ПРОЄКТ

Приватне акціонерне товариство «Вищий навчальний заклад

«Міжрегіональна Академія управління персоналом»

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

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА»

Рівень вищої освіти: **перший (бакалаврський)**

Ступінь вищої освіти: **бакалавр**

Галузь знань: **F Інформаційні технології**

Спеціальність: **F5 Кібербезпека та захист інформації**

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

Освітня програма вводиться в дію з
01 вересня 2025 року
наказ № _____від «_____» _____ 2025 р.
Ректор /_____/ Кирило МУРАВЙОВ

КИЇВ - 2025

ПЕРЕДМОВА

Освітньо-професійна програма «Кібербезпека» першого (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 першого (бакалаврського) вищої освіти, затверджений та введений в дію наказом Міністерства освіти і науки України від 04.10.2018 р. № 1074

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

Керівник групи:
Когут Юрій Іванович – кандидат юридичних наук, доцент кафедри Інформаційної безпеки Інституту безпеки ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом» – гарант програми.

Члени групи:
Сервецький Іван Васильович - доктор юридичних наук, доцент, професор кафедри Національної безпеки Інституту безпеки ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом».
Підюков Петро Павлович - доктор юридичних наук, професор, професор кафедри Національної безпеки Інституту безпеки ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом».
Сидоренко Сергій Миколайович - керівник Всеукраїнського об'єднання організацій роботодавців охоронної галузі «Федерація професіоналів безпеки».
Здобувач освіти:
Мазур Андрій, здобувач 2 курсу ОП «Кібербезпека».

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 першим (бакалаврським) 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		

1. Профіль 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	Перший (бакалаврський) рівень
Ступінь вищої освіти	Бакалавр
Галузь знань	F – «Інформаційні технології»
Спеціальність	F5 Кібербезпека та захист інформації
Обмеження щодо форм навчання	Без обмеження
Освітня кваліфікація	Бакалавр з кібербезпеки та захисту інформації
Професійна кваліфікація	Не надається
Кваліфікація в дипломі	Ступінь вищої освіти – бакалавр Спеціальність – F5 Кібербезпека та захист інформації Освітня програма – «Кібербезпека»
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС,термін навчання: денна форма – 4 роки, заочна – 4 роки і 6 місяців.
Наявність акредитації	-
Цикл/рівень	НРК України – 6 рівень, FQ-EHEA – 1 цикл,EQF LLL – 6 рівень
Передумови	Повна загальна середня освіта (або освітньо-кваліфікаційний рівень «молодшого бакалавра», «фахового молодшого бакалавру», «молодшого спеціаліста») Умови прийому на навчання до закладів вищої освіти України. Правила прийому на навчання до Приватного акціонерного

	товариства “Вищий навчальний заклад “Міжрегіональна Академія управління персоналом”.
Мова(и) викладання	Українська мова
Термін дії освітньоїпрограми	До повного завершення періоду навчання або наступного оновлення програми
Інтернет-адреса постійного розміщення опису освітньої програми	https://maup.com.ua/assets/files/opp/bezpeka/kiber-bezpeka-bakalavr-2025.pdf
2 – Мета освітньої програми	
Підготовка висококваліфікованих та конкурентоспроможних фахівців здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, пов'язаних із забезпеченням цілісного підходу до захисту систем від атак, вірусів, несанкціонованого доступу до конфіденційних даних тощо у різних сферах професійної діяльності	
3 - Характеристика освітньої програми	
Опис предметної області	***F - Інформаційні технології*** ***F5 Кібербезпека та захист інформації*** ***Об’єкти професійної діяльності випускників***: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту. ***Цілі навчання***: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. ***Теоретичний зміст предметної області***: Знання – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних

	технологій; – автоматизованих систем проектування. <u>Методи, методики та технології:</u> Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. <u>Інструменти та обладнання:</u> – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій
Орієнтація освітньої програми	Освітньо-професійна програма
Основний фокус освітньої професійної програми та спеціалізації	Вивчення новітніх концепцій, моделей і методів теорії алгоритмів, основних парадигм проєктування автоматизованих систем захисту інформації, розробки сучасного програмно- апаратного забезпечення інформаційно-комунікаційних технологій; принципів супроводусистем та комплексів інформаційної та кібербезпеки, методів та засобів технічного та криптографічного захисту інформації, методіввиявлення та ідентифікації ризиків. Ключові слова: кібербезпека; інформаційна безпека, інформаційно-комунікаційні системи, загрози і ризики, моніторинг, програмні і програмно-апаратні засоби захисту, технічні засоби захисту, криптографічний захист, антивірусний захист, стандарти інформаційної безпеки, політики інформаційної та/або кібербезпеки, системи управління інформаційною та/або кібербезпекою.
Особливості програми	Програма розроблена з урахуванням загальноєвропейських вимог до студентоцентрованого навчання, міжнародних зразків та директив European Standards und Guidelines der ENQA, враховуються рекомендації міжнародної асоціації обчислювальної техніки (Association for Computing Machinery, Curricula Recommendations: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science, Curriculum Guidelines for Undergraduate Programs in Computer Science). Проходження практики на базі підприємств-партнерів та участь студентів у виконанні спільних проєктів на замовлення установ та провідних ІТ-компаній України за фахом. Кваліфікація, здобута в результаті освоєння програми, чітко відповідає бакалаврському рівню Національної рамки кваліфікацій у вищій освіті й системі кваліфікацій в європейському просторі вищої освіти.
4 – Придатність випускників до працевлаштування та подальшогонавчання	

Придатність до працевлаштування	Випускник освітнього рівня бакалавр після успішного виконання освітньої програми здатен виконувати професійну роботу і, відповідно до Національного класифікатора України: Класифікатор професій (ДКП 003:2010), займати первинну посаду за категоріями: 2132.2 Розробник систем захисту інформації 2139.2 Адміністратор мереж і систем 2139.2 Аналітик загроз безпеки 2139.2 Аналітик систем захисту інформації та оцінки вразливостей 2139.2 Аналітик з безпеки інформаційно-телекомунікаційних систем 2139.2 Дізнавач (сфера кібербезпеки та захисту інформації) 2139.2 Експерт-криміналіст (сфера кібербезпеки та захисту інформації) 2139.2 Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації) 2139.2 Слідчий з кіберзлочинів 2139.2 Фахівець з криптографічного захисту інформації 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології) 2139.2 Фахівець з підтримки інфраструктури кіберзахисту 2139.2 Фахівець з реагування на інциденти кібербезпеки 2139.2 Фахівець з тестування систем захисту інформації 2139.2 Фахівець з технічного захисту інформації 2139.2 Фахівець сфери захисту інформації 2359.2 Інструктор-методист з інформаційної безпеки та кібербезпеки 3439 Фахівець із організації інформаційної безпеки 3439 Фахівець із організації захисту інформації з обмеженим доступом
Академічні права випускників	Можливість навчання за програмою другого (магістерського) рівня вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Методи, засоби та технології: Проблемно-орієнтоване навчання, яке передбачає формулювання та вирішення проблеми під час лекцій, розв`язання ситуативних задач на семінарах, практичних заняттях, дослідження проблеми під час самостійної роботи здобувачів вищої освіти. Практико-орієнтоване навчання через різні види практик на підприємствах, установах та організаціях різних форм власності на підставі договорів про проходження практики. Виконання практичних та лабораторних робіт в умовах наближених до професійного застосування. Технології дистанційного навчання, що реалізуються шляхом проведення дистанційних занять, конференцій, семінарів, лабораторних робіт, практикумів й інших форм навчальних занять, які проводяться за допомогою засобів телекомунікацій з використанням веб-технологій. Інформаційні технології навчання: робота здобувачів вищої освіти у спеціалізованих кабінетах та лабораторіях облаштованих

	мультимедійними комплексами, комп'ютерною технікою та відповідним програмним забезпеченням, що надає можливість проведення інтерактивних лекцій, застосування пошукової методики здобуття нових знань та організації проєктної роботи, виконання лабораторних тв курсових робіт. Проєктні технології навчання реалізуються через курсові проєкти зі сталого розвитку та фахового спрямування. Інструменти та обладнання: Комп'ютери, комп'ютерні мережі, хмарні технології, системи управління базами даних, спеціалізовані програмні бібліотеки, когнітивні інтерфейси, операційні системи
Оцінювання	Усні, письмові, творчі, тестові та комбіновані екзамени, диференційовані заліки, лабораторні звіти, звіти із практичних робіт та практик, реферати, захист курсових робіт (проєктів), презентації, поточний контроль, публічний захист кваліфікаційної роботи. 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) 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 – Перелік компетентностей випускника	
Інтегральна компетентність (ІК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. 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; КЗ 7. 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.
Фахові компетентності	КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
7 – Нормативний зміст підготовки здобувачів вищої освіти, сформульований у контексті результатів навчання (ПРН)	
ПРН1.	застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

ПРН2.	організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;.
ПРН3.	використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
ПРН4.	аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
ПРН5.	адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
ПРН6.	критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності
ПРН7.	діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
ПРН8.	готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
ПРН9.	впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
ПРН10.	виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
ПРН11.	виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах;
ПРН12.	розробляти моделі загроз та порушника;
ПРН13.	аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
ПРН 14.	вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
ПРН 15.	використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;

ПРН 16.	реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
ПРН 17.	забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
ПРН 18.	використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
ПРН 19.	застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
ПРН 20.	забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;
ПРН 21.	вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
ПРН 22.	вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
ПРН 23.	реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
ПРН 24.	вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
ПРН 25.	забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;
ПРН 26.	впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
ПРН 27.	вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
ПРН 28.	аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-

	телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;
ПРН 29.	здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
ПРН 30.	здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
ПРН 31.	застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
ПРН 32.	вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
ПРН 33.	вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
ПРН 34.	приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
ПРН 35.	вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;
ПРН 36.	виявляти небезпечні сигнали технічних засобів;
ПРН 37.	вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;
ПРН 38.	інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
ПРН 39.	проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
ПРН 40.	інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;

ПРН 41.	забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
ПРН 42.	впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
ПРН 43.	застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;
ПРН 44.	вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;
ПРН 45.	застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
ПРН 46.	здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
ПРН 47.	вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
ПРН 48.	виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;
ПРН 49	забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;
ПРН 50.	забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
ПРН 51.	підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;
ПРН 52.	використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;
ПРН 53.	вирішувати задачі аналізу програмного коду на наявність можливих загроз.
ПРН 54.	усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
8- Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Всі науково-педагогічні працівники, що забезпечують освітньо-професійну програму за кваліфікацією відповідають профілю і напряму дисциплін, що викладаються, мають необхідний стаж педагогічної роботи та досвід практичної роботи. В процесі організації навчального

	процесу (включає і проведення аудиторних занять) залучаються професіонали з досвідом дослідницької, управлінської, інноваційної, творчої та фахової роботи, експерти галузі та представники роботодавців. До освітнього процесу залучаються роботодавці ІТ-сфери та професіонали- практики в галузі кібербезпеки та захисту інформації. Відбувається постійне підвищення кваліфікації та стажування науково-педагогічних працівників, які забезпечують освітній процес
Матеріально-технічне забезпечення	Реалізація програми забезпечується: Приміщеннями для проведення навчальних занять та контрольних заходів; спеціалізованими лабораторіями; Мультимедійним обладнанням для одночасного використання в навчальних аудиторіях; Наявністю соціально-побутової інфраструктури, зокрема бібліотеки з читальним залом комп'ютерними робочими місцями; лабораторій, вільний доступу до Інтернет та інформаційних ресурсів, необхідних для навчання, викладацької та наукової діяльності; Наявна вся необхідна соціально-побутова інфраструктура, кількість місць у гуртожитках відповідає вимогам.
Інформаційне та навчально-методичне забезпечення	Офіційний веб-сайт https://maup.com.ua; міжнародний бібліотечно-інформаційний центр імені Ярослава Мудрого: https://library.iapm.edu.ua, читальний зал; доступ до системи дистанційного навчання Moodle https://do.iapm.edu.ua, навчальна, наукова, навчально-методична література, фахові журнали; робочі навчальні плани; графіки освітнього процесу, навчально- методичні комплекси дисциплін; робочі програми дисциплін; дидактичні матеріали для самостійної роботи студентів з дисциплін; програми практики;
9 – Академічна мобільність	
Національна кредитна мобільність	На загальних підставах у межах України. На основі двосторонніх договорів між ПрАТ «ВНЗ «МАУП» та закладами вищої освіти України.Можливість подвійного дипломування.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між ПрАТ «ВНЗ «МАУП» та навчальними закладами іноземних країн-партнерів. Можливість подвійного дипломування.
Навчанняіноземних здобувачів вищої освіти	На основі договорів (угод) між ПрАТ «ВНЗ «МАУП» та закладами вищої освіти іноземних країн.Умовою зарахування іноземців на навчання для отримання певного освітнього ступеня є володіння ними мовою навчання на рівні, достатньому для засвоєння навчального матеріалу.

ІІ. Обсяг кредитів ЄКТС, необхідних для здобуття першого (бакалаврського) ступеня вищої освіти

Обсяг освітньої програми бакалавра:
- на базі повної загальної середньої освіти– 240 кредитів ЄКТС - на базі

ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста).

На основі ступеня «фаховий молодший бакалавр» заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти.

Прийом на основі ступенів «молодший бакалавр», «фаховий молодший бакалавр» або освітньо-кваліфікаційного рівня «молодший спеціаліст» здійснюється за результатами зовнішнього незалежного оцінювання в порядку, визначеному законодавством.

Мінімум 75% обсягу освітньої програми має бути спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю визначеною стандартом вищої освіти.

2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1 Перелік компонент ОП «Кібербезпека»

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проєкти (роботи),практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ			
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
ОК1	Історія та культура України	4	Екзамен
ОК2	Українська мова професійного спрямування	4	Екзамен
ОК3	Філософія	4	Екзамен
ОК4	Фізичне виховання	4	Залік
ОК5	Іноземна мова	12	Залік/Екзамен
ОК6	Вища математика	9	Залік/Екзамен
ОК7	Основа безпеки організацій	3	Залік
ОК8	Ділова іноземна мова	12	Залік/Екзамен
Всього за циклом:		**52**	
ОБОВ’ЯЗКОВІ КОМПОНЕНТИ			
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОК9	Теоретичні основи захисту інформації	4	Екзамен
ОК10	Програмування та комп’ютерна техніка	5	Екзамен
ОК11	Дискретна математика	5	Залік
ОК12	Програмування та алгоритмізація	5	Екзамен
ОК13	Інформаційна безпека держави	6	Екзамен
ОК14	Сигнали та процеси інформаційних систем	4	Залік
ОК15	Комп’ютерні системи та мережі Частина 1	5	Екзамен
ОК16	Теорія ймовірностей та математична статистика	4	Екзамен
ОК17	Об’єктно-орієнтоване програмування	6	Залік/Екзамен
ОК18	Курсова робота з об’єктно-орієнтованого програмування	3	КР
ОК19	Бази даних і знань	4	Екзамен
ОК20	Нормативно-організаційне забезпечення інформаційної безпеки	4	Екзамен
ОК21	Теорія держави і права	3	Залік
ОК22	Теорія інформації та кодування	4	Екзамен
ОК23	Фізичні основи захисту інформації	4	Екзамен
ОК24	Криптографічні системи захисту інформації	6	Екзамен
ОК25	Курсова робота з криптографічних систем захисту інформації	3	КР
ОК26	Безпека комп’ютерних мереж і систем	4	Екзамен
ОК27	Інформаційно-телекомунікаційні системи	6	Екзамен

ОК28	Технології виявлення шкідливого трафіку	4	Екзамен
ОК29	Математичний аналіз	5	Екзамен
ОК30	Управління інформаційною безпекою	4	Екзамен
ОК31	Розвідка на основі відкритих джерел (OSINT)	4	Екзамен
ОК32	Комп'ютерна та мережева криміналістика	4	Екзамен
ОК33	Аудит та моніторинг кібернетичної безпеки	4	Екзамен
Практика			
ОК 34	Навчальна	4	Захист звіту
ОК 35	Виробнича	4	Захист звіту
ОК 36	Переддипломна	7	Захист звіту
Кваліфікаційна робота			
ОК37	Кваліфікаційна робота	3	Кваліфікаційна атестація
Всього за циклом		**128**	
Загальний обсяг обов'язкових компонент:		**180**	
ВИБІРКОВІ КОМПОНЕНТИ			
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ (за вибором здобувача)*			
ВК1	Освітній компонент 1 з Каталогу Академії*	3	Залік
ВК2	Освітній компонент 2 з Каталогу Академії*	3	Залік
ВК3	Освітній компонент 3 з Каталогу Академії*	3	Залік
ВК4	Освітній компонент 4 з Каталогу Академії*	3	Залік
Всього за циклом:		**12**	
ВИБІРКОВІ КОМПОНЕНТИ			
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ (за вибором здобувача)*			
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
ВК9	Освітній компонент 9 з Каталогу Інституту**	3	Залік
ВК10	Освітній компонент 10 з Каталогу Інституту**	3	Залік
ВК11	Освітній компонент 11 з Каталогу Інституту**	3	Залік
ВК12	Освітній компонент 12 з Каталогу Інституту**	3	Залік
ВК13	Освітній компонент 13 з Каталогу Інституту**	3	Залік
ВК14	Освітній компонент 14 з Каталогу Інституту**	3	Залік
ВК15	Освітній компонент 15 з Каталогу Інституту**	3	Залік
ВК16	Освітній компонент 16 з Каталогу Інституту**	3	Залік
ВК17	Освітній компонент 17 з Каталогу Інституту**	3	Залік
ВК18	Освітній компонент 18 з Каталогу Інституту**	3	Залік
ВК19	Освітній компонент 19 з Каталогу Інституту**	3	Залік
ВК20	Освітній компонент 20 з Каталогу Інституту**	3	Залік
Всього за циклом:		**48**	
Загальний обсяг вибіркових компонент:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

* Здобувач вищої освіти обирає одну ВК із Каталогу Академії

** Здобувач вищої освіти обирає одну ВК із Каталогу Інституту

2.2 Структурно-логічна схема ОП «Кібербезпека»

Рік навчання	Семестр	
І курс	**1 семестр**	**2 семестр**
	ОК1	ОК4
	ОК2	ОК5
	ОК3	ОК6
	ОК4	ОК11
	ОК5	ОК12
	ОК6	ВК1
	ОК9	ВК2
	ОК10	ВК3
ІІ курс	**3 семестр**	**4 семестр**
	ОК5	ОК5
	ОК13	ОК7
	ОК14	ОК17
	ОК15	ОК19
	ОК16	ОК20
	ОК17	ВК6
	ВК4	ВК7
	ВК5	ОК34
ІІІ курс	**5 семестр**	**6 семестр**
	ОК8	ОК8
	ОК21	ОК24
	ОК22	ОК27
	ОК23	ОК28
	ОК24	ВК10
	ОК26	ВК11
	ВК8	ВК12
	ВК9	ОК35
IV курс	**7 семестр**	**8 семестр**
	ОК8	ОК8
	ОК29	ОК32
	ОК30	ОК33
	ОК31	ВК17
	ВК13	ВК18
	ВК14	ВК19
	ВК15	ВК20
	ВК16	ОК36
		ОК37

III. Форми атестації здобувачів першого (бакалаврського) ступеня вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.
Вимоги до кваліфікаційної роботи	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом та освітньою програмою.

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 тазабезпечення 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 Стандарт вищої освіти

1. Закон України «Про вищу освіту» 01.07.2014 №1556-VII - Режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18.
2. Закон України «Про захист інформації в інформаційнотелекомунікаційних системах» - відомості Верховної Ради України (ВВР), 1994, N 31, ст.286
3. Закон України "Про основні засади забезпечення кібербезпеки України"- відомості Верховної Ради (ВВР), 2017, № 45, ст.403;
4. «Доктрина інформаційної безпеки України», затверджено Указом Президента України від 25 лютого 2017 року № 47/2017.
5. Постанова Кабінету Міністрів «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29.04.2015 р. № 266
6. Рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 27.01.2016 р., уведеного в дію Указом Президента України від 15.03.2016 р. № 96.
7. Постанова Кабінету Міністрів «Про затвердження Ліцензійних умов провадження освітньої діяльності» від 30.12.2015 № 1187Наказ МОН України №166 «Деякі питання оприлюднення інформації про діяльність вищих навчальних закладів» від 19.02.2015 р.
8. Наказ МОН України «Про особливості запровадження переліку галузей знань, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29.04. 2015 р.» № 266 від 06.11.2015 р. №1151.
9. Національний класифікатор України: "Класифікатор професій" ДК 003:2010 // Видавництво "Соцінформ". - К.: 2010
10. Наказ Міністерства економічного розвитку і торгівлі України від «Про затвердження зміни до національного класифікатора України ДК 003:2010» від 18.11. 2014 р. № 1361 (зміна № 2)

Таблиця 1

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

Загальні обов'язкові компетентності

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК12	ОК 13	ОК 14	ОК15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
КЗ 1									+	+	+	+						+	+				+		+		+	+			+	+		+	
КЗ 2		+						+	+			+	+		+			+	+	+	+	+	+			+	+	+	+						+
КЗ 3		+			+		+																												
КЗ 4								+	+		+		+		+	+		+					+	+		+	+	+		+	+	+	+	+	+
КЗ 5						+				+	+		+	+		+	+	+	+		+	+		+	+					+	+	+			+
КЗ 6	+		+																+	+															
КЗ 7	+		+	+									+							+													+			

Таблиця 2

Фахові обов'язкові компетентності

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК12	ОК 13	ОК 14	ОК15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35
КФ 1																			+	+							+			+	+	+	+		
КФ 2						+			+	+	+				+	+	+	+	+		+	+	+	+			+		+		+	+	+		
КФ 3										+					+		+	+			+		+	+	+		+			+		+			
КФ 4											+							+				+		+		+		+		+				+	
КФ 5																					+		+	+	+									+	
КФ 6												+		+				+				+		+	+					+		+			
КФ 7												+															+	+				+			+
КФ 8																				+								+	+	+					+
КФ 9																+									+					+		+		+	
КФ 10										+							+						+			+	+	+	+					+
КФ 11															+									+	+	+		+					+	+	
КФ 12									+	+				+			+									+	+					+		+

Таблиця 3

Матриця забезпечення результатів навчання (ПРН)

відповідним компонентам освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК12	ОК 13	ОК 14	ОК15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35
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									+						+							+		+	+							+	+		

Продовження таблиці 3

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК12	ОК 13	ОК 14	ОК15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35
ПРН 14												+			+			+					+	+		+			+	+					+
ПРН 15										+					+		+	+						+	+	+								+	
ПРН 16															+									+		+	+	+							+
ПРН 17												+			+						+		+	+	+	+		+						+	
ПРН 18										+		+			+		+	+						+										+	
ПРН 19														+					+		+	+		+		+						+			
ПРН 20										+		+					+							+				+						+	
ПРН 21						+																		+				+							+
ПРН 22									+															+		+			+			+			
ПРН 23								+	+							+			+					+				+							+
ПРН 24																		+						+										+	
ПРН 25											+													+				+							
ПРН 26						+			+															+	+				+						+
ПРН 27																					+														
ПРН 28									+																							+	+		

Продовження таблиці 3

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК12	ОК 13	ОК 14	ОК15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35
ПРН 29									+	+							+				+						+		+					+	
ПРН 30		+			+				+																+	+								+
ПРН 31										+							+							+	+				+			+		
ПРН 32					+									+	+									+	+					+			+	
ПРН 33								+	+									+									+								
ПРН 34									+										+											+				+	+
ПРН 35															+	+					+ +			+	+		+							+	
ПРН 36														+												+									+
ПРН 37														+				+																+	
ПРН 38						+																			+	+									+
ПРН 39																											+					+	+	+	
ПРН 40						+																+													
ПРН 41					+		+											+						+				+							+
ПРН 42					+		+																	+			+	+							+
ПРН 43		+			+		+																					+			+			+	

Продовження таблиці 3

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК12	ОК 13	ОК 14	ОК15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35
ПРН 44		+							+																	+		+							+
ПРН 45		+																								+		+							+
ПРН 46					+	+			+																+	+		+							
ПРН 47										+		+					+			+	+		+									+			
ПРН 48				+						+					+		+		+		+			+		+		+				+			
ПРН 49					+							+								+				+	+		+	+			+	+		+
ПРН 50				+				+					+													+			+	+				+	
ПРН 51					+					+							+							+	+		+							+	
ПРН 52																									+				+						+
ПРН 53							+			+		+					+					+				+						+			
ПРН 54	+	+	+	+									+						+	+												+	+		

Гарант освітньої програми **Юрій КОГУТ**