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
_____ М.С. Коваль
(протокол № 12 від „20" 06 2019 р.)

Освітньо-професійна програма вводиться в дію
з „02" 09 2019 р.
(наказ № 1210 від „30" 08 2019 р.)

Львів 2019

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

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

ВНЕСЕНО:

Кафедроюуправління інформаційною безпекою

Протокол № 5 від «15» 02 2019 р.

РЕКОМЕНДОВАНО:
Методичною радою навчально-наукового інститутуцивільного захисту

Протокол № 8 від «7» 05 2019 р.

ПОГОДЖЕНО

Проректор з навчальної та методичної роботи
Д.О. Чалий
„11" 06 2019 р.

Начальник навчально-наукового інституту цивільного захисту
В.В. Попович
„11" 06 2019 р.

Начальник навчально-методичного центру
Р.І. Стасьо
„11" 06 2019 р.

ПЕРЕДМОВА

Освітньо-професійна програма розроблена на підставі Стандарту вищої освіти за першим (бакалаврським) рівнемвищої 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.

РОЗРОБЛЕНОпроектною групою спеціальності 125 «Кібербезпека» Львівського державного університету безпеки життєдіяльності у складі:

Керівник проектної групи

Самотий Володимир Васильович	– доктор технічних наук, професор, завідувач кафедри управління інформаційною безпекою.

Члени проектної групи:

Кухарська Наталія Павлівна	– кандидат фізико-математичних наук, доцент, доцент кафедри управління інформаційною безпекою;
Лагун Андрій Едуардович	– кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою;
Полотай Орест Іванович	– кандидат технічних наук, доцент кафедри управління інформаційною безпекою;
Шабатура Марія Миколаївна	– кандидат технічних наук, доцент кафедри управління інформаційною безпекою.

До розроблення програми залучено зовнішніх стейкголдерів:

Роман Карпюк	– SecOps Analyst компаніїSoftServe
Михайло Кропива	– InfoSec Director компанії SoftServe

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:

_____

_____

_____

_____

_____

Освітня програма «Управління інформаційною безпекою» вводиться вперше.

Термін перегляду освітньої програми 1 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*	Тип: диплом бакалавра, одиничний Обсяг: 240 кредитів ЄКТС, термін навчання 4 роки
5.	*Наявність акредитації*	Національне агентство забезпечення якості вищої освіти Україна Термін подання програми на акредитацію – 1 липня 2024 р.
6.	*Рівень програми*	НРК України – 7 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 мова
9.	*Термін дії освітньої програми*	4 роки
10.	*Інтернет-адреса постійного розміщення опису освітньої програми*	https://ldubgd.edu.ua/abituriientu

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 інформаційнітехнології, 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*	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 криптографічногозахисту 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.
14	*Особливості програми*	Програма розвиває перспективні напрями інформаційної та кібербезпеки, а саме моделювання, проектування, розробку, впровадження та супровідсистем кібербезпеки.

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:

		• 2131.2 - адміністратор баз даних • 2131.2 - аналітик комп'ютерних систем • 2132.2 22481 інженер-програміст • 2132.2 - прикладний програміст • 2132.2 - системний програміст • 1495 - менеджер (управитель) систем з інформаційної безпеки • 1229.7 - керівник (директор, начальник та ін.) підрозділу (служби, управління, департаменту та ін.) з безпеки (фінансово-економічної, інформаційної) • 2149.2 - професіонал із організації інформаційної безпеки • 1210.1 - керівник підприємства (установи, організації) (сфера захисту інформації) • 1226.2 - керівник структурного підрозділу (сфера захисту інформації) • 1226.2 - начальник відділення (сфера захисту інформації) • 2149.2 - професіонал із організації захисту інформації з обмеженим доступом • 2149.2 - фахівець (сфера захисту інформації) Відповідно до здобутої кваліфікації бакалавр здатний виконувати професійні роботи за базовими професіями, визначеними наказом ДСНС України від 05.12.2018 № 707 „Про затвердження Довідника кваліфікаційних характеристик професій працівників у сфері цивільного захисту": • 3114 - технік електрозв'язку (аварійно-рятувального підрозділу) • 2149.2 - фахівець із забезпечення оперативно-рятувальних служб цивільного захисту • 3439 - фахівець оперативно-рятувальної служби цивільного захисту
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*	Комбінація лекцій, практичних занять, виконання проектів, дослідницьких лабораторних робіт, самостійної роботи в віртуальному навчальному середовищі, консультацій з викладачами; підготовка дипломної роботи.
18	*Система оцінювання*	Письмові та усні екзамени, реферати, лабораторні звіти, презентації проектів, захист дипломної 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 неповною визначеністю 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 використанняінформаційнокомунікаційних 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 інформаційноюта/або кібербезпекою.
		ФК10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
		ФК11	Здатністьвиконувати моніторинг процесів функціонування інформаційних,інформаційно-телекомунікаційних(автоматизованих)систем згідновстановленої політики інформаційної та/абокібербезпеки.
		ФК12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/абокібербезпеки

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 міжнароднихстандартах, 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 тапорушника.
	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	Використовуватисучаснепрограмно-апаратнезабезпеченняінформаційно-комунікаційних технологій.
	РН16	Реалізовуватикомплекснісистемизахистуінформації вавтоматизованих 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 захистуінформації 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	Вирішуватизадачіуправлінняпроцедурамиідентифікації,автентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і\абокібербезпеки.
	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\абокібербезпеки.
	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 функціонуванняінформаційно-телекомунікаційних систем звикористанням процедур резервування згідно встановленої політики безпеки.
	РН33	Вирішувати задачізабезпечення безперервності бізнес процесіворганізації на основі теорії ризиків.
	РН34	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або 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\абокібербезпеки.
	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/або кібербезпеки.
	РН43	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або 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/ або 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 можливихзагроз.
	РН54	Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
	РН55	Здатність аналізувати взаємозв'язки між процесами у минулому та на сучасному етапі, оцінювати альтернативні варіанти інтерпретації основних тенденцій та особливостей історичного розвитку пожежно-рятувальної служби у певні історичні періоди

	РН56	Передбачати необхідний рівень індивідуальної безпеки у разі виникнення небезпечних подій
	РН57	Застосовувати отримані знання правових основ цивільного захисту в практичній діяльності

	8-Ресурсне забезпечення реалізації програми	
23	Кадрове забезпечення	100% науково-педагогічних працівників задіяних до викладання дисциплін зі спеціальності 125 «Кібербезпека» мають наукові ступені з відповідних спеціальностей та (або) вчені звання
24	Матеріально-технічне забезпечення	Використання сучасних комп'ютерних засобів та програмного забезпечення розподіленого між мультимедійним навчальним комплексом, навчально-науковим центром інтелектуального моделювання безпечного майбутнього, лабораторії телекомунікаційних систем та комп'ютерної схемотехніки, лабораторії комп'ютерної графіки та іншим аудиторним фондом Університету.
25	Інформаційне та навчально-методичне забезпечення	Використання віртуального навчального середовища Львівського державного університету безпеки життєдіяльності; авторських розробок працівників; підручників на навчальних посібників з грифом Вченої ради Університету; іншим навчальних та методичних матеріалів розміщених на відкритих он-лайн платформах.

	9-Академічна мобільність	
26	Національна кредитна мобільність	Може реалізуватись в рамках двосторонніх договорів між закладами вищої освіти про встановлення науково-освітянських відносин. Допускаються індивідуальні угоди про академічну мобільність для навчання (проходження практики) та проведення досліджень в університетах та наукових установах України.
27	Міжнародна кредитна мобільність	Індивідуальна у рамках програми Erasmus+ та на основі підписаних двосторонніх угод між Львівським державним університетом безпеки життєдіяльності та вищими навчальними закладами країн-партнерів.
28	Навчання іноземних здобувачів вищої освіти	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

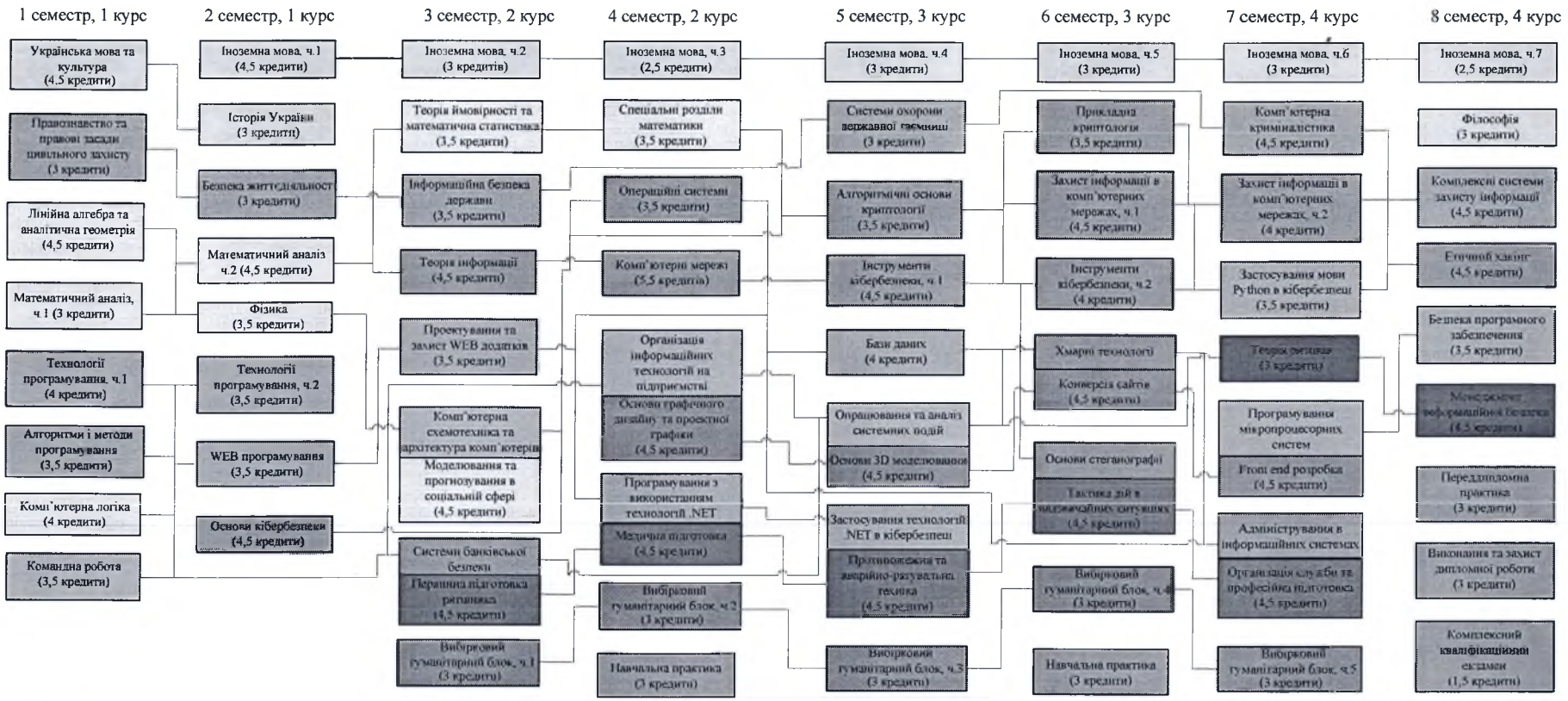
Код	Компоненти освітньої програми	Кількість кредитів	Форма підсумкового контролю
Обов'язкові компоненти освітньої програми			
1.1. Цикл загальної підготовки			
ОК1	Українська мова та культура	4,5	залік
ОК2	Історія України	3,0	залік
ОК3	Філософія	3,0	екзамен
ОК4	Іноземна мова	21,5	залік
ОК 5	Правознавство та правові засади цивільного захисту	3,0	залік
ОК 6	Безпека життєдіяльності	3,0	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	залік
ОК 10	Спеціальні розділи математики	3,5	залік
ОК 11	Фізика	3,5	екзамен
Разом за циклом		60,5	
1.2. Цикл профільної підготовки			
ОК 12	Алгоритми і методи програмування	3,5	залік
ОК 13	Комп'ютерна логіка	4,0	залік
ОК 14	Командна робота	3,5	екзамен
ОК 15	Технології програмування	7,5	екзамен
ОК 16	Основи кібербезпеки	4,5	екзамен
ОК 17	WEB програмування	3,5	залік
ОК 18	Інформаційна безпека держави	3,5	екзамен
ОК19	Проектування та захист WEB додатків	3,5	екзамен
ОК20	Теорія інформації	4,5	екзамен
ОК21	Операційні системи	3,5	екзамен
ОК22	Комп'ютерні мережі	5,5	екзамен
ОК23	Системи охорони державної таємниці	3,0	залік
ОК24	Алгоритмічні основи криптології	3,5	залік
ОК25	Інструменти кібербезпеки	8,5	екзамен
ОК26	Бази даних	4,0	екзамен
ОК27	Прикладна криптологія	3,5	екзамен
ОК28	Захист інформації в комп'ютерних мережах	8,5	екзамен
ОК29	Застосування мови Python в кібербезпеці	3,5	екзамен
ОК30	Комп'ютерна криміналістика	4,5	екзамен
ОК31	Теорія ризиків	3,0	залік
ОК32	Комплексні системи захисту інформації	4,5	екзамен
ОК33	Менеджмент інформаційної безпеки	4,5	екзамен
ОК34	Етичний хакінг	4,5	екзамен

ОК35	Безпека програмного забезпечення	3,5	залік
ОК36	Навчальна практика	6,0	залік
ОК37	Переддипломна практика	3,0	залік
Разом за циклом		115	
1.3. Атестація			
ОК38	Виконання та захист дипломної роботи	3,0	захист
ОК39	Комплексний кваліфікаційний екзамен	1,5	екзамен
Разом за циклом		4,5	
Загальний обсяг обов'язкових компонент: 180			
Вибіркові компоненти освітньої програми			
Блок А дисциплін за вибором студентів			
ВД А1	Комп'ютерна схемотехніка та архітектура комп'ютерів	4,5	залік
ВД А2	Організація інформаційних технологій на підприємстві	4,5	залік
ВД А3	Опрацювання та аналіз системних подій	4,5	залік
ВД А4	Хмарні технології	4,5	залік
ВД А5	Програмування мікропроцесорних систем	4,5	залік
Разом за блоком А		22,5	
Блок Б дисциплін за вибором студентів			
ВД Б1	Моделювання та прогнозування в соціальній сфері	4,5	залік
ВД Б2	Основи графічного дизайну та проектної графіки	4,5	залік
ВД Б3	Основи 3D моделювання	4,5	залік
ВД Б4	Конверсія сайтів	4,5	залік
ВД Б5	Frontend розробка	4,5	залік
Разом за блоком Б		22,5	
Блок В дисциплін за вибором студентів			
ВД В1	Системи банківської безпеки	4,5	залік
ВД В2	Програмування з використанням технологій .NET	4,5	залік
ВД В3	Застосування технологій .NET в кібербезпеці	4,5	залік
ВД В4	Основи стеганографії	4,5	залік
ВД В5	Адміністрування в інформаційних системах	4,5	залік
Разом за блоком В		22,5	
Блок Г дисциплін за вибором студентів			
ВД Г1	Первинна підготовка рятівника	4,5	залік
ВД Г2	Медична підготовка	4,5	залік
ВД Г3	Протипожежна та аварійно-рятувальна техніка	4,5	залік
ВД Г4	Тактика дій в надзвичайних ситуаціях	4,5	залік
ВД Г5	Організація служби та професійної підготовки	4,5	залік
Разом за блоком Г		22,5	
Дисципліни з каталогу за вибором студентів			
ВД К1	Дисципліна за вибором студентів №1	3,0	залік

ВД К2	Дисципліна за вибором студентів №2	3,0	залік
ВД К3	Дисципліна за вибором студентів №3	3,0	залік
ВД К4	Дисципліна за вибором студентів №4	3,0	залік
ВД К5	Дисципліна за вибором студентів №5	3,0	залік
Разом за каталогом		15	
Загальний обсяг вибіркових компонент: 60			
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ:240			

2.2. Структурно-логічна схема

Структурно-логічна схема підготовки бакалавра за спеціальністю «Кібербезпека»



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.

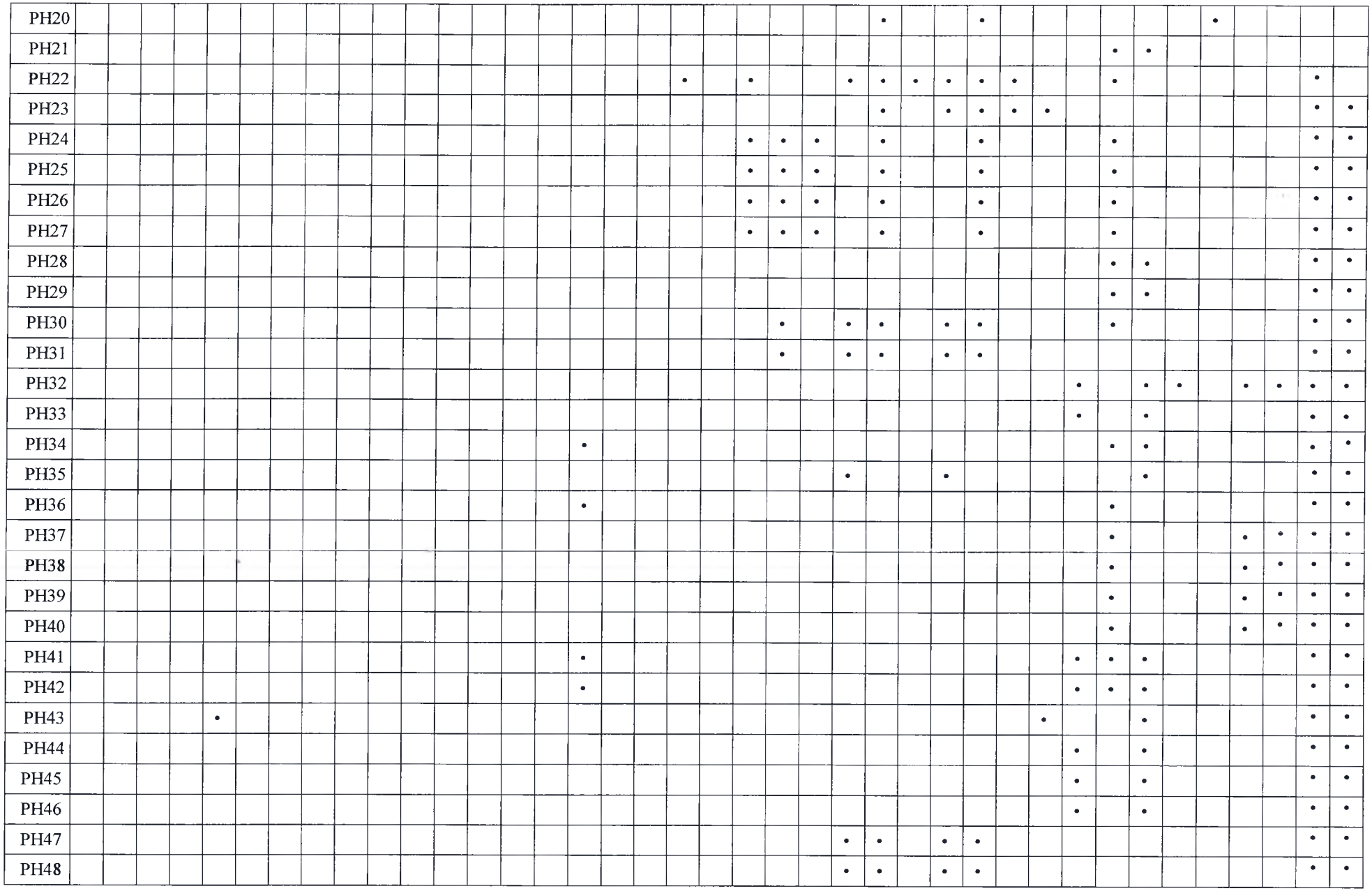
4. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

Програмні компетентності	Перелік компонент освітньої програми Обов'язкові компоненти освітньої програми																																									
	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37	ОК38	ОК39
ЗК1	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
ЗК2														•		•			•				•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
ЗК3	•			•																														•	•							
ЗК4										•	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•
ЗК5	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
ЗК6	•	•	•		•											•							•							•											
ЗК7	•	•												•		•																										
ЗК8	•	•	•		•	•												•																								
ЗК9					•	•										•		•																		•						
ЗК10					•	•												•					•																			
ФК1					•									•		•							•		•			•		•	•	•	•			•	•	•	•		
ФК2										•	•			•	•	•			•	•	•	•			•	•		•	•	•	•	•	•			•	•	•	•		
ФК3										•				•					•	•	•		•	•			•	•		•		•		•	•						
ФК4																															•		•					•	•		
ФК5																	•		•			•	•		•	•	•	•				•			•						
ФК6															•		•		•		•					•				•	•		•		•			•	•		
ФК7																							•									•						•	•		
ФК8																														•	•		•					•	•		
ФК9																		•			•	•	•					•	•			•	•								
ФК10																			•				•	•		•	•	•				•			•						
ФК11																					•							•			•			•							
ФК12																			•						•			•	•		•	•	•	•	•						

Програмні компетентності	Перелік компонент освітньої програми																										
	Вибіркові компоненти освітньої програми																										
	ВД А1	ВД А2	ВД А3	ВД А4	ВД А5	ВД Б1	ВД Б2	ВД Б3	ВД Б4	ВД Б5	ВД В1	ВД В2	ВД В3	ВД В4	ВД В5	ВД Г1	ВД Г2	ВД Г3	ВД Г4	ВД Г5	ВД К1	ВД К2	ВД К3	ВД К4	ВД К5
ЗК1	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
ЗК2	•	•									•								•	•					
ЗК3	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
ЗК4		•	•					•			•	•	•						•						
ЗК5	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•
ЗК6																•					•	•	•	•	•
ЗК7																•	•				•	•	•	•	•
ЗК8		•														•	•			•					
ЗК9		•	•												•	•	•	•	•	•					
ЗК10																•	•	•	•	•					
ФК1	•										•								•	•					
ФК2	•	•		•	•	•					•	•	•	•	•										
ФК3	•			•							•			•	•										
ФК4		•	•	•							•														
ФК5	•			•					•	•	•			•	•										
ФК6	•			•						•					•				•						
ФК7																									
ФК8			•								•														
ФК9																									
ФК10														•	•										
ФК11											•				•										
ФК12						•					•				•		•	•	•	•					•

5. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

Програмні компетентності	Перелік компонент освітньої програми Обов'язкові компоненти освітньої програми																																										
	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37	ОК38	ОК39
РН1	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
РН2					•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
РН3					•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
РН4							•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
РН5							•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
РН6			•		•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
РН7					•	•										•		•					•						•	•	•	•			•	•	•	•				
РН8					•											•		•							•			•		•		•	•									
РН9																•			•					•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
РН10							•	•	•	•			•			•				•	•	•		•	•	•	•	•						•	•	•	•	•	•	•	•
РН11																					•	•			•			•	•													
РН12					•																				•			•	•		•	•				•	•	•	•			
РН13												•										•			•			•											•			
РН14												•			•		•		•	•					•										•	•			•			
РН15												•			•		•		•	•					•										•	•			•			
РН16					•																		•						•		•	•								
РН17														•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
РН18																											•	•				•									
РН19														•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•


PH20
PH21
PH22
PH23
PH24
PH25
PH26
PH27
PH28
PH29
PH30
PH31
PH32
PH33
PH34
PH35
PH36
PH37
PH38
PH39
PH40
PH41
PH42
PH43
PH44
PH45
PH46
PH47
PH48

PH49										•										•										•					•	•
PH50																								•			•				•	•			•	•
PH51																								•			•				•	•			•	•
PH52																								•			•				•				•	•
PH53																											•	•				•	•			
PH54	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
PH55	•	•			•	•																														
PH56						•																														
PH57					•	•																														

Програмні компетентності	Перелік компонент освітньої програми																												
	Вибіркові компоненти освітньої програми																												
	ВД А1	ВД А2	ВД А3	ВД А;	ВД А5	ВД Б1	ВД Б2	ВД Б3	ВД Б4	ВД Б5	ВД В1	ВД В2	ВД В3	ВД В4	ВД В5	ВД Г1	ВД Г2	ВД Г3	ВД Г4	ВД Г5	ВД К1	ВД К2	ВД К3	ВД К4	ВД К5
РН1	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
РН2	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•													
РН3	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•													
РН4	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
РН5	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
РН6	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
РН7		•		•							•				•														
РН8		•																											
РН9		•																											
РН10				•							•	•	•		•														
РН11				•							•	•	•		•														
РН12		•									•			•	•														
РН13		•										•	•		•														
РН14											•	•	•	•															
РН15	•		•	•	•	•	•	•	•	•	•	•	•	•	•														
РН16		•												•															
РН17	•			•							•	•	•		•														
РН18	•		•	•	•	•	•	•	•	•	•	•	•	•	•														
РН19		•		•											•														
РН20				•							•	•	•		•														
РН21		•		•							•				•														
РН22											•				•														
РН23		•									•				•														
РН24											•				•														
РН25											•				•														
РН26															•														
РН27												•	•	•															
РН28		•													•														
РН29				•							•				•														
РН30				•							•			•	•														

РН31	•	•	•								•				•										
РН32															•										
РН33		•																							
РН34		•																							
РН35		•													•										
РН36	•				•																				
РН37	•																								
РН38	•																								
РН39		•									•														
РН40		•													•										
РН41				•							•				•										
РН42		•													•										
РН43		•																							
РН44		•									•														
РН45		•									•														
РН46		•									•														
РН47											•	•	•	•											
РН48											•	•	•	•	•										
РН49															•										
РН50											•				•										
РН51		•									•				•										
РН52		•		•											•										
РН53				•	•						•	•	•												
РН54	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•
РН55		•														•	•	•	•	•					
РН56																•	•	•	•	•					
РН57																				•					

Керівник проектної групи
д.т.н., професор **В.В. Самотий**