МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

Назва вищого навчального закладу

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Адміністративний менеджмент у сфері захисту інформації»

другого рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: Магістр, Кібербезпека, Адміністративний менеджмент у сфері захисту інформації

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ

Голова вченої ради

_____ / В.В. Семенець /

(протокол № 4 від "23" 03 2019 р.)

Освітня програма вводиться в дію з 1.09 2019 р.

Ректор_____ / В.В. Семенець /

(наказ № 178 від "03" 04 2019 р.)

Харків 2019 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«Адміністративний менеджмент у сфері захисту інформації»
другого рівня вищої освіти
за спеціальністю 125 Кібербезпека

УЗГОДЖЕНО

Перший проректор
_____ І.В. Рубан

В.о. начальника відділу ЛА та ВСЗЯО
_____ С.В. Макашев
25.03.19

Розглянуто на засіданні вченої ради
факультету ІК
Протокол №5 від 18.03.2019 р.
Декан факультету ІК
_____ А.В. Снігуров

Розглянуто на засіданні кафедри ІКІ
Протокол № 8 від 13.03.2019 р.
Завідувач кафедри ІКІ
_____ О.В. Лемешко

РОЗРОБЛЕНО
Проектна група:
керівник проектної групи:
Руженцев Віктор Ігоревич,
доктор технічних наук, доцент,
професор каф. БІТ, ХНУРЕ _____ В.І. Руженцев

Члени проектної групи:
Халімов Геннадій Зайдулович,
доктор технічних наук, професор,
завідувач каф. БІТ, ХНУРЕ _____ Г.З. Халімов

Олейніков Анатолій Миколайович
кандидат технічних наук, доцент,
професор каф. КРСТЗІ, ХНУРЕ _____ А.М. Олейніков

Снігуров Аркадій Владиславович
кандидат технічних наук, доцент,
доцент каф. ІКІ, ХНУРЕ _____ А.В. Снігуров

Заболотний Володимир Ілліч,
кандидат технічних наук, доцент,
професор каф. БІТ, ХНУРЕ _____ В.І. Заболотний

ПЕРЕДМОВА

Розроблено робочою групою у складі:

1. Руженцев Віктор Ігоревич (керівник проектної групи)	– доктор технічних наук, доцент, професор кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки
2. Халімов Геннадій Зайдулович,	– доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки
3. Олейніков Анатолій Миколайович	- кандидат технічних наук, доцент, професор кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації Харківського національного університету радіоелектроніки
4. Снігуров Аркадій Владиславович	- кандидат технічних наук, доцент, доцент кафедри інфокомунікаційної інженерії Харківського національного університету радіоелектроніки
5. Заболотний Володимир Ілліч	– кандидат технічних наук, доцент, професор кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки

І. Профіль освітньої програми «Адміністративний менеджмент у сфері захисту інформації» за спеціальністю 125 Кібербезпека

1 Загальна інформація

Повна назва вищого навчального закладу та структурного підрозділу	Харківський національний університет радіоелектроніки. Факультет Інфокомунікацій (ІК) Кафедра інфокомунікаційної інженерії (ІКІ)
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Магістр, Кібербезпека, Адміністративний менеджмент у сфері захисту інформації
Офіційна назва освітньої програми	Адміністративний менеджмент у сфері захисту інформації
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 120 кредитів ЄКТС, термін навчання 1 рік 9 місяців
Наявність акредитації	
Цикл/рівень	НРК України –8 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра (або освітньо-кваліфікаційний рівень спеціаліста)
Мова(и) викладання	Українська, англійська для іноземних студентів.
Термін дії освітньої програми	До повного завершення періоду навчання або наступного оновлення програми
Інтернет-адреса постійного розміщення опису освітньої програми	http://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-125-kiberbezpeka/magistr-125-kiberbezpeka/osvitnja-programa-administrativnij-menedzhment-u-sferi-zahistu-informacii

2 - Мета освітньої програми
– підготовка висококваліфікованих та конкурентоспроможних фахівців з ґрунтовними компетентностями у використанні методів дослідження і проектування систем та комплексів забезпечення інформаційної та кібербезпеки; – надання ґрунтовної освіти в кібербезпеки із широким доступом до працевлаштування або продовження навчання за третім (освітньо-науковим) рівнем вищої освіти.

3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	12 Інформаційні технології. 125 Кібербезпека
Орієнтація освітньої програми	Освітньо-професійна програма прикладної орієнтації. Акцентована на розвиток здатності розв'язувати складні задачі і проблеми у галузі при побудові системи менеджменту

	інформаційної безпеки, складовою якої є система кіберзахисту сучасних інформаційно-комунікаційних систем.
Основний фокус освітньої програми та спеціалізації	Загальна вища освіта другого (магістерського) рівня в галузі 12 «Інформаційні технології» спеціальності 125 Кібербезпека. Ключові слова: кібербезпека, інформаційна безпека, цифрова криміналістика, кібербезпека хмарних технологій, захист від шкідливих програм, етичний хакінг, безпечне програмне забезпечення, кібербезпека безпроводових мереж, система менеджменту інформаційної безпеки, аудит, оцінка ризиків інформаційної безпеки, обробка інцидентів та оцінка якості системи менеджменту інформаційної безпеки
Особливості програми	Освітньо-професійна програма включає навчальні дисципліни, які поглиблюють дослідницькі компетентності та знання спеціальних розділів фундаментальних та професійно-орієнтованих дисциплін та готують випускника для посади фахівця (інженера) системи менеджменту інформаційної безпеки з поглибленим знанням заходів щодо кіберзахисту сучасних інформаційно-комунікаційних систем. Різниця з освітньо-науковою програмою зі спеціальності 125 Кібербезпека, Адміністративний менеджмент у сфері захисту інформації, полягає в більш поглибленому отриманні студентами професійних компетентностей для роботі в установах (компаніях) для побудови та експлуатації комплексної системи інформаційної безпеки (системи менеджменту інформаційної безпеки). Освітньо-професійна програма 1рік 9 місяців порівняно з освітньо-професійною програмою 1 рік 4 місяці додатково містить блок навчальних дисциплін по вивченню нових технологій Big Data, моделювання процесів в інформаційно-комунікаційних системах в умовах кіберзагроз, захисту мультимедійних сервісів, нових технологій мережевого захисту. Сім навчальних курсів освітньо-професійної програми: Розробка програмного забезпечення в сфері інформаційної безпеки (Security Software Development); Інформаційна безпека телекомунікаційних та хмарних технологій (Advanced Networks and Cloud Security); Цифрова криміналістика (Digital Forensic); Методи виявлення та аналізу шкідливого програмного забезпечення (Malware); Системи аналізу вразливостей та етичний хакінг (Penetration testing and ethical hacking); Проектування, експлуатація та захист бездротових мереж (Wireless & Mobile Security); Адміністрування, аудит та безпека інформаційних служб Internet (Web-security), були розроблені в рамках Міжнародної програми Темпус Проект No. 544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR "Підготовка наступного покоління експертів з кібербезпеки: нова визнана ЄС магістерська програма" (ENGENSEC), яка фінансується Європейським Союзом.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Назви професій згідно Національного класифікатора України: Класифікатор професій (ДК 003:2010)

	1495 Менеджери (управителі) систем з інформаційної безпеки 2149.2 Професіонал із організації інформаційної безпеки. 2149.2 Професіонал із організації захисту інформації з обмеженим доступом
Подальше навчання	Можливість навчання за програмою третього (освітньо-наукового) рівня вищої освіти
5 - Викладання та оцінювання	
Викладання та навчання	Лекції, практичні заняття, виконання курсової роботи, лабораторні роботи, самостійна робота на основі підручників, навчальних посібників та конспектів лекцій, консультації з викладачами, професійна практика, підготовка атестаційної роботи.
Оцінювання	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)
6 - Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні задачі і проблеми у галузі професійної діяльності або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.
Загальні компетентності (ЗК)	1. Здатність застосовувати знання у практичних ситуаціях. 2. Здатність спілкуватися іноземною мовою (українською мовою для іноземних студентів). 3. Навички використання інформаційних і телекомунікаційних технологій. 4. Здатність проведення наукових досліджень на відповідному рівні. 5. Здатність до пошуку, оброблення та аналізу науково-технічної інформації з різних джерел. 6. Вміння виявляти, ставити та вирішувати науково-технічні проблеми. 7. Здатність приймати обґрунтовані рішення. 8. Здатність проводити педагогічну роботу зі студентами
Фахові компетентності спеціальності (ФК)	1. Здатність застосовувати відповідні математичні, наукові і технічні методи, а також комп'ютерне програмне забезпечення для вирішення наукових завдань в сфері інформаційної та кібербезпеки; 2. Здатність продемонструвати практичні уміння досліджень в сфері інформаційної та кібербезпеки; 3. Здатність продемонструвати знання і розуміння наукових фактів, концепцій, теорій, принципів і методів, необхідних для підтримки спеціалізацій з інформаційної та кібербезпеки; 4. Здатність застосовувати системний підхід до вирішення проблем інформаційної та кібербезпеки; 5. Здатність продемонструвати розуміння проблем інформаційної та кібербезпеки; 6. Здатність продемонструвати розуміння питань використання технічної літератури та інших джерел інформації 7. Здатність виявляти і описувати ефективність рішень в сфері інформаційної та кібербезпеки на основі використання аналітичних методів і методів моделювання; 8. Здатність продемонструвати знання і розуміння математичних принципів і методів, необхідних для підтримки спеціалізації з інформаційної та кібербезпеки; 9. Здатність розробляти плани і проекти для забезпечення досягнення поставленої певної мети з урахуванням всіх аспектів вирішуваної проблеми 10. Здатність продемонструвати розуміння вимог до діяльності в сфері

	інформаційної та кібербезпеки; 11. Здатність проводити аналіз сучасних інформаційних технологій на предмет вразливостей до кібератак, знати існуючі та розробляти нові механізми кіберзахисту.
7 - Програмні результати навчання	
	1. Знання і розуміння сучасних методів ведення науково-дослідних робіт, організації та планування експерименту, фізико-математичних методів, що застосовуються в інженерній і дослідницькій практиці, на рівні, необхідному для досягнення інших результатів освітньої програми
	2. Здатність аналізувати складні інженерні продукти, процеси і системи відповідно до спеціалізації; обирати і застосовувати придатні типові аналітичні, розрахункові та експериментальні методи; правильно інтерпретувати результати таких досліджень
	3. Здатність виявляти, формулювати і вирішувати завдання в сфері інформаційної та кібербезпеки відповідно до спеціалізації; обирати і застосовувати адекватні аналітичні, розрахункові та експериментальні методи
	4. Здатність розробляти і проектувати, відповідно до спеціалізації, складні вироби, процеси і системи, які задовольняють встановлені вимоги
	5. Здатність виявляти, формулювати і вирішувати незнайомі складні задачі в умовах технічної невизначеності, обирати і застосовувати найбільш прийнятні і відповідні методи з відомих аналітичних, обчислювальних й експериментальних, або нових і новаторських
	6. Здатність здійснювати пошук літератури, консультуватися і критично використовувати наукові бази даних та інші відповідні джерела інформації, здійснювати моделювання та аналіз з метою детального вивчення і дослідження питань інформаційної та кібербезпеки відповідно до спеціалізацій
	7. Розуміння застосовуваних методик та методів аналізу, проектування і дослідження, а також обмежень їх використання
	8. Практичні навички вирішення складних завдань, реалізації складних інженерних проектів і проведення досліджень в сфері інформаційної та кібербезпеки
	9. Розуміння технічних наслідків діяльності в сфері інформаційної та кібербезпеки
	10. Здатність продемонструвати мовні компетентності, достатні для представлення та обговорення своїх наукових результатів іноземною мовою (англійською або іншою, відповідно до специфіки спеціальності; для іноземних студентів – українською мовою) в усній та письмовій формах, а також для повного розуміння іншомовних наукових текстів
	11. Знати та уміти застосовувати засоби сучасних інформаційних технологій для вирішення задач в сфері інформаційної та кібербезпеки
	12. Орієнтуватися в патентній інформації і документації, досліджувати і правильно формувати ознаки новизни в об'єктах
	13. Формувати навчально-методичний матеріал змістовних блоків для навчання студентів
8 – Ресурсне забезпечення реалізації	
Кадрове забезпечення	Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями та вченими званнями, які мають великий досвід навчально-методичної, науково-дослідної роботи та відповідають кваліфікації відповідно до спеціальності згідно ліцензійних умов. Фахівці, залучені до професійної підготовки, пройшли стажування відповідно до наступних програм: - Міжнародна програма Темпус Проект No. 544455-TEMPUS-1-2013-

	1-SE-TEMPUS-JPCR "Підготовка наступного покоління експертів з кібербезпеки: нова визнана ЄС магістерська програма" (ENGENSEC), яка фінансується Європейським Союзом. - Програма міжнародної мобільності Erasmus+ (стажування в Блекінге технологічному інституті, Швеція). - Програма підготовки по міжнародний стандартам ISO/IEC 27001:2013, ISO 19011:2011, ISO 9001:2015.
Матеріально-технічне забезпечення	1.Забезпеченість приміщеннями для проведення навчальних занять та контрольних заходів. 2. Забезпеченість мультимедійним обладнанням для одночасного використання в навчальних аудиторіях. 3. Наявність соціально-побутової інфраструктури. 4. Забезпеченість здобувачів вищої освіти гуртожитком. 5. Забезпеченість комп'ютерними робочими місцями, лабораторіями, полігонами, обладнанням, устаткуванням, необхідними для виконання навчальних планів. Засоби обчислювальної техніки з відповідним програмним забезпеченням, спеціальні радіовимірювальні прилади, засоби ТЗІ, апаратно-програмні комплекси. Високий рівень практичної підготовки фахівців забезпечується розвиненою міжнародною співпрацею в науковій і освітній сферах, наявністю спеціалізованих лабораторій: компанії CISCO, компанії D-Link, компанії Oracle, компаній CS, Avaya, Samsung, Alcatel, Monis, лабораторії супутникового та мобільного зв'язку, безпроводових мереж, моніторингу радіочастотного ресурсу, мереж наступного покоління, систем доступу та комутації, транспортних мереж, хмарних обчислень в Інтернет-технологіях. В 2017 р. Європейським союзом в рамках програми Темпус закуплено обладнання для створення кіберполігону для вивчення кібербезпеки хмарних технологій.
Інформаційне та навчально-методичне забезпечення	1. Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді. 2. Наявність доступу до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. 3. 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 їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація). 4. Наявність електронного ресурсу закладу освіти, який містить навчально-методичні матеріали з дисциплін навчального плану, в тому числі в системі дистанційного навчання. Специфічними характеристиками інформаційного та навчально-методичного забезпечення є: - використання національних стандартів в галузі інформаційної та кібербезпеки, - використання національних та міжнародних наукових видань, - використання міжнародних стандартів в галузі інформаційної та кібербезпеки; - використання навчально-методичних комплексів та навчальних посібників, що розроблені в рамках Міжнародної програми Темпус Проект No. 544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR "Підготовка наступного покоління експертів з кібербезпеки: нова визнана ЄС магістерська програма" (ENGENSEC), яка фінансується Європейським Союзом.

9 — Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та закладами вищої освіти України
Міжнародна кредитна мобільність	Згідно з укладеними угодами про міжнародну академічну мобільність (Еразмус+ К.1), про подвійне дипломування, про тривалі міжнародні проекти, які передбачають включене навчання студентів тощо. Особливості освітньо-професійної програми: 1. Наявність програми подвійних дипломів з Блекінге технологічним інститутом (Швеція, Карлскруна). 2. Участь освітньо-професійної програми в програмі академічної мобільності Erasmus+ KA1 з Блекінге технологічним інститутом (Швеція, Карлскруна).
Навчання іноземних здобувачів вищої освіти	Для англомовних іноземних громадян викладання здійснюється на англійській мові

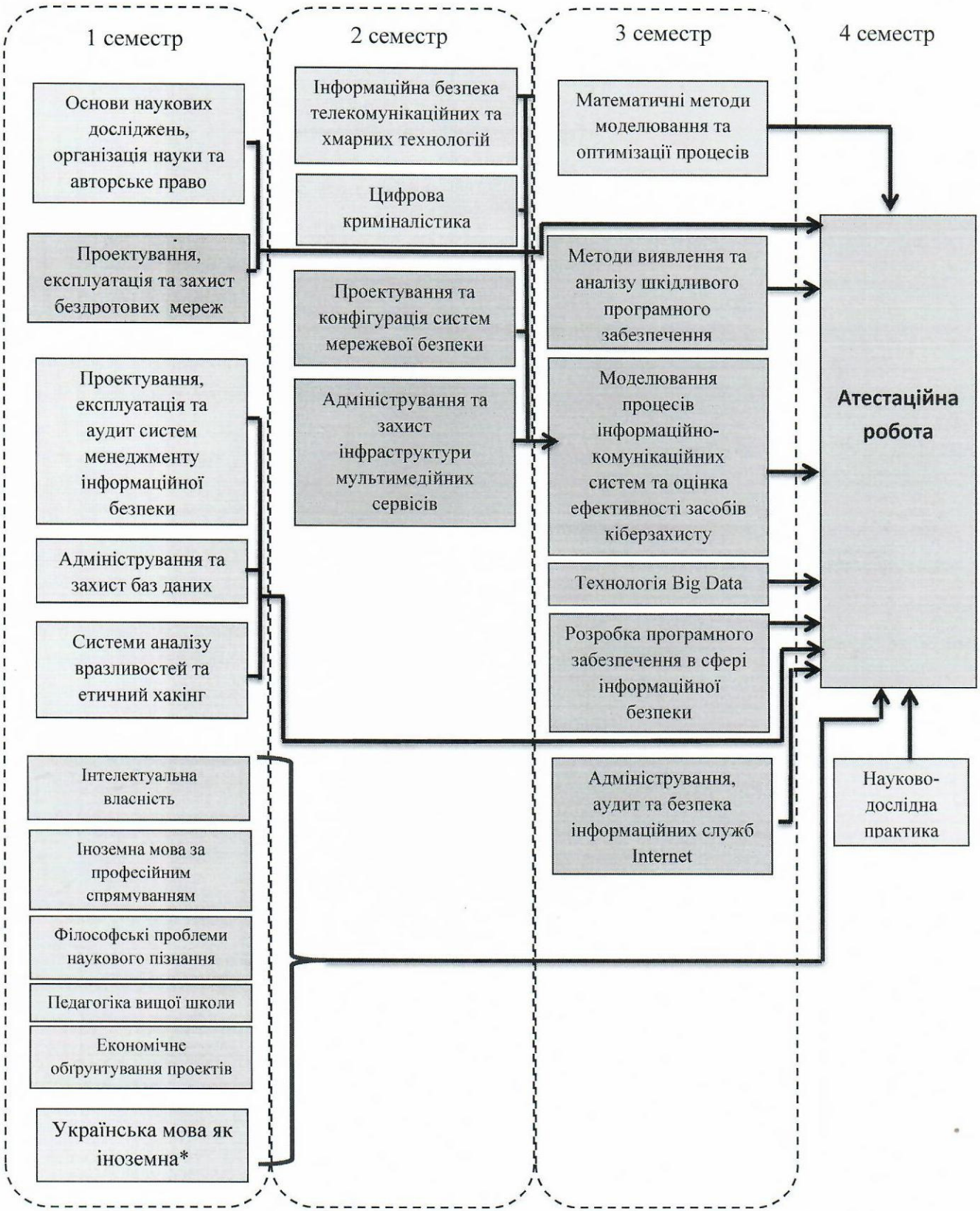
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
	Обов'язкові компоненти ОП		
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Дисципліни базової (професійної) підготовки за спеціальністю125 Кібербезпека			
ОК 1.	Математичні методи моделювання та оптимізації процесів	5	іспит
ОК 2.	Основи наукових досліджень, організація науки та авторське право	4	іспит
ОК 2*	Українська мова як іноземна	4	залік
ОК 3.	Професійна практика	15	залік
ОК 4.	Атестаційна робота	15	Захист атестаційної роботи
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
Дисципліни професійної та практичної підготовки за освітньою програмою Адміністративний менеджмент у сфері захисту інформації			
ОК 5.	Проектування, експлуатація та аудит систем менеджменту інформаційної безпеки	4,5	іспит
ОК 6.	Адміністрування та захист баз даних	4,5	залік
ОК 7.	Системи аналізу вразливостей та етичний хакінг	7	іспит
ОК 8.	Інформаційна безпека телекомунікаційних та хмарних технологій	7,5	Іспит, курсова робота
ОК 9.	Цифрова криміналістика	7,5	іспит
	Загальний обсяг обов'язкових компонент:	**70**	

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
Вибіркові компоненти ОП			
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Гуманітарні та соціально-економічні дисципліни			
ВБ 1.1	Інтелектуальна власність	3	залік
ВБ 1.2	Іноземна мова за професійним спрямуванням	3	залік
ВБ 1.3	Філософські проблеми наукового пізнання	3	залік
ВБ. 1.4	Педагогіка вищої школи	3	залік
ВБ 1.5	Економічне обґрунтування проектів	3	залік
	Фізичне виховання (за рахунок вільного часу студентів)	0	
	Всього:	3	
Дисципліни професійної та практичної підготовки за освітньою програмою Адміністративний менеджмент у сфері захисту інформації			
	Вибірковий блок 1		
ВБ 2.1	Розробка програмного забезпечення в сфері інформаційної безпеки	5	іспит
ВБ 2.2	Методи виявлення та аналізу шкідливого програмного забезпечення	5	залік
ВБ 2.3	Проектування, експлуатація та захист бездротових мереж	7	залік
ВБ 2.4	Адміністрування, аудит та безпека інформаційних служб Internet	5	залік
	Вибірковий блок 2		
ВБ 3.1	Адміністрування та захист інфраструктури мультимедійних сервісів	7,5	залік
ВБ 3.2	Проектування та конфігурація систем мережевої безпеки	7,5	іспит
ВБ 3.3	Моделювання процесів інформаційно-комунікаційних систем та оцінка ефективності засобів кіберзахисту	5	залік
ВБ 3.4	Технологія Big Data	5	залік
Загальний обсяг вибіркових компонент:		**50**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**120**	

2.2. Структурно-логічна схема ОП



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Адміністративний менеджмент у сфері захисту інформації» спеціальності 125 Кібербезпека проводиться у формі захисту атестаційної роботи та завершується видачею документу встановленого зразка про присудження йому ступеня магістра із присвоєнням кваліфікації: Магістр, Кібербезпека, Адміністративний менеджмент у сфері захисту інформації.

Атестація здійснюється відкрито і публічно.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1	ОК 2	ОК 2*	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ВБ 1	ВБ 2.1	ВБ 2.2	ВБ 2.3	ВБ 2.4	ВБ 3.1	ВБ 3.2	ВБ 3.3	ВБ 3.4
ЗК-1				*		*	*	*	*	*		*	*	*	*	*	*	*	
ЗК-2			*								*								
ЗК-3									*					*	*	*	*	*	
ЗК-4	*	*			*							*							
ЗК-5		*			*														*
ЗК-6	*	*			*														*
ЗК-7	*	*		*	*									*					
ЗК-8				*															
ФК-1	*																	*	
ФК-2				*		*										*	*		
ФК-3		*			*														*
ФК-4					*	*		*										*	*
ФК-5							*	*	*	*		*	*	*	*			*	
ФК-6					*														
ФК-7	*	*																*	
ФК-8				*	*		*											*	
ФК-9		*				*			*										
ФК-10						*		*	*			*	*	*	*	*	*		
ФК-11							*	*	*	*		*	*	*		*	*		*

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

	ОК 1	ОК 2	ОК2*	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ВБ 1	ВБ 2.1	ВБ 2.2	ВБ 2.3	ВБ 2.4	ВБ 3.1	ВБ 3.2	ВБ 3.3	ВБ 3.4
ПРН - 1	*	*									*							*	
ПРН - 2		*			*	*		*		*						*	*	*	
ПРН - 3					*		*	*	*	*		*	*	*	*	*	*		
ПРН - 4						*	*	*						*					*
ПРН - 5	*				*	*												*	*
ПРН - 6	*	*			*									*	*			*	*
ПРН - 7						*	*	*				*		*				*	
ПРН - 8				*		*	*	*	*	*		*	*	*	*	*	*		*
ПРН - 9				*										*					
ПРН-10			*								*								
ПРН-11						*	*	*	*	*		*	*	*	*	*	*		*
ПРН-12											*								