МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ВАСИЛЯ СТУСА

ЗАТВЕРДЖЕНО
Вченою радою ДонНУ
імені Василя Стуса
Протокол №__ від «___»_____2020 р.
Голова Вченої ради
_____А.П. Загнітко

ВВЕДЕНО В ДІЮ
Наказ № ___
від «___»_____2020 р.
Ректор
_____Р.Ф.Гринюк

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

КІБЕРБЕЗПЕКА / CYBERSECURITY

РІВЕНЬ ВИЩОЇ ОСВІТИ	**ПЕРШИЙ**
СТУПІНЬ ВИЩОЇ ОСВІТИ	**БАКАЛАВР**
ГАЛУЗЬ ЗНАНЬ	**12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ**
СПЕЦІАЛЬНІСТЬ	**125 КІБЕРБЕЗПЕКА (CYBERSECURITY)**

Вінниця – 2020

ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
(КІБЕРБЕЗПЕКА / CYBERSECURITY)

РЕКОМЕНДОВАНО
Радою з якості вищої освіти
Донецького національного
університету імені Василя Стуса
протокол №__ від_____2020 р.

Заступник голови Ради з якості,
Перший проректор _____ Т.Л. Нагорняк

РЕКОМЕНДОВАНО
Вченою радою
фізико-технічного факультету

протокол №__ від_____2020 р.

Голова _____ О.І. Барибін

Експерт з якості
_____
(спеціальність)
_____ Ткаченко В.С.

Декан
фізико-технічного факультету

_____ Барибін О.І.

ІНІЦІЙОВАНО:
Кафедрою радіофізики та
кібербезпеки
протокол № ___ від _____ 2020 р.
В.о. завідувача кафедри
_____ Крижановський В.Г.

ПРОЄКТНА ГРУПА

Гарант:
_____ Барибін О.І
Члени групи:
_____ Крижановський В.Г.
_____ Фурса С.Є.

РЕЦЕНЗЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

І. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Тип диплому та обсяг програми (в кредитах ЄКТС)		Диплом бакалавра, одиничний ступінь, тривалість програми: – на базі повної загальної середньої освіти – 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців; – на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста).
Заклад вищої освіти		Донецький національний університет імені Василя Стуса, Україна Vasyl' Stus Donetsk National University, Ukraine
Акредитаційна організація		Національна агенція забезпечення якості вищої освіти
Період акредитації		Спеціальність акредитована у 2015р., на 5 років. Сертифікат про акредитацію: НД 0289350 21.08.2017р., термін дії до 01.07.2020 р.
Рівень програми		НРК України – 7 рівень, FQ EHEA – First cycle, EQF LLL – 6 рівень, рівень освіти – перший (бакалаврський)
A	**МЕТА ПРОГРАМИ**	
	Метою програми є підготовка затребуваних фахівців, які здатні розв'язувати типові задачі за спеціальністю, розробляти і використовувати технології кібербезпеки (інформаційної безпеки) та технології програмування.	
B	**ХАРАКТЕРИСТИКА ПРОГРАМИ**	
1	*Фокус програми: загальна/спеціальна*	Спеціальна
2	*Особливості програми*	Додаткові особливості даної ступеневої програми, які відрізняють її від інших подібних програм: • володіння та використання здобувачами вищої освіти технологій програмування; • залучення викладачів-практиків до аудиторних занять; • викладання окремих освітніх компонентів англійською мовою.
C	**ПРАЦЕВЛАШТУВАННЯ ТА ПРОДОВЖЕННЯ ОСВІТИ**	
1	*Працевлаштування*	Професії, на підготовку з яких спрямована ОП (згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010) 1495 Менеджери (управителі) систем з інформаційної безпеки, 2149.2 Фахівець (сфера захисту інформації), 3119 Технік (сфера захисту інформації), 2131.2 Адміністратор бази даних, 2131.2 Адміністратор даних, 2131.2 Адміністратор доступу, 2131.2 Адміністратор доступу (груповий).
D	**СТИЛЬ ТА МЕТОДИКА НАВЧАННЯ**	
1	*Підходи до викладання та навчання*	Студентоцентроване, інтерактивне, проблемно-орієнтоване навчання, навчання під керівництвом викладача, самостійне та індивідуальне навчання. Викладання проводиться у вигляді лекції, мультимедійних лекцій, семінарів, практичних занять, лабораторних робіт,

		самостійного навчання, індивідуальних занять, онлайн-консультацій.
2	*Система оцінювання*	Усні та письмові екзамени, заліки, захисти звітів з практик, тематичні дослідження, презентації, поточні оцінювання, модульні контролі, захист курсових робіт, захист кваліфікаційної роботи та кваліфікаційний екзамен.
Е	**ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ ВИПУСКНИКА**	
	Інтегральна компетентність (ІК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов. ІК-1
	Загальні компетентності (ЗК)	Здатність застосовувати знання у практичних ситуаціях. ЗК-1 Знання та розуміння предметної області та розуміння професії. ЗК-2 Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК-3 Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК-4 Здатність до пошуку, оброблення та аналізу інформації. ЗК-5 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. ЗК-6 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. ЗК-7
	Фахові, компетентності (ФК)	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. ФК-1 Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. ФК-2 Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК-3 Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК-4 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. ФК-5 Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК-6 Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). ФК-7 Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК-8 Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. ФК-9

		Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. ФК-10 Здатність виконувати моніторинг ресурсів і процесів функціонування, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. ФК-11 Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної та/або кібербезпеки. ФК-12
F	**ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ**	
	Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН 1 Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН 2 Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН 3 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. ПРН 4 Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН 5 Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ПРН 6 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН 7 Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. ПРН 8 Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПРН 9 Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. ПРН 10 Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. ПРН 11 Розробляти моделі загроз та порушника. ПРН 12 Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. ПРН 13 Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. ПРН 14 Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. ПРН 15 Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. ПРН 16 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. ПРН 17 Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН 18 Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах. ПРН 19	

	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. ПРН 20 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. ПРН 21 Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН 22 Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН 23 Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). ПРН 24 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. ПРН 25 Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем. ПРН 26 Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. ПРН 27 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. ПРН 28 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. ПРН 29 Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. ПРН 30 Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем. ПРН 31 Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. ПРН 32 Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. ПРН 33 Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. ПРН 34 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. ПРН 35 Виявляти небезпечні сигнали технічних засобів. ПРН 36 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. ПРН 37 Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 38

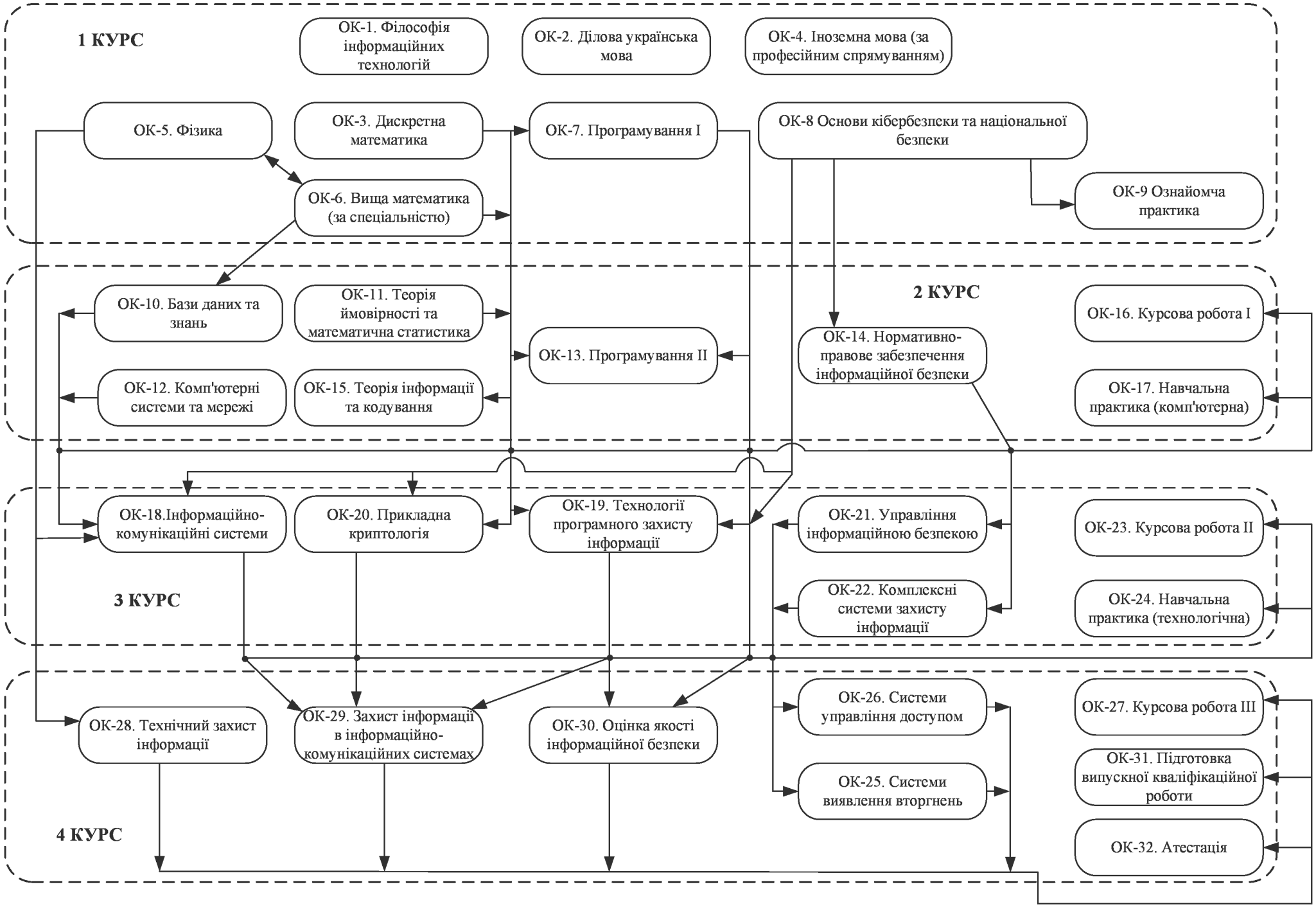
	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ПРН 39 Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 40 Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. ПРН 41 Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ПРН 42 Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН 43 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. ПРН 44 Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. ПРН 45 Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. ПРН 46 Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН 47 Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. ПРН 48 Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно телекомунікаційних системах. ПРН 49 Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). ПРН 50 Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. ПРН 51 Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. ПРН 52 Вирішувати задачі аналізу програмного коду на наявність можливих загроз. ПРН 53 Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ПРН 54	
G	**РЕСУРСНЕ ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ ПРОГРАМИ**	
1	Кадрове забезпечення	До викладання залучаються штатні працівники університету та провідні співробітники організацій, що працюють у професійно-орієнтованій сфері. Кадровий склад проектної групи та групи забезпечення відповідає ліцензійним вимогам та складається з викладачів, які мають науковий ступінь та / або вчене звання.
2	Матеріально-технічне забезпечення	При викладанні дисциплін професійної підготовки використовується матеріально-технічна база Донецького національного університету імені Василя Стуса та організацій, що працюють у професійно-орієнтованій галузі.
3	Інформаційне та навчально-методичне забезпечення	Інформаційний пакет спеціальності представлено на сайті Донецького національного університету імені Василя Стуса. Навчальні ресурси: – доступ до онлайн-бібліотеки Донецького національного університету імені Василя Стуса;

		– доступ до електронної бази наукових журналів; – доступ до бази електронних бібліотечних ресурсів світу. З усіх компонент освітньо-професійної програми розроблено робочі програми, навчальні посібники з лекційних курсів, методичні вказівки щодо виконання лабораторних та практичних робіт. Академічна підтримка – консультації з вибору окремих вибіркових дисциплін, проектування індивідуальних навчальних траєкторій.
Н	**АКАДЕМІЧНА МОБІЛЬНІСТЬ**	
1	Національна кредитна мобільність	У рамка програм співпраці між Донецьким національним університетом імені Василя Стуса та ЗВО України здобувачі вищої освіти мають право впродовж окремих семестрів навчатися у відповідних ЗВО, приймати участь у наукових коференціях, олімпіадах, семінарах тощо
2	Міжнародна кредитна мобільність	Донецький національний університет імені Василя Стуса є учасником програми міжнародної співпраці Erasmus та Tempus. В рамках цих програм здобувачі вищої освіти мають змогу проходити стажування в закордонних закладах вищої освіти, що є учасниками програм Erasmus та Tempus.
3	Навчання іноземних здобувачів вищої освіти	Більшість викладачів, які забезпечують навчальний процес за освітньою програмою мають підтверджений рівень володіння англійською мовою на рівні B2 (C1).

ІІ. КАТАЛОГ КОМПОНЕНТІВ ОСВІТНЬОЇ ПРОГРАМИ ТА ЇХ ЛОГІКО-СТРУКТУРНА СХЕМА

Код	Компоненти освітньої програми (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Дисципліни професійної та практичної підготовки			
ОК-1	Філософія інформаційних технологій	4	Залік
ОК-2	Ділова українська мова	3	Залік
ОК-3	Дискретна математика	4	Залік
ОК-4	Іноземна мова (за професійним спрямуванням)	5	Залік, залік
ОК-5	Фізика	7	Залік, залік
ОК-6	Вища математика (за спеціальністю)	8	Залік, залік
ОК-7	Програмування І	8	Екзамен, екзамен
ОК-8	Основи кібербезпеки та національної безпеки	8	Екзамен, екзамен
ОК-9	Ознайомча практика	3	
ОК-10	Бази даних та знань	4	Екзамен
ОК-11	Теорія ймовірності та математична статистика	4	Залік
ОК-12	Комп'ютерні системи та мережі	6,5	Залік, екзамен
ОК-13	Програмування ІІ	8	Залік, екзамен
ОК-14	Нормативно-правове забезпечення ІБ	6,5	Екзамен, екзамен
ОК-15	Теорія інформації та кодування	5	Екзамен
ОК-16	Курсова робота	3	
ОК-17	Навчальна практика (комп'ютерна)	3	
ОК-18	Інформаційно-комунікаційні системи	4	Екзамен
ОК-19	Технології програмного захисту інформації	4	Залік
ОК-20	Прикладна криптологія	9	Залік, екзамен
ОК-21	Управління інформаційною безпекою	8	Екзамен, екзамен
ОК-22	Комплексні системи захисту інформації	9	Залік, екзамен
ОК-23	Курсова робота	3	
ОК-24	Навчальна практика (технологічна)	3	
ОК-25	Системи виявлення вторгнень	4,5	Екзамен
ОК-26	Системи управління доступом	5	Екзамен
ОК-27	Курсова робота	3	
ОК-28	Технічний захист інформації	8	Залік, екзамен
ОК-29	Захист інформації в інформаційно-комуникаційних системах	8	Залік, екзамен
ОК-30	Оцінка якості інформаційної безпеки	8	Залік, екзамен
ОК-31	Підготовка кваліфікаційної бакалаврської роботи	9	Захист бакалаврської роботи
ОК-32	Атестація	4,5	
Загальний обсяг дисциплін професійної та практичної підготовки		180	
Дисципліни за вибором здобувача вищої освіти			
Варіант 1	Minor	60	
Варіант 2	Сертифікатна освітня програма	60	
Варіант 3	Довільно обрані дисципліни	60	
Загальний обсяг дисциплін за вибором здобувача вищої освіти		60	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

ЛОГІКО-СТРУКТУРНА СХЕМА ПІДГОТОВКИ ФАХІВЦЯ



ІІІ. ВИЗНАЧЕННЯ ФОРМ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ЗА ОСВІТНЬОЮ ПРОГРАМОЮ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі: ▪ публічного захисту (демонстрації) випускної кваліфікаційної роботи; ▪ комплексного екзамену з професійно-орієнтованих дисциплін.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має передбачати розв'язання спеціалізованої задачі в галузі інформаційної та / або кібербезпеки. Кваліфікаційна робота проходить перевірку на плагіат. Оприлюднення роботи на корпоративному сайті та/або репозиторії Донецького національного університету імені Василя Стуса.

IV. ВИМОГИ ДО НАЯВНОСТІ СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

Процедури і заходи забезпечення якості освіти	Визначено та легітимізовано «Положенням про організацію освітньої діяльності у Донецькому національному університеті імені Василя Стуса», «Положенням про систему внутрішнього забезпечення якості вищої освіти», «Системою заходів внутрішнього забезпечення якості вищої освіти». Моніторинг освітніх програм проводиться на локальному і загальноуніверситетському рівнях. Локальний моніторинг здійснюється, як правило, членами проектної групи за участі провідних фахівців профільних кафедр із залученням представників студентського самоврядування. Результати локального моніторингу не менше як один раз на рік обговорюються на засіданні Навчально-методичної комісії та Вченої ради факультету. Загальноуніверситетський моніторинг проводиться з метою узагальнення та поширення кращих практик у межах Університету та своєчасного виявлення негативних тенденцій
Моніторинг та періодичний перегляд освітніх програм	Оцінювання результатів навчання здобувачів вищої освіти здійснюється згідно із «Порядком оцінювання знань здобувачів вищої освіти у Донецькому національному університеті імені Василя Стуса» із дотриманням оприлюднених критеріїв, правил та процедур. Оцінювання знань здобувачів з дисциплін, в яких за навчальним планом передбачено екзамен, здійснюється на основі результатів поточного та підсумкового контролю знань, з навчальних дисциплін, формою контролю в яких є залік на основі результатів поточного модульного контролю
Оцінювання здобувачів вищої освіти	Систематичне підвищення кваліфікації та стажування викладачів здійснюється відповідно до «Положення про підвищення кваліфікації та стажування науково-педагогічних та педагогічних працівників у Донецькому національному університеті імені Василя Стуса». Підвищення кваліфікації науково-педагогічних працівників здійснюється не менше одного разу на 5 років
Підвищення кваліфікації науково-педагогічних	Освітній процес в Університеті забезпечується: • комп'ютерною технікою та пакетами прикладних комп'ютерних програм

працівників, педагогічних та наукових працівників	• безперебійним доступом до мережі «Internet» • використанням хмарних технологій • хмарний інтернет-сервіс Офіс-365 • платформою дистанційного навчання Moodle програмно-технологічним комплексом управління навчальним процесом АС «Деканат»
Наявність інформаційних систем для ефективного управління освітнім процесом	Електронний варіант освітньої програми розміщено на сайті університету та на сайті факультету.
Публічність інформації про освітні програми, ступені освіти та кваліфікації	Підготовка здобувачів здійснюється на основі принципів академічної доброчесності та корпоративної етики визначених в «Кодексі академічної доброчесності та корпоративної етики Донецького національного університету імені Василя Стуса», за дотримання якого відповідає Комісія з питань академічної доброчесності та корпоративної етики Донецького національного університету імені Василя Стуса
Забезпечення дотримання академічної доброчесності працівниками закладів вищої освіти та здобувачами вищої освіти, у тому числі запобігання та виявлення академічного плагіату	Визначено та легітимізовано «Положенням про організацію освітньої діяльності у Донецькому національному університеті імені Василя Стуса», «Положенням про систему внутрішнього забезпечення якості вищої освіти», «Системою заходів внутрішнього забезпечення якості вищої освіти». Моніторинг освітніх програм проводиться на локальному і загальноуніверситетському рівнях. Локальний моніторинг здійснюється, як правило, членами проектної групи за участі провідних фахівців профільних кафедр із залученням представників студентського самоврядування. Результати локального моніторингу не менше як один раз на рік обговорюються на засіданні Навчально-методичної комісії та Вченої ради факультету. Загальноуніверситетський моніторинг проводиться з метою узагальнення та поширення кращих практик у межах Університету та своєчасного виявлення негативних тенденцій

V. Матриця відповідності програмних результатів навчання та компетентностей

Програмні результати навчання	Компетентності																			
		Загальні компетентності							Спеціальні компетентності											
	ІК	ЗК-1	ЗК-2	ЗК-3	ЗК-4	ЗК-5	ЗК-6	ЗК-7	СК-1	СК-2	СК-3	СК-4	СК-5	СК-6	СК-7	СК-8	СК-9	СК-10	СК-11	СК-12
ПРН-1	●	●	●	●																
ПРН-2	●	●	●		●	●														
ПРН-3	●	●	●		●	●														
ПРН-4	●	●	●		●	●														
ПРН-5	●	●	●		●	●														
ПРН-6	●	●	●		●	●														
ПРН-7	●								●											
ПРН-8	●								●											
ПРН-9	●								●		●	●	●			●	●		●	●
ПРН-10	●									●									●	
ПРН-11	●									●									●	
ПРН-12	●								●						●		●			●
ПРН-13	●								●	●	●	●	●			●	●		●	●
ПРН-14	●									●	●		●			●		●	●	
ПРН-15	●									●	●								●	
ПРН-16	●								●						●		●			●
ПРН-17	●									●	●		●			●			●	
ПРН-18	●									●	●		●			●			●	
ПРН-19	●									●	●		●	●		●			●	
ПРН-20	●										●									
ПРН-21	●												●						●	
ПРН-22	●												●						●	
ПРН-23	●										●		●	●					●	
ПРН-24	●												●						●	
ПРН-25	●												●						●	
ПРН-26	●												●						●	
ПРН-27	●										●			●						
ПРН-28	●																			●
ПРН-29	●								●			●	●			●	●			●
ПРН-30	●																			●
ПРН-31	●										●			●						
ПРН-32	●										●		●			●			●	
ПРН-33	●								●			●	●			●	●			●

ПРН-34	●								●			●	●			●	●			●
ПРН-35	●								●			●	●		●	●	●			●
ПРН-36	●																	●		
ПРН-37	●																	●		
ПРН-38	●																	●		
ПРН-39	●																	●		
ПРН-40	●																	●		
ПРН-41	●										●		●			●			●	
ПРН-42	●								●		●	●	●			●	●		●	●
ПРН-43	●								●		●	●	●			●	●		●	●
ПРН-44	●								●			●	●			●	●			●
ПРН-45	●								●			●	●			●	●			●
ПРН-46	●								●			●	●			●	●			●
ПРН-47	●									●								●		
ПРН-48	●										●		●			●		●	●	
ПРН-49	●										●		●	●		●			●	
ПРН-50	●										●		●			●			●	
ПРН-51	●										●		●			●			●	
ПРН-52	●									●	●		●	●		●			●	
ПРН-53	●										●									
ПРН-54	●		●				●	●												

VI. Матриця відповідності програмних компетентностей освітнім компонентам освітньої програми

Освітні компоненти	Компетентності																			
		Загальні компетентності							Спеціальні компетентності											
	ІК	ЗК-1	ЗК-2	ЗК-3	ЗК-4	ЗК-5	ЗК-6	ЗК-7	СК-1	СК-2	СК-3	СК-4	СК-5	СК-6	СК-7	СК-8	СК-9	СК-10	СК-11	СК-12
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	●	●	●																	

VII. Матриця відповідності програмних результатів навчання компонентам освітньої програми

Освітні компоненти	Програмні результати навчання																	
	ПРН 1	ПРН 2	ПРН 3	ПРН 4	ПРН 5	ПРН 6	ПРН 7	ПРН 8	ПРН 9	ПРН 10	ПРН 11	ПРН 12	ПРН 13	ПРН 14	ПРН 15	ПРН 16	ПРН 17	ПРН 18
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	●				●	●												

Освітні компоненти	Програмні результати навчання																	
	ПРН 19	ПРН 20	ПРН 21	ПРН 22	ПРН 23	ПРН 24	ПРН 25	ПРН 26	ПРН 27	ПРН 28	ПРН 29	ПРН 30	ПРН 31	ПРН 32	ПРН 33	ПРН 34	ПРН 35	ПРН 36
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																		
	Програмні результати навчання																	

Освітні компоненти	ПРН 37	ПРН 38	ПРН 39	ПРН 40	ПРН 41	ПРН 42	ПРН 43	ПРН 44	ПРН 45	ПРН 46	ПРН 47	ПРН 48	ПРН 49	ПРН 50	ПРН 51	ПРН 52	ПРН 53	ПРН 54
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																		