МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет радіоелектроніки

ОСВІТНЬО – НАУКОВА 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 № 1 від "28 " січня 2021 р.)
зі змінами
протокол № 5 від «28» травня 2021р.

Освітня програма вводиться в дію з 01.09 2021 р.
Ректор_____ / В.В. Семенець /
(наказ № 46 від " 2 " лютого 2021 р.)
зі змінами
наказ №173 від "03 " червня 2021 р.

Харків 2021 р.

ЛИСТ ПОГОДЖЕННЯ

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

УЗГОДЖЕНО

Перший проректор

_____ І.В. Рубан
«31» 05 2021р.

В.о. начальника відділу ЛА та ВСЗЯО

_____ С.Б. Макашев
«12» 05 2021р.

Начальник навчального відділу

_____ А.В. Міхнова
«__» 05 2021р.

Розглянуто на засіданні вченої ради
факультету ІК
Протокол № 4 від 11.05.2021 р.
Декан факультету ІК

_____ А.В. Снігуров

Розглянуто на засіданні кафедри ІКІ
Протокол № 4 від 28.04.2021 р.
Завідувач кафедри ІКІ
ім. В.В.Поповського

_____ О.В. Лемешко

Представник роботодавців
MNC Group

_____

Голова студентського сенату факультету ІК

_____ А.Ю. Литвиненко

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

Сєвєрінов Олександр Васильович,
кандидат технічних наук, доцент,
доц. каф. БІТ, ХНУРЕ _____ О.В. Сєвєрінов

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. Сєвєрінов Олександр Васильович	– канд. техн. наук, доцент, доцент 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 ім. В.В. Поповського (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	Сертифікат про акредитацію спеціальності НД 2190672 від 2.10.2017. Діє до 01.07.2025.
Цикл/рівень	НРК України – 7 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-наукова програма прикладної орієнтації. Акцентована на розвиток здатності розв'язувати складні задачі і проблеми у галузі професійної діяльності в сфері кібербезпеки та систем менеджменту інформаційної безпеки, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.
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, математичне моделювання
Особливості програми	Освітньо-наукова програма включає навчальні дисципліни освітньо-професійної програми та додаткові дисципліни, які поглиблюють дослідницькі компетентності та знання спеціальних розділів фундаментальних та професійно-орієнтованих дисциплін і тим самим забезпечують можливість засвоєння складніших програм для наукових дослідників. Сім навчальних курсів освітньо-наукової 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 2310 Викладачі університетів та вищих навчальних закладів 2310.2 Викладач вищого навчального закладу
Подальше навчання	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти.

	Набуття додаткових кваліфікацій в системі освіти дорослих
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, науково-дослідна практика, підготовка кваліфікаційної 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 особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (ЗК)	ЗК-1. Здатність застосовувати знання у практичних ситуаціях. ЗК-2. Здатність проводити дослідження на відповідному рівні. ЗК-3. Здатність до абстрактного мислення, аналізу та синтезу. ЗК-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові компетентності спеціальності (ФК)	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і

	заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. КФ11. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність
7 - Кінцеві, підсумкові та інтегративні результати навчання	
	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

	РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних,

	оцінювати достовірність результатів досліджень, аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики. РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.
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, LifeCell, 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-наукової програми: 1. Наявність програми подвійних дипломів з Блекінге технологічним інститутом (Швеція, Карлскруна). 2. Участь освітньо-наукової 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-наукової 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
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Гуманітарні та соціально-економічні дисципліни (обов'язкові)			
ОК * 1.1	Українська мова як іноземна	3	залік
Гуманітарні та соціально-економічні дисципліни (вибіркові)			
ВБ 1.1	Ділова іноземна мова	3	Зл
ВБ 1.2	Філософські проблеми наукового пізнання	3	Зл
ВБ 1.3	Педагогіка вищої школи	3	Зл
ВБ 1.4	Стилістика наукового тесту	3	Зл
Всього:		**3**	
Дисципліни базової (професійної) підготовки за спеціальністю (обов'язкові) *за освітньою програмою Адміністративний менеджмент у сфері захисту інформації за профілем випускової кафедри Інфокомунікаційної інженерії ім. В.В. Поповського*			
ОК 1.1	Основи наукових досліджень в сферах кібернетичного і технічного захисту інформації	5	екзамен
ОК 1.2	Моделювання та оцінка ефективності засобів криптографічного і технічного захисту інформації	4	екзамен
ОК 1.3	Проектування, експлуатація та аудит систем менеджменту інформаційної безпеки	4	екзамен
ОК 1.4	Системи аналізу вразливостей та етичний хакінг	7	екзамен
ОК 1.5	Інформаційна безпека телекомунікаційних та хмарних технологій	7	екзамен, курсова робота
ОК 1.6	Цифрова криміналістика	6	екзамен
ОК 1.7	Адміністрування та захист баз даних	4	залік
Всього:		**37**	
Загальний обсяг освітніх компонент циклу загальної та спеціальної (фахової) підготовки:		**40**	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
Дисципліни професійної та практичної підготовки (обов'язкові) *за освітньою програмою Адміністративний менеджмент у сфері захисту інформації за профілем випускової кафедри Інфокомунікаційної інженерії ім. В.В. Поповського*			
ОК 2.1	Проектування, експлуатація та захист бездротових мереж	6	залік
ОК 2.2	Розробка програмного забезпечення в сфері інформаційної безпеки	5	екзамен
ОК 2.3	Методи виявлення та аналізу шкідливого програмного забезпечення	5	залік
ОК 2.4	Адміністрування, аудит та безпека інформаційних служб Internet	5	залік
Всього:		**21**	
ОК 2.5	Науково-дослідна практика	15	залік

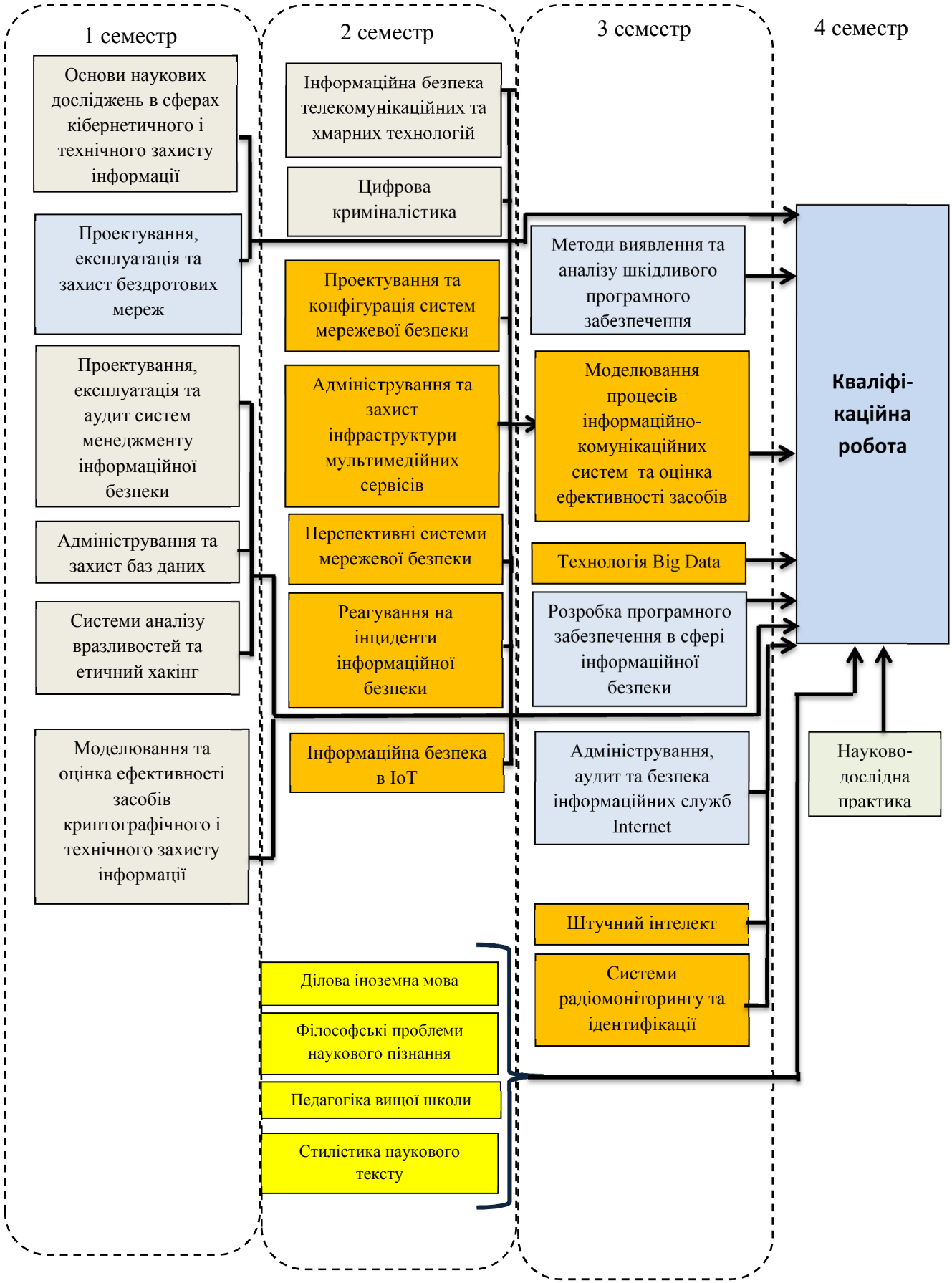
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
ОК 2.6	Кваліфікаційна робота	15	Захист кваліфікаційної роботи
Дисципліни професійної та практичної підготовки (вибіркові) за освітньою програмою *Адміністративний менеджмент у сфері захисту інформації за профілем випускової кафедри Інфокомунікаційної інженерії ім. В.В. Поповського*			
ВБ 2.1	Штучний інтелект	5	залік
ВБ 2.2	Системи радіомоніторингу та ідентифікації об'єктів	5	залік
ВБ 2.3	Адміністрування та захист інфраструктури мультимедійних сервісів	7	залік
ВБ 2.4	Проектування та конфігурація систем мережевої безпеки	7	екзамен
ВБ 2.5	Перспективні системи мережевої безпеки	7	екзамен
ВБ 2.6	Моделювання процесів інформаційно-комунікаційних систем та оцінка ефективності засобів кіберзахисту	5	залік
ВБ 2.7	Технологія Big Data	5	залік
ВБ 2.8	Реагування на інциденти інформаційної безпеки	7	екзамен
ВБ 2.9	Інформаційна безпека в IoT	7	екзамен
Всього:		**29**	
Загальний обсяг освітніх компонент циклу професійної підготовки:		**80**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**120**	

* – для іноземних здобувачів вищої освіти;

2.1. Структурно-логічна схема ОП

1 семестр	2 семестр	3 семестр	4 семестр
	ОК* 1.1.	ОК 2.2.	ОК 2.5
ОК 1.1.		ОК 2.3.	ОК 2.6
ОК 1.2.		ОК 2.3.	
ОК 1.3.	ОК 1.5.		
ОК 1.4.	ОК 1.6.	ВБ 2.1.	
ОК 1.7.		ВБ 2.2.	
		ВБ 2.6.	
ОК 2.1.	ВБ 1.1., ВБ 1.2., ВБ 1.3., ВБ 1.4.	ВБ 2.7.	
	ВБ 2.3., ВБ 2.4. ВБ 2.5., ВБ2.8, ВБ 2.9		

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 кваліфікаційної 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* 1.1	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ОК 1.1	ОК 1.2	ОК 1.3	ОК 1.4	ОК 1.5	ОК 1.6	ОК 1.7	ОК 2.1	ОК 2.2	ОК 2.3	ОК 2.4	ОК 2.5	ОК 2.6	ВБ 2.1	ВБ 2.2	ВБ 2.3	ВБ 2.4	ВБ 2.5	ВБ 2.6	ВБ 2.7	ВБ 2.8	ВБ 2.9
ЗК-1			*			*	*	*	*		*		*	*	*	*	*	*				*		*			
ЗК-2						*	*																	*			
ЗК-3						*	*											*						*			
ЗК-4							*	*																*			
ЗК-5	*	*																	*						*		
КФ-1							*		*	*	*		*	*	*	*			*		*	*	*	*	*		
КФ-2					*			*									*	*									
КФ-3									*	*	*	*	*	*	*	*				*	*	*	*				*
КФ-4								*	*		*															*	
КФ-5								*	*	*	*	*	*	*	*	*					*			*		*	
КФ-6										*		*	*			*					*	*	*				
КФ-7									*		*				*											*	
КФ-8							*						*							*							
КФ-9								*	*							*								*			*
КФ-10				*	*												*										
КФ-11					*	*	*										*	*									

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

	ОК* 1.1	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ОК 1.1	ОК 1.2	ОК 1.3	ОК 1.4	ОК 1.5	ОК 1.6	ОК 1.7	ОК 2.1	ОК 2.2	ОК 2.3	ОК 2.4	ОК 2.5	ОК 2.6	ВБ 2.1	ВБ 2.2	ВБ 2.3	ВБ 2.4	ВБ 2.5	ВБ 2.6	ВБ 2.7	ВБ 2.8	ВБ 2.9
РН - 1	*	*			*												*	*									
РН - 2			*			*	*										*	*						*			
РН - 3						*	*										*	*						*			
РН - 4						*	*			*			*	*	*	*		*	*		*	*	*	*	*		*
РН - 5						*	*		*	*	*		*	*	*	*		*	*		*	*	*	*	*		*
РН - 6									*	*		*	*	*	*	*						*	*	*			*
РН - 7								*										*				*	*			*	
РН - 8								*	*	*		*	*	*	*	*				*	*	*	*			*	*
РН - 9								*	*		*															*	
РН-10								*	*	*	*	*	*	*	*	*					*			*		*	
РН-11										*		*	*			*					*	*	*				
РН-12									*		*				*											*	
РН–13							*						*							*							
РН-14								*	*							*								*			
РН-15								*									*	*									
РН-16							*	*				*	*								*	*		*			
РН-17				*		*													*						*		
РН-18				*																							
РН-19							*																	*			
РН-20						*		*		*			*				*	*				*					
РН-21							*																	*			
РН-22						*	*											*						*			
РН-23										*	*	*	*	*	*	*			*	*	*	*			*		
РН-24					*	*	*										*	*									
РН-25						*											*	*									

6. Матриця відповідності визначених Стандартом компетентностей / результатів навчання дескрипторам НРК

Класифікація компетентностей (результатів навчання) за НРК	**Знання** **Зн1** Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та на межі галузей знань	**Уміння/Навички Ум1** Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур **Ум2** Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах **Ум3** Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	**Комунікація К1** Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	**Відповідальність і автономія АВ1** Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів **АВ2** Відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів **АВ3** Здатність продовжувати навчання з високим ступенем автономії
Загальні компетентності				
КЗ1	Зн1,	Ум1, Ум3	К1	АВ1, АВ2
КЗ2	Зн1,	Ум1, Ум2, Ум3		АВ2, АВ3
КЗ3	Зн1	Ум2, Ум3		АВ1
КЗ4	Зн1	Ум3		АВ1, АВ2
КЗ5	Зн1	Ум2	К1	АВ1
Спеціальні (фахові) компетентності				
КФ1	Зн1	Ум2		АВ2
КФ2	Зн1,	Ум2		АВ2
КФ3	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
КФ4	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
КФ5	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
КФ6	Зн1	Ум1, Ум2	К1	АВ1
КФ7	Зн1	Ум1, Ум2	К1	АВ1
КФ8	Зн1	Ум1, Ум2	К1	АВ1
КФ9	Зн1	Ум1, Ум2	К1	АВ1
КФ10	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
КФ11	Зн1,	Ум1, Ум2, Ум3		АВ2, АВ3

7. Матриця відповідності визначених Стандартом результатів навчання та компетентностей

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ -5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ11
РН 1	+		+			+										
РН 2		+	+			+	+	+								+
РН 3	+					+										+
РН 4	+	+	+	+		+	+									
РН 5			+		+		+									+
РН 6	+			+		+		+		+	+	+		+		
РН 7	+		+				+									
РН 8	+	+		+	+			+						+	+	
РН 9	+	+	+	+					+					+	+	
РН 10	+		+	+						+				+		
РН 11	+		+	+							+				+	
РН 12	+		+	+					+			+			+	
РН 13	+		+	+									+		+	
РН 14	+		+	+					+					+	+	
РН 15				+	+										+	
РН 16	+	+	+	+				+	+	+	+	+		+	+	+
РН 17								+							+	
РН 18	+			+	+										+	
РН 19	+			+	+	+	+	+	+		+	+	+	+		
РН 20	+	+	+	+	+	+		+								+
РН 21	+	+	+	+		+		+		+		+	+			+
РН 22		+	+	+		+		+								+
РН 23	+		+	+		+	+	+			+	+	+	+		
РН 24		+	+	+	+			+							+	+
РН 25	+	+	+	+				+								+