Приватне акаціонерне товариство «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»

ЗАТВЕРДЖЕНО:
Вченою радою
ПрАТ «ВНЗ МАУП»
протокол № ___ від ___ 20__ р.
Голова Вченої ради, президент
_____ **Ростислав ШОКІН**

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Рівень вищої освіти:	**Перший (бакалаврський) рівень вищої освіти**
Ступінь вищої освіти:	**Бакалавр**
Галузь знань:	**12 Інформаційні технології**
Спеціальність:	**125 Кібербезпека**
Кваліфікація:	**бакалавр з кібербезпеки**

Освітня программа вводиться в дію з
09. 2022 р.
Ректор _____ /_____/
наказ №05/1-0 від "27" 01 2022р.

Київ 2022

Лист погодження
освітньо - професійної програми

«РОЗРОБЛЕНО»
Робочою групою Інституту
Комп'ютерно-інформаційних
технологій та дизайну
ПрАТ «ВНЗ «МАУП»
керівник робочої групи
_____ А.Ю.Голобобов
«13» 01 2022 р.

«СХВАЛЕНО»
Вченою радою Інституту
Комп'ютерно-інформаційних
технологій та дизайну
Протокол № 6
від «24» 01 2022 р.
Голова Вченої ради Інституту
_____ О.Г.Чорнишкіна

«РЕКОМЕНДОВАНО»
Науково-методичною комісією
вченої ради
ПрАТ «ВНЗ «МАУП»
Протокол № 1
від «26» 01 2022р.
Голова комісії Академії
_____ С.В.Храпатий

«УХВАЛЕНО»
на засіданні кафедри інформаційної
безпеки
ПрАТ «ВНЗ «МАУП»
Протокол № 6
«13» 01 2022 р.
Завідувач кафедри _____ А.Ю.Голобобов

«ПОГОДЖЕНО»
Директор Навчально-методичного
інституту ПрАТ «ВНЗ «МАУП»»
_____ О.І.Борисенко
«25» 01 2022р.

ПЕРЕДМОВА

1. Затверджено та надано чинності рішенням Вченої ради ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», протокол №_____

2. Освітня програма була розроблена на підставі Закону України «Про вищу освіту» з урахуванням Стандарту зі спеціальності 125 «Кібербезка» для першого (бакалаврського) вищої освіти робочою групою у складі:

Гарант освітньої програми:

Гололобов Андрій Юрійович – доцент кафедри інформаційної безпеки, кандидат технічних наук.

Члени робочої групи:

Чолишкіна Ольга Геннадіївна – директор ІКІТД МАУП, кандидат технічних наук, доцент;

Людвиченко Валентин Олександрович – доцент кафедри комп'ютерних інформаційних систем і технологій, старший науковий співробітник, кандидат фізико-математичних наук..

Зовнішні стейкхолдери:

1. Кучук Георгій Анатолійович – доктор технічних наук, професор, професор кафедри електронних обчислювальних машин ХНУРЕ;
2. Рябий Мирослав Олександрович – кандидат технічних наук, директор IT компанії ТОВ «Омега-девелопмент»

Ліцензія на провадження освітньої діяльності була отримана 12.07.2016 р. наказ МОН України №1405-л від 12.07.2016 року.

Профіль освітньо-професійної програми зі спеціальності
125 Кібербезпека

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	ПрАТ «Вищий навчальний заклад»Міжрегіональна Академія управління персоналом» Інституту комп'ютерно-інформаційних систем і дизайну Кафедра інформаційної безпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Бакалавр з кібербезпеки
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 р.10 міс.
Наявність акредитації	-
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA– перший цикл, EQF LLL – 6 рівень
Передумови	Повна загальна середня освіта (або освітньо-кваліфікаційний рівень молодшого спеціаліста)
Мова(и) викладання	Українська мова
Термін дії освітньої програми	До повного завершення періоду навчання або наступного оновлення програми
Інтернет-адреса постійного розміщення опису освітньої програми	http://maup.com.ua
2 – Мета освітньої програми	
Підготовка фахівців, здатних використовувати і впроваджувати інноваційні технології, математичні методи в сфері захисту інформації та кібербезпеки.	
3 - Характеристика освітньої програми	

Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	*Галузь знань:* 12 Інформаційні технології *Спеціальність:* 125 Кібербезпека *Об'єкт вивчення та / або професійної діяльності:* - 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 кібербезпекою об'єктів, що підлягають захисту.
	Цілі навчання: - підготовка фахівців, здатних проводити теоретичні та експериментальні дослідження в галузі кібербезпеки та інфокомунікаційних технологій, застосовувати математичні методи й алгоритмічні принципи в моделюванні, проєктуванні, розробці та супроводі систем захисту інформації; - освоєння компетенцій в області кібербезпеки, визначених стандартом вищої освіти шляхом здобуття практичного досвіду при розробці технологій інформаційної та кібербезпеки; - формування у здобувачів ОП Soft Skills, шляхом заохочення до всебічного використання індивідуальної освітньої траєкторії та популяризації активності у житті органів студентського самоврядування, наукових, творчих та спортивних колективах, що існують при Академії *Теоретичний зміст предметної області*: сучасні моделі, методи, алгоритми, технології інформаційної та кібербезпеки. <u>Знання</u> - 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. Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. Інструменти та обладнання: - системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; - сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	*Освітньо-професійна* Освітньо-професійна програма підготовки бакалаврів розроблена для студентів, які прагнуть стати висококваліфікаційними фахівцями у сфері кібербезпеки, забезпечує здобуття теоретичних та практичних знань, необхідних для виконання спеціалізованих завдань та вирішення практичних проблем у галузі кібербезпеки. Програма ґрунтується на загальновідомих положеннях та результатах сучасних наукових досліджень у галузі кібербезпеки із урахуванням актуального стану ІТ- сфери та орієнтує на спеціалізації, у межах яких можлива професійна кар'єра майбутніх фахівців.

Основний фокус освітньої програми та спеціалізації	Загальна вища освіта першого (бакалаврського) рівня в галузі інформаційних технологій за спеціальністю «Кібербезпека» на основі базової підготовки та здатності до швидкого самостійного опанування новими технологіями та системами. Вивчення новітніх концепцій, моделей і методів теорії алгоритмів, основних парадигм проєктування автоматизованих систем захисту інформації, розробки сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; принципів супроводу систем та комплексів інформаційної та кібербезпеки, методів та засобів технічного та криптографічного захисту інформації, методів виявлення та ідентифікації ризиків. *Ключові слова*: Ключові слова: захист інформації, кіберпростір, кібератаки, система захисту, проектування комплексних систем захисту, захист програмного забезпечення, сервіси безпеки.
Особливості програми	Програма розроблена з урахуванням загальноєвропейских 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 переддипломної практики на базі підприємств-партнерів та участь студентів у виконанні спільних проектів 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 подальшого навчання	
Придатність до працевлаштування	Випускник може працювати на підприємствах державного та приватного сектору, у виробничих та науково-виробничих об’єднаннях, науково-дослідних організаціях, у державних та банківських

	установах, інформаційних центрах на посадах відповідно до Національного класифікатора України (Класифікатор професій - ДК 003:2010): 3439 - Фахівець із захисту інформації в інформаційних і комунікаційних системах, Фахівець із організації інформаційної безпеки. 3121 - Фахівець з інформаційних технологій. Можуть працювати фахівцями із захисту інформації та кібербезпеки в складі відповідних департаментів організацій, підприємств та банків, розробниками та тестувальниками застосунків, що потребують виконання особливих вимог щодо інформаційної та кібернетичної безпеки; співробітниками служб захисту інформації; адміністраторами інформаційної та кібернетичної безпеки, проектувальниками систем захисту в кіберпросторі; розробниками програмних та програмно-апаратних засобів захисту інформації в кіберпросторі, консультантами-інструкторами з кібербезпеки, спеціалістами в галузі кібербезпеки в складі правоохоронних органів, спеціалістами з забезпечення кібербезпеки в кіберпросторі (зокрема, в соціальних мережах; об'єктах з використанням "інтернету речей", об'єктах критичної інфраструктури (електростанції, водо-, газопостачання тощо)).
Подальше навчання	Можливість продовження навчання за програмами другого циклу вищої освіти (НРК України - 7 рівень, FQ-EHEA - другий цикл, EQF LLL - 7 рівень).
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 застосуваня. Технології дистанційного навчання, що реалізуються за допомогою комп'ютерної техніки, 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 облаштованих мультимедійними комплексами, що забезпечує можливість проведення інтерактивних лекцій, застосування пошукової методики здобуття нових знань та організації проєктної роботи. Проєктні технології навчання реалізуються через курсові проєкти зі сталого розвитку та фахового спрямування. *Інструменти та обладнання:* Комп'ютер, комп'ютерні мережі, хмарні технології, системи управління базами даних, спеціалізовані програмні бібліотеки, когнітивні інтерфейси, операційні системи, обладнання Cisco.
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, заліки та диференційовані заліки проводяться відповідно до вимог п.6.5 та розділу 7 Положення про організацію освітнього процесу в ПрАТ «ВНЗ «МАУП» та п.5.3 «Положення про внутрішню систему забезпечення якості вищої освіти у ПрАТ «ВНЗ «МАУП», «Положення про оцінювання навчальних досягнень здобувачів вищої освіти у ПрАТ «ВНЗ «МАУП».
6 – Програмні компетентності	
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 (ЗК)	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної сфери та розуміння професійної діяльності. ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК 5. Здатність до пошуку, оброблення та аналізу інформації. ЗК 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. ЗК 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності й досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної галузі, її місця у загальній системі знань про природу й суспільство та у розвитку суспільства, техніки й технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Фахові компетентності (ФК)	ФК 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. ФК 2. Здатність до використання інформаційнокомунікаційних технологій, сучасних методів і моделей інформаційної безпеки. ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики безпеки. ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-

	телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК 7. Здатність забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою. ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційнотелекомунікаційних (автоматизованих) систем. ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам. ФК 13. *Здатність до розробки мережевого програмного забезпечення, що функціонує на основі різних топологій структурованих кабельних систем, використовує комп'ютерні системи й мережі передачі даних та аналізує якість роботи комп'ютерних мереж.* ФК. 14. *Здатність до аналізу характеристик джерел інформації, вибору ефективних методів та алгоритмів кодування даних в комп'ютерних інформаційних технологіях.*
7 – Програмні результати навчання	
ПР1	Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
ПР2	Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

ПР3	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
ПР4	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;
ПР5	Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
ПР6	Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
ПР7	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
ПР8	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
ПР9	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
ПР10	Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
ПР11	Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;
ПР12	Розробляти моделі загроз та порушника;
ПР13	Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
ПР14	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

ПР15	Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
ПР16	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
ПР17	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;
ПР18	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
ПР19	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
ПР20	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;
ПР21	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;
ПР22	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційнотелекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
ПР23	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
ПР24	Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на

	основі моделей управління доступом (мандатних, дискреційних, рольових);
ПР25	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;
ПР26	Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
ПР27	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
ПР28	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;
ПР29	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;
ПР30	Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
ПР31	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
ПР32	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
ПР33	Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

ПР34	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
ПР35	Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;
ПР36	Виявляти небезпечні сигнали технічних засобів;
ПР37	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;
ПР38	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
ПР39	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
ПР40	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
ПР41	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
ПР42	Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
ПР43	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;

ПР44	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;
ПР45	Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
ПР46	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
ПР47	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
ПР48	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;
ПР49	Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;
ПР50	Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
ПР51	Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;
ПР52	Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;
ПР53	Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
ПР54	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	До реалізації програми залучається не менше ніж 50% науково-педагогічних працівників, які мають науковий ступінь та/або вчене звання, не менше ніж 25% мають науковий ступінь доктора наук або вчене звання професора. 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. 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, гуртожитків; комп'ютерних робочих місць, лабораторій, полігонів, обладнання, устаткування, доступу до Інтернету 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	Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого освітній програмі профілю, зокрема електронних. Наявність безоплатного доступу викладачів і здобувачів вищої освіти до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. Наявність офіційного веб-сайту закладу освіти, на якому розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня/освітньо-наукова/ видавнича/ атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їхній склад, перелік навчальних дисциплін, правила прийому, контактна інформація). Наявність електронного ресурсу закладу освіти, який містить матеріали, необхідні для навчання, викладацької та наукової діяльності. Відповідне інформаційне та навчально-методичне забезпечення розташоване на серверах Академії, на освітніх платформах Moodle.
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 зарубіжних країн- партнерів. Можливість подвійного дипломування.
Навчання іноземних 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.

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

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
1. Обов'язкові компоненти ОП			
1.1 ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
1.1.1. ДИСЦИПЛІНИ ГУМАНІТАРНОЇ ПІДГОТОВКИ		**40**	
ОК.1	Англійська мова	12	залік /іспит
ОК.2	Українська мова професійного спрямування	4	залік
ОК.3	Історія та культура України	4	іспит
ОК.4	Правознавство	4	іспит
ОК 5	Фізичне виховання	4	залік
ОК 6	Ділова іноземна мова	12	залік /іспит
1.1.2 ДИСЦИПЛІНИ ФУНДАМЕНТАЛЬНОЇ ПІДГОТОВКИ		**32**	
ОК.7	Теоретичні основи захисту інформації	4	залік
ОК.8	Вища математика	9	залік /іспит
ОК.9	Програмування та комп'ютерна техніка	5	іспит
ОК.10	Програмування та алгоритмізація	5	іспит
ОК.11	Теорія ймовірності та математична статистика	4	іспит
ОК.12	Структура баз даних	5	залік
1.2 ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ		**108**	
ОК.13	Інформаційна безпека держави	6	іспит
ОК.14	Комп'ютерні мережі (Частина 1)	5	іспит
ОК.15	Комп'ютерні мережі (Частина 2) Курсова робота	3 2	Іспит захист
ОК.16	Сигнали та процеси інформаційних ситем	4	залік
ОК.17	Об'єктно-орієнтоване програмування	10	залік/ іспит
ОК.17	Проектування баз даних	5	іспит
ОК.18	Нормативно-організаційне забезпечення інформаційної безпеки	4	іспит
ОК.19	Теорія інформації та кодування	5	іспит
ОК.20	Фізичні основи захисту інформації	4	іспит
ОК.21	Безпека комп'ютерних систем та мереж	5	іспит
ОК.22	Інформаційно-телекомунікаційні системи	6	іспит
ОК.23	Криптографічні системи захисту інформації	8	іспит
	Курсова робота	2	залік
ОК.24	Технології виявлення шкідливого трафіку	4	іспит
ОК.25	Комплексні системи захисту інформації	5	іспит
ОК.26	Управління інформаційною безпекою	4	іспит
ОК.27	Спеціальні та інтелектуальні системи інформаційної безпеки	3	іспит
ОК.28	Комп'ютерна та мережева криміналістика	4	іспит

ОК.29	Аудит та моніторінг кібернетичної безпеки	5	іспит
ОК.30	Навчальна практика	4	залік
ОК.31	Виробнича практика	4	залік
ОК.32	Переддипломна практика	4	залік
ОК.33	Кваліфікаційна робота	2	іспит
Загальний обсяг обов'язкових компонент:		**180**	
2 Вибіркові компоненти ОП			
2.1 ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ		**10**	
ВК.1	Безпека життєдіяльності	3	залік
ВК. 2	Екологія		
ВК. 3	Основи психології	4	іспит
ВК. 4	Логіка		
ВК.5	Соціально-політичні студії	3	залік
ВК.6	Оснои академічного письма		
2.2 ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ		**50**	
ВК.7	Операційні системи	3	залік
ВК.8	Захист персональних даних і класифікована інформація		
ВК.9	Інфраструктура кіберпростіру	4	залік
ВК.10	Етика та естетика		
ВК.11	Web-програмування	4	залік
ВК.12	Безпека банковських технологій		
ВК.13	Теорія ризиків	4	залік
ВК.14	Захист бездротових мереж та мобільних додатків		
ВК.15	Системи технічного захисту інформації	4	залік
ВК.16	Схемотехніка пристроїв технічного захисту інформації		
ВК.17	Кібернетичний захист інформаційних ресурсів	4	іспит
ВК.18	Боротьба із злочинами в кіберспорті		
ВК.19	Стеганографія	4	залік
ВК.20	Методи штучного інтелекту (Частина 1)		
ВК.21	Науковий семінар з кібербезпеки	4	залік
ВК.22	Методи штучного інтелекту (Частина 2)		
ВК.23	Адміністрування серверних операційних систем	4	залік
ВК.24	Технології глобальних мереж		
ВК.25	Патентознавство в сфері ІТ та інформація спецільного призначення	3	залік
ВК.26	Захищені технології IoT		
ВК.27	Квантова криптологія	4	залік
ВК.28	Основи Big Data		
ВК.29	Інформаційна та кібербезпека підприємства	4	залік
ВК.30	Бездротові мережі та сенсорні технології		
Загальний обсяг вибіркових компонент:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

3 Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація випускників освітньо-професійної програми «Кібербезпека» здійснюється екзаменаційною комісією у формі публічного захисту кваліфікаційного проекту/роботи та кваліфікаційного екзамену. На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за даною програмою. До атестації допускаються студенти, які виконали всі вимоги програми та навчального плану. Результати атестації визначаються оцінками за національною шкалою і шкалою ECTS.
Вимоги до кваліфікаційної роботи	Кваліфікаційний проект/робота має передбачати розв'язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки. Випускна кваліфікаційна робота (ВКР) містить: - файли з розробленими студентом програмними додатками та їх початковими текстами; - пояснювальну записку; - демонстраційні матеріали. Випускна кваліфікаційна робота має продемонструвати здатність випускника виконувати актуальні завдання спеціальності та вміння використовувати надбані компетентності та результати навчання, логічно, на підставі проведених досліджень обґрунтувати проєктні рішення, робити аргументовані висновки та формулювати конкретні пропозиції та рекомендації щодо виконаного завдання. Кваліфікаційна робота має бути перевірена на академічний плагіат. Вимоги до змісту, обсягу й структури кваліфікаційної роботи визначаються вищим навчальним закладом. На підставі кваліфікаційної роботи екзаменаційна комісія визначає рівень теоретичної підготовки випускника, його готовність до самостійної роботи за фахом і приймає рішення щодо присвоєння відповідної освітньої кваліфікації та

	видачу диплома. Кваліфікаційна робота має бути оприлюднена на офіційному сайті кафедри або в репозитарії ПрАТ «ВНЗ «МАУП»

VII. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

В Академії функціонує система забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості), 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 Академії та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті Академії, на інформаційних стендах тощо;

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 закладом вищої освіти якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) за поданням ВНЗ 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 із забезпечення якості вищої освіти, та міжнародним стандартам і рекомендаціям щодо забезпечення якості вищої освіти.

VIII. Перелік нормативних документів, на яких базується освітня програма

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)

11.Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 р. № 1229;

12.Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22 травня 1998 р. № 505;

13. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29 березня 2006 р. № 373.