

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТУСА

ЗАТВЕРДЖЕНО

Вченою радою ДонНУ
імені Василя Стуса
Протокол № 17 від 29.05.2026

ВВЕДЕНО В ДІЮ

Наказ АР/01/02 від 29.05.2026
Ректор
Філія ХАДЖИНОВ



ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ/
CYBER SECURITY AND DATA PROTECTION

РІВЕНЬ ВИЩОЇ ОСВІТИ	ПЕРШИЙ
СТУПІНЬ ВИЩОЇ ОСВІТИ	БАКАЛАВР
ГАЛУЗЬ ЗНАНЬ	F ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
СПЕЦІАЛЬНІСТЬ	F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ F5 CYBER SECURITY AND DATA PROTECTION

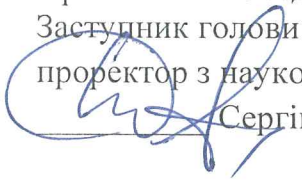
**ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
(КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ /
CYBER SECURITY AND DATA PROTECTION)**

РЕКОМЕНДОВАНО

Радою з якості з вищої освіти ДонНУ
імені Василя Стуса

Протокол №10 від 27.05.2026

Заступник голови Ради з якості,
проректор з наукової роботи

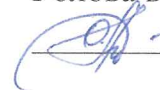
 Сергій РАДІО

РЕКОМЕНДОВАНО

Вченою радою факультету
інформаційних і прикладних
технологій

Протокол № 12 від 20.05.2026

Голова вченої ради

 Ольга АНІСІМОВА

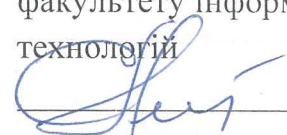
Експерт з якості

F5 Кібербезпека та захист інформації

 Алла Луценко

В.о. декана

факультету інформаційних та прикладних
технологій

 Сергій СЕГЕДА

ІНІЦІЙОВАНО:

Кафедрою прикладної математики
та кібербезпеки

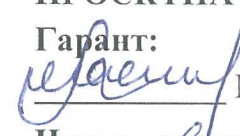
протокол № 18 від 13.05.2026 р.

В.о. завідувача кафедри
прикладної математики та кібербезпеки

 Алла ЛУЦЕНКО

ПРОЄКТНА ГРУПА

Гарант:

 Михайло ПРОКОФЬЄВ

Члени групи:

 Любов ЗАГОРУЙКО

 Дмитро ЧЕРНОВ

РЕЦЕНЗЕНТИ ОСВІТНЬОЇ ПРОГРАМИ:

Начальник ВПК у Вінницькій області Департаменту кіберполіції НПУ України,
підполковник

Олександр УЛЬЯНЕНКОВ

Директор департаменту інформаційних технологій Вінницької міської ради

Володимир РОМАНЕНКО

Директор ТОВ «Об'єднаний центр захисту інформації»

Борис РАЙСЬКИЙ

Доктор фіз.-мат. наук, професор, головний науковий співробітник ТОВ
«Об'єднаний центр захисту інформації»

Михайло ДІВІЗІНІОК

Доктор техн. наук, професор, професор кафедри захисту інформації
Національного університету «Львівська політехніка»

Галина МИКИТИН

І. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

1. Загальна характеристика	
Повна назва ЗВО	Донецький національний університет імені Василя Стуса Vasyl' Stus Donetsk National University, Ukraine
Рівень вищої освіти	Перший (бакалаврський) рівень
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.
Рівень програми	НРК України – 6 рівень, FQ ENEA – First cycle, EQF LLL – 6 рівень, рівень освіти – перший (бакалаврський)
Форми здобуття освіти	Денна
Освітня кваліфікація	Бакалавр з кібербезпеки та захисту інформації
Галузь знань	F Інформаційні технології
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – F5 Кібербезпека та захист інформації Освітня програма – Кібербезпека та захист інформації
Додаткові вимоги до правил прийому	Немає
Опис предметної області	Об'єкти вивчення: – технології кібербезпеки та захисту інформації; – процеси управління кібербезпекою та захистом інформації: об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. Теоретичний зміст предметної області: Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Методи, методики та технології: Методи, методики та інші технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. Інструменти та обладнання: засоби, пристрої, мережеве устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Академічні права випускників	Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
Придатність працевлаштування	На посаді у структурних підрозділах установ/підприємств/організацій, які передбачають наявність

	вищої освіти зі спеціальності F5 Кібербезпека та захист інформації
Вимоги до рівня осіб, які можуть розпочати навчання за освітніми програмами відповідно спеціальності, та їх результатів навчання	Для здобуття освітнього рівня бакалавра зі спеціальності F5 Кібербезпека та захист інформації можуть вступати особи, які здобули повну загальну середню освіту. Прийом на основі здобутого ступеня молодшого бакалавра або освітньо-кваліфікованого рівня молодшого спеціаліста здійснюється в порядку, визначеному законодавством.
2. Мета програми	
Метою ОП є підготовка затребуваних фахівців, які здатні розв'язувати типові задачі за спеціальністю, вирішувати практичні проблеми в галузі інформаційної безпеки, використовувати і впроваджувати технології інформаційної та кібербезпеки. Відповідно до Пріоритетів розвитку Університету, ОП зорієнтована: - на підготовку високоінтелектуального універсального фахівця, здатного до застосування математичного апарату, використання інформаційних технологій та засобів кібербезпеки, що є суттєвою конкурентною перевагою на ринку праці та диверсифікує можливості працевлаштування; - формування особистості, що поєднує загальнолюдські і національні цінності, консолідує українську націю, просуває Україну в світі як незламну, соборну, непереможну.	
3. Характеристика програми	
Фокус програми: загальна/спеціальна	Загальна
Особливості програми	Особливість програми: – акцент на підготовці фахівців, здатних до використання технологій розробки кіберстійких інформаційно-комунікаційних систем; • націленість на вирішення проблем безпеки системи Інтернету речей та кіберфізичних систем; • прикладна спрямованість математичних дисциплін у сфері інформаційної та/або кібербезпеки; • орієнтованість на бізнес і потреби регіону.
Працевлаштування	Професії, на підготовку з яких спрямована ОП (відповідно до Державного класифікатора професій ДК 003:2010, а також з врахуванням нових професійних стандартів): - адміністратор безпеки мереж і систем, 2139.2 - фахівець сфери захисту інформації, 2139.2 - фахівець з систем безпеки (інформаційно-комунікаційні технології), 2139.2 - конструктор систем кібербезпеки, 2139.2 - фахівець з підтримки інфраструктури кіберзахисту, 2139.2 - фахівець з реагування на інциденти кібербезпеки, 2139.2 - фахівець з криптографічного захисту інформації, 2139.2 - фахівець з технічного захисту інформації, 2139.2 - фахівець з тестування систем захисту інформації, 2139.2 - аудитор інформаційних технологій (з кібербезпеки), 2139.2 - фахівець з оцінки заходів захисту інформації (кібербезпеки), 2139.2
4. Стиль та методика навчання	
Підходи до викладання та навчання	Студентоцентроване, інтерактивне, проблемно-орієнтоване навчання, навчання під керівництвом викладача, самостійне та індивідуальне навчання, практичне навчання.

	Викладання проводиться у вигляді лекцій, мультимедійних лекцій, семінарів, практичних занять, лабораторних робіт, самостійного навчання, індивідуальних занять, онлайн-консультацій. Здобувачам забезпечено широкі можливості для формування індивідуальної освітньої траєкторії за рахунок програм мініор (надає додаткову кваліфікацію з інших галузей та/або спеціальностей); сертифікатних освітніх програм (спрямована на набуття Soft skills); набору вибіркових ОК (практики, курсові роботи, навчальні дисципліни тощо).
Система оцінювання	Визначена «Порядком оцінювання знань здобувачів вищої освіти у Донецькому національному університеті імені Василя Стуса». Методи оцінювання: усні та письмові екзамени, захист звітів з практик, наукова робота здобувача, виконання індивідуального завдання / проекту, усне опитування, письмовий контроль (у тому числі електронний).
5. Перелік компетентностей випускника	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності. ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК4. Здатність спілкуватися іноземною мовою. ЗК5. Здатність вчитися і оволодівати сучасними знаннями. 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 ухвалювати рішення й діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. ЗК8. 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. ЗК9. Здатність до прояву національно-патріотичної свідомості, громадянської стійкості та набуття комплексну теоретичних знань і практичних навичок, необхідних для виконання конституційного обов'язку щодо захисту Вітчизни, незалежності та територіальній цілісності України.
Спеціальні (фахові, предметні) компетентності	СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності. СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та систем захисту інформації.

	СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
--	--

6. Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання

- РН1.** Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
- РН2.** Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
- РН3.** Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
- РН4.** Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язування складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
- РН5.** Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
- РН6.** Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
- РН7.** Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
- РН8.** Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
- РН9.** Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
- РН10.** Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
- РН11.** Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації.

- РН12.** Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
- РН13.** Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.
- РН14.** Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.
- РН15.** Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
- РН16.** Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
- РН17.** Забезпечувати функціонування систем управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
- РН18.** Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
- РН19.** Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
- РН20.** Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
- РН21.** Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.
- РН22.** Володіння базовими знаннями щодо структури, завдань і функцій національного спротиву та вміння застосовувати їх на практиці.

7. Ресурсне забезпечення реалізації програми

Кадрове забезпечення	Кадрове забезпечення освітньо-професійної програми включає науково-педагогічних працівників кафедри прикладної математики та кібербезпеки, а також інших кафедр Університету, які володіють досвідом та компетентностями, що дозволяють сформувати програмні результати навчання за освітніми компонентами ОП. Гарант, члени проектної групи та групи забезпечення відповідають вимогам, які визначені Ліцензійними умовами провадження освітньої діяльності. До викладання професійних дисциплін залучаються професіонали-практики, які працюють у галузі кібербезпеки та захисту інформації. Всі науково-педагогічні працівники, задіяні у викладанні, мають підтверджений рівень наукової і професійної активності, більшість з яких є штатними співробітниками університету, мають наукові ступені та вчені звання.
Матеріально-технічне забезпечення	Освітній процес за ОП здійснюється на базі навчального корпусу № 1 у м. Вінниця, за адресою вул. 600-річчя, 21. Для забезпечення належної якості навчального процесу за ОП лекційні аудиторії обладнані дошками для письма та проекційною технікою (4

		проектори), навчальні лабораторії обладнані спеціальними навчальними установками та комп'ютерами, що об'єднані в локальну мережу, оснащені відповідним програмним забезпеченням та підключенням до Інтернету. Спеціалізована навчальна кіберлабораторія облаштована в рамках реалізації проекту USAID Кібербезпека. Бібліотека університету, яка під'єднана до системи WebIrbis 2.0, постійно поповнюється літературою, методичними виданнями ДонНУ імені Василя Стуса.
Інформаційне та навчально-методичне забезпечення		Інформаційний пакет (розміщено на офіційному сайті Університету) https://www.donnu.edu.ua/uk/informatsiyniy-paket/ Інформаційне забезпечення включає доступ до: - онлайн-бібліотеки Університету; - електронної бази наукових журналів та електронних бібліотечних ресурсів світу. Навчально-методичне забезпечення включає: - робочі програми практичної підготовки; - посібники (навчальні, навчально-методичні), конспекти лекцій; - методичні вказівки до написання та захисту курсових робіт, до лабораторних та практичних занять, щодо організації самостійної роботи здобувачів освіти; - інші навчально-методичні матеріали. Всі навчально-методичні матеріали розміщено на дистанційній платформі Moodle та на OneDrive (з наданням доступу здобувачам освіти).
8. Академічна мобільність		
Національна мобільність	кредитна	Реалізується в ДонНУ імені Василя Стуса відповідно до вимог чинного законодавства та регулюється внутрішніми локальними документами: Положенням про реалізацію права на академічну мобільність в ДонНУ імені Василя Стуса, Положенням про організацію освітньої діяльності в ДонНУ імені Василя Стуса. Перезарахування отриманих кредитів на основі Європейської кредитно-трансферної системи (ЄКТС), отриманих під час участі здобувача вищої освіти у програмах національної академічної мобільності відбувається шляхом порівняння змісту навчальних програм та з урахуванням програмних результатів навчання здобутих студентом. Здобувачі вищої освіти освітньо-професійної програми Кібербезпека та захист інформації в межах співпраці Університету з провідними закладами вищої освіти України мають право впродовж окремих семестрів навчатися в інших ЗВО, проходити фахові стажування та фахові тренінги в профільних організаціях.
Міжнародна мобільність	кредитна	Міжнародна кредитна мобільність здійснюється згідно з вимогами чинного законодавства та регулюється внутрішніми локальними документами: Положенням про реалізацію права на академічну мобільність в ДонНУ імені Василя Стуса, Положенням про організацію освітньої діяльності в ДонНУ імені Василя Стуса, а також відповідно до укладених договорів про співробітництво Університету з іноземними закладами вищої освіти – партнерами. Перезарахування отриманих кредитів на основі Європейської кредитно-трансферної системи (ЄКТС) шляхом порівняння змісту навчальних програм та з урахуванням програмних результатів навчання здобутих здобувачем вищої освіти.

Навчання іноземних здобувачів вищої освіти	Не передбачено.
---	-----------------

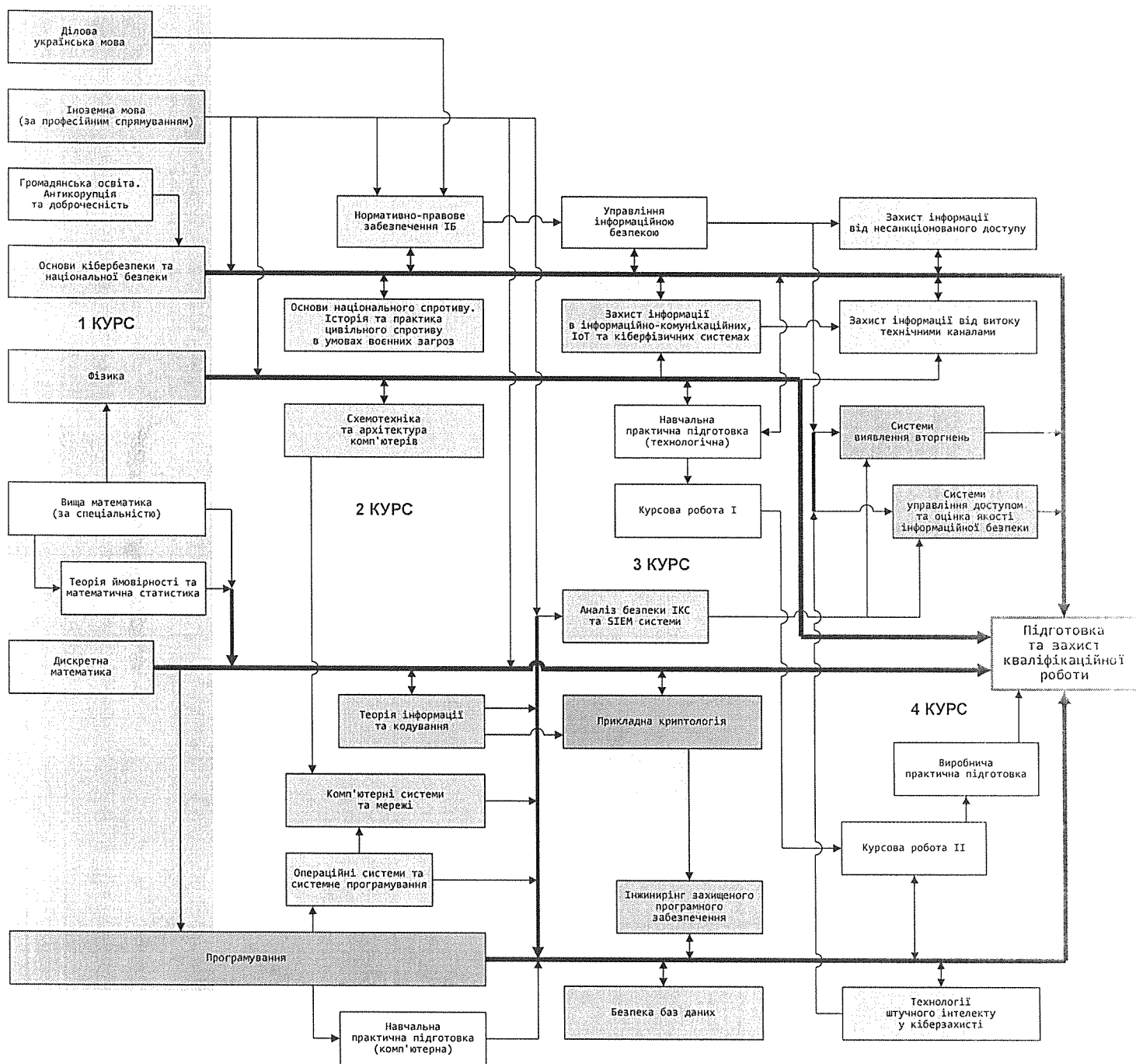
II. КАТАЛОГ КОМПОНЕНТІВ ОСВІТНЬОЇ ПРОГРАМИ ТА ЇЇ ЛОГІКО-СТРУКТУРНА СХЕМА

Код	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Дисципліни професійної та практичної підготовки			
ОК-1	Громадянська освіта. Антикорупція та доброчесність.	4	Залік
ОК-2	Ділова українська мова	3	Залік
ОК-3	Дискретна математика	4	Екзамен
ОК-4	Іноземна мова (за професійним спрямуванням)	5	Залік
ОК-5	Фізика	8	Залік, залік
ОК-6	Вища математика (за спеціальністю)	9	Екзамен, екзамен
ОК-7	Програмування	14	Екзамен, екзамен, екзамен, екзамен
ОК-8	Основи кібербезпеки та національної безпеки	6	Екзамен, екзамен
ОК-9	Теорія ймовірності та математична статистика	4	Екзамен
ОК-10	Основи національного спротиву/Історія та практика цивільного спротиву в умовах воєнних загроз	5	Диф. залік
ОК-11	Комп'ютерні системи та мережі	7	Залік, екзамен
ОК-12	Схемотехніка та архітектура комп'ютерів	6	Залік, екзамен
ОК-13	Операційні системи та системне програмування	4	Екзамен
ОК-14	Теорія інформації та кодування	4	Екзамен
ОК-15	Нормативно-правове забезпечення ІБ	4	Екзамен
ОК-16	Навчальна практична підготовка (комп'ютерна)	3	Диф. залік
ОК-17	Безпека баз даних	8	Залік, екзамен
ОК-18	Управління інформаційною безпекою	4	Екзамен
ОК-19	Прикладна криптологія	8	Екзамен, екзамен
ОК-20	Аналіз безпеки ІКС та SIEM системи	4	Екзамен
ОК-21	Інжинирінг захищеного програмного забезпечення	4,5	Залік
ОК-22	Захист інформації в інформаційно-комунікаційних, IoT та кіберфізичних системах	7	Залік, екзамен
ОК-23	Курсова робота з дисциплін професійної підготовки	3	Диф. Залік, диф. залік
ОК-24	Навчальна практична підготовка (технологічна)	3	Диф. залік
ОК-25	Системи виявлення вторгнень	5	Залік
ОК-26	Системи управління доступом та оцінка якості інформаційної безпеки	5	Залік
ОК-27	Захист інформації від несанкціонованого доступу	9	Залік, екзамен
ОК-28	Захист інформації від витоку технічними каналами	7	Залік, екзамен
ОК-29	Технології штучного інтелекту у кіберзахисті	7,5	Залік, екзамен
ОК-30	Виробнича практична підготовка	6	Диф. залік
ОК-31	Підготовка та захист кваліфікаційної роботи	9	Захист
Загальний обсяг компонентів професійної та практичної підготовки		180	
Дисципліни за вибором здобувача вищої освіти			
	Дисципліна за вибором (з переліку світоглядних дисциплін) (2 семестр)	5	Залік
	Дисципліна за вибором (з переліку практико-орієнтованих дисциплін) (2 семестр)	5	Залік

Цикл дисципліни за вибором здобувача вищої освіти			
Варіант 1	Програма MINOR		
	Дисципліна 1,2	10	Залік
	Дисципліна 3,4	10	Залік
	Дисципліна 5,6	10	Залік
	Дисципліна 7,8	10	Залік
	Дисципліна 9	5	Залік
	Дисципліна 10	5	Залік
Разом		50	
Варіант 2	СЕРТИФІКАТНА ОСВІТНЯ ПРОГРАМА + набір вибіркового дисциплін)		
	Дисципліна 1,2	10	Залік
	Дисципліна 3,4	10	Залік
	Дисципліна 5	5	Залік
	Дисципліна 6	5	Залік
	Дисципліни з переліку*	10	Залік
	Дисципліни з переліку*	10	Залік
Разом		50	
Варіант 3	Набір вибіркового дисциплін		
	Дисципліни з переліку*	10	Залік
	Дисципліни з переліку*	10	Залік
	Дисципліни з переліку*	10	Залік
	Дисципліни з переліку*	10	Залік
	Дисципліни з переліку*	10	Залік
Разом		50	
Загальний обсяг дисциплін за вибором здобувача вищої освіти		63	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

* переліки дисциплін формуються за поданням кафедр університету щорічно, затверджуються Радою з якості вищої освіти університету.

ЛОГІКО-СТРУКТУРНА СХЕМА ПІДГОТОВКИ ФАХІВЦЯ



ІІІ. ВИЗНАЧЕННЯ ФОРМ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ЗА ОСВІТНЬОЮ ПРОГРАМОЮ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту (ЄДКІ) та формі публічного захисту кваліфікаційної роботи.
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом (Наказ №1547 від 29.10.2024 р.) та цією освітньою програмою.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має передбачати вирішення складного спеціалізованого завдання або практичної проблеми в галузі комп'ютерних наук, яке характеризується комплексністю та невизначеністю умов і потребує застосування теорій та методів і засобів інформаційних технологій. У кваліфікаційній роботі не має бути академічного плагіату, фальсифікації та фабрикації. Кваліфікаційна робота має бути оприлюднена у репозитарії Донецького національного університету імені Василя Стуса. Оприлюднення кваліфікаційних робіт, що містять інформацію з обмеженим доступом, має здійснюватися у відповідності до вимог чинного законодавства.

ІV. ВИМОГИ ДО НАЯВНОСТІ СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

Процедури і заходи забезпечення якості освіти	Відповідно до Стратегії розвитку Донецького національного університету імені Василя Стуса 2017 – 2025 рр. одним з наскрізних завдань є забезпечення якості вищої освіти. Оновленою Стратегією розвитку Донецького національного університету імені Василя Стуса 2017 – 2025 рр. (наказ 202/05 від 01.09.2022) визначено, що одним з наскрізних завдань є забезпечення якості вищої освіти, що відповідає пріоритетам розвитку, а саме: 1. Прагматизація освітньої діяльності з метою забезпечення якості людського капіталу України. 2. Зміцнення Університету як науково-інноваційного простору реалізації можливостей і створення суспільних благ. На виконання пункту 3 статті 41 Закону України «Про освіту» №2145-19 від 5 вересня 2017 року в рамках внутрішнього забезпечення якості освіти в Університеті затверджено Положення про систему заходів внутрішнього забезпечення якості вищої освіти в Донецькому національному університеті імені Василя Стуса та відповідно цими документами передбачено: моніторинг та перегляд ОП, оцінювання здобувачів освіти, забезпечення якості кадрового складу, забезпечення ресурсів для організації навчального процесу, забезпечення інформаційних систем для ефективного управління освітньою діяльністю, забезпечення публічності і прозорості інформації, забезпечення ефективної системи запобігання та виявлення плагіату в наукових дослідженнях науково-педагогічних працівників та здобувачів вищої освіти університету.
--	--

	В Університеті функціонує Рада з якості вищої освіти, діяльність якої регулюється відповідним Положенням та має на меті успішне впровадження системи внутрішнього забезпечення якості вищої освіти задля досягнення стратегічних пріоритетів Університету. Окрім того, кафедра ініціює та проводить громадські обговорення освітньої програми зі стейкхолдерами (роботодавцями, викладачами, здобувачами) та враховує висловлені зауваження.
Моніторинг та періодичний перегляд освітніх програм	Моніторинг та періодичний перегляд освітніх програм проводиться відповідно до локальних нормативних документів Університету. Процедури розроблення, затвердження, моніторингу та періодичного перегляду ОП регламентуються «Положенням про освітню програму у Донецькому національному університеті імені Василя Стуса» та «Положенням про організацію освітньої діяльності у Донецькому національному університеті імені Василя Стуса». Крім того, в Університеті запроваджене щосеместрове опитування здобувачів вищої освіти щодо якості освітнього процесу та якості викладання навчальних дисциплін. Опитування проводиться за допомогою онлайн сервісів, зокрема автоматизованої системи опитувань «ФОРУМ». Результати опитування обов'язково враховуються при перегляді існуючих та формуванні нових ОП усіх рівнів.
Оцінювання здобувачів вищої освіти	Оцінювання навчальних досягнень здобувачів здійснюється відповідно до «Порядку оцінювання знань здобувачів вищої освіти у Донецькому національному університеті імені Василя Стуса». Обов'язковим є ознайомлення здобувачів вищої освіти з видами роботи та критеріями оцінювання з кожної дисципліни на початку семестру, що забезпечує прозорість та співвідповідальність викладача та здобувача в процесі навчання та оцінювання результатів навчання.
Підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників	Згідно з «Положенням про підвищення кваліфікації науково-педагогічних та педагогічних працівників у Донецькому національному університеті імені Василя Стуса» всі викладачі, які залучені до реалізації освітнього процесу в рамках ОП, пройшли підвищення кваліфікації впродовж останніх п'яти років. Положення регулює усі формальні аспекти підвищення кваліфікації, в тому числі професійного розвитку викладачів. Крім того, Університет підтримує та заохочує участь викладачів у внутрішньокорпоративних програмах навчання та підвищення кваліфікації (наприклад, «Майстерня «Teaching Art»), Школа управління змінами»).
Наявність інформаційних систем для ефективного управління освітнім процесом	В Університеті функціонує єдина інформаційна система управління, як програмно-апаратний комплекс, що забезпечує низку основних функцій роботи з документами та базами даних в електронному вигляді з використанням хмарних технологій, спеціалізованого програмного забезпечення та ІТ-сервісів Офіс-365. В усіх навчальних корпусах забезпечений доступ до мережі Інтернет завдяки технології Wi-Fi. Автоматизація основних функцій управління освітнім процесом запроваджено на базі програмно-технологічного комплексу АС «Деканат».

	Окремо здійснюється періодичний аналіз щодо відповідності ліцензійним умовам, підсистеми збору, обробки та збереження інформації в «Єдиній електронній базі даних з питань освіти».
Публічність інформації про освітні програми, ступені вищої освіти та кваліфікації	З метою забезпечення інформаційної відкритості університету та виконання вимог законів України «Про освіту» та «Про вищу освіту», на офіційному сайті університету створений спеціальний розділ «Інформаційна відкритість», в якому зібрано посилання на всі публічні документи та публічну інформацію. Інформацію про ОП, ступені вищої освіти та кваліфікації розміщено на офіційних веб-ресурсах Університету та відділу аспірантури та докторантури, а також на цих ресурсах проводиться громадське обговорення проєктів ОП.
Забезпечення дотримання академічної доброчесності працівниками закладів вищої освіти та здобувачами вищої освіти, у тому числі запобігання та виявлення академічного плагіату	Забезпечення дотримання академічної доброчесності учасниками освітнього процесу регламентується Кодексом академічної доброчесності та корпоративної етики. Органом, що здійснює контроль за дотриманням академічної доброчесності учасниками освітнього процесу в Університеті є Комісія з академічної доброчесності та корпоративної етики. Результати роботи Комісії регулярно оприлюднюються на офіційних ресурсах Університету. Для запобігання та виявлення плагіату в наукових дослідженнях працівників та здобувачів вищої освіти в Університеті діє система запобігання та виявлення плагіату з широким використанням спеціалізованого програмного забезпечення. Запроваджена посада Омбудсмена з захисту прав здобувачів та його представників на факультетах.

Зведена таблиця фахових компетентностей та результатів навчання

Спеціальні (фахові) компетентності	Результати навчання
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності.	РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та систем захисту інформації.	РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.	РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.	РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.
СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.	РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).	РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.	РН17. Забезпечувати функціонування систем управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.	РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.	РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.	РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Матриця відповідності результатів навчання та компетентностей

[illegible]

Матриця відповідності компетентностей освітнім компонентам програми

Освітні компоненти	Інтегральна компетентність	Компетентності																			
		Загальні компетентності										Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	
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	+				+					+	+			+			+			+	

Освітні компоненти	Інтегральна компетенція	Компетентності																		
		Загальні компетентності									Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
ОК 27	+	+	+							+	+								+	
ОК 28	+		+								+	+			+	+		+	+	+
ОК 29	+		+								+	+	+						+	+
ОК 30	+		+								+	+	+	+			+			+
ОК 31	+	+	+	+							+	+	+		+				+	
ОК 32	+		+								+	+					+		+	

Матриця відповідності результатів навчання освітнім компонентам програми

Освітні компоненти	Результати навчання																			
	PH 1	PH 2	PH 3	PH 4	PH 5	PH 6	PH 7	PH 8	PH 9	PH 10	PH 11	PH 12	PH 13	PH 14	PH 15	PH 16	PH 17	PH 18	PH 19	PH 20
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				+					+	+	+		+		+	+	+			+

Результати навчання		Освітні компоненти	
ОК 27	РН 1		
ОК 28	РН 2		
ОК 29	РН 3	+	
ОК 30	РН 4	+	
ОК 31	РН 5		+
ОК 32	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		

Матриця відповідності визначених Стандартом компетентностей дескрипторам НРК

Класифікація компетентностей (результатів навчання за НРК)	Знання Зн1. Концептуальні наукові та практичні знання. Зн2. Критичне осмислення теорій, принципів, методів і понять у сфері професійної діяльності та/або навчання.	Уміння Ум1. Поглиблені когнітивні та практичні уміння/навички, майстерність та інноваційність на рівні, необхідному для розв'язання складних спеціалізованих задач і практичних проблем у сфері професійної діяльності або навчання.	Комунікація К1. Донесення до фахівців і нефахівців інформації, ідей, проблем, рішень, власного досвіду та аргументації. К2. Збір, інтерпретація та застосування даних. К3. Спілкування з професійних питань, у тому числі іноземною мовою, усно та письмово.	Відповідальність та автономія АВ1. Управління складною технічною або професійною діяльністю чи проектами. АВ2. Спроможність нести відповідальність за вироблення та ухвалення рішень у непередбачуваних робочих та/або навчальних контекстах. АВ3. Формування суджень, що враховують соціальні, наукові та етичні аспекти. АВ4. Організація та керівництво професійним розвитком осіб та груп. АВ5. Здатність продовжувати навчання із значним ступенем автономії.
ЗК1	Зн2	Ум1		
ЗК2	Зн2	Ум1	К1	
ЗК3			К1, К3	
ЗК4			К1, К3	
ЗК5	Зн1, Зн2	Ум1	К2	АВ3
ЗК6	Зн1		К1	АВ2, АВ3, АВ4
ЗК7			К1	АВ2
ЗК8	Зн2		К2	АВ3
СК1	Зн1, Зн2	Ум1	К2	
СК2		Ум1	К2	

CK3			Y _{M1}			AB1
CK4			Y _{M1}			AB1
CK5			Y _{M1}		K2	AB1, AB2
CK6			Y _{M1}		K1	AB1
CK7			Y _{M1}		K1	AB1
CK8		3H2	Y _{M1}			
CK9		3H2	Y _{M1}			
CK10			Y _{M1}		K2	AB2