



Міністерство освіти і науки України

**ДНІПРОВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЗАЛІЗНИЧНОГО ТРАНСПОРТУ
імені академіка В. ЛАЗАРЯНА**

Схвалено

Вченою радою університету

«02» 07 2020 р. протокол № 10

Голова вченої ради



Ректор

О. М. Пшінько

Надано чинності та
введено в дію
наказом ректора

від «07» 07 2020 р.

№ 19

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

назва «Кібербезпека»

другого (магістерського) рівня вищої освіти

спеціальність 125 Кібербезпека
(код та назва)

галузь знань 12 Інформаційні технології
(шифр та назва)

кваліфікація Магістр з кібербезпеки

Дніпро–2020

АРКУШ ПОГОДЖЕННЯ

освітньо-професійної програми

другого (магістерського) рівня вищої освіти

(рівень вищої освіти: перший (бакалаврський) або другий (магістерський))

«Кібербезпека»

(назва освітньо-професійної програми)

1 Вчена рада факультету «Комп'ютерні технології і системи»

«04» 03 2020 р.

Голова вченої ради, проф.

протокол № 5

Векант
(підпис)

В.В. Скалозуб
ПІБ

2 Голова комісії ВР

«02» 07 2020 р.

Костін
(підпис)

М.О. Костін
ПІБ

3 Навчально-методичний відділ

Начальник НМВ

«02» 07 2020 р.

Казаріна
(підпис)

Л.С. Казаріна
ПІБ

4 Перший проректор, проф.

«02» 07 2020 р.

Б. Є. Боднар
(підпис)

Б. Є. Боднар
ПІБ

ПЕРЕДМОВА
освітньо-професійної програми
«Кібербезпека»
другого (магістерського) рівня вищої освіти

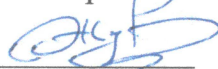
1 ВНЕСЕНО

Кафедрою «Електронні обчислювальні машини»

«03» 03 2020р.

протокол № 8

Завідувач кафедри, проф.

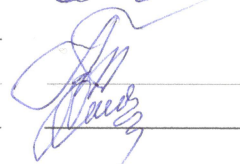
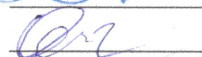


І.В. Жуковицький

(підпис)

2 Розробники програми:

1. Жуковицький І.В., д.т.н, проф., зав. кафедрою ЕОМ – гарант
2. Остапець Д.О., к.т.н, доц., доцент кафедри ЕОМ
3. Тараскін Г.О., головний інженер ВП «ДВ» філії «ГІОЦ»
ПАТ «Укрзалізниця»
4. Биковська Д.Г., студентка групи КБ1921



3 До ОПП надані такі рецензії-відгуки

1. Гиря А.О. – Начальник виробничого підрозділу «Дніпровське відділення»
філії «Головний ІОЦ» ПАТ «Укрзалізниця»
2. Чепіжко С.П. – Заступник директора філії «ІКТБ ІТ» ПАТ «Укрзалізниця»
3. Городецький О.О. – в.о. керівника Напрямку інформаційної безпеки
АТ КБ «Приватбанк»
4. Мусієнко М.І. – студент групи КБ1921

1. Профіль освітньо-професійної програми
спеціальність 125 Кібербезпека
назва «Кібербезпека»

1.1 - Загальна інформація	
Повна назва закладу вищої освіти	Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Кваліфікація – Магістр з кібербезпеки
Офіційна назва освітньої програми	ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА другого (магістерського) рівня вищої освіти Галузь знань 12 Інформаційні технології Спеціальність 125 Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, кредитів ЄКТС - 90, термін навчання 1 рік 4 місяці
Наявність акредитації	Міністерство освіти і науки України, Національне агентство із забезпечення якості вищої освіти 2020-2021 рр.
Рівень	НРК України - 8 рівень / другий (магістерський) рівень
Передумови	Вимоги щодо попередньої освіти. • Диплом бакалавра за ОПП «Кібербезпека» • Решта вимог визначаються правилами прийому на освітньо-професійну програму магістра
Мова(и) викладання	Українська мова
Термін дії освітньої програми	Щорічний аналіз діяльності за ОПП, кожні 2-3 роки доопрацювання та затвердження
Інтернет-адреса постійного розміщення опису освітньої програми	http://pk.diit.edu.ua/?view=static&id=49
1.2 - Мета освітньої програми	
Мета (цілі): забезпечення високого рівня підготовки здобувачів освіти у сфері кібербезпеки шляхом формування компетентностей, що необхідні для виконання професійних обов'язків в рамках професійної діяльності у складі колективу з урахуванням особливостей майбутньої професії і можливих первинних посад магістра з кібербезпеки.	
1.3 - Характеристика освітньої програми	
Предметна область	Об'єктами професійної діяльності магістра є: математичне, алгоритмічне, програмне та апаратне забезпечення, яке забезпечує безпеку роботи комп'ютерних систем та мереж. Цілями навчання є: формування компетентностей (загальних 11, фахових 15, та 20 програмних результатів навчання), що необхідні для виконання професійних обов'язків у галузі кібербезпеки в рамках професійної діяльності у складі колективу з урахуванням особливостей майбутньої професії і можливих первинних посад магістра з кібербезпеки. Обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти на базі ОС бакалавра становить 90 кредитів, загальна підготовка становить 12

	кредитів (13,33%), професійна підготовка – 78 кредитів (86,67%).
Орієнтація освітньої програми	Освітньо-професійна з елементами наукової компоненти. Види професійної діяльності , до виконання яких готуються випускники, що освоїли програму магістра: науково-дослідна, науково-педагогічна, проектно-технологічна; виробничо-технологічна; організаційно-управлінська; інноваційна.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта в галузі «Інформаційні технології» за спеціальністю «Кібербезпека». Ключові слова: • Апаратні засоби забезпечення безпеки комп'ютерних систем та мереж; • Програмні засоби забезпечення безпеки комп'ютерних систем та мереж; • Інформаційна безпека комп'ютерних систем та мереж.
Особливості програми	Підготовка висококваліфікованих фахівців для роботи в галузі 12 «Інформаційні технології», враховуючи потреби організацій, промислових підприємств, підприємств транспорту, науково-дослідних та освітніх закладів Придніпровського регіону, України та інших країн. Системний підхід до підготовки магістрів, інтеграції класичних методів освіти та практичного досвіду.
1.4. Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Назви професій згідно з Національним класифікатором професій України (ДК 003:2010): 2 Професіонали 21 Професіонали в галузі фізичних, математичних та технічних наук 213 Професіонали в галузі обчислень (комп'ютеризації) 2131 Професіонали в галузі обчислювальних систем Інженер з захисту інформації 2131.2 Конструктор систем захисту інформації 2132 Професіонали в галузі програмування 2132.2 Розробники комп'ютерних програм захисту інформації http://www.dk003.com/?code=2132.2&list=2132.2 - 2132.2 2139 Професіонали в інших галузях обчислень (комп'ютеризації) 2139.2 Професіонали в інших галузях обчислень http://www.dk003.com/?code=2139.2&list=2139.2 - 2139.2
Подальше навчання	Можливість навчання за PhD-програмою за цією або суміжною галуззю знань (що узгоджується з отриманим дипломом магістра)
1.5. Викладання та оцінювання	
Викладання та навчання	Студентоцентризоване навчання, проблемно-орієнтоване навчання, самонавчання на основі інформаційних

	технологій дистанційного навчання. Основними формами організації навчального процесу є лекції, мультимедійні лекції, семінари, практичні заняття, лабораторні роботи, консультації, курсове проектування, самостійна робота (зокрема, з використанням технології дистанційного online навчання), виробнича практика, підготовка та захист кваліфікаційної магістерської роботи.
Оцінювання	<i>Види оцінювання:</i> поточний, семестровий, підсумковий, самоконтроль, атестація. <i>Форми оцінювання:</i> усне та письмове опитування, тестові завдання, захист лабораторних та практичних робіт, захисти курсових проектів і робіт, кваліфікаційна магістерська робота тощо.
1.6. Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні задачі і проблеми в галузі кібербезпеки або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.
Загальні компетентності (ЗК)	ЗК1. Здатність до абстрактного мислення, аналізу та синтезу ЗК2. Здатність спілкуватися та користуватися інформаційними джерелами іноземною мовою. ЗК3. Здатність використання інформаційних і комунікаційних технологій. ЗК4. Здатність проведення досліджень на відповідному рівні. ЗК5. Здатність до пошуку, опрацювання та аналізу інформації з різних джерел. ЗК6. Здатність до генерації нових ідей і варіантів розв'язання задач, до комбінування та експериментування, до оригінальності, конструктивності, економічності та простих рішень. ЗК7. Здатність приймати обґрунтовані рішення. ЗК8. Здатність працювати в міжнародному контексті. ЗК9. Здатність розробляти та управляти проектами. ЗК10. Здатність здійснення безпечної діяльності. ЗК11. Здатність діяти на основі етичних міркувань (мотивів)
Фахові компетентності спеціальності (ФК)	ФК1. Здатність застосовувати практичні методи, методологічні аспекти та комп'ютерну логіку при конструюванні, побудові та схемотехніці апаратних та програмних засобів захисту комп'ютерних систем та мереж, з врахуванням вимог техніки безпеки, охорони праці та протипожежної безпеки в професійній діяльності. ФК2. Здатність до побудови ефективних алгоритмів формального прогнозу, моделей та методів змістовного прогнозування в методах захисту шляхом використання принципів функціонування та структури технічних засобів, математичних моделей, історії та логіки розвитку галузі у контексті відповідних величин, феноменів, моделей, методів, функцій та структур технічних засобів,

	формальних та змістовних методів прогнозування функцій, структур, характеристик та параметрів комп'ютерних систем та мереж. ФК3. Здатність проводити розробку і дослідження теоретичних та експериментальних моделей захисту об'єктів професійної діяльності. ФК4. Здатність здійснювати авторський супровід процесів проектування, впровадження засобів захисту інформаційних систем і технологій ФК5. Здатність аналізувати, оптимізувати та моделювати складність архітектури комп'ютерних систем та мереж із застосуванням сучасних принципів побудови математичного, програмного, лінгвістичного, технічного та інформаційного забезпечення для захисту інформації. ФК6. Здатність до планування експериментального і теоретичного дослідження, вибору алгоритмів опрацювання цифрових сигналів та інтерпретації отримуваних результатів. ФК7. Здатність розробляти стратегії проектування, визначення цілей проектування, критеріїв ефективності захисних засобів, обмежень застосовності, уміння розробляти нові методи і засоби проектування захищених комп'ютерних систем та мереж. ФК8. Знання основних принципів побудови засобів захисту комп'ютерних систем та мереж, принципів побудови та функціонування їх периферійних засобів. ФК9. Здатність застосовувати теоретичні та практичні навички для вирішення комплексу питань від аксіоматичних умов можливості побудови захищених комп'ютерних систем та мереж до оцінювання їх ФК10. Здатність застосовувати практичні методи, методологічні аспекти та логіку комп'ютерного дизайну при конструюванні, побудові та схемотехніці захищених комп'ютерних систем та мереж, з врахуванням вимог техніки безпеки, охорони праці та протипожежної безпеки в професійній діяльності. ФК11. Здатність до побудови ефективних алгоритмів формального прогнозу, моделей та методів змістовного прогнозування в науці та техніці шляхом використання принципів функціонування та структури технічних засобів, математичних моделей, історії та логіки розвитку галузі у контексті відповідних величин, феноменів, моделей, методів, функцій та структур технічних засобів, формальних та змістовних методів прогнозування функцій, структур, характеристик та параметрів комп'ютерних систем та мереж. ФК12. Здатність проводити розробку і дослідження теоретичних та експериментальних моделей систем захисту об'єктів професійної діяльності. ФК13. Здатність здійснювати авторський супровід процесів проектування, впровадження інформаційних систем і технологій ФК14. Здатність до застосування сучасних інформаційних та безпекових технологій в сфері захисту
--	--

	інформації ФК15. Здатність використовувати механізми штучного інтелекту для вирішення проблем забезпечення кібербезпеки, що складно формалізувати
1.7. Програмні результати навчання (ПРН)	
Знання	ПРН1. Знати і розуміти наукові і математичні положення, що лежать в основі функціонування програмних, і програмно-технічних засобів захисту інформації в комп'ютерних, системах та мережах. ПРН2. Знати професійно-орієнтовані дисципліни спеціальності. ПРН3. Мати знання та навички щодо проведення експериментів, збору даних та моделювання загроз в комп'ютерних системах. ПРН4. Мати знання із новітніх технологій в галузі кібербезпеки. ПРН5. Знати та розуміти вплив технічних рішень, в т.ч. механізмів штучного інтелекту, в суспільному, економічному, соціальному і екологічному контексті.
Уміння	ПРН6. Уміння застосовувати знання і розуміння для розв'язання задач синтезу та аналізу захисних засобів в системах, які характерні обраній спеціальності. ПРН7. Уміння використовувати сучасні комп'ютерні засоби системного, функціонального, конструкторського та технологічного проектування для створення сучасних захисних систем ПРН8. Уміння виконувати експериментальні дослідження та застосовувати дослідницькі навички за професійною тематикою. ПРН9. Уміння здійснювати збір, аналіз науково-технічної інформації, вітчизняного і зарубіжного досвіду з тематики дослідження. ПРН10. Уміння використовувати набуті знання з спеціальності для знаходження нових, нешаблонних рішень і засобів їх здійснення при проведенні експериментальних досліджень для розв'язку поставлених задач. ПРН11. Уміння публічних, ділових та наукових комунікацій як рідною так і іноземною мовами. ПРН12. Уміння опрацьовувати отримані результати, аналізувати та осмислювати їх, представляти результати роботи і обґрунтовувати запропоновані рішення на сучасному науково-технічному і професійному рівні ПРН13. Уміння використовувати та володіти засобами дотримання норм, вимог та правил охорони праці та безпеки життєдіяльності в професійній сфері для проведення безпечної діяльності.

	ПРН14. Уміння використовувати сучасні комп'ютерні засоби системного, функціонального, конструкторського та технологічного проектування програмних та апаратних засобів захисту інформації. ПРН15. Уміння приймати обґрунтовані рішення та оцінювати їх наслідки.
Комунікація	ПРН16. Вміння спілкуватись, включаючи усну та письмову комунікацію українською мовою та однією з іноземних мов (англійською, німецькою, італійською, французькою, іспанською). ПРН17. Вміння використовувати інформаційні технології та інші методи для ефективного спілкування на професійному та соціальному рівнях.
Автономія і відповідальність	ПРН18. Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення. ПРН19. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення. ПРН20. Відповідально ставитись до виконуваної роботи та досягати поставленої мети з дотриманням вимог професійної етики.
1.8. Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Лекційні заняття забезпечують 4 доктори наук, професори та 5 кандидатів наук, доценти, фахівці відповідних спеціальностей
Матеріально-технічне забезпечення	• Лекційні аудиторії, що мають мультимедійне обладнання; • Лабораторії, що мають обладнання, яке відповідає предметній галузі (вимірювальні пристрої, комп'ютери, мережеве обладнання, стенди, тощо). • Відповідно договору про консорціум з 3 провідними ЗВО м. Дніпра, можливо використання лабораторій цих ЗВО в начальному процесі кафедри. • Відповідно договорам про філії кафедри ЕОМ: виробничий підрозділ «Дніпровського відділення» філії «Головний інформаційно-обчислювальний центр», філії «Проектно-конструкторське технологічне бюро інформаційних технологій» ПАТ «Українська залізниця», лабораторії спецв'язку та захисту інформації першого відділку «Дніпровського відділення» ПАТ «Українська залізниця» можливо використання лабораторій цих підприємств в начальному процесі кафедри.
Інформаційне та навчально-методичне забезпечення	Інформаційно-технологічне забезпечення освітнього процесу Бібліотека:

	• можливість використання онлайн-ресурсів та баз даних; • інформаційне забезпечення студентів навчальною та методичною. Навчальні ресурси: • довгострокові і короткострокові позики книг, доступ до онлайн-ресурсів, міжбібліотечні позики, відеотека; • доступ до електронних журналів; • доступ до електронних бібліотечних ресурсів світу; • доступ до електронного навчального середовища Moodle; • технологічне і матеріально-технічне забезпечення освітнього процесу. Академічна підтримка – • консультації з вибору програми, окремих вибіркових дисциплін; • проектування індивідуальних навчальних траєкторій • Персональне консультування.
1.9. Академічна мобільність	
Національна кредитна мобільність	Регламентується «Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу» та договором про консорціум з 3 провідними ЗВО м. Дніпра. Для забезпечення студентської мобільності може здійснюватись трансфер кредитів у порядку перезарахування кредитів, які були встановлені студентам під час навчання на інших освітніх програмах, та можливого визнання результатів неофіційного та неформального навчання.
Міжнародна кредитна мобільність	Міжнародна кредитна мобільність забезпечена умовами договорів між іноземними університетами та ДНУЗТ. Магістранти мають право вибору навчальних дисциплін з інших ОП та в іншому ЗВО при участі в програмах академічної мобільності
Навчання іноземних здобувачів вищої освіти	Навчання іноземних студентів здійснюється на загальних умовах з додатковою мовною підготовкою та методичним забезпеченням окремих компонент освітньої програми російською мовою. Організацію навчального процесу для іноземних студентів здійснює відділ роботи з іноземними студентами. Іноземним студентам надається гуртожиток.

2. Перелік компонентів освітньо-професійної програми та її логічна послідовність

2.1 Перелік компонентів ОП

Код навчальної дисципліни	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. Обов'язкові компоненти (ОК)			
ОК 1	Ділове (наукове) спілкування іноземною мовою	3	Залік
ОК 2	Фізичне виховання	4*	Залік
ОК 3	Використання механізмів штучного інтелекту в системах кіберзахисту	11	Екзамен / Залік
ОК 4	Теорія проектування захищених комп'ютерних мереж	7	КЗ
ОК 5	Практика проектування захищених інформаційних систем	7	Екзамен
ОК 6	Практика використання апаратно-програмних засобів CISCO для кіберзахисту комп'ютерних мереж	8	Залік
ОК 7	Проектування захищених WEB-систем	6	Екзамен
ОК 8	Комплексні системи захисту	6	КЗ
ОК 9	Виробнича практика	4	Залік
ОК 10	Дипломовання	15	Залік
Загальний обсяг обов'язкових компонент: 67			
2. Вибіркові компоненти (можна обрати одну компоненту з одного блоку)			
ВБ 1.1	Інформаційні технології в управлінській, науковій та викладацькій діяльності	3	Залік
ВБ 1.2	Інформаційні системи залізничного транспорту		
ВБ 1.3	Телематика та інтелектуальні технології залізничного транспорту		
ВБ 2.1	Охорона праці в галузі та цивільний захист	3	Екзамен
ВБ 2.2	Профілактика і локалізація техногенних аварій і катастроф		
ВБ 2.3	Безпека виробничих процесів		
ВБ 2.4	Небезпека сучасного світу		
ВБ 3.1	Інтелектуальна власність	3	Залік
ВБ 3.2	Інноваційний розвиток підприємств		
ВБ 3.3	Управління змінами на транспорті		
Міnor 1			
ВБ 4.1	Сучасні напрями розвитку систем кібербезпеки	4	Залік
			Реф.

ВБ 5.1	Системи антивірусного захисту	5	Залік
ВБ 6.1	Захист інформації в мережах ІНТЕРНЕТ	5	Екзамен
Міnor 2			
ВБ 4.2	Безпека інтелектуальних систем залізничного транспорту	4	Залік
ВБ 5.2	Принципи проектування систем	5	Реф.
ВБ 6.2	Захист інформації в бездротових системах	5	Залік
Екзамен			
Загальний обсяг вибірових компонент: 23			

Примітка *: компонент ОК2 є позакредитним

Розподіл змісту освітньо-професійної програми за групами компонентів та циклами підготовки

Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів / %)		
	обов'язкові компоненти	вибіркові компоненти	всього за весь термін навчання
Цикл загальної підготовки	3/3,33	9/10	12/13,33
Цикл професійної підготовки	64/71,11	14/15,56	78/86,67
Всього за весь термін навчання	67/74,44	23/25,56	90/100

2.2 . Структурно-логічна схема освітньої програми

Код навчальної дисципліни	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Код навчальної дисципліни, яка забезпечується зазначеною в стовпчику 1
1	2	3
1. Обов'язкові компоненти (ОК)		
ОК1	Ділове (наукове) спілкування іноземною мовою	ОК3, ОК4, ОК6, ВБ4.1, ВБ4.2, ВБ6.1
ОК2	Фізичне виховання	—
ОК3	Використання механізмів штучного інтелекту в системах кіберзахисту	ОК4, ВБ4.1, ВБ4.2, ВБ5.1, ВБ5.2, ВБ6.1, ВБ6.2
ОК4	Теорія проектування захищених комп'ютерних мереж	ОК6, ВБ4.1, ВБ4.2, ВБ6.1, ВБ6.2
ОК5	Практика проектування захищених інформаційних систем	ОК6, ВБ4.1, ВБ4.2
ОК6	Практика використання апаратно-програмних засобів CISCO для кіберзахисту комп'ютерних мереж	ОК7, ОК8, ОК9, ВБ4.1, ВБ4.2
ОК7	Проектування захищених WEB-	ОК6, ОК3

	систем	
OK8	Комплексні системи захисту	OK5, ВБ4.1, ВБ4.2
OK9	Виробнича практика	OK10
OK10	Дипломування	—
2. Вибіркові компоненти		
ВБ 1.1	Інформаційні технології в управлінській, науковій та викладацькій діяльності	OK3, OK9, ВБ2
ВБ 1.2	Інформаційні системи залізничного транспорту	
ВБ 1.3	Телематика та інтелектуальні технології залізничного транспорту	
ВБ 2.1	Охорона праці в галузі та цивільний захист	OK10, ВБ3
ВБ 2.2	Профілактика і локалізація техногенних аварій і катастроф	
ВБ 2.3	Безпека виробничих процесів	
ВБ 2.4	Небезпека сучасного світу	
ВБ 3.1	Інтелектуальна власність	OK10
ВБ 3.2	Інноваційний розвиток підприємств	
ВБ 3.3	Управління змінами на транспорті	
Міnor 1		
ВБ 4.1	Сучасні напрями розвитку систем кібербезпеки	OK10
ВБ 5.1	Системи антивірусного захисту	ВБ6.1
ВБ 6.1	Захист інформації в мережах ІНТЕРНЕТ	ВБ4.1
Міnor 2		
ВБ 4.2	Безпека інтелектуальних систем залізничного транспорту	OK10
ВБ 5.2	Принципи проектування систем	ВБ6.2
ВБ 6.2	Захист інформації в бездротових системах	ВБ4.2

3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності **125 Кібербезпека** проводиться у формі захисту кваліфікаційної магістерської роботи та завершується видачею документу встановленого зразка про присудження йому ступеня магістра із присвоєнням кваліфікації: Магістр з кібербезпеки.

Заклад вищої освіти забезпечує перевірку кваліфікаційної роботи на плагіат. Реферат кваліфікаційної роботи оприлюднюється у репозитарії університету.

Атестація здійснюється відкрито і публічно.

4. Матриця відповідності програмних компетентностей основним компонентам освітньої програми

	ОК1	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ВБ1	ВБ2	ВБ3	ВБ4	ВБ5	ВБ6
ЗК1		+	+		+			+		+	+	+			
ЗК2	+		+										+		
ЗК3			+	+	+	+		+	+	+					
ЗК4		+								+		+			
ЗК5		+	+	+	+	+		+	+	+	+	+	+	+	+
ЗК6			+				+		+	+	+				
ЗК7			+		+		+		+	+					
ЗК8	+				+										
ЗК9							+			+		+			
ЗК10								+	+		+				
ЗК11		+							+		+				
ФК1			+	+		+	+	+		+	+			+	+
ФК2		+	+											+	
ФК3			+		+		+	+		+					
ФК4		+				+						+			
ФК5			+		+	+	+	+		+				+	+
ФК6								+	+	+					
ФК7							+	+	+						
ФК8					+		+				+				+
ФК9		+				+		+							
ФК10								+	+		+				
ФК11		+			+					+					
ФК12					+								+		
ФК13						+						+			
ФК14		+		+					+				+		
ФК15		+	+										+		

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

	ОК1	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ВБ1	ВБ2	ВБ3	ВБ4	ВБ5	ВБ6
ПРН1			+		+					+					
ПРН2			+		+	+	+	+		+	+			+	+
ПРН3		+	+		+		+	+		+					
ПРН4				+	+			+					+		
ПРН5		+									+	+			
ПРН6			+	+	+	+	+	+	+	+				+	+
ПРН7			+	+	+	+	+	+	+	+					
ПРН8		+	+		+	+			+	+				+	+
ПРН9			+		+					+	+	+	+		
ПРН10			+		+	+			+	+				+	+
ПРН11	+				+							+	+		
ПРН12			+		+	+	+	+		+				+	+
ПРН13								+	+		+				
ПРН14			+					+		+					
ПРН15					+		+	+	+		+	+			
ПРН16	+											+			
ПРН17	+				+							+			
ПРН18					+		+	+			+				
ПРН19	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН20	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+