львівській області
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 4 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: бакалавр Спеціальність: 125 Кібербезпека та захист інформації Освітня кваліфікація: бакалавр з кібербезпеки, управління інформаційною безпекою
3.	*Офіційна назва освітньої програми*	Управління інформаційною безпекою
4.	*Тип диплому та обсяг освітньої програми*	Диплом бакалавра, одиничний: – на основі повної загальної середньої освіти – 240 кредитів ЄКТС, термін навчання – 3 роки 10 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 №1487329, рішення Акредитаційної комісії від 17 листопада 2015 року, протокол №119 (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 – 6 рівень; FQ-EHEA – перший цикл; EQF-LLL – 6 рівень.
7.	*Передумови*	Наявність повної загальної середньої освіти або освітнього ступеня молодшого бакалавра (освітньо-кваліфікаційного рівня молодшого спеціаліста). Передумови вступу визначаються «Правилами прийому до Львівського державного університету безпеки життєдіяльності», затвердженими в поточному році Вченою радою університету.
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

2-Мета освітньої програми
Ця програма призначена для розвитку професійних і творчих здібностей здобувачів до розв'язання практичних проблем, які характеризується комплексністю та невизначеністю, на основі методів і засобів забезпечення кібербезпеки та захисту інформації. Крім того освітня програма націлена на підготовку фахівців, здатних розробляти, впроваджувати та супроводжувати інформаційні технології, знаходити раціональні методи та засоби їх розв'язку, вирішувати прикладні і наукові завдання, пов'язані з кібербезпекою та захистом інформації.

3- Характеристика освітньої програми		
11	*Предметна область*	Галузь знань: 12 Інформаційні технології Спеціальність: 125 Кібербезпека та захист інформації Об'єкти вивчення: – об'єкти інформатизації, включаючи комп'ютерні,автоматизовані,телекомунікаційні,інформаційні,інформаційно-аналітичні,інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та кібербезпекою об'єктів, що підлягають захисту. Мета навчання: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та кібербезпеки. Теоретичний зміст предметної області: Знання: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування.
12	*Орієнтація освітньої програми*	Освітньо-професійна програма. Професійний акцент на готовність працювати й набувати навички знань з інформаційної та кібербезпеки, задач прогнозування, проектування, оптимізації, системного аналізу та прийняття рішень, аналізу і синтезу даних і знань пов'язаних з кібербезпекою та захистом інформації.
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, цілісності та можливості використання даних в організаційних, технічних, природничих та соціально-економічних системах. А також з додатковим акцентом на задачі зі сфери технічного захисту інформації, які виникають в підрозділах ДСНС України.

		Ключові слова: алгоритми, програмування, бази даних та знань, комп'ютерні мережі, Web-технології, операційні системи, моделювання, комплексна система захисту інформації, етичний хакінг, інформаційна безпека, комп'ютерна криміналістика, інструменти кібербезпеки, криптографія.
14	*Особливості програми*	Програма розвиває перспективні напрями інформаційної безпеки та кібербезпеки, а саме моделювання, проектування, розробку, впровадження та супровід систем кібербезпеки. Готує фахівців здатних розв'язувати, крім загальних завдань в області кібербезпеки, прикладні задачі щодо створення та підтримки функціонування інформатизації процесів оперативної та повсякденної діяльності підрозділів ДСНС України; організації обміну інформацією між підрозділами ДСНС України із використанням програмно-технічних засобів в умовах надзвичайної ситуації або у повсякденній діяльності; проектування, розробки та супроводу інформаційних, комп'ютерних та програмних систем в підрозділах (формуваннях), робота яких пов'язана з оперативною діяльністю (ДСНС України, Національна поліція, Національна гвардія, ДПС України, ЗС України тощо). ОП передбачає практичну підготовку в органах та підрозділах Державної служби України з надзвичайних ситуацій (підрозділи телекомунікацій, інформаційних технологій та Системи 112, технічного захисту інформації та радіотехнічного контролю, інформаційних технологій та телекомунікаційних систем), ІТ-компаніях та організаціях (підприємствах, установах) незалежно від форм власності, які в своїй повсякденній діяльності використовують інформаційні технології.

4 - Придатність випускників до працевлаштування та подальшого навчання		
15	*Придатність до працевлаштування*	Згідно з Національним класифікатором професій ДК 003-2010 фахівці, які здобули освіту за освітньою програмою «Управління інформаційною безпекою» можуть обіймати такі первинні посади: • фахівець з технічного захисту інформації, • фахівець із організації інформаційної безпеки, • фахівець із організації захисту інформації з обмеженим доступом, • фахівець з інформаційних технологій, • фахівець з організації та проведення тестування на проникнення, • менеджер систем з інформаційної безпеки, • аналітик систем забезпечення кібербезпеки, • адміністратор баз даних, • адміністратор комп'ютерних систем та мереж, • аудитор з кібербезпеки, • розробник засобів захисту інформації, • проектувальник систем захисту інформації, • провідний спеціаліст/керівник служби ТЗІ, тощо. Згідно з штатним розписом територіальних управлінь ДСНС України фахівці, які здобули кваліфікацію

		«бакалавр з кібербезпеки, управління інформаційною безпекою» за освітньою програмою «Управління інформаційною безпекою» можуть обіймати такі первинні посади: • фахівець (інженер) підрозділу телекомунікаційних систем та інформаційних технологій.
16	*Подальше навчання*	Мають право продовжити навчання на другому (магістерському) рівні вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.

5 - Стиль викладання та оцінювання		
17	*Підходи до викладання та навчання*	Студентоцентроване навчання та самонавчання. Викладання та навчання проводиться у вигляді лекцій, практичних і семінарських занять, лабораторних робіт, виконання курсових робіт, виконання проектів та індивідуальних завдань, консультацій з викладачами. Практичне навчання забезпечується на базі підрозділів ДСНС України (підрозділи телекомунікаційних систем та інформаційних технологій), ІТ-компаній та організацій (підприємств, установ) незалежно від форм власності, які в своїй повсякденній діяльності використовують інформаційні технології. На самостійне навчання відводиться понад 50 % часу, реалізовується на базі навчально-наукового фонду бібліотечного комплексу Університету та курсів електронного освітнього середовища «Віртуальний університет». Завершується навчання підготовкою та проходженням єдиного державного кваліфікаційного іспиту (ЄДКІ).
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 складання єдиного державного кваліфікаційного іспиту.
	6-Програмні компетентності	
19	*Інтегральна*	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і кібербезпеки, що характеризується комплексністю та невизначеністю умов.

20	*Загальні*		*Компетентності відповідно до стандарту вищої освіти*
		ЗК1	Здатність застосовувати знання у практичних ситуаціях.
		ЗК2	Знання та розуміння предметної області та розуміння професії.
		ЗК3	Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
		ЗК4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
		ЗК5	Здатність до пошуку, оброблення та аналізу інформації.
		ЗК6	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.
		ЗК7	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.
			Компетентності освітньої програми передбачені закладом вищої освіти
		ЗК8	Формування ідентичності та почуття особистої гідності в результаті осмислення соціального та морального досвіду минулих поколінь, розуміння історії і культури України в контексті історичного процесу.
		ЗК9	Формування навиків здійснення безпечної діяльності.
		ЗК10	Усвідомлення функцій держави, форм реалізації цих функцій, правових основ цивільного захисту, дотримання основних принципів здійснення цивільного захисту.
21	*Фахові*		*Компетентності відповідно до стандарту вищої освіти*
		ФК1	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 кібербезпеки.
		ФК2	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та кібербезпеки.
		ФК3	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

		ФК4	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та кібербезпеки.
		ФК5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та кібербезпеки.
		ФК6	Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
		ФК7	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
		ФК8	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
		ФК9	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
		ФК10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
		ФК11	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та кібербезпеки.
		ФК12	Здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та кібербезпеки.

7-Програмні результати навчання		
22		*Програмні результати навчання відповідно до стандарту вищої освіти*
	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.
РН6	Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
РН7	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та кібербезпеки.
РН8	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та кібербезпеки.
РН9	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки.
РН10	Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
РН11	Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
РН12	Розробляти моделі загроз та порушника.
РН13	Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
РН14	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
РН15	Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
РН16	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
РН17	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.
РН18	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН19	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
РН20	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
РН21	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.
РН22	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН23	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН24	Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

	РН25	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.
	РН26	Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
	РН27	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
	РН28	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.
	РН29	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.
	РН30	Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
	РН31	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
	РН32	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
	РН33	Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
	РН34	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та кібербезпеки відповідно до цілей і завдань організації.
	РН35	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 кібербезпеки.
	РН36	Виявляти небезпечні сигнали технічних засобів.
	РН37	Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
	РН38	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
	РН39	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
	РН40	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
	РН41	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
	РН42	Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і кібербезпеки.

	РН43	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та кібербезпеки для розслідування інцидентів.
	РН44	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.
	РН45	Застосовувати різні класи політик інформаційної безпеки та кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
	РН46	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
	РН47	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
	РН48	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
	РН49	Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
	РН50	Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
	РН51	Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
	РН52	Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
	РН53	Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
	РН54	Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
		Програмні результати навчання передбачені закладом вищої освіти
	РН55	Демонструвати навички аналізу категорій цивільної безпеки, оцінювати стан та використовувати сучасні безпекові механізми для захисту інтересів людини, а також демонструвати готовність до зміцнення особистого здоров'я шляхом використання рухової активності.
	РН56	Володіти технологіями кібербезпеки та захисту інформації у системі цивільного захисту.
	РН57	Застосовувати отримані знання основ цивільно захисту в практичній діяльності.

	8 - Ресурсне забезпечення реалізації програми	
23	*Кадрове забезпечення*	Реалізація програми забезпечується науково-педагогічними працівниками, що мають кваліфікацію відповідно до спеціальності. До реалізації програми залучається не менше ніж 50% науково-педагогічних працівників, які мають науковий ступінь та/або вчене звання, з яких не менше ніж 10% мають науковий ступінь доктора наук та/або вчене звання професора. Реалізована система професійного розвитку викладачів, зокрема шляхом співпраці з ІТ-компаніями та підрозділами ДСНС України.

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 електронного освітнього середовища Львівського державного університету безпеки життєдіяльності; авторських розробок працівників; підручників та навчальних посібників з грифом Вченої ради Університету; навчально-наукового фонду бібліотечного комплексу Університету; іншого навчального контенту та методичного матеріалу розміщеного 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.

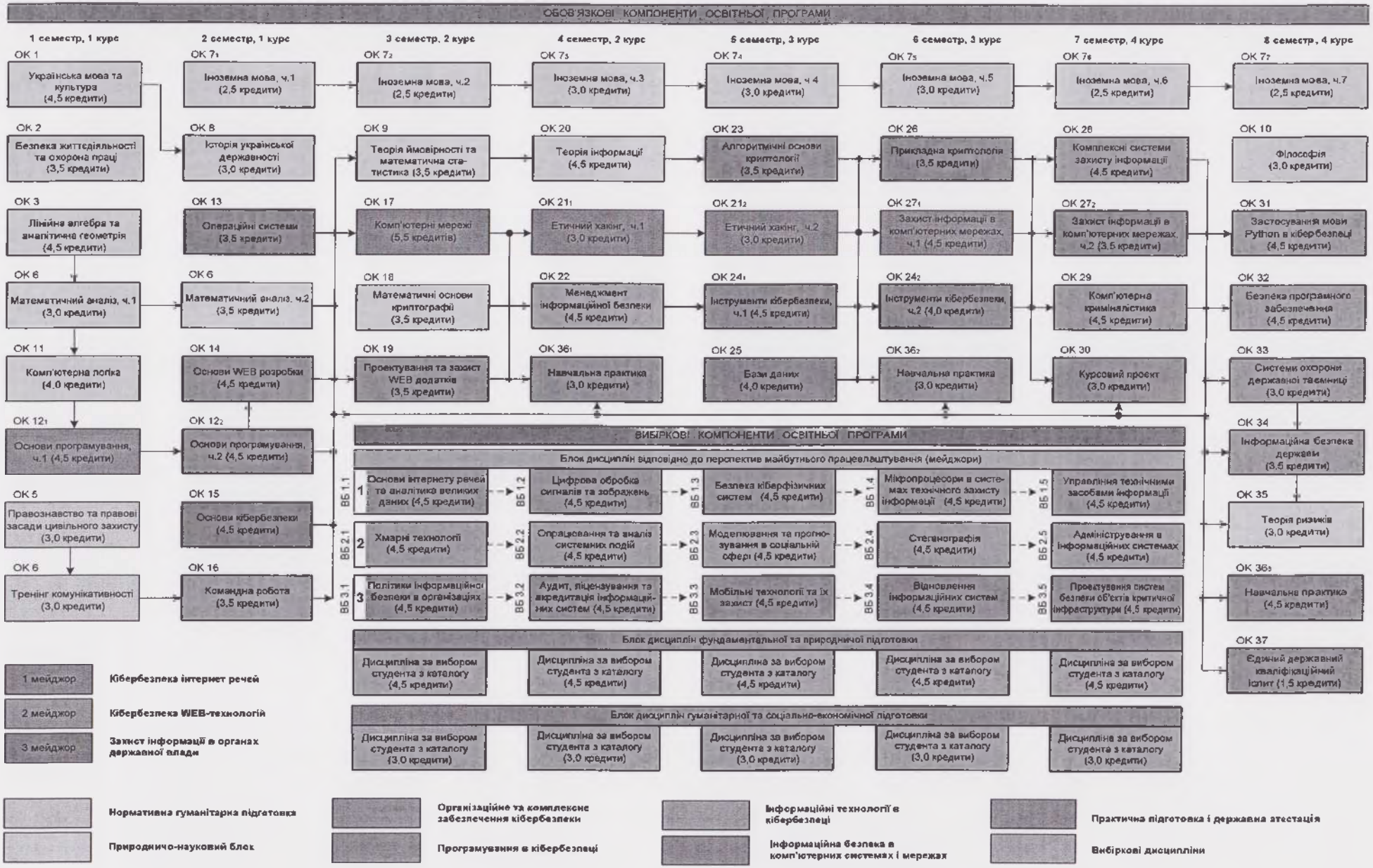
2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1. Перелік компонент освітньо-професійної програми

Код	Компоненти освітньої програми	Кількість кредитів	Форма підсумкового контролю
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ			
1.1. Цикл загальної підготовки			
ОК 1	Українська мова та культура	4,5	диф. залік
ОК 2	Безпека життєдіяльності та охорона праці	3,5	диф. залік
ОК 3	Лінійна алгебра та аналітична геометрія	4,5	екзамен
ОК 4	Правознавство та правові засади цивільного захисту	3,0	диф. залік
ОК 5	Тренінг комунікативності	3,0	диф. залік
ОК 6	Математичний аналіз	6,5	екзамен
ОК 7	Історія української державності	3,0	диф. залік
ОК 8	Іноземна мова	19,0	диф. залік
ОК 9	Теорія ймовірності та математична статистика	3,5	екзамен
ОК 10	Математичні основи криптографії	3,5	екзамен
ОК 11	Філософія	3,0	екзамен
Разом за циклом		***57,0***	
1.2. Цикл профільної підготовки			
ОК 12	Комп'ютерна логіка	4,0	диф. залік
ОК 13	Основи програмування	9,0	екзамен
ОК 14	Операційні системи	3,5	екзамен
ОК 15	Основи WEB розробки	4,5	диф. залік
ОК 16	Основи кібербезпеки	4,5	екзамен
ОК 17	Командна робота	3,5	диф. залік
ОК 18	Комп'ютерні мережі	5,5	екзамен
ОК 19	Проектування та захист WEB додатків	3,5	екзамен
ОК 20	Теорія інформації	4,5	екзамен
ОК 21	Менеджмент інформаційної безпеки	4,5	екзамен
ОК 22	Етичний хакінг	6,0	екзамен
ОК 23	Алгоритмічні основи криптології	3,5	екзамен
ОК 24	Бази даних	4,0	екзамен
ОК 25	Інструменти кібербезпеки	8,5	екзамен
ОК 26	Прикладна криптологія	3,5	екзамен
ОК 27	Захист інформації в комп'ютерних мережах	8,0	екзамен
ОК 28	Комплексні системи захисту інформації	4,5	екзамен
ОК 29	Комп'ютерна криміналістика	4,5	екзамен
ОК 30	Курсовий проєкт	3,0	диф. захист
ОК 31	Застосування мови Python в кібербезпеці	4,5	екзамен
ОК 32	Безпека програмного забезпечення	4,5	диф. залік
ОК 33	Системи охорони державної таємниці	3,0	диф. залік
ОК 34	Інформаційна безпека держави	3,5	екзамен
ОК 35	Теорія ризиків	3,0	диф. залік
ОК 36	Навчальна практика	10,5	диф. залік
Разом за циклом		***121,5***	
1.3. Атестація			
ОК 37	Єдиний державний кваліфікаційний іспит	1,5	екзамен
Разом за циклом		***1,5***	
Загальний обсяг обов'язкових компонент: 180			

ВИБІРКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ			
Цикл освітніх компонент відповідно до перспектив майбутнього працевлаштування			
Мейджор №1 ***Кібербезпека інтернет речей***			
ВБ 1.1	Основи інтернету речей та аналітика великих даних	4,5	диф. залік
ВБ 1.2	Цифрова обробка сигналів та зображень	4,5	диф. залік
ВБ 1.3	Безпека кіберфізичних систем	4,5	диф. залік
ВБ 1.4	Мікропроцесори в системах технічного захисту інформації	4,5	диф. залік
ВБ 1.5	Управління технічними засобами інформації	4,5	диф. залік
Мейджор №2 ***Кібербезпека WEB-технологій***			
ВБ 2.1	Хмарні технології	4,5	диф. залік
ВБ 2.2	Опрацювання та аналіз системних подій	4,5	диф. залік
ВБ 2.3	Моделювання та прогнозування в соціальній сфері	4,5	диф. залік
ВБ 2.4	Стеганографія	4,5	диф. залік
ВБ 2.5	Адміністрування в інформаційних системах	4,5	диф. залік
Мейджор №3 ***Захист інформації в органах державної влади***			
ВБ 3.1	Політики інформаційної безпеки в організаціях	4,5	диф. залік
ВБ 3.2	Аудит, ліцензування та акредитація інформаційних систем	4,5	диф. залік
ВБ 3.3	Мобільні технології та їх захист	4,5	диф. залік
ВБ 3.4	Відновлення інформаційних систем	4,5	диф. залік
ВБ 3.5	Проектування систем безпеки об'єктів критичної інфраструктури	4,5	диф. залік
Разом за циклом		***22,5***	
Цикл освітніх компонент за вибором студентів з каталогу дисциплін			
Дисципліни фундаментальної та природничої підготовки			
ВК 1.1	Дисципліна за вибором студентів №1	4,5	диф. залік
ВК 1.2	Дисципліна за вибором студентів №2	4,5	диф. залік
ВК 1.3	Дисципліна за вибором студентів №3	4,5	диф. залік
ВК 1.4	Дисципліна за вибором студентів №4	4,5	диф. залік
ВК 1.5	Дисципліна за вибором студентів №5	4,5	диф. залік
Разом за циклом		***22,5***	
Дисципліни гуманітарної та соціально-економічної підготовки			
ВК 2.1	Дисципліна за вибором студентів №1	3,0	диф. залік
ВК 2.2	Дисципліна за вибором студентів №2	3,0	диф. залік
ВК 2.3	Дисципліна за вибором студентів №3	3,0	диф. залік
ВК 2.4	Дисципліна за вибором студентів №4	3,0	диф. залік
ВК 2.5	Дисципліна за вибором студентів №5	3,0	диф. залік
Разом за циклом		***15,0***	
Загальний обсяг вибіркових компонент: 60			
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ: 240			

2.2. Структурно-логічна схема



3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників освітньо-професійної програми спеціальності 125 Кібербезпека та захист інформації здійснюється у формі єдиного державного кваліфікаційного іспиту та завершується видачею документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації: Бакалавр з кібербезпеки та управління інформаційною безпекою.

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання.

4.1. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ (НОРМАТИВНА ЧАСТИНА)

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	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35	ОК 36	ОК 37
ЗК 1															•		•													•						•	
ЗК 2																•					•				•		•		•	•		•				•	•
ЗК 3	•				•			•														•										•					
ЗК 4			•			•		•	•				•	•			•	•				•	•	•							•					•	
ЗК 5			•			•			•	•		•	•							•			•	•	•					•							•
ЗК 6	•			•			•				•																							•			
ЗК 7	•	•			•		•				•																										
ЗК 8	•						•				•																										
ЗК 9		•								•						•			•							•						•					
ЗК 10		•		•																													•				
ФК 1				•																									•	•				•		•	•
ФК 2												•	•	•		•				•				•				•	•		•					•	•
ФК 3												•		•	•		•			•		•	•			•	•										•
ФК 4																		•	•		•				•		•										•
ФК 5										•								•	•		•					•	•			•			•		•		•
ФК 6																		•			•				•		•										
ФК 7																					•						•	•		•					•	•	
ФК 8																					•								•				•	•	•		•
ФК 9																					•				•			•		•	•			•			•
ФК 10										•													•			•							•		•		•
ФК 11														•								•					•					•					•
ФК 12																			•			•			•			•		•	•	•				•	•

4.2. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ (ВИБІРКОВА ЧАСТИНА)

Програмні компетентності	Перелік вибіркових компонент освітньої програми														
	Мейджор №1					Мейджор №2					Мейджор №3				
	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ВБ 1.5	ВБ 2.1	ВБ 2.2	ВБ 2.3	ВБ 2.4	ВБ 2.5	ВБ 3.1	ВБ 3.2	ВБ 3.3	ВБ 3.4	ВБ 3.5
ЗК 1								•					•		
ЗК 2	•														
ЗК 3				•											
ЗК 4															
ЗК 5	•	•					•	•							
ЗК 6															
ЗК 7															
ЗК 8															
ЗК 9						•			•		•				•
ЗК 10															
ФК 1					•					•	•	•			•
ФК 2		•	•			•		•					•	•	
ФК 3		•	•										•		•
ФК 4					•		•	•		•	•			•	
ФК 5		•		•		•	•		•				•		•
ФК 6					•					•				•	
ФК 7			•								•			•	•
ФК 8	•				•		•			•	•	•			
ФК 9					•		•			•		•		•	•
ФК 10		•	•	•					•						•
ФК 11					•					•		•			
ФК 12		•			•	•	•		•	•		•			•

5.1. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ (НОРМАТИВНА ЧАСТИНА)

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	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35	ОК 36	ОК 37
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													•			•				•	•								•										•	

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	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35	ОК 36	ОК 37
РН 20															•							•					•					•					•
РН 21																		•	•			•									•						•
РН 22										•						•							•			•					•						•
РН 23																		•							•	•	•										•
РН 24																		•			•															•	•
РН 25														•											•												•
РН 26														•				•							•												•
РН 27																	•	•									•										•
РН 28																	•		•		•												•				•
РН 29																			•														•		•		•
РН 30																									•			•									•
РН 31																							•		•											•	•
РН 32																											•			•						•	
РН 33																					•									•					•		•
РН 34																•					•									•							
РН 35																					•						•	•									
РН 36																		•							•		•									•	
РН 37																												•		•						•	
РН 38																												•		•							•
РН 39																												•					•				•
РН 40																					•							•		•							•
РН 41																					•									•							•
РН 42																•													•						•		•
РН 43																					•								•							•	•

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	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35	ОК 36	ОК 37
РН 44																					•													•	•		
РН 45																					•										•					•	•
РН 46																					•						•								•		•
РН 47										•													•			•											•
РН 48										•													•			•				•							•
РН 49																				•					•											•	
РН 50																						•			•		•										
РН 51																						•								•							•
РН 52														•							•				•											•	•
РН 53																			•			•									•	•					•
РН 54				•			•				•																									•	
РН 55		•		•																																	
РН 56																												•		•							
РН 57		•		•																																	

5.2. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ (ВИБІРКОВА ЧАСТИНА)

Програмні компетентності	Перелік вибіркових компонент освітньої програми														
	Мейджор №1					Мейджор №2					Мейджор №3				
	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ВБ 1.5	ВБ 2.1	ВБ 2.2	ВБ 2.3	ВБ 2.4	ВБ 2.5	ВБ 3.1	ВБ 3.2	ВБ 3.3	ВБ 3.4	ВБ 3.5
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					•										•
РН 25															
РН 26															
РН 27	•	•													
РН 28											•				
РН 29							•								
РН 30						•							•		•
РН 31															
РН 32											•			•	

Програмні компетентності	Перелік вибіркових компонент освітньої програми														
	Мейджор №1					Мейджор №2					Мейджор №3				
	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ВБ 1.5	ВБ 2.1	ВБ 2.2	ВБ 2.3	ВБ 2.4	ВБ 2.5	ВБ 3.1	ВБ 3.2	ВБ 3.3	ВБ 3.4	ВБ 3.5
РН 33					•					•					
РН 34								•			•				
РН 35											•				
РН 36		•													
РН 37		•													
РН 38		•													
РН 39												•			
РН 40															
РН 41												•			
РН 42															
РН 43										•		•			
РН 44										•		•			
РН 45											•				
РН 46														•	
РН 47									•						
РН 48									•						
РН 49															•
РН 50						•									
РН 51			•			•							•		
РН 52															
РН 53															
РН 54															
РН 55															
РН 56											•	•	•	•	•
РН 57															

РОЗПОДІЛ КОМПЕТЕНЦІЙ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ

Шифр	Компетенції	Найменування освітніх компонентів
ЗК 1	Здатність застосовувати знання у практичних ситуаціях.	ОК 15 Основи WEB розробки; ОК 17 Командна робота; ОК 30 Курсовий проект; ОК 36 Навчальна практика; *ВБ 2.3 Моделювання та прогнозування в соціальній сфері;* *ВБ 3.3 Мобільні технології та їх захист.*
ЗК 2	Знання та розуміння предметної області та розуміння професії.	ОК 16 Основи кібербезпеки; ОК 21 Менеджмент інформаційної безпеки; ОК 25 Інструменти кібербезпеки; ОК 27 Захист інформації в комп'ютерних мережах; ОК 29 Комп'ютерна криміналістика; ОК 30 Курсовий проект; ОК 32 Безпека програмного забезпечення; ОК 36 Навчальна практика; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.1 Основи інтернету речей та аналітика великих даних.*
ЗК 3	Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.	ОК 1 Українська мова та культура; ОК 5 Тренінг комунікативності; ОК 8 Іноземна мова; ОК 22 Етичний хакінг; ОК 32 Безпека програмного забезпечення; *ВБ 1.4 Мікропроцесори в системах технічного захисту інформації.*
ЗК 4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.	ОК 3 Лінійна алгебра та аналітична геометрія; ОК 6 Математичний аналіз; ОК 8 Іноземна мова; ОК 9 Теорія ймовірності та математична статистика; ОК 13 Основи програмування; ОК 14 Операційні системи; ОК 17 Командна робота; ОК 18 Комп'ютерні мережі; ОК 22 Етичний хакінг; ОК 23 Алгоритмічні основи криптології; ОК 24 Бази даних; ОК 31 Застосування мови Python в кібербезпеці; ОК 36 Навчальна практика.
ЗК 5	Здатність до пошуку, оброблення та аналізу інформації.	ОК 3 Лінійна алгебра та аналітична геометрія; ОК 6 Математичний аналіз; ОК 9 Теорія ймовірності та математична статистика; ОК 12 Комп'ютерна логіка; ОК 13 Основи програмування; ОК 20 Теорія інформації; ОК 23 Алгоритмічні основи криптології; ОК 25 Інструменти кібербезпеки;

Шифр	Компетенції	Найменування освітніх компонентів
		ОК 24 Бази даних; ОК 30 Курсовий проект; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.1 Основи інтернету речей та аналітика великих даних;* *ВБ 1.2 Цифрова обробка сигналів та зображень;* *ВБ 2.2 Опрацювання та аналіз системних подій;* *ВБ 2.3 Моделювання та прогнозування в соціальній сфері.*
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.	ОК 1 Українська мова та культура; ОК 4 Правознавство та правові основи цивільного захисту; ОК 7 Історія української державності; ОК 11 Філософія; ОК 16 Основи кібербезпеки; ОК 34 Інформаційна безпека держави.
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.	ОК 1 Українська мова та культура; ОК 5 Тренінг комунікативності; ОК 7 Історія української державності; ОК 11 Філософія.
ЗК 8	Формування ідентичності та почуття особистої гідності в результаті осмислення соціального та морального досвіду минулих поколінь, розуміння історії і культури України в контексті історичного процесу.	ОК 1 Українська мова та культура; ОК 7 Історія української державності; ОК 11 Філософія.
ЗК 9	Формування навиків здійснення безпечної діяльності.	ОК 2 Безпека життєдіяльності та охорона праці; ОК 16 Основи кібербезпеки; ОК 19 Проектування та захист WEB додатків; ОК 26 Прикладна криптологія; ОК 32 Безпека програмного забезпечення; *ВБ 2.1 Хмарні технології;*

Шифр	Компетенції	Найменування освітніх компонентів
		ВБ 2.4 Стеганографія; *ВБ 3.1 Політики інформаційної безпеки в організаціях;* *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*
ЗК 10	Усвідомлення функцій держави, форм реалізації цих функцій, правових основ цивільного захисту, дотримання основних принципів здійснення цивільного захисту.	ОК 2 Безпека життєдіяльності та охорона праці; ОК 4 Правознавство та правові основи цивільного захисту; ОК 33 Системи охорони державної таємниці.
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 кібербезпеки.	ОК 4 Правознавство та правові основи цивільного захисту; ОК 29 Комп'ютерна криміналістика; ОК 30 Курсовий проект; ОК 34 Інформаційна безпека держави; ОК 36 Навчальна практика; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.5 Управління технічними засобами інформації;* *ВБ 2.5 Адміністрування в інформаційних системах;* *ВБ 3.1 Політики інформаційної безпеки в організаціях;* *ВБ 3.2 Аудит, ліцензування та акредитація інформацій-них систем;* *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*
ФК 2	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та кібербезпеки.	ОК 12 Комп'ютерна логіка; ОК 13 Основи програмування; ОК 14 Операційні системи; ОК 16 Основи кібербезпеки; ОК 20 Теорія інформації; ОК 24 Бази даних; ОК 28 Комплексні системи захисту інформації; ОК 29 Комп'ютерна криміналістика; ОК 31 Застосування мови Python в кібербезпеці; ОК 36 Навчальна практика; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.2 Цифрова обробка сигналів та зображень;* *ВБ 1.3 Безпека кіберфізичних систем;* *ВБ 2.1 Хмарні технології;* *ВБ 2.3 Моделювання та прогнозування в соціальній сфері;* *ВБ 3.3 Мобільні технології та їх захист;* *ВБ 3.4 Відновлення інформаційних систем.*
ФК 3	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.	ОК 12 Комп'ютерна логіка; ОК 14 Операційні системи; ОК 15 Основи WEB розробки; ОК 17 Командна робота; ОК 20 Теорія інформації; ОК 22 Етичний хакінг; ОК 23 Алгоритмічні основи криптології;

Шифр	Компетенції	Найменування освітніх компонентів
		ОК 26 Прикладна криптологія; ОК 27 Захист інформації в комп'ютерних мережах; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.2 Цифрова обробка сигналів та зображень;* *ВБ 1.3 Безпека кіберфізичних систем;* *ВБ 3.3 Мобільні технології та їх захист;* *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*
ФК 4	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та кібербезпеки.	ОК 18 Комп'ютерні мережі; ОК 19 Проектування та захист WEB додатків; ОК 21 Менеджмент інформаційної безпеки; ОК 25 Інструменти кібербезпеки; ОК 27 Захист інформації в комп'ютерних мережах; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.5 Управління технічними засобами інформації;* *ВБ 2.2 Опрацювання та аналіз системних подій;* *ВБ 2.3 Моделювання та прогнозування в соціальній сфері;* *ВБ 2.5 Адміністрування в інформаційних системах;* *ВБ 3.1 Політики інформаційної безпеки в організаціях;* *ВБ 3.4 Відновлення інформаційних систем.*
ФК 5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та кібербезпеки.	ОК 18 Комп'ютерні мережі; ОК 19 Проектування та захист WEB додатків; ОК 21 Менеджмент інформаційної безпеки; ОК 26 Прикладна криптологія; ОК 27 Захист інформації в комп'ютерних мережах; ОК 30 Курсовий проект; ОК 33 Системи охорони державної таємниці; ОК 35 Теорія ризиків; *ВБ 1.2 Цифрова обробка сигналів та зображень;* *ВБ 1.4 Мікропроцесори в системах технічного захисту інформації;* *ВБ 2.1 Хмарні технології;* *ВБ 2.2 Опрацювання та аналіз системних подій;* *ВБ 2.4 Стеганографія;* *ВБ 3.3 Мобільні технології та їх захист;* *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*
ФК 6	Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	ОК 18 Комп'ютерні мережі; ОК 21 Менеджмент інформаційної безпеки; ОК 25 Інструменти кібербезпеки; ОК 27 Захист інформації в комп'ютерних мережах; *ВБ 1.5 Управління технічними засобами інформації;* *ВБ 2.5 Адміністрування в інформаційних системах;* *ВБ 3.4 Відновлення інформаційних систем.*

Шифр	Компетенції	Найменування освітніх компонентів
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.).	ОК 21 Менеджмент інформаційної безпеки; ОК 27 Захист інформації в комп'ютерних мережах; ОК 28 Комплексні системи захисту інформації; ОК 30 Курсовий проект; ОК 35 Теорія ризиків; ОК 36 Навчальна практика; *ВБ 1.3 Безпека кіберфізичних систем;* *ВБ 3.1 Політики інформаційної безпеки в організаціях;* *ВБ 3.4 Відновлення інформаційних систем;* *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*
ФК 8	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	ОК 21 Менеджмент інформаційної безпеки; ОК 29 Комп'ютерна криміналістика; ОК 33 Системи охорони державної таємниці; ОК 34 Інформаційна безпека держави; ОК 35 Теорія ризиків; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.1 Основи інтернету речей та аналітика великих даних;* *ВБ 1.5 Управління технічними засобами інформації;* *ВБ 2.2 Опрацювання та аналіз системних подій;* *ВБ 2.5 Адміністрування в інформаційних системах;* *ВБ 3.1 Політики інформаційної безпеки в організаціях;* *ВБ 3.2 Аудит, ліцензування та акредитація інформаційних систем.*
ФК 9	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.	ОК 21 Менеджмент інформаційної безпеки; ОК 25 Інструменти кібербезпеки; ОК 28 Комплексні системи захисту інформації; ОК 30 Курсовий проект; ОК 31 Застосування мови Python в кібербезпеці; ОК 34 Інформаційна безпека держави; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.5 Управління технічними засобами інформації;* *ВБ 2.2 Опрацювання та аналіз системних подій;* *ВБ 2.5 Адміністрування в інформаційних системах;* *ВБ 3.2 Аудит, ліцензування та акредитація інформаційних систем;* *ВБ 3.4 Відновлення інформаційних систем;* *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*
ФК 10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	ОК 23 Алгоритмічні основи криптології; ОК 26 Прикладна криптологія; ОК 33 Системи охорони державної таємниці; ОК 35 Теорія ризиків; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.2 Цифрова обробка сигналів та зображень;* *ВБ 1.3 Безпека кіберфізичних Систем;* *ВБ 1.4 Мікропроцесори в системах технічного захисту інформації;*

Шифр	Компетенції	Найменування освітніх компонентів
		ВБ 2.4 Стеганографія; *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*
ФК 11	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та кібербезпеки.	ОК 14 Операційні системи; ОК 22 Етичний хакінг; ОК 27 Захист інформації в комп'ютерних мережах; ОК 32 Безпека програмного забезпечення; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.5 Управління технічними засобами інформації;* *ВБ 2.5 Адміністрування в інформаційних системах;* *ВБ 3.2 Аудит, ліцензування та акредитація інформаційних систем.*
ФК 12	Здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та кібербезпеки.	ОК 19 Проектування та захист WEB додатків; ОК 22 Етичний хакінг; ОК 25 Інструменти кібербезпеки; ОК 28 Комплексні системи захисту інформації; ОК 30 Курсовий проект; ОК 31 Застосування мови Python в кібербезпеці; ОК 32 Безпека програмного забезпечення; ОК 36 Навчальна практика; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.2 Цифрова обробка сигналів та зображень;* *ВБ 1.5 Управління технічними засобами інформації;* *ВБ 2.1 Хмарні технології;* *ВБ 2.2 Опрацювання та аналіз системних подій;* *ВБ 2.4 Стеганографія;* *ВБ 2.5 Адміністрування в інформаційних системах;* *ВБ 3.2 Аудит, ліцензування та акредитація інформаційних систем;* *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*

РОЗПОДІЛ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ

Шифр	Результати навчання	Найменування освітніх компонентів
РН 1	Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.	ОК 1 Українська мова та культура; ОК 5 Тренінг комунікативності; ОК 8 Іноземна мова; ОК 17 Командна робота.
РН 2	Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.	ОК 3 Лінійна алгебра та аналітична геометрія; ОК 6 Математичний аналіз; ОК 9 Теорія ймовірності та математична статистика; ОК 12 Комп'ютерна логіка.

Шифр	Результати навчання	Найменування освітніх компонентів
РН 3	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.	ОК 6 Математичний аналіз; ОК 9 Теорія ймовірності та математична статистика; ОК 11 Філософія; ОК 12 Комп'ютерна логіка; ОК 27 Захист інформації в комп'ютерних мережах; ОК 34 Інформаційна безпека держави; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 2.2 Опрацювання та аналіз системних подій;* *ВБ 3.4 Відновлення інформаційних систем.*
РН 4	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.	ОК 3 Лінійна алгебра та аналітична геометрія; ОК 6 Математичний аналіз; ОК 9 Теорія ймовірності та математична статистика; ОК 17 Командна робота; ОК 29 Комп'ютерна криміналістика; ОК 33 Системи охорони державної таємниці; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 2.3 Моделювання та прогнозування в соціальній сфері;* *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*
РН 5	Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.	ОК 5 Тренінг комунікативності; ОК 8 Іноземна мова; ОК 13 Основи програмування; ОК 15 Основи WEB розробки; ОК 24 Бази даних; ОК 32 Безпека програмного забезпечення; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.1 Основи інтернету речей та аналітика великих даних;* *ВБ 2.3 Моделювання та прогнозування в соціальній сфері;* *ВБ 3.3 Мобільні технології та їх захист.*
РН 6	Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.	ОК 9 Теорія ймовірності та математична статистика; ОК 11 Філософія; ОК 13 Основи програмування; ОК 20 Теорія інформації; ОК 37 Єдиний державний кваліфікаційний іспит.
РН 7	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та кібербезпеки.	ОК 18 Правознавство та правові засади цивільного захисту; ОК 19 Проектування та захист WEB додатків; ОК 29 Комп'ютерна криміналістика; ОК 30 Курсовий проект; ОК 34 Інформаційна безпека держави; ОК 36 Навчальна практика;

Шифр	Результати навчання	Найменування освітніх компонентів
		ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.5 Управління технічними засобами інформації;* *ВБ 2.5 Адміністрування в інформаційних системах;* *ВБ 3.2 Аудит, ліцензування та акредитація інформаційних систем;* *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*
РН 8	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та кібербезпеки.	ОК 30 Курсовий проект; ОК 34 Інформаційна безпека держави; ОК 36 Навчальна практика.
РН 9	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки.	ОК 16 Основи кібербезпеки; ОК 29 Комп'ютерна криміналістика; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.5 Управління технічними засобами інформації;* *ВБ 2.5 Адміністрування в інформаційних системах;* *ВБ 3.2 Аудит, ліцензування та акредитація інформаційних систем.*
РН 10	Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.	ОК 18 Комп'ютерні мережі; ОК 20 Теорія інформації; ОК 24 Бази даних; ОК 37 Єдиний державний кваліфікаційний іспит.
РН 11	Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.	ОК 24 Бази даних; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.1 Основи інтернету речей та аналітика великих даних;* *ВБ 1.3 Безпека кіберфізичних систем;* *ВБ 2.1 Хмарні технології.*
РН 12	Розробляти моделі загроз та порушника.	ОК 28 Комплексні системи захисту інформації; ОК 35 Теорія ризиків; ОК 36 Навчальна практика.
РН 13	Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.	ОК 12 Комп'ютерна логіка; ОК 18 Комп'ютерні мережі; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*
РН 14	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.	ОК 20 Теорія інформації; ОК 32 Безпека програмного забезпечення; ОК 36 Навчальна практика; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.4 Мікропроцесори в системах технічного захисту інформації.*

Шифр	Результати навчання	Найменування освітніх компонентів
РН 15	Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	ОК 14 Операційні системи; ОК 18 Комп'ютерні мережі; ОК 32 Безпека програмного забезпечення; ОК 36 Навчальна практика; *ВБ 2.3 Моделювання та прогнозування в соціальній сфері;* *ВБ 3.3 Мобільні технології та їх захист.*
РН 16	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.	ОК 17 Командна робота; ОК 28 Комплексні системи захисту інформації; ОК 33 Системи охорони державної таємниці; *ВБ 3.4 Відновлення інформаційних систем;* *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*
РН 17	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.	ОК 15 Основи WEB розробки; ОК 18 Комп'ютерні мережі; ОК 27 Захист інформації в комп'ютерних мережах; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.3 Безпека кіберфізичних систем;* *ВБ 3.1 Політики інформаційної безпеки в організаціях.*
РН 18	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.	ОК 12 Комп'ютерна логіка; ОК 14 Операційні системи; ОК 26 Прикладна криптологія; ОК 27 Захист інформації в комп'ютерних мережах.
РН 19	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.	ОК 13 Основи програмування; ОК 16 Основи кібербезпеки; ОК 20 Теорія інформації; ОК 23 Алгоритмічні основи криптології; ОК 29 Комп'ютерна криміналістика; ОК 21 Менеджмент інформаційної безпеки; ОК 29 Комп'ютерна криміналістика; ОК 37 Єдиний державний кваліфікаційний іспит.
РН 20	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.	ОК 15 Основи WEB розробки; ОК 22 Етичний хакінг; ОК 27 Захист інформації в комп'ютерних мережах; ОК 32 Безпека програмного забезпечення; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.3 Безпека кіберфізичних систем.*

Шифр	Результати навчання	Найменування освітніх компонентів
РН 21	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.	ОК 18 Комп'ютерні мережі; ОК 19 Проектування та захист WEB додатків; ОК 22 Етичний хакінг; ОК 31 Застосування мови Python в кібербезпеці; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.1 Основи інтернету речей та аналітика великих даних;* *ВБ 3.3 Мобільні технології та їх захист.*
РН 22	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і кібербезпеки.	ОК 16 Основи кібербезпеки; ОК 23 Алгоритмічні основи криптології; ОК 26 Прикладна криптологія; ОК 31 Застосування мови Python в кібербезпеці; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 2.1 Хмарні технології;* *ВБ 3.3 Мобільні технології та їх захист.*
РН 23	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.	ОК 18 Комп'ютерні мережі; ОК 25 Інструменти кібербезпеки; ОК 26 Прикладна криптологія; ОК 27 Захист інформації в комп'ютерних мережах; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.3 Безпека кіберфізичних систем;* *ВБ 2.1 Хмарні технології;* *ВБ 3.3 Мобільні технології та їх захист.*
РН 24	Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).	ОК 18 Комп'ютерні мережі; ОК 21 Менеджмент інформаційної безпеки; ОК 36 Навчальна практика; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.5 Управління технічними засобами інформації;* *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*
РН 25	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.	ОК 14 Операційні системи; ОК 25 Інструменти кібербезпеки; ОК 37 Єдиний державний кваліфікаційний іспит.

Шифр	Результати навчання	Найменування освітніх компонентів
РН 26	Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.	ОК 14 Операційні системи; ОК 18 Комп'ютерні мережі; ОК 25 Інструменти кібербезпеки; ОК 37 Єдиний державний кваліфікаційний іспит.
РН 27	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.	ОК 17 Командна робота; ОК 18 Комп'ютерні мережі; ОК 27 Захист інформації в комп'ютерних мережах; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.1 Основи інтернету речей та аналітика великих даних;* *ВБ 1.2 Цифрова обробка сигналів та зображень.*
РН 28	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 кібербезпеки.	ОК 17 Командна робота; ОК 19 Проектування та захист WEB додатків; ОК 21 Менеджмент інформаційної безпеки; ОК 33 Системи охорони державної таємниці; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 3.1 Політики інформаційної безпеки в організаціях.*
РН 29	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.	ОК 19 Проектування та захист WEB додатків; ОК 33 Системи охорони державної таємниці; ОК 35 Теорія ризиків; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 2.2 Опрацювання та аналіз системних подій.*
РН 30	Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.	ОК 25 Інструменти кібербезпеки; ОК 28 Комплексні системи захисту інформації; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 2.1 Хмарні технології;* *ВБ 3.3 Мобільні технології та їх захист;* *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*
РН 31	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.	ОК 23 Алгоритмічні основи криптології; ОК 25 Інструменти кібербезпеки; ОК 36 Навчальна практика; ОК 37 Єдиний державний кваліфікаційний іспит.
РН 32	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.	ОК 27 Захист інформації в комп'ютерних мережах; ОК 30 Курсовий проект; ОК 36 Навчальна практика; *ВБ 3.1 Політики інформаційної безпеки в організаціях;* *ВБ 3.4 Відновлення інформаційних систем.*

Шифр	Результати навчання	Найменування освітніх компонентів
РН 33	Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.	ОК 21 Менеджмент інформаційної безпеки; ОК 30 Курсовий проект; ОК 35 Теорія ризиків; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.5 Управління технічними засобами інформації;* *ВБ 2.5 Адміністрування в інформаційних системах.*
РН 34	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та кібербезпеки відповідно до цілей і завдань організації.	ОК 16 Основи кібербезпеки; ОК 21 Менеджмент інформаційної безпеки; ОК 30 Курсовий проект; *ВБ 2.3 Моделювання та прогнозування в соціальній сфері;* *ВБ 3.1 Політики інформаційної безпеки в організаціях.*
РН 35	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 кібербезпеки.	ОК 21 Менеджмент інформаційної безпеки; ОК 27 Захист інформації в комп'ютерних мережах; ОК 28 Комплексні системи захисту інформації; *ВБ 3.1 Політики інформаційної безпеки в організаціях.*
РН 36	Виявляти небезпечні сигнали технічних засобів.	ОК 17 Комп'ютерні мережі; ОК 25 Інструменти кібербезпеки; ОК 27 Захист інформації в комп'ютерних мережах; ОК 36 Навчальна практика; *ВБ 1.2 Цифрова обробка сигналів та зображень.*
РН 37	Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.	ОК 28 Комплексні системи захисту інформації; ОК 30 Курсовий проект; ОК 36 Навчальна практика; *ВБ 1.2 Цифрова обробка сигналів та зображень.*
РН 38	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.	ОК 28 Комплексні системи захисту інформації; ОК 30 Курсовий проект; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.2 Цифрова обробка сигналів та зображень.*

Шифр	Результати навчання	Найменування освітніх компонентів
РН 39	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.	ОК 28 Комплексні системи захисту інформації; ОК 33 Системи охорони державної таємниці; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 3.2 Аудит, ліцензування та акредитація інформаційних систем.*
РН 40	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.	ОК 21 Менеджмент інформаційної безпеки; ОК 28 Комплексні системи захисту інформації; ОК 30 Курсовий проект; ОК 37 Єдиний державний кваліфікаційний іспит.
РН 41	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.	ОК 21 Менеджмент інформаційної безпеки; ОК 30 Курсовий проект; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 3.2 Аудит, ліцензування та акредитація інформаційних систем.*
РН 42	Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і кібербезпеки.	ОК 16 Основи кібербезпеки; ОК 29 Комп'ютерна криміналістика; ОК 35 Теорія ризиків; ОК 37 Єдиний державний кваліфікаційний іспит.
РН 43	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та кібербезпеки для розслідування інцидентів.	ОК 18 Правознавство та правові засади цивільного захисту; ОК 21 Менеджмент інформаційної безпеки; ОК 29 Комп'ютерна криміналістика; ОК 36 Навчальна практика; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 2.5 Адміністрування в інформаційних системах;* *ВБ 3.2 Аудит, ліцензування та акредитація інформаційних систем.*
РН 44	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.	ОК 21 Менеджмент інформаційної безпеки; ОК 34 Інформаційна безпека держави; ОК 35 Теорія ризиків; *ВБ 2.5 Адміністрування в інформаційних системах;* *ВБ 3.2 Аудит, ліцензування та акредитація інформаційних систем.*
РН 45	Застосовувати різні класи політик інформаційної безпеки та кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.	ОК 21 Менеджмент інформаційної безпеки; ОК 31 Застосування мови Python в кібербезпеці; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 3.1 Політики інформаційної безпеки в організаціях.*

Шифр	Результати навчання	Найменування освітніх компонентів
РН 46	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.	ОК 21 Менеджмент інформаційної безпеки; ОК 27 Захист інформації в комп'ютерних мережах; ОК 35 Теорія ризиків; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 3.4 Відновлення інформаційних систем.*
РН 47	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.	ОК 23 Алгоритмічні основи криптології; ОК 26 Прикладна криптологія; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 2.4 Стеганографія.*
РН 48	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.	ОК 23 Алгоритмічні основи криптології; ОК 26 Прикладна криптологія; ОК 30 Курсовий проект; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 2.4 Стеганографія.*
РН 49	Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.	ОК 20 Теорія інформації; ОК 25 Інструменти кібербезпеки; ОК 36 Навчальна практика; *ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.*
РН 50	Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).	ОК 22 Етичний хакінг; ОК 25 Інструменти кібербезпеки; ОК 27 Захист інформації в комп'ютерних мережах; *ВБ 2.1 Хмарні технології.*
РН 51	Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.	ОК 22 Етичний хакінг; ОК 30 Курсовий проект; ОК 37 Єдиний державний кваліфікаційний іспит; *ВБ 1.3 Безпека кіберфізичних систем;* *ВБ 2.1 Хмарні технології;* *ВБ 3.3 Мобільні технології та їх захист.*
РН 52	Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.	ОК 14 Операційні системи; ОК 21 Менеджмент інформаційної безпеки; ОК 25 Інструменти кібербезпеки; ОК 36 Навчальна практика; ОК 37 Єдиний державний кваліфікаційний іспит.

Шифр	Результати навчання	Найменування освітніх компонентів
РН 53	Вирішувати задачі аналізу програмного коду на наявність можливих загроз.	ОК 19 Проектування та захист WEB додатків; ОК 22 Етичний хакінг; ОК 31 Застосування мови Python в кібербезпеці; ОК 32 Безпека програмного забезпечення; ОК 37 Єдиний державний кваліфікаційний іспит.
РН 54	Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	ОК 1 Українська мова та культура; ОК 7 Історія української державності; ОК 11 Філософія; ОК 18 Правознавство та правові засади цивільного захисту; ОК 36 Навчальна практика.
РН 55	Демонструвати навички аналізу категорій цивільної безпеки, оцінювати стан та використовувати сучасні безпекові механізми для захисту інтересів людини, а також демонструвати готовність до зміцнення особистого здоров'я шляхом використання рухової активності.	ОК 2 Безпека життєдіяльності та охорона праці; ОК 18 Правознавство та правові засади цивільного захисту.
РН 56	Володіти технологіями кібербезпеки та захисту інформації у системі цивільного захисту.	ВБ 3.1 Політики інформаційної безпеки в організаціях; ВБ 3.2 Аудит, ліцензування та акредитація інформаційних систем; ВБ 3.3 Мобільні технології та їх захист; ВБ 3.4 Відновлення інформаційних систем; ВБ 3.5 Проектування систем безпеки об'єктів критичної інфраструктури.
РН 57	Застосовувати отримані знання основ цивільного захисту в практичній діяльності.	ОК 18 Правознавство та правові засади цивільного захисту.

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	Українська мова та культура	ЗК3, ЗК6, ЗК7, ЗК8	РН1
ОК 2	Безпека життєдіяльності та охорона праці	ЗК9, ЗК10	РН55, РН57
ОК 3	Лінійна алгебра та аналітична геометрія	ЗК4, ЗК5	РН2, РН4
ОК 4	Правознавство та правові засади цивільного захисту	ЗК6, ЗК10, ФК1	РН7, РН54, РН55, РН57
ОК 5	Тренінг комунікативності	ЗК3, ЗК7	РН1, РН5
ОК 6	Математичний аналіз	ЗК4, ЗК5	РН2, РН3, РН4
ОК 7	Історія Української державності	ЗК6, ЗК7, ЗК8	РН54
ОК 8	Іноземна мова	ЗК3, ЗК4	РН1, РН5
ОК 9	Теорія ймовірності та математична статистика	ЗК4, ЗК5	РН2, РН3, РН4, РН6
ОК 10	Математичні основи криптографії	ЗК5, ЗК9, ФК5, ФК10	РН18, РН22, РН47, РН48
ОК 11	Філософія	ЗК6, ЗК7, ЗК8	РН3, РН6, РН54
1.2. Цикл профільної підготовки			
ОК 12	Комп'ютерна логіка	ЗК5, ФК2, ФК3	РН2, РН3, РН13, РН18
ОК 13	Основи програмування	ЗК4, ЗК5, ФК2	РН5, РН6, РН19
ОК 14	Операційні системи	ЗК4, ФК2, ФК3, ФК11	РН15, РН18, РН25, РН26, РН52
ОК 15	Основи WEB розробки	ЗК1, ФК3	РН5, РН17, РН20
ОК 16	Основи кібербезпеки	ЗК2, ЗК9, ФК2	РН9, РН19, РН22, РН34, РН42
ОК 17	Командна робота	ЗК1, ЗК4, ФК3	РН1, РН4, РН16, РН27, РН28
ОК 18	Комп'ютерні мережі	ЗК4, ФК4, ФК5, ФК6	РН10, РН13, РН15, РН17, РН21, РН23, РН24, РН26, РН27, РН36
ОК 19	Проектування та захист WEB додатків	ЗК9, ФК4, ФК5, ФК12	РН7, РН21, РН28, РН29, РН53
ОК 20	Теорія інформації	ЗК5, ФК2, ФК3	РН6, РН10, РН14, РН19, РН49
ОК 21	Менеджмент інформаційної безпеки	ЗК2, ФК4, ФК5, ФК6, ФК7, ФК8, ФК9	РН19, РН24, РН28, РН33, РН34, РН35, РН41, РН43, РН44, РН45, РН46, РН52
ОК 22	Етичний хакінг	ЗК3, ЗК4, ФК3, ФК11, ФК12	РН20, РН21, РН50, РН51, РН53
ОК 23	Алгоритмічні основи криптології	ЗК4, ЗК5, ФК3, ФК10	РН22, РН31, РН47, РН48
ОК 24	Бази даних	ЗК4, ЗК5, ФК2	РН5, РН10, РН11
ОК 25	Інструменти кібербезпеки	ЗК2, ЗК5, ФК4, ФК6, ФК9, ФК12	РН23, РН25, РН26, РН30, РН31, РН36, РН49, РН50, РН52
ОК 26	Прикладна криптологія	ЗК9, ФК3, ФК5, ФК10	РН18, РН22, РН23, РН47, РН48

ОК	Назва дисципліни	Компетенції	Програмні результати
ОК 27	Захист інформації в комп'ютерних мережах	ЗК2, ФК3, ФК4, ФК5, ФК6, ФК7, ФК11	РН3, РН17, РН18, РН20, РН23, РН27, РН32, РН35, РН36, РН46, РН50
ОК 28	Комплексні системи захисту інформації	ФК2, ФК7, ФК9, ФК12	РН12, РН16, РН30, РН35, РН37, РН38, РН40
ОК 29	Комп'ютерна криміналістика	ЗК2, ФК1, ФК2, ФК8	РН4, РН7, РН9, РН19, РН42, РН43
ОК 30	Курсовий проєкт	ЗК1, ЗК2, ЗК5, ФК1, ФК5, ФК7, ФК9, ФК12	РН7, РН8, РН32, РН33, РН34, РН37, РН38, РН40, РН41, РН48, РН51
ОК 31	Застосування мови Python в кібербезпеці	ЗК4, ФК2, ФК9, ФК12	РН21, РН22, РН45, РН53
ОК 32	Безпека програмного забезпечення	ЗК2, ЗК3, ЗК9, ФК11, ФК12	РН5, РН14, РН15, РН20, РН53
ОК 33	Системи охорони державної таємниці	ЗК10, ФК5, ФК8, ФК10	РН4, РН16, РН28, РН29, РН39
ОК 34	Інформаційна безпека держави	ЗК6, ФК1, ФК8, ФК9	РН3, РН7, РН8, РН44
ОК 35	Теорія ризиків	ФК5, ФК7, ФК8, ФК10	РН12, РН29, РН33, РН42, РН44, РН46
ОК 36	Навчальна практика	ЗК1, ЗК2, ЗК4, ФК1, ФК2, ФК7, ФК12.	РН7, РН8, РН12, РН14, РН15, РН24, РН31, РН32, РН36, РН37, РН43, РН45, РН49, РН52, РН54
1.3. Атестація			
ОК 37	Єдиний державний кваліфікаційний іспит	ЗК2, ЗК5, ФК1, ФК2, ФК3, ФК4, ФК5, ФК8, ФК9, ФК10, ФК11, ФК12	РН3, РН4, РН5, РН6, РН7, РН9, РН10, РН11, РН13, РН14, РН17, РН19, РН20, РН21, РН22, РН23, РН24, РН25, РН26, РН27, РН28, РН29, РН30, РН31, РН33, РН38, РН39, РН40, РН41, РН42, РН43, РН45, РН46, РН47, РН48, РН51, РН52, РН53
ВИБІРКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ			
Цикл освітніх компонент відповідно до перспектив майбутнього працевлаштування			
Мейджор №1 Кібербезпека інтернет речей			
ВБ 1.1	Основи інтернету речей та аналітика великих даних	ЗК2, ЗК5, ФК8	РН5, РН11, РН21, РН27
ВБ 1.2	Цифрова обробка сигналів та зображень	ЗК5, ФК2, ФК3, ФК5, ФК10, ФК12	РН27, РН36, РН37, РН38
ВБ 1.3	Безпека кіберфізичних систем	ФК2, ФК3, ФК7, ФК10	РН11, РН17, РН20, РН23, РН51
ВБ 1.4	Мікропроцесори в системах технічного захисту інформації	ЗК3, ФК5, ФК10	РН14
ВБ 1.5	Управління технічними засобами інформації	ФК1, ФК4, ФК6, ФК8, ФК9, ФК11, ФК12	РН7, РН9, РН24, РН33

ОК	Назва дисципліни	Компетенції	Програмні результати
Мейджор №2 Кібербезпека WEB-технологій			
ВБ 2.1	Хмарні технології	ЗК9, ФК2, ФК5, ФК12	РН11, РН22, РН23, РН30, РН50, РН51
ВБ 2.2	Опрацювання та аналіз системних подій	ЗК5, ФК4, ФК5, ФК8, ФК9, ФК12	РН3, РН29
ВБ 2.3	Моделювання та прогнозування в соціальній сфері	ЗК1, ЗК5, ФК2, ФК4	РН4, РН5, РН15, РН34
ВБ 2.4	Стеганографія	ЗК9, ФК5, ФК10	РН47, РН48
ВБ 2.5	Адміністрування в інформаційних системах	ФК1, ФК4, ФК6, ФК8, ФК9, ФК11, ФК12	РН7, РН9, РН33, РН43, РН44
Мейджор №3 Захист інформації в органах державної влади			
ВБ 3.1	Політики інформаційної безпеки в організаціях	ЗК9, ФК1, ФК4, ФК7, ФК8	РН17, РН28, РН32, РН34, РН35, РН45, РН56
ВБ 3.2	Аудит, ліцензування та акредитація інформаційних систем	ФК1, ФК8, ФК9, ФК11, ФК12	РН7, РН9, РН39, РН41, РН43, РН44, РН56
ВБ 3.3	Мобільні технології та їх захист	ЗК1, ФК2, ФК3, ФК5	РН5, РН15, РН21, РН22, РН23, РН30, РН51
ВБ 3.4	Відновлення інформаційних систем	ФК2, ФК4, ФК6, ФК7, ФК9	РН3, РН16, РН32, РН46, РН56
ВБ 3.5	Проектування систем безпеки об'єктів критичної інфраструктури	ЗК9, ФК1, ФК3, ФК5, ФК7, ФК9, ФК10, ФК12	РН4, РН7, РН13, РН16, РН24, РН30, РН49, РН56

Керівник робочої групи **Орест ПОЛОТАЙ**

ТАБЛИЦЯ ПРОПОЗИЦІЙ
ДО ПРОЄКТУ ОСВІТНЬОЇ ПРОГРАМИ ЗА РЕЗУЛЬТАТАМИ ГРОМАДСЬКОГО ОБГОВОРЕННЯ

Вид та назва освітньої програми — освітньо-професійна програма «Управління інформаційною безпекою»
Рівень вищої освіти — перший (бакалаврський)
Назва спеціальності — 125 Кібербезпека та захист інформації
Керівник групи забезпечення — ПОЛОТАЙ Орест Іванович

№п/п	Автор пропозиції (прізвище, ініціали, належність до групи stakeholders)	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.	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», зокрема вилучити наступні освітні компоненти: - «Спеціальні розділи математики» (3,5); - «Фізика» (3,5); - «Алгоритми і методи програмування» (3,5). *Громадське обговорення змін до ОПП 17.03.2023 р.*	Внесені в ОПП наступні освітні компоненти: - «Правознавство та правові засади цивільного захисту» обсягом 3,0 кредити для вивчення у 1 семестрі; - «Математичні основи криптографії» обсягом 3,5 кредити для вивчення у 3 семестрі; - «Курсовий проєкт» обсягом 3,0 кредити для вивчення у 7 семестрі; - «Навчальна практика» обсягом 4,5 кредити для вивчення у 8 семестрі; - «Єдиний державний кваліфікаційний іспит» обсягом 1,5 кредити для вивчення у 8 семестрі.	**Враховано повністю**
2.	Ткачук Ростислав – 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 наступні освітні компоненти:	Внесені в ОПП наступні освітні компоненти: - «Математичні основи криптографії» обсягом 3,5 кредити для вивчення у 3 семестрі; - «Курсовий проєкт» обсягом 3,0 кредити для вивчення у 7 семестрі;	**Враховано повністю**

№п/п	Автор пропозиції (прізвище, ініціали, належність до групи stakeholders)	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
		- «Виконання та захист дипломної роботи» (3,0); - «Комплексний кваліфікаційний екзамен» (1,5). *Громадське обговорення змін до ОПП 17.03.2023 р.*	- «Єдиний державний кваліфікаційний іспит» обсягом 1,5 кредити для вивчення у 8 семестрі.	
3.	Смілевський Максим – начальник управління безпеки міста Львівської міської ради, 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», зокрема вилучити наступні освітні компоненти: - «Переддипломна практика» (3,0). *Громадське обговорення змін до ОПП 17.03.2023 р.*	Внесені в ОПП наступні освітні компоненти: - «Навчальна практика» обсягом 4,5 кредити для вивчення у 8 семестрі.	**Враховано повністю**
4.	Полотай Орест - гарант освітньо-професійної програми, 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». Зокрема змінити обсяг кредитів та порядок вивчення освітніх компонент: - «Операційні системи», 3,5 кредита, 4 семестр. - «Інформаційна безпека держави», 3,5 кредита, 3 семестр. - «Система охорони державної таємниці», 3,0 кредити, 5 семестр. - «Теорія ризиків», 3,0 кредити, 7 семестр.	Внесені 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 змінити обсяг кредитів та порядок вивчення освітніх компонент: - «Операційні системи», 3,5 кредита, 2 семестр; - «Інформаційна безпека держави» 3,5 кредита, 8 семестр; - «Система охорони державної таємниці», 3,0 кредити, 8 семестр; - «Теорія ризиків», 3,0 кредити, 8 семестр.	**Враховано повністю**

№п/п	Автор пропозиції (прізвище, ініціали, належність до групи stakeholders)	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
		Громадське обговорення змін до ОПП 17.03.2023 р.		
5.	Карпюк Роман - SecOps Analyst компанії 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». Зокрема змінити обсяг кредитів та порядок вивчення освітніх компонент: - «Теорія інформації», 4,5 кредита, 3 семестр. - «Менеджмент інформаційної безпеки», 4,5 кредита, 8 семестр. *Громадське обговорення змін до ОПП 17.03.2023 р.*	Внесені 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 змінити обсяг кредитів та порядок вивчення освітніх компонент: - «Теорія інформації», 4,5 кредита, 4 семестр; - «Менеджмент інформаційної безпеки», 4,5 кредита, 4 семестр.	**Враховано повністю**
6.	Леськів Олег - менеджер освітніх проєктів Львівського IT Кластеру, 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». Зокрема змінити обсяг кредитів та порядок вивчення освітніх компонент: - «Застосування мови Python в кібербезпеці», 3,0 кредити, 8 семестр. - «Безпека програмного забезпечення», 3,5 кредита, 8 семестр. *Громадське обговорення змін до ОПП 17.03.2023 р.*	Внесені 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 змінити обсяг кредитів та порядок вивчення освітніх компонент: - «Застосування мови Python в кібербезпеці», 4,5 кредита, 8 семестр; - «Безпека програмного забезпечення», 4,5 кредита, 8 семестр.	**Враховано повністю**
7.	Філіпчук Богдан	Внести зміни до розділу 2 «Перелік компонент освітньо-професійної програми	Внесені зміни до розділу 2 «Перелік компонент освітньо-професійної програми	**Враховано повністю**

№п/п	Автор пропозиції (прізвище, ініціали, належність до групи stakeholders)	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
	– здобувач вищої освіти за ОПП «Управління інформаційною безпекою», внутрішній stakeholder	та їх логічна послідовність», п. 2.1 «Перелік компонент освітньо-професійної програми» та п. 2.2. «Структурно-логічна схема». Зокрема змінити обсяг кредитів та порядок вивчення освітніх компонент: - «Етичний хакінг», 4,5 кредита, 8 семестр. *Громадське обговорення змін до ОПП 17.03.2023 р.*	та їх логічна послідовність», п. 2.1 «Перелік компонент освітньо-професійної програми» та п. 2.2. «Структурно-логічна схема». Зокрема змінити обсяг кредитів та порядок вивчення освітніх компонент: - «Етичний хакінг», 6,0 кредитів, 4 семестр (3,0) та 5 семестр (3,0).	
8.	Івануса Андрій – доцент кафедри 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». Вилучити «Блок дисциплін відповідно до перспектив майбутнього працевлаштування». *Громадське обговорення змін до ОПП 17.03.2023 р.*	Внесені 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». Створити новий «Блок дисциплін відповідно до перспектив майбутнього працевлаштування (мейджори)». Блок дисциплін за вибором студентів розділити на три освітні траєкторії (мейджори) та включити до кожної наступні освітні компоненти: ***Мейджор «Захист інформації в органах державної влади»*** - «Політики інформаційної безпеки в організаціях», 4,5 кредита, 3 семестр. - «Аудит, ліцензування та акредитація інформаційних систем», 4,5 кредита, 4 семестр. - «Мобільні технології та їх захист», 4,5 кредита, 5 семестр. - «Відновлення інформаційних систем», 4,5	

№п/п	Автор пропозиції (прізвище, ініціали, належність до групи stakeholders)	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
			кредита, 6 семестр. - «Проектування систем безпеки об'єктів критичної інфраструктури» , 4,5 кредита, 7 семестр. ***Мейджор «Кібербезпека WEB-технологій»*** - «Хмарні технології», 4,5 кредита, 3 семестр. - «Опрацювання та аналіз системних подій», 4,5 кредита, 4 семестр. - «Моделювання та прогнозування в соціальній сфері», 4,5 кредита, 5 семестр. - «Стеганографія», 4,5 кредита, 6 семестр. - «Адміністрування в інформаційних системах» , 4,5 кредита, 7 семестр. ***Мейджор 3 «Кібербезпека інтернет речей»*** - «Основи інтернету речей та аналітика великих даних», 4,5 кредита, 3 семестр. - «Цифрова обробка сигналів та зображень», 4,5 кредита, 4 семестр. - «Безпека кіберфізичних систем», 4,5 кредита, 5 семестр. - «Мікропроцесори в системах технічного захисту інформації», 4,5 кредита, 6 семестр. - «Управління технічними засобами інформації», 4,5 кредита, 7 семестр.	

Розглянуто на засіданні кафедри управління інформаційною безпекою,
протокол № 12 від 17.03. 2023 р.

Керівник групи забезпечення ОПП Орест ПОЛОТАЙ