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
СПЕЦІАЛІЗАЦІЯ	
КВАЛІФІКАЦІЯ	Бакалавр з кібербезпеки, управління інформаційною безпекою

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Львівського державного університету безпеки життєдіяльності
Голова Вченої ради
_____ Мирослав КОВАЛЬ
(протокол № 12 від „ 13 ” 07 2022 р.)

Освітньо-професійна програма вводиться в дію
з „ 14 ” 07 2022 р.
(наказ № 140-ос від „14 ” 07 2022 р.)

Львів 202_

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Рівень вищої освіти	перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Спеціалізація	
Кваліфікація	Бакалавр з кібербезпеки, управління інформаційною безпекою

ВНЕСЕНО:

Кафедрою управління інформаційною безпекою

Протокол № 9 від «27» 04 2022 р.

РЕКОМЕНДОВАНО:

Вченою радою навчально-наукового інституту цивільного захисту

Протокол № 1 від «12» липня 2022р.

ПОГОДЖЕНО:

Проректор з навчальної та методичної роботи
_____ Дмитро ЧАЛИЙ
„12” 07 2022р.

Начальник навчально-наукового інституту цивільного захисту
_____ Василь ПОПОВИЧ
„12” 07 2022р.

Начальник навчально-методичного центру
_____ Микола СИЧЕВСЬКИЙ
„12” 07 2022р.

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.
Стандарт затверджено і введено в дію наказом Міністерства освіти і науки України від 04.10.2018 № 1074.

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

Керівник робочої групи

Ткачук Ростислав Львович	– доктор технічних наук, доцент, 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;
Чмир Оксана Юріївна	кандидат фізико-математичних наук, доцент кафедри прикладної математики та механіки

До розроблення програми залучено зовнішніх стейкголдерів:

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

Рецензенти:

Ромака Володимир Афанасійович	професор, д.т.н., професор кафедри захисту 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.	*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 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, 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, 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 Наявність диплому молодшого бакалавра (спеціаліста)
8.	*Мова викладання*	Українська
9.	*Термін дії освітньої програми*	До наступного планового оновлення програми, але не перевищуючи періоду акредитації
10.	*Інтернет-адреса постійного розміщення опису освітньої програми*	https://ldubgd.edu.ua/content/upravlinnya-informaciynoyu-bezpekoyu

2-Мета освітньої програми
Ця програма призначена для розвитку професійних і творчих здібностей студентів до розв'язання практичних проблем, які характеризується комплексністю та невизначеністю, на основі методів і засобів забезпечення кібербезпеки. 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 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/або кібербезпекою об'єктів, що підлягають захисту. Мета навчання: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або 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/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	*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.
13	*Основний фокус освітньої програми*	Загальна освіта в області кібербезпеки. Програма спрямована на підготовку аналітиків-професіоналів, здатних застосувати математичні основи, алгоритмічні принципи в моделюванні, проектуванні, розробці, впровадженні та супроводі інформаційних, інтелектуальних систем задля забезпечення конфіденційності, 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*	Програма розвиває перспективні напрями інформаційної

	програми	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 студенти, 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 захистом дипломної кваліфікаційної роботи.	
18	*Система оцінювання*	*Види контролю*: поточний, підсумковий (семестровий та підсумкова атестація). *Форми контролю*: Поточний контроль передбачає опитування в усній або письмові формі, тестування, захист виконання індивідуальних практичних завдань, реферати, захист звітів лабораторних робіт, презентацію проектів. Підсумковий (семестровий) контроль знань проводиться у вигляді диференційного заліку або екзамену (у письмовій формі, у письмовій формі з подальшою усною співбесідою, на базі електронного навчального середовища), захист результатів проходження навчальної практики та захист курсової роботи. Підсумкова атестація передбачає складання комплексного кваліфікаційного екзамену та публічний захист кваліфікаційної роботи.	
	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*	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	Формування ідентичності та почуття особистої гідності в результаті осмислення соціального та морального досвіду минулих поколінь, розуміння історії і культури України, історії пожежно-рятувальної служби в контексті історичного процесу
		ЗК9	Навики здійснення безпечної діяльності
		ЗК10	Усвідомлення функцій держави, форм реалізації цих функцій, правових основ цивільного захисту, дотримання основних принципів здійснення цивільного захисту
21	*Фахові*	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 згідно встановленої політики інформаційної та/або кібербезпеки.
		ФК5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або 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/або 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/або кібербезпеки.
		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.

7-Програмні результати навчання		
22	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 /або кібербезпеки.
	РН8	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
	РН9	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або 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

РН31	елементів інформаційно-телекомунікаційних систем.
РН32	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
РН33	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
РН34	Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
РН35	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
РН36	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.
РН37	Виявляти небезпечні сигнали технічних засобів.
РН38	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.
РН39	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
РН40	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
РН41	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
РН42	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН43	Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
РН44	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
РН45	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.
РН46	Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до
РН47	інформаційних активів.
РН48	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
РН49	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
РН50	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
	Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних

	системах.
РН51	Забезпечувати функціонування програмних та програмно-апаратних
РН52	комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
РН53	Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
РН54	Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
РН55	Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
	Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав
РН56	і свобод людини і громадянина в Україні.
	Здатність аналізувати взаємозв'язки між процесами у минулому та на
РН57	сучасному етапі, оцінювати альтернативні варіанти інтерпретації основних тенденцій та особливостей історичного розвитку пожежно-рятувальної служби у певні історичні періоди.
	Передбачати необхідний рівень індивідуальної безпеки у разі виникнення небезпечних подій
	Застосовувати отримані знання правових основ цивільного 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 загальною кількістю понад 200 робочих місць, а також іншого аудиторного фонду Університету, бібліотечним комплексом, читальними залами та соціально-побутовою інфраструктурою.
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*	Підготовка іноземних громадян за акредитованими напрямами (спеціальностями), наказ МОН України від 04.06.2013 № 2070 л. Мова викладання – українська.

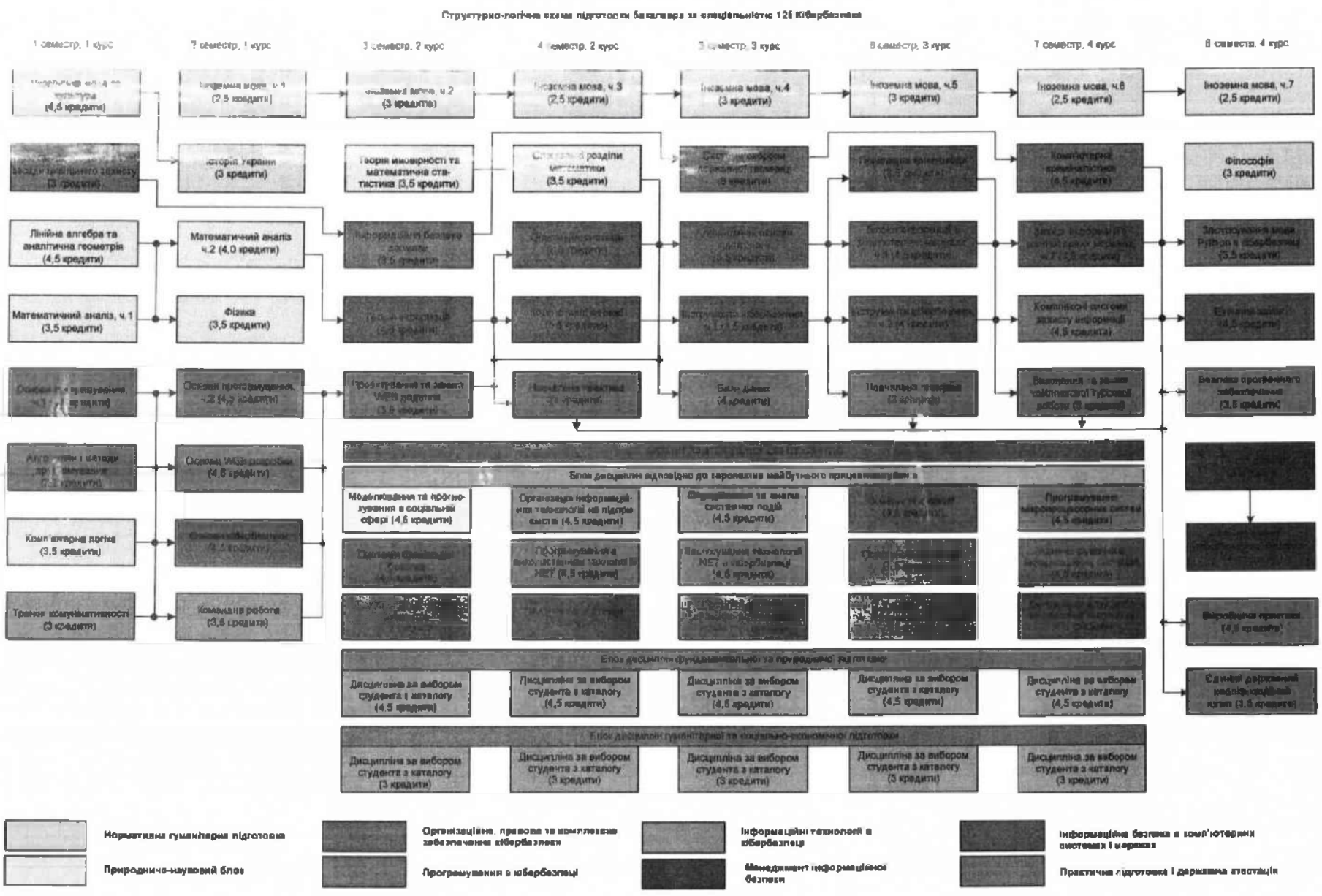
2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

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			
ОК 1	Українська мова та культура	4,5	диф. залік
ОК 2	Історія Української державності	3,0	диф. залік
ОК 3	Філософія	3,0	екзамен
ОК 4	Іноземна мова	19,0	диф. залік
ОК 5	Правознавство та правові засади цивільного захисту	3,0	диф. залік
ОК 6	Тренінг комунікативності	3,0	диф. залік
ОК 7	Лінійна алгебра та аналітична геометрія	4,5	екзамен
ОК 8	Математичний аналіз	7,5	екзамен
ОК 9	Теорія ймовірності та математична статистика	3,5	диф. залік
ОК 10	Спеціальні розділи математики	3,5	екзамен
ОК 11	Фізика	3,5	екзамен
Разом за циклом		***58,0***	
1.2. Цикл профільної підготовки			
ОК 12	Алгоритми і методи програмування	3,5	диф. залік
ОК 13	Комп'ютерна логіка	3,5	диф. залік
ОК 14	Командна робота	3,5	екзамен
ОК 15	Основи програмування	9,0	екзамен
ОК 16	Основи кібербезпеки	4,5	екзамен
ОК 17	WEB програмування	4,5	диф. залік
ОК 18	Інформаційна безпека держави	3,5	екзамен
ОК 19	Проектування та захист WEB додатків	3,5	екзамен
ОК 20	Теорія інформації	4,5	екзамен
ОК 21	Операційні системи	3,5	екзамен
ОК 22	Комп'ютерні мережі	5,5	екзамен
ОК 23	Системи охорони державної таємниці	3,0	диф. залік
ОК 24	Алгоритмічні основи криптології	3,5	диф. залік
ОК 25	Інструменти кібербезпеки	8,5	екзамен
ОК 26	Бази даних	4,0	екзамен
ОК 27	Прикладна криптологія	3,5	екзамен
ОК 28	Захист інформації в комп'ютерних мережах	8,0	екзамен
ОК 29	Застосування мови Python в кібербезпеці	3,5	екзамен
ОК 30	Комп'ютерна криміналістика	4,5	екзамен
ОК 31	Теорія ризиків	3,0	диф. залік
ОК 32	Комплексні системи захисту інформації	4,5	екзамен
ОК 33	Менеджмент інформаційної безпеки	4,0	екзамен
ОК 34	Етичний хакінг	4,5	екзамен
ОК 35	Безпека програмного забезпечення	3,5	диф. залік
ОК 36	Навчальна практика	6,0	диф. залік
ОК 37	Виробнича практика	4,5	диф. залік
ОК 38	Виконання та захист комплексної курсової роботи	3,0	диф. захист
Разом за циклом		***120,5***	

1.3. Атестація			
ОК 39	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 рятівника	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 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» проводиться у формі здачі комплексного кваліфікаційного екзамену та захисту кваліфікаційної роботи бакалавра, і завершується видачею документу встановленого Університетом зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації: Бакалавр з кібербезпеки, управління інформаційною безпекою.

Атестація здійснюється відкрито і публічно.

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	ОК 38	ОК 39
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														
	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
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	ОК 38	ОК 39
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	ОК 38	ОК 39
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 професійної 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	ОК 38	ОК 39
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														
	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
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														
	Блок №1					Блок №2					Блок №3				
	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ЗБ 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													•		•

Керівник робочої групи **Ростислав ТКАЧУК**