

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 № ____ від „ ____ ” _____ 20__ р.)

Освітньо-професійна програма

вводиться в дію

з „ ____ ” _____ 20__ р.
(наказ № ____ від „ ____ ” _____ 20__ р.)

**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:

Методичною радою навчально-наукового інституту цивільного захисту

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

ПОГОДЖЕНО:

Проректор з навчальної та методичної роботи

_____ Дмитро ЧАЛИЙ
„ ____ ” _____ 20__ р.

Начальник навчально-наукового інституту цивільного захисту

_____ Василь ПОПОВИЧ
„ ____ ” _____ 20__ р.

Начальник навчально-методичного центру

_____ Микола СИЧЕВСЬКИЙ
„ ____ ” _____ 20__ р.

ПЕРЕДМОВА

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

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

Члени робочої групи:

Полотай Орест Іванович кандидат технічних наук, доцент кафедри управління інформаційною безпекою;

Лагун Андрій Едуардович кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою;

Івануса Андрій Іванович кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою.

До розроблення програми залучено зовнішніх стейкхолдерів:

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

Рецензенти:

Ромака Володимир професор, д.т.н., професор кафедри захисту
Афанасійович інформації Національного університету
«Львівська політехніка»
Гайдар Ігор Богданович 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.	<i>Повна назва закладу вищої освіти та структурного підрозділу</i>	Львівський державний університет безпеки життєдіяльності Навчально-науковий інститут цивільного захисту Кафедра управління інформаційною безпекою
2.	<i>Ступінь вищої освіти та назва кваліфікації мовою оригіналу</i>	Ступінь вищої освіти: бакалавр Спеціальність: 125 Кібербезпека та захист інформації Освітня кваліфікація: бакалавр з кібербезпеки, управління інформаційною безпекою
3.	<i>Офіційна назва освітньої програми</i>	Управління інформаційною безпекою
4.	<i>Тип диплому та обсяг освітньої програми</i>	Диплом бакалавра, одиничний: – на основі повної загальної середньої освіти – 240 кредитів ЄКТС, термін навчання – 3 роки 10 місяців; – на основі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») – 120 кредитів ЄКТС, термін навчання – 1 рік 10 місяців; – на основі ступеня «фаховий молодший бакалавр» – 180 кредитів ЄКТС, термін навчання – 2 роки 10 місяців.
5.	<i>Наявність акредитації</i>	Підготовка здобувачів освіти за даною освітньою програмою здійснюється на основі сертифікату про акредитацію спеціальності 125 Кібербезпека, 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.	<i>Рівень програми</i>	НРК України – 6 рівень; FQ-EHEA – перший цикл, EQF-LLL – 6 рівень.
7.	<i>Передумови</i>	Наявність повної загальної середньої освіти Наявність диплому молодшого бакалавра (спеціаліста)
8.	<i>Мова викладання</i>	Українська
9.	<i>Термін дії освітньої програми</i>	До наступного планового оновлення програми, але не перевищуючи періоду акредитації
10.	<i>Інтернет-адреса постійного розміщення опису освітньої програми</i>	https://ldubgd.edu.ua/content/upravlinnya-informaciynoyu-bezpekoju

2-Мета освітньої програми

Ця програма призначена для розвитку професійних і творчих здібностей студентів до розв'язання практичних проблем, які характеризуються 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	<i>Предметна область</i>	Галузь знань: 12 Інформаційні технології Спеціальність: 125 Кібербезпека та захист інформації
----	--------------------------	--

		<p><u>Об'єкти вивчення:</u></p> <ul style="list-style-type: none"> – 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/або кібербезпекою об'єктів, що підлягають захисту. <p><u>Мета навчання:</u> підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки.</p> <p><u>Теоретичний зміст предметної області:</u> <u>Знання:</u></p> <ul style="list-style-type: none"> – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або 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	<i>Орієнтація освітньої програми</i>	<p>Освітньо-професійна програма.</p> <p>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.</p>
13	<i>Основний фокус освітньої програми</i>	<p>Загальна освіта в області кібербезпеки.</p> <p>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.</p> <p>А також з додатковим акцентом на задачі зі сфери технічного захисту інформації, які виникають в підрозділах ДСНС України.</p> <p><i>Ключові слова:</i> алгоритми, програмування, бази даних та</p>

		знань, комп'ютерні мережі, Web-технології, операційні системи, моделювання, комплексна система захисту інформації, етичний хакінг, інформаційна безпека, комп'ютерна криміналістика, інструменти кібербезпеки, криптографія.
14	<i>Особливості програми</i>	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	<i>Придатність до працевлаштування</i>	<p>Згідно з Національним класифікатором професій ДК 003-2010 студенти, які здобули освіту за освітньою програмою «Управління інформаційною безпекою» можуть обіймати такі первинні посади:</p> <ul style="list-style-type: none"> • 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. <p>Згідно з штатним розписом територіальних управлінь ДСНС України фахівці, які здобули кваліфікацію «бакалавр з кібербезпеки, управління інформаційною</p>

		безпекою» за освітньою програмою «Управління інформаційною безпекою» можуть обіймати такі первинні посади: <ul style="list-style-type: none"> 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 проєктів 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 захистом дипломної кваліфікаційної роботи.
18	Система оцінювання	<i>Види контролю:</i> поточний, підсумковий (семестровий та підсумкова атестація). <i>Форми контролю:</i> Поточний контроль передбачає опитування в усній або письмовій формі, тестування, захист виконання індивідуальних практичних завдань, реферати, захист звітів лабораторних робіт, презентацію проєктів. 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\або кібербезпеки, що характеризується комплексністю та невизначеністю умов.
20	Загальні	<i>Компетентності відповідно до стандарту вищої освіти</i>

		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.
		ЗК8	<i>Компетентності освітньої програми</i> 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	<i>Фахові</i>		<i>Компетентності відповідно до стандарту вищої освіти</i>
		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/або кібербезпеки.
		ФК2	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
		ФК3	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
		ФК4	Здатність забезпечувати неперервність бізнесу

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

7-Програмні результати навчання		
22		<i>Програмні результати навчання відповідно до стандарту вищої освіти</i>
	РН1	Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
	РН2	Організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.
	РН3	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
	РН4	Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
	РН5	Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

RH6	Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
RH7	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
RH8	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
RH9	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
RH10	Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
RH11	Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
RH12	Розробляти моделі загроз та порушника.
RH13	Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
RH14	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
RH15	Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
RH16	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
RH17	Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
RH18	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
RH19	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
RH20	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
RH21	Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
RH22	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
RH23	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
RH24	Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
RH25	Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з

	використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
RH26	Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
RH27	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
RH28	Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки.
RH29	Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
RH30	Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
RH31	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
RH32	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
RH33	Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
RH34	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
RH35	Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки.
RH36	Виявляти небезпечні сигнали технічних засобів.
RH37	Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
RH38	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
RH39	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
RH40	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
RH41	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
RH42	Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
RH43	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

RH44	Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
RH45	Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
RH46	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
RH47	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
RH48	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
RH49	Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
RH50	Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
RH51	Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
RH52	Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
RH53	Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
<i>Програмні результати навчання освітньої програми</i>	
RH54	Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
RH55	Демонструвати навички аналізу категорій цивільної безпеки, оцінювати стан та використовувати сучасні безпекові механізми для захисту інтересів людини.
RH56	Передбачати рівень індивідуальної безпеки та застосовувати основні заходи щодо самопорятунку і надання допомоги іншим у разі виникнення небезпечних подій, орієнтуватись в різновидах рятувального обладнання, особливостях організації рятувальних робіт та пожежогасіння, а також порядку проходження служби в органах та підрозділах цивільно захисту.
RH57	Застосовувати отримані знання основ цивільно захисту в практичній діяльності

8 - Ресурсне забезпечення реалізації програми		
23	<i>Кадрове забезпечення</i>	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	<i>Матеріально-технічне забезпечення</i>	Використання сучасних комп'ютерних засобів та ліцензійного програмного забезпечення (ПЗ з відкритою ліцензією) розподіленого між спеціалізованими лабораторіями та комп'ютерними класами загальною кількістю понад 200 робочих місць, а також іншого аудиторного фонду Університету, бібліотечним комплексом, читальними залами та соціально-побутовою інфраструктурою.
25	<i>Інформаційне та навчально-методичне забезпечення</i>	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	<i>Національна кредитна мобільність</i>	Може реалізуватись в рамках двосторонніх договорів між закладами вищої освіти про встановлення науково-освітніх відносин. Допускаються індивідуальні угоди про академічну мобільність для навчання (проходження практики) та проведення досліджень в університетах та наукових установах України.
27	<i>Міжнародна кредитна мобільність</i>	Індивідуальна у рамках програми Erasmus+ та на основі підписаних двосторонніх угод між Львівським державним університетом безпеки життєдіяльності та вищими навчальними закладами країн-партнерів.
28	<i>Навчання іноземних здобувачів вищої освіти</i>	Підготовка іноземних громадян за акредитованими напрямами (спеціальностями), наказ МОН України від 04.06.2013 № 2070 л. Мова викладання – українська.

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

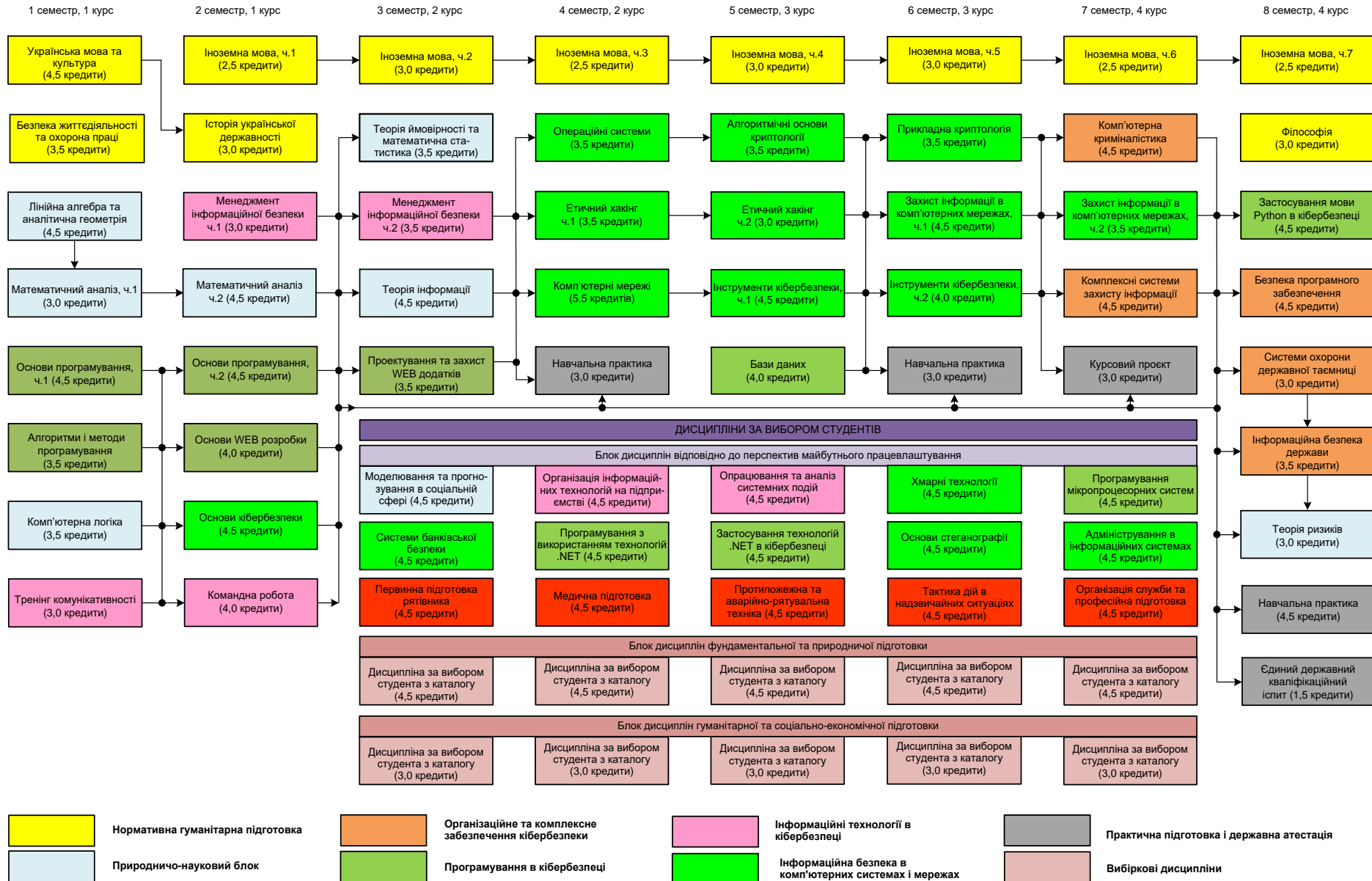
2.1. Перелік компонент освітньо-професійної програми

Код	Компоненти освітньої програми	Кількість кредитів	Форма підсумкового контролю
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ			
1.1. Цикл загальної підготовки			
OK 1	Українська мова та культура	4,5	диф. залік
OK 2	Історія української державності	3,0	диф. залік
OK 3	Філософія	3,0	екзамен
OK 4	Іноземна мова	19,0	диф. залік
OK 5	Безпека життєдіяльності та охорона праці	3,5	диф. залік
OK 6	Тренінг комунікативності	3,0	диф. залік
OK 7	Лінійна алгебра та аналітична геометрія	4,5	екзамен
OK 8	Математичний аналіз	7,5	екзамен
OK 9	Теорія ймовірності та математична статистика	3,5	диф. залік
Разом за циклом		51,5	
1.2. Цикл профільної підготовки			
OK 10	Алгоритми і методи програмування	3,5	диф. залік
OK 11	Комп'ютерна логіка	3,5	диф. залік
OK 12	Командна робота	4,0	екзамен
OK 13	Основи програмування	9,0	екзамен
OK 14	Основи кібербезпеки	4,5	екзамен
OK 15	Основи WEB розробки	4,0	диф. залік
OK 16	Інформаційна безпека держави	3,5	екзамен
OK 17	Проектування та захист WEB додатків	3,5	екзамен
OK 18	Теорія інформації	4,5	екзамен
OK 19	Операційні системи	3,5	екзамен
OK 20	Комп'ютерні мережі	5,5	екзамен
OK 21	Системи охорони державної таємниці	3,0	диф. залік
OK 22	Алгоритмічні основи криптології	3,5	диф. залік
OK 23	Інструменти кібербезпеки	8,5	екзамен
OK 24	Бази даних	4,0	екзамен
OK 25	Прикладна криптологія	3,5	екзамен
OK 26	Захист інформації в комп'ютерних мережах	8,0	екзамен
OK 27	Застосування мови Python в кібербезпеці	4,5	екзамен
OK 28	Комп'ютерна криміналістика	4,5	екзамен
OK 29	Теорія ризиків	3,0	диф. залік
OK 30	Комплексні системи захисту інформації	4,5	екзамен
OK 31	Менеджмент інформаційної безпеки	6,5	екзамен
OK 32	Етичний хакінг	6,5	екзамен
OK 33	Безпека програмного забезпечення	4,5	диф. залік
OK 34	Курсовий проєкт	3,0	диф. захист
OK 35	Навчальна практика	10,5	диф. залік
Разом за циклом		127,0	
1.3. Атестація			
OK 36	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			
Блок дисциплін №1			
ВБ 1.1	Моделювання та прогнозування в соціальній сфері	4,5	диф. залік
ВБ 1.2	Організація інформаційних технологій на підприємстві	4,5	диф. залік
ВБ 1.3	Опрацювання та аналіз системних подій	4,5	диф. залік
ВБ 1.4	Хмарні технології	4,5	диф. залік
ВБ 1.5	Програмування мікропроцесорних систем	4,5	диф. залік
Блок дисциплін №2			
ВБ 2.1	Системи банківської безпеки	4,5	диф. залік
ВБ 2.2	Програмування з використанням технологій .NET	4,5	диф. залік
ВБ 2.3	Застосування технологій .NET в кібербезпеці	4,5	диф. залік
ВБ 2.4	Основи стеганографії	4,5	диф. залік
ВБ 2.5	Адміністрування в інформаційних системах	4,5	диф. залік
Блок дисциплін №3			
ВБ 3.1	Первинна підготовка рятувника	4,5	диф. залік
ВБ 3.2	Медична підготовка	4,5	диф. залік
ВБ 3.3	Протипожежна та аварійно-рятувальна техніка	4,5	диф. залік
ВБ 3.4	Тактика дій в надзвичайних ситуаціях	4,5	диф. залік
ВБ 3.5	Організація служби та професійної підготовки	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 вибіркового компонент: 60			
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ: 240			

2.2. Структурно-логічна схема

Структурно-логічна схема підготовки бакалавра за спеціальністю 125 Кібербезпека та захист інформації



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 захисту інформації.

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		
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																			•								•							•	•			•

Програмні компетентності	Перелік вибірових компонент освітньої програми														
	Блок №1					Блок №2					Блок №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
PH 33															
PH 34															
PH 35															
PH 36															
PH 37															
PH 38															
PH 39															
PH 40															
PH 41				•				•							
PH 42								•							
PH 43															
PH 44		•													
PH 45															
PH 46															
PH 47									•						
PH 48			•						•						
PH 49															
PH 50															
PH 51															
PH 52			•							•					
PH 53							•	•							
PH 54											•		•	•	
PH 55												•		•	
PH 56										•	•		•	•	
PH 57												•		•	

Керівник робочої групи

Ростислав ТКАЧУК