Приватне акціонерне товариство «Вищий навчальний заклад

«Міжрегіональна Академія управління персоналом»

ЗАТВЕРДЖЕНО
Вченою радою
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом»
Протокол № 3 від «26» березня 2025 р.
Голова Вченої ради, Президент
_____ **Ростислав ЩОКІН**

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА»

Рівень вищої освіти: **другий (магістерський)**

Ступінь вищої освіти: **магістр**

Галузь знань: **F – «Інформаційні технології»**

Спеціальність: **F5 Кібербезпека та захист інформації**

Освітня кваліфікація: **магістр з кібербезпеки та захисту інформації**

Освітня програма вводиться в дію з
01 вересня 2025 року
наказ № 30/1-О від «26» березня 2025 р.
Ректор _____ / Кирило МУРАВЙОВ

КИЇВ - 2025

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

«РОЗРОБЛЕНО» **Робочою групою (проектною) групою** **ПрАТ «ВНЗ «МАУП»** **керівник робочої групи** **_____ Іван СЕРВЕЦЬКИЙ** 04 березня 2025 р.	**«УХВАЛЕНО»** **на засіданні кафедри** **інформаційної безпеки** **ПрАТ «ВНЗ «МАУП»,** **протокол № 8 від 06 березня 2025 р.** **завідувач кафедри** **_____ Сергій ЛИСЕНКО**
«СХВАЛЕНО» **Вченою радою Інституту безпеки** **Голова Вченої ради** **_____ Сергій ЛИСЕНКО** 10 березня 2025 р.	**«ПОГОДЖЕНО»** **Департаментом навчально-методичного забезпечення та якості вищої освіти ПрАТ «ВНЗ «МАУП»** **Директор** **_____ Анатолій ТАЛАХ** 14 березня 2025 р.
«РЕКОМЕНДОВАНО» **Науково-методичною радою** **ПрАТ «ВНЗ «МАУП»** **Голова ради** **_____ Михайло ГОНЧАРЕНКО** 17 березня 2025 р.	**«ПОГОДЖЕНО»** **Ректор ПрАТ «ВНЗ «МАУП»** **_____ Кирило МУРАВЙОВ** 18 березня 2025 р.

ПЕРЕДМОВА

Освітньо-професійна програма «Кібербезпека» другого (магістерського) рівня вищої освіти зі спеціальності F5 Кібербезпека та захист інформації у галузі знань F - «Інформаційні технології» розроблена відповідно до Закону України «Про вищу освіту», Постанови КМУ від 29.04. 2015 року № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» (зі змінами), Постанови КМУ від 23.11. 2011 року № 1341 «Про затвердження національної рамки кваліфікацій» із змінами та інших чинних нормативних документів. У зв'язку з відсутністю Стандарту за спеціальністю F5 Кібербезпека та захист інформації за новим Переліком, під час розробки ОПП взято за основу Стандарт вищої освіти зі спеціальності 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 18.03.2021 року № 332.

Освітньо-професійна програма є нормативним документом, в якому визначено профіль, перелік компонентів програми та їх логічна послідовність, кількість кредитів ЄКТС, необхідних для виконання цієї програми, форма атестації здобувачів вищої освіти.

Освітньо-професійна програма розроблена **робочою (проєктною) групою у складі**:

Керівник групи:
Сервецький Іван Васильович - доктор юридичних наук, доцент, професор кафедри Національної безпеки Інституту безпеки ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом» – гарант програми.

Члени групи:
Підюков Петро Павлович - доктор юридичних наук, професор, професор кафедри Національної безпеки Інституту безпеки ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом».
Когут Юрій Іванович – кандидат юридичних наук, доцент кафедри Інформаційної безпеки Інституту безпеки ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом».
Сидоренко Сергій Миколайович - керівник Всеукраїнського об'єднання організацій роботодавців охоронної галузі «Федерація професіоналів безпеки».

Рецензії-відгуки зовнішніх стейкхолдерів:

1. Гуз Анатолій Михайлович – доктор юридичних наук, професор, завідувач кафедри організації інформації з обмеженим доступом Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України.

2. Драган Іван Олександрович - доктор наук з державного управління, професор, завідувач кафедри права та правоохоронної діяльності Факультету національної безпеки, права та міжнародних відносин Державного університету «Житомирська політехніка».
3. Хоменко Вадим Валерійович перший заступник Голови Всеукраїнської професійної спілки «Національна спілка приватних виконавців».

Оновлення, перегляд, зміни та доповнення освітньо-професійної програми «Кібербезпека» за другим (магістерським) рівнем вищої освіти зі спеціальності F5 Кібербезпека та захист інформації у галузі знань F - «Інформаційні технології»

Навчальний рік	**Затверджено Вченою радою ПрАТ «ВНЗ «МАУП» (протокол, номер, дата)**	**Дата введення в дію ОПП відповідно з наказом ректора**
2025-2026		

І. Загальна характеристика освітньо-професійної програми зі спеціальності F5 Кібербезпека та захист інформації

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» Інститут безпеки Кафедра інформаційної безпеки
Рівень вищої освіти	Другий (магістерський)
Ступінь вищої освіти	Магістр
Галузь знань	F – «Інформаційні технології»
Спеціальність	F5 Кібербезпека та захист інформації
Обмеження щодо форм навчання	Без обмеження
Освітня кваліфікація	Магістр з кібербезпеки
Професійна кваліфікація	Не надається
Кваліфікація в дипломі	Ступінь вищої освіти - магістр Спеціальність – F5 Кібербезпека та захист інформації Освітня програма – «Кібербезпека»
Офіційна назва освітньої програми	«Кібербезпека»
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання – 1 рік 6 місяців
Наявність акредитації	
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Для здобуття освітнього ступеня магістра можуть вступати особи, що здобули освітній ступень бакалавра та виконали Правила прийому до Приватного акціонерного товариства «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»
Мова(и) викладання	Українська
Термін дії освітньої програми	2 роки зі щорічним плановим переглядом та оновленням
Інтернет-адреса постійного розміщення опису освітньої програми	https://maup.com.ua/assets/files/opp/bezpeka/kiberbezpeka-drugogo-magisterskogo-rivnya-2025.pdf

2 – Мета освітньої програми	
Підготовка висококваліфікованого фахівця, спроможного здійснювати професійний аналіз, формулювати та вирішувати прикладні завдання, а також розв’язувати складні фізико-технічні й логіко-організаційні проблеми у сфері кібернетичної безпеки та захисту інформації в умовах високої комплексності та невизначеності технологічних, екологічних, соціально-економічних і політичних загроз, із забезпеченням всебічного професійного, інтелектуального, соціального й творчого розвитку особистості на найвищих рівнях досконалості в контексті сучасного освітньо-наукового середовища.	
3 - Характеристика освітньої програми	
Опис предметної області	***F - Інформаційні технології*** ***F5 Кібербезпека та захист інформації*** ***Об’єкти вивчення***: ➢ сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; ➢ інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; ➢ інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; ➢ системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); ➢ інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); ➢ програмне та програмно-апаратне забезпечення (засоби) кібернетичного захисту інформації; ➢ системи управління інформаційною безпекою та/або кібербезпекою; ➢ технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. ***Цілі навчання*** – підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. ***Теоретичний зміст предметної області*** – теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки.. ***Методи, методики та технології*** – методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту інформаційних ресурсів у кібернетичному просторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та

	забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кібернетичному просторі. ***Інструменти та обладнання*** – Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньої програми	Освітньо-професійна програма спрямована на підготовку здобувачів другого (магістерського) рівня вищої освіти галузі знань ***F - Інформаційні технології спеціальності F5 Кібербезпека та захист інформації*** та передбачає набуття фахових компетентностей, необхідних для подальшого особистісного розвитку та кібербезпекового розвитку держави, суспільства та громади для виконання функцій і завдань територіальної оборони.
Основний фокус освітньої професійної програми та спеціалізації	Освітня програма зосереджена на таких аспектах, як мережна безпека, тестування інформаційних систем на предмет проникнення, виявлення, реагування та розслідування інцидентів кібербезпеки, а також на організації діяльності центрів оперативного реагування на кіберзагрози (SOC). В основі програми лежить міждисциплінарний підхід, що охоплює адміністрування операційних систем, системне та прикладне програмування, аналіз вразливостей і ризиків, а також впровадження технологій протидії атакам і захисту критичної інформаційної інфраструктури. Особлива увага приділяється сучасним методам моніторингу, управління інформаційною безпекою, розбудові систем виявлення та попередження вторгнень, управлінню кібероперaціями та функціонуванню спеціалізованих засобів кіберзахисту та шифрування. *Ключові слова:* кібербезпека, комп'ютерна система, комп'ютерна мережа, інформаційна система, інформаційно-телекомунікаційна система, операційна система, адміністрування систем, прикладне програмування, системне програмування, вразливість, атака, ризик, компрометація, протидія, захист інформації, тестування на проникнення, моніторинг, розслідування інциденту, міжмережне екранування, система виявлення та попередження вторгнень, кібероперації, спеціальні системи забезпечення кібербезпеки, управління інформаційною безпекою.
Особливості програми	Освітньо-професійна програма зосереджена на практичному застосуванні теоретичних знань і навичок для вирішення завдань, що стосуються кібербезпеки та інформаційної безпеки України в усіх її проявах. Студенти отримують як теоретичні, так і практичні знання,. Програма відрізняється своєю унікальною спрямованістю на розвиток професійних управлінських компетенцій для захисту національних інтересів країни. Співпраця Академії з різними державними установами, органами місцевого самоврядування, приватним сектором та іншими організаціями забезпечує студентам можливості для проходження тривалої практики (20 ЄКТС) і подальшої кар'єри як у

	державному секторі, так і в неурядових та міжнародних організаціях, територіальних громадах, підприємствах і організаціях. Особливу увагу присвячено політичній складовій, розвитку громадянського суспільства та управлінню медіа.
4 – Придатність випускників до працевлаштування та подальшогонавчання	
Придатність до працевлаштування	Випускники можуть бути працевлаштовані на керівних посадах структурних підрозділів центральних органів виконавчої влади, в органах управління стратегічного рівня сил оборони, органах управління сил безпеки, політичних організаціях, органах самоуправління, територіальних громадах тощо. Сферами економічної діяльності магістра з кібербезпеки згідно з ДКП 003:2010 є: ➢ Розробник систем захисту інформації; ➢ Адміністратор мереж і систем; ➢ Аналітик загроз безпеки; ➢ Аналітик систем захисту інформації та оцінки вразливостей; ➢ Аналітик з безпеки інформаційно-телекомунікаційних систем; ➢ Дізнавач (сфера кібербезпеки та захисту інформації); ➢ Експерт-криміналіст (сфера кібербезпеки та захисту інформації); ➢ Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації); ➢ Слідчий з кіберзлочинів; ➢ Фахівець з криптографічного захисту інформації; ➢ Фахівець з питань безпеки (інформаційно-комунікаційні технології; ➢ Фахівець з підтримки інфраструктури кіберзахисту; ➢ Фахівець з реагування на інциденти кібербезпеки; ➢ Фахівець з тестування систем захисту інформації; ➢ Фахівець з технічного захисту інформації; ➢ Фахівець сфери захисту інформації. Згідно міжнародної класифікації ➢ Головний фахівець з інформаційної безпеки (Chief Infosec Officer); ➢ Фахівець-менеджер з кібербезпеки (Security Manager); ➢ Директор з кібербезпеки (Security Director); ➢ Фахівець-аудитор з кібербезпеки (Security Auditor); ➢ Фахівець з оцінки вразливостей (Vulnerability Assessor); ➢ Фахівець з тестування на проникнення (Penetretion Tester); ➢ Фахівець-аудитор безпеки коду (Security Code Auditor); ➢ Фахівець-експерт з розслідування інцидентів кібербезпеки (Forensics Expert); ➢ Фахівець-архітектор з кібербезпеки (Security Architect); ➢ Фахівець-аналітик з кібербезпеки (Security Analyst);

	➢ Спеціаліст з кібербезпеки (Security Specialist); ➢ Фахівець-адміністратор безпеки (Security Administrator); ➢ Інженер з кібербезпеки (Security Engineer); ➢ Фахівець з реагування на інциденти кібербезпеки (Incident Responder); ➢ Фахівець з криптографії (Cryptographer); ➢ Фахівець з розробки програмного забезпечення для кібербезпеки (Security Software Developer); ➢ Фахівець-консультант з кібербезпеки (Security Consultant). Рівень завдань, що належить розв'язувати магістру спеціальності F5 Кібербезпека та захист інформації, обумовлюється потребами сучасної суспільно-політичної практики, а також спроможністю та потребами безперервного підвищення наукового та кваліфікаційного потенціалу.
Академічні права випускників	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	Основні види навчальних занять в Інституті безпеки ПрАТ «ВНЗ «МАУП»: лекції, практичні заняття, семінарські заняття, консультації, індивідуальні заняття, самостійна позааудиторна робота, виробнича практики. Проблемно-орієнтоване та студентоцентроване навчання з використанням активних та інтерактивних форм.
Оцінювання	Контрольні заходи оцінювання навчальної діяльності здобувачів вищої освіти включають поточний, тематичний, періодичний, підсумковий контроль, самоконтроль. Підсумковий контроль включає семестровий контроль та державну атестацію здобувачів вищої освіти. Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано); 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F). Підсумкова атестація за ОПП здійснюється у формі Атестаційного іспиту та публічного захисту демонстрації кваліфікаційної роботи. Екзамени та заліки проводяться відповідно до вимог «Положення про оцінювання навчальних досягнень здобувачів вищої освіти в ПрАТ «ВНЗ «МАУП» (https://maup.com.ua/assets/files/publ-adm/nakaz-191.1-0.pdf) та «Критеріїв оцінювання знань і умінь студентів в ПрАТ «ВНЗ «МАУП» (https://maup.com.ua/assets/files/pdf/ocin-znan-stud.pdf).
6- Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Науково-педагогічні працівники кафедр Академії повністю забезпечують підготовку здобувачів вищої освіти за спеціальністю F5 Кібербезпека та захист інформації (Постанова КМУ від 30.12. 2015 року № 1187 «Про затвердження ліцензійних умов провадження освітньої діяльності закладів освіти» (зі змінами та доповненнями)).

	Формування якісного складу науково-педагогічних працівників відбувається за рахунок викладачів з науковими ступенями та вченими званнями зі спеціальності на постійній основі, прийнятих за конкурсом, шляхом укладення контрактів та залучення до професійно-педагогічної діяльності професіоналів-практиків в галузі знань F – Інформаційні технології та за сумісництвом. Члени групи забезпечення, які реалізують виконання освітньої складової ОП, мають кваліфікації відповідно до спеціальності: вищу освіту, науковий ступінь та/або вчене звання, підтверджений рівень наукової та професійної активності; 85% науково-педагогічних працівників групи забезпечення є штатними працівниками Академії. Портфоліо науково-педагогічних працівників кафедри Інформаційної безпеки розміщено на сайті (https://maup.com.ua/ua/pro-akademiyu/instituti/institut-bezpeki-prat-vnz-maup/informaci-bezpeka.html).
Матеріально-технічне забезпечення	Матеріально-технічна база ПрАТ «ВНЗ «МАУП» дозволяє здійснювати навчальний процес, наукову та практичну роботу на сучасному рівні, згідно з нормативними вимогами щодо підготовки фахівців, навчального плану та програмних компонентів освітньо-професійної програми. Усі приміщення відповідають вимогам правил пожежної безпеки та санітарним нормам. Матеріально технічна база забезпечує проведення всіх видів навчальних занять та науково-дослідної роботи здобувачів вищої освіти. Виконання навчального плану забезпечено мультимедійним обладнанням, комп'ютерним класом на 21 робоче місце (комп'ютери 12th Gen Intel® Core ™ i5-12400 2.5GHz), повний пакет Microsoft Office, необхідним програмним забезпеченням і необмеженим доступом до інтернет-мережі; матеріально-технічною базою для проведення практик здобувачів вищої освіти або діючих угод на проведення практик в установах громадської безпеки, правоохоронних органах та в недержавних закладах охорони і безпеки. Навчальна база Інституту безпеки дозволяє організувати та проводити заняття з усіх навчальних дисциплін на належному науково-методичному рівні. Для реалізації всіх навичок практичної роботи здобувачів під керівництвом викладачів з практичним досвідом роботи, в Академії створено і достатньо обладнані «Лабораторія криміналістики та аудиту», «Лабораторія цивільного захисту та громадянської оборони», «Лабораторія вогневої підготовки», «Лабораторія-полігон кібербезпеки» та «Лабораторія використання поліграфічних та психологічних технологій». Наявна уся необхідна соціально-побутова інфраструктура. Кількість місць у гуртожитку відповідає вимогам. У Академії створено умови для навчання осіб з особливими освітніми потребами, а також для осіб з інвалідністю та інших маломобільних груп населення.
Інформаційне та навчально-методичне забезпечення	Інформаційне та навчально-методичне забезпечення відповідає Ліцензійним умовам провадження освітньої діяльності з підготовки фахівців за другим (магістерським) рівнем та включає: графік навчального процесу, навчальний план, робочі навчальні програми, силабуси, тематичні плани лекцій і семінарських занять, критерії оцінювання знань, перелік питань до поточного та підсумкового контролів, переліки питань до іспитів, переліки ситуаційних і тестових завдань, перелік рекомендованої навчально-методичної літератури,

	наочні і технічні засоби навчання. Навчально-методична документація підготовлена науково-педагогічними працівниками кафедри, забезпеченість навчальними матеріалами кожної освітньої компоненти ОП становить 100%. На офіційному сайті Інституту безпеки розміщена основна інформація про ОП та його діяльність, а також наявний електронний ресурс, який містить усі навчальні матеріали компонентів ОПП. На офіційному веб-сайті Академії також у відкритому доступі наявна уся необхідна інформація https://maup.com.ua. До послуг учасників освітнього процесу є вільний доступ до ресурсу Міжнародного бібліотечно-інформаційного центру імені Яросава Мудрого МАУП https://maup.com.ua/ua/pro-akademiyu/biblioteka.html, а також доступ до системи електронного навчання Moodle, де наявна навчальна, навчально-методична література, фахові журнали.
7 – Перелік компетентностей випускника	
Інтегральна компетентність (ІК)	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Здатність проводити дослідження на відповідному рівні. ЗК3. Здатність до абстрактного мислення, аналізу та синтезу. ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).
Спеціальні (фахові) компетентності (ФК)	ФК1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. ФК2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. ФК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ФК4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. ФК5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії політики інформаційної безпеки та/або кібербезпеки організації. ФК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої

	стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ФК8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. ФК10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
8 – Нормативний зміст підготовки здобувачів вищої освіти, сформульований у контексті програмних результатів навчання (ПРН)	
Програмні результати навчання (ПРН)	ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби

	інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ПРН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. ПРН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес операційних процесів у сфері інформаційної та або кібербезпеки в цілому. ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

	ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
9 – Академічна мобільність	
Національна кредитна мобільність	Право на національну кредитну мобільність реалізується на підставі Закону України «Про вищу освіту» та Постанови КМУ № 579 «Про затвердження положення про порядок реалізації права на академічну мобільність» з наданням права на участь в програмах академічної мобільності всім учасникам освітнього процесу за чітким визначенням її видів та форм закріплення принципів перезарахування отриманих кредитів на основі Європейської кредитно-трансферної системи (ЄКТС). Кредити ЄКТС отримані в інших ВНЗ України при наявності договорів між закладами вищої освіти (науковими установами України або їхніми основними структурними підрозділами), перезараховуються відповідно до положення «Про організацію освітнього процесу ПрАТ «ВНЗ «МАУП». Максимальний обсяг кредитів ЄКТС, що може бути перезарахований, становить 25% від загального обсягу освітньої програми.
Міжнародна кредитна мобільність	Право на міжнародну кредитну мобільність реалізується на підставі міжнародних договорів про співробітництво в галузі освіти і науки, міжнародних програм і проектів (Erasmus+), а також може бути реалізовано на підставі індивідуальних запрошень для учасників освітнього процесу з власної ініціативи, підтриманої керівництвом Академії.
Навчання іноземних здобувачів вищої освіти	--

ІІ. Обсяг кредитів ЄКТС, необхідних для здобуття другого (магістерського) ступеня вищої освіти

Обсяг освітньо-професійної програми магістра у кредитах Європейської кредитної трансферно-накопичувальної системи (далі – ЄКТС) становить 90 кредитів ЄКТС.

Мінімум 60% обсягу освітньої програми має бути спрямовано на формування загальних та спеціальних (фахових) компетентностей за спеціальністю, визначених Стандартом вищої освіти.

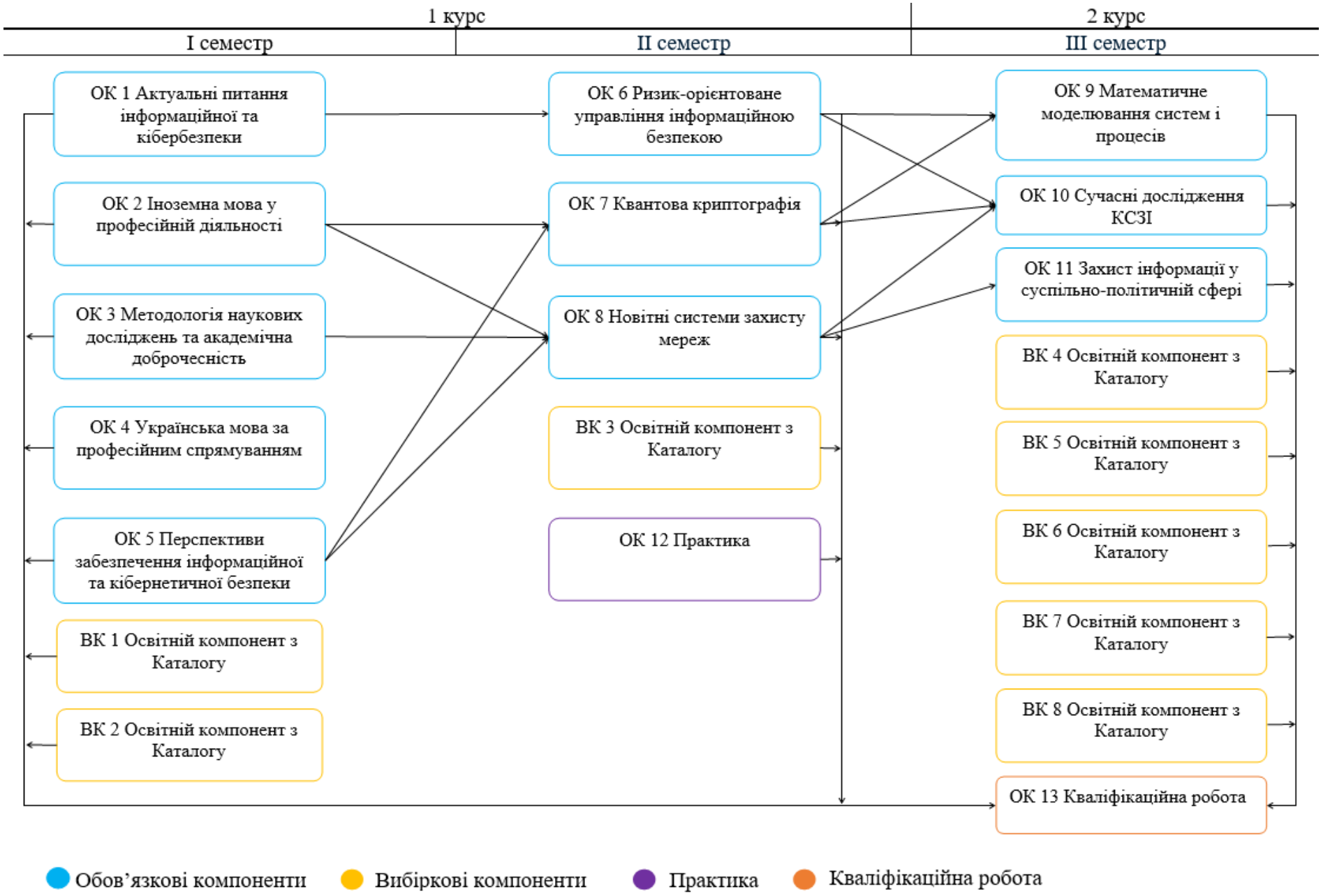
Мінімум 15 кредитів ЄКТС має бути призначено для практики.

2.1 Перелік компонент ОПП «Кібербезпека»

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумковог о контролю
1	2	3	4
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ			
ОК1	Актуальні питання інформаційної та кібербезпеки	5	Екзамен
ОК2	Іноземна мова у професійній діяльності	3	Екзамен
ОК3	Методологія наукових досліджень та академічна доброчесність	3	Залік
ОК4	Українська мова за професійним спрямуванням	3	Екзамен
ОК5	Перспективи забезпечення інформаційної та кібернетичної безпеки	8	Екзамен, Захист КСР
ОК6	Ризик-орієнтоване управління інформаційною безпекою	3	Залік
ОК7	Квантова криптографія	3	Екзамен
ОК8	Новітні системи захисту мереж	3	Екзамен
ОК9	Математичне моделювання систем і процесів	3	Екзамен
ОК10	Сучасні дослідження КСЗІ	3	Екзамен
ОК11	Захист інформації у суспільно-політичній сфері	3	Залік
	Всього	**40**	
	Практика та атестація		
ОК12	Практика	20	Звіт
	Всього	**20**	
	Атестація		
ОК13	Кваліфікаційна робота	6	Захист
	Всього	**6**	
Загальний обсяг обов'язкових компонент:		**66**	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ВИБІРКОВІ КОМПОНЕНТИ (за вибором здобувача)*			
ВК1	Освітній компонент 1 з Каталогу Інституту*	3	Залік
ВК2	Освітній компонент 2 з Каталогу Інституту *	3	Залік
ВК3	Освітній компонент 3 з Каталогу Інституту *	3	Залік
ВК4	Освітній компонент 4 з Каталогу Інституту *	3	Залік
ВК5	Освітній компонент 5 з Каталогу Інституту *	3	Залік
ВК6	Освітній компонент 6 з Каталогу Інституту *	3	Залік
ВК7	Освітній компонент 7 з Каталогу Інституту *	3	Залік
ВК8	Освітній компонент 8 з Каталогу Інституту *	3	Залік
Загальний обсяг вибіркових компонент:		**24**	
ЗАГАЛЬНИЙ ОБСЯГ ОПП		**90**	

* Здобувач вищої освіти обирає один ВК із Каталогу Інституту

2.2 Структурно-логічна схема ОПП «Кібербезпека»



III. Форми атестації здобувачів другого (магістерського) ступеня вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів вищої освіти здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Роботи, які виконані не за спеціальними темами, оприлюднюються на офіційному сайті або в репозитарії Академії. Рішення щодо оприлюднення таких робіт приймається екзаменаційною комісією Академії із залученням представників режимно-секретного органу з дотриманням вимог законодавства України у сфері охорони державної таємниці.

IV. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

В Академії функціонує система забезпечення якості освітньої діяльності та якості вищої освіти, яка передбачає здійснення таких процедур і заходів:

1) визначення принципів та процедур забезпечення якості вищої освіти;

2) здійснення моніторингу та періодичного перегляду освітніх програм;

3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників закладу вищої освіти та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті Академії, на інформаційних стендах та в будь-який інший спосіб;

4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою;

6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;

8) забезпечення дотримання академічної доброчесності працівниками Академії та здобувачами вищої освіти, у тому числі створення і забезпечення функціонування ефективної системи запобігання та виявлення академічного плагіату;

9) інших процедур і заходів.

Система забезпечення Академією якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) за поданням оцінюється Національним агентством із забезпечення якості вищої освіти або акредитованими

ним незалежними установами оцінювання та забезпечення якості вищої освіти на предмет її відповідності вимогам до системи забезпечення якості вищої освіти, що затверджуються Національним агентством забезпечення якості вищої освіти, та міжнародним стандартам і рекомендаціям щодо забезпечення якості вищої освіти.

V. Перелік нормативних документів, на яких базується освітньо-професійна програма

1. Закон «Про освіту» – http://zakon5.rada.gov.ua/laws/show/2145-19.
2. Закон «Про вищу освіту» – http://zakon4.rada.gov.ua/laws/show/1556-18.
3. Закон України від 21.06.2018 р. № 2469-VIII "Про національну безпеку України" – https://zakon.rada.gov.ua/laws/show/2469-19.
4. Національний класифікатор України: "Класифікація видів економічної діяльності" ДК 009: 2010 – [Режим доступу: http://www.ukrstat.gov.ua/].
5. Національний класифікатор України: Класифікатор професій ДК 003:2010. – https://zakon.rada.gov.ua/rada/show/va327609-10.
6. НРК, 2019 – http://zakon4.rada.gov.ua/laws/show/1341-2011-п.
7. Перелік галузей знань і спеціальностей, 2015 – http://zakon4.rada.gov.ua/laws/show/266-2015-п.
8. Стандарт вищої освіти України за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, затверджений Наказом МОН України від 18.03.2021 № 332.
9. Професійний стандарт «Фахівець сфери захисту інформації», затверджений наказом Адміністрації Держспецзв'язку № 715 від 25.11.2022.
10. Положення про акредитацію освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти, затверджене Наказом Міністерства освіти і науки України від 11 липня 2019 р. № 977.

Таблиця 1

Матриця відповідності визначених Стандартом компетентностей дескрипторам Національної рамки кваліфікацій

Класифікація компетентностей (результатів навчання) за НРК	**Знання** **Зн1** Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та на межі галузей знань	**Уміння/Навички Ум1** Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур **Ум2** Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах **Ум3** Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	**Комунікація К1** Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	**Відповідальність і автономія АВ1** Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів **АВ2** Відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів **АВ3** Здатність продовжувати навчання з високим ступенем автономії
Загальні компетентності				
ЗК1	Зн1,	Ум1, Ум3	К1	АВ1, АВ2
ЗК2	Зн1,	Ум1, Ум2, Ум3		АВ2, АВ3
ЗК3	Зн1	Ум2, Ум3		АВ1
ЗК4	Зн1	Ум3		АВ1, АВ2
ЗК5	Зн1	Ум2	К1	АВ1
Спеціальні (фахові) компетентності				
ФК1	Зн1	Ум2		АВ2
ФК2	Зн1,	Ум2		АВ2
ФК3	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
ФК4	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
ФК5	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
ФК6	Зн1	Ум1, Ум2	К1	АВ1
ФК7	Зн1	Ум1, Ум2	К1	АВ1
ФК8	Зн1	Ум1, Ум2	К1	АВ1
ФК9	Зн1	Ум1, Ум2	К1	АВ1
ФК10	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2

Таблиця 2

Матриця відповідності визначених Стандартом результатів навчання та компетентностей

Програмні результати навчання	Компетентності														
	Інтегральна компетентність														
	Загальні компетентності					Спеціальні (фахові) компетентності									
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ФК1	ФК2	ФК3	ФК4	ФК5	ФК6	ФК7	ФК8	ФК9	ФК10
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	+		+	+		+	+	+			+	+	+	+	

Таблиця 3

Матриця відповідності програмних компетентностей обов'язковим компонентам освітньої програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13
ІК	+	+	+	+	+		+		+	+	+	+	+
ЗК1	+		+		+	+		+		+		+	+
ЗК2	+			+	+	+	+	+		+	+	+	+
ЗК3			+						+			+	+
ЗК4	+			+	+	+		+					+
ЗК5					+			+			+		+
ФК1	+	+	+	+	+		+		+	+	+	+	+
ФК2	+				+	+	+					+	+
ФК3							+						+
ФК4				+	+	+		+					+
ФК5					+	+		+				+	+
ФК6	+			+	+	+						+	+
ФК7								+			+		+
ФК8	+		+	+	+	+	+			+		+	+
ФК9	+							+			+		+
ФК10	+		+	+	+	+	+	+		+		+	+

Таблиця 4

Матриця забезпечення програмних результатів навчання обов'язковими компонентами освітньо-професійної програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13
ПРН1	+			+	+	+		+				+	+
ПРН2			+	+	+		+	+		+	+		+
ПРН3	+			+	+		+	+		+			+
ПРН4		+	+				+	+			+		+
ПРН5	+			+	+	+	+			+			+
ПРН6	+	+		+	+	+			+		+		+
ПРН7	+		+	+	+	+	+	+		+		+	+
ПРН8								+			+		+
ПРН9	+		+	+	+						+		+
ПРН10	+				+	+	+			+			+
ПРН11			+	+	+			+			+		+
ПРН12	+			+	+	+						+	+
ПРН13			+		+								+
ПРН14	+	+		+	+	+		+					+
ПРН15			+		+		+	+		+	+	+	+
ПРН16				+	+	+		+		+			+
ПРН17	+	+		+	+			+	+	+	+	+	+
ПРН18	+	+	+	+			+	+			+		+
ПРН19	+				+		+	+			+	+	+
ПРН20	+					+		+	+	+			+
ПРН21									+				+
ПРН22			+			+					+		+
ПРН23	+					+					+	+	+

Гарант освітньої програми **Іван СЕРВЕЦЬКИЙ**