МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО–НАУКОВА ПРОГРАМА

«Адміністративний менеджмент у сфері захисту інформації»

другого (магістерського) рівня вищої освіти

за спеціальністю 125 Кібербезпека та захист інформації

галузі знань 12 Інформаційні технології

Кваліфікація: «Магістр з кібербезпеки та захисту інформації»

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ
Заступник голови Вченої ради_____Олександр ФИЛИПЕНКО
(протокол від "28"лютого 2023 р. № 2)

Освітня програма вводиться в дію з 01 вересня 2023 р.
В.о. ректора_____ Ігор РУБАН
(наказ від "02"березня 2023 р. № 34)

Харків 2023 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-наукової програми
«Адміністративний менеджмент у сфері захисту інформації»
спеціальності 125 Кібербезпека та захист інформації
другого (магістерського) рівня вищої освіти

УЗГОДЖЕНО
Перший проректор
_____ Ігор РУБАН
« 21 » лютого 2023 р.

Начальник відділу ЛА та ВСЗЯО
_____ Сергій МАКАШЕВ
« 17 » лютого 2023 р.

Начальник навчального відділу
_____ Аліна МІХНОВА
« 17 » лютого 2023 р.

Розглянуто на засіданні Вченої ради
Факультету ІК
Протокол від «21» 02. 2023 № 2
Декан факультету ІК
_____ Аркадій СНІГУРОВ

Розглянуто на засіданні кафедри ІКІ
Протокол від «25» 01. 2023 № 1
Завідувач кафедри ІКІ
ім.В.В.Поповського
_____ Олександр ЛЕМЕШКО

Представники роботодавців
MNC Group _____ Григорій МАЗУР

Представник студентського самоврядування
Заступник Голови студентського сенату факультету ІК _____ Світлана МАСЛОВА

РОЗРОБЛЕНО
Проектна група:
керівник проектної групи:
Руженцев Віктор Ігоревич,
доктор технічних наук, доцент
професор кафедри БІТ ХНУРЕ _____

члени проектної групи:
Халімов Геннадій Зайдулович,
доктор технічних наук, професор,
завідувач кафедри БІТ ХНУРЕ _____

Олейніков Анатолій Миколайович
кандидат технічних наук, професор,
професор кафедри КРСТЗІ ХНУРЕ _____

Радівілова Тамара Анатоліївна,
доктор технічних наук, професор,
професор кафедри ІКІ ім. В.В Поповського ХНУРЕ _____

ПЕРЕДМОВА

Розроблено проектною групою у складі:

Керівник проектної групи:

Руженцев Віктор Ігоревич, доктор технічних наук, доцент, професор кафедри БІТ факультету КІУ ХНУРЕ

Члени проектної групи:

Халімов Геннадій Зайдулович, доктор технічних наук, професор, завідувач кафедри БІТ факультету КІУ ХНУРЕ.

Олейніков Анатолій Миколайович, кандидат технічних наук, доцент, професор кафедри КРСТЗІ факультету ІРТЗІ ХНУРЕ.

Радівілова Тамара Анатоліївна, доктор технічних наук, професор, професор кафедри ІКІ ім. В.В. Поповського факультету ІК ХНУРЕ.

Керівник проектної групи  Віктор РУЖЕНЦЕВ

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

1 - Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Харківський національний університет радіоелектроніки, Факультет інфокомунікацій Кафедра інфокомунікаційної інженерії ім. В.В. Поповського
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Магістр з кібербезпеки та 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. Строк дії сертифікату 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 мова, англійська мова
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 та захист інформації
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	Загальна вища освіта другого (магістерського) рівня в галузі 12 «Інформаційні технології» спеціальності 125 Кібербезпека та захист інформації. Ключові слова: кібербезпека, захист інформації, 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-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. Також особливістю освітньої програми є: - участь в проєкті USAID «Кібербезпека критично важливої інфраструктури в Україні», в якій викладачі кафедри пройшли відповідну підготовку та отримали навчально-методичні матеріали від учасників проекту; - участі та головного реалізатора проекту ERASMUS+ Жан Моне «Інтеграція рамок та політик кібербезпеки ЄС в Україні» (з 2020 року); - участі і головного реалізатора проєкту ERASMUS+ модуль Жан Моне «Європейський досвід для підвищення стійкості критично важливих об'єктів в Україні» (з 2022 року).
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 Викладач вищого навчального закладу
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, 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)	1. Здатність застосовувати знання у практичних ситуаціях. 2. Здатність проводити дослідження на відповідному рівні. 3. Здатність до абстрактного мислення, аналізу та синтезу. 4. Здатність оцінювати та забезпечувати якість виконуваних робіт. 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові компетентності спеціальності (ФК)	1. 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. 2. 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. 3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. 4. 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. 5. 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. 6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно

	встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. 7. 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. 8. 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. 9. 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. 10. 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. 11. 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 - Програмні результати навчання	
	1. 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. 2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. 3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. 4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. 5. 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. 6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання

	спеціалізованого програмного забезпечення. 7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. 8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. 9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. 10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. 11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. 12. 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. 13. 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. 14. 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. 15. 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. 16. 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. 17. 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. 18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. 19. 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. 20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. 21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. 22. 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. 23. 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. 24. 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. 25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.
8 - Ресурсне забезпечення реалізації програми	
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 міжнародним стандартам ISO/IEC 27001:2022, ISO 19011:2011, ISO 9001:2015. - програма підготовки викладачів з кібербезпеки відповідно проекту США USAID.
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; - використання навчально-методичних комплексів з курсу підготовки викладачів з кібербезпеки відповідно проекту США USAID
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 тривалі міжнародні проекти, які передбачають включене навчання студентів тощо.

	Особливості освітньо-професійної програми: 1. Участь освітньо-професійної програми в програмі академічної мобільності Erasmus+ KA1 з Блекінге технологічним інститутом (Швеція, Карлскруна).
Навчання іноземних здобувачів вищої освіти	На основі договорів (угод) між Харківським національним університетом радіоелектроніки та закладами вищої освіти іноземних країн

2. Перелік компонент освітньої програми та їх логічна послідовність

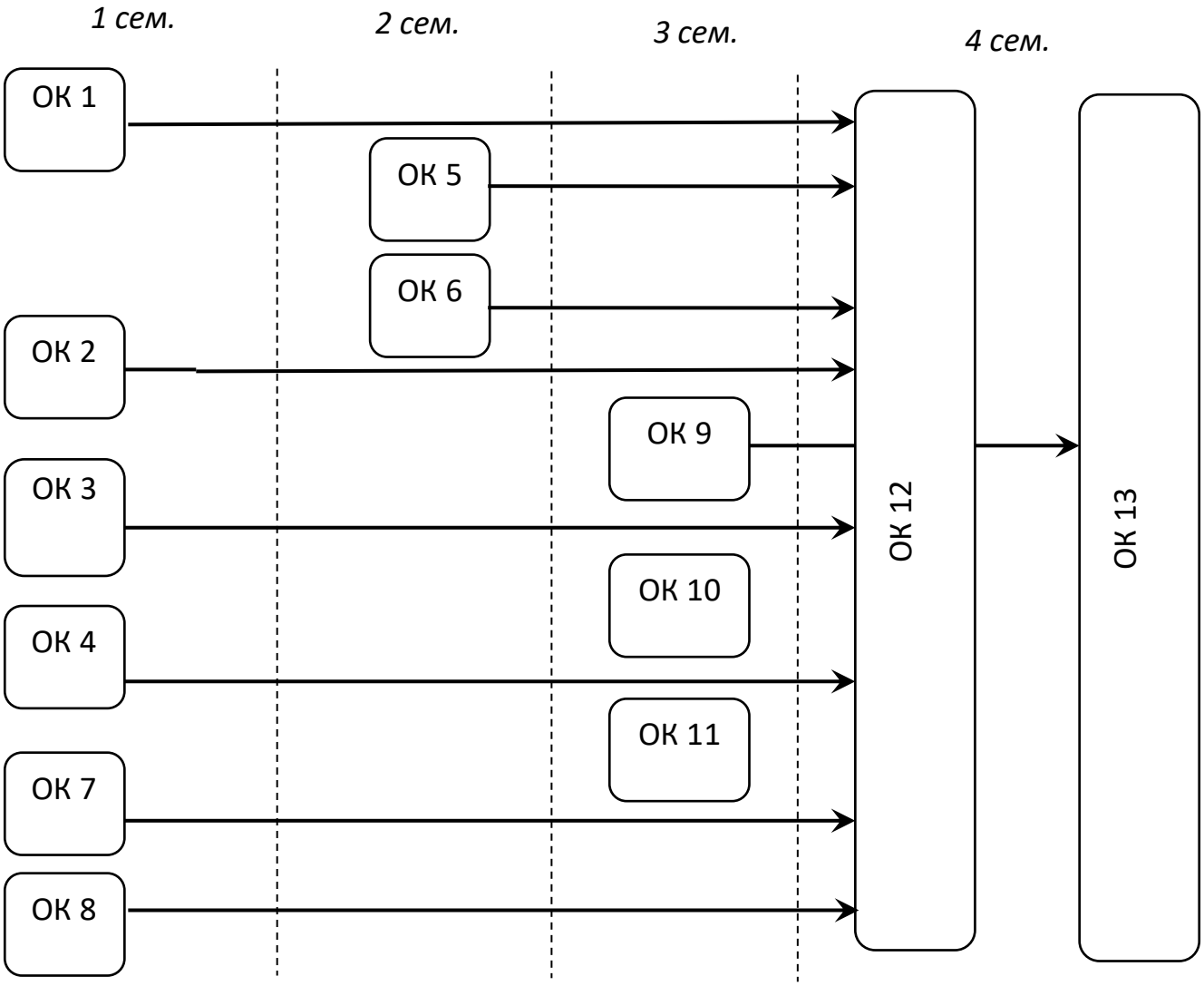
2.1. Перелік компонент ОП

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 спеціальністю (обов'язкові)		
ОК 1	Основи наукових досліджень в сферах кібернетичного і технічного захисту інформації	5	Екзамен
ОК 2	Моделювання та оцінка ефективності засобів криптографічного і технічного захисту інформації	4	Екзамен
ОК 3	Проектування, експлуатація та аудит систем управління інформаційною безпекою	4	Екзамен
ОК 4	Системи аналізу вразливостей та етичний хакінг	7	Екзамен
ОК 5	Інформаційна безпека телекомунікаційних та хмарних технологій	7	Екзамен, курсова робота
ОК 6	Цифрова криміналістика	6	Екзамен
ОК 7	Адміністрування та захист баз даних	4	залік
	ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ		
	Дисципліни професійної та практичної підготовки за освітньою програмою «Адміністративний менеджмент у сфері захисту інформації» (обов'язкові)		
ОК 8	Проектування, експлуатація та захист безпроводових мереж	6	залік
ОК 9	Розробка програмного забезпечення в сфері інформаційної безпеки	5	Екзамен
ОК 10	Методи виявлення та аналізу шкідливого програмного забезпечення	5	залік
ОК 11	Адміністрування, аудит та безпека інформаційних служб Internet	5	залік
ОК 12	Передатестаційна практика	15	Залік
ОК 13	Кваліфікаційна робота	15	Екзамен
	Загальний обсяг обов'язкових компонентів	**88**	
	ВИБІРКОВІ КОМПОНЕНТИ ОП*		
	ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ		
	Гуманітарні та соціально-економічні дисципліни		
	Всього:	3	
	Загальний обсяг вибіркових компонентів за циклом	3	
	ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ		
	Дисципліни професійної та практичної підготовки за освітньою програмою «Адміністративний менеджмент у сфері захисту інформації»		
ВК 1	Методи штучного інтелекту у кібербезпеці	5	Залік
ВК 2	Системи радіомоніторингу та ідентифікації об'єктів	5	Залік
ВК 3	Адміністрування та захист інфраструктури мультимедійних сервісів	7	Залік
ВК 4	Проектування та конфігурація систем мережної безпеки	7	Екзамен
ВК 5	Перспективні системи мережної безпеки	7	Екзамен
ВК 6	Моделювання процесів інформаційно-комунікаційних	5	Залік

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
	систем та оцінка ефективності засобів кіберзахисту		
ВК 7	Безпека технологій Big Data	5	Залік
ВК 8	Реагування на інциденти інформаційної безпеки	7	Екзамен
ВК 9	Інформаційна безпека в IoT та кіберфізичних системах	7	Екзамен
	Загальний обсяг вибіркових компонентів за циклом	**29**	
	Загальний обсяг вибіркових компонентів	**32**	
	ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ	**120**	

* Перелік вибіркових компонентів може бути доповнено у робочому навчальному плані з загального каталогу вибіркових дисциплін Університету – у разі вибору здобувачами вищої освіти

2.2 Структурно-логічна схема ОП



3. Форма атестації здобувачів вищої освіти

Форма атестації здобувачів вищої освіти за освітньою програмою «Адміністративний менеджмент у сфері захисту інформації» спеціальності 125 Кібербезпека та захист інформації – захист кваліфікаційної роботи з видачею документу встановленого зразка про присудження здобувачеві ступеня магістра із присвоєнням освітньої кваліфікації: «Магістр з кібербезпеки та захисту інформації».

Форми атестації

Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.

Вимоги до кваліфікаційної роботи

Кваліфікаційна робота має продемонструвати здатність випускника розв’язувати складні задачі і проблеми сфери кібербезпеки на основі досліджень та/або здійснення інновацій за невизначених умов і вимог.

Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації.

Кваліфікаційна робота має бути оприлюднена на офіційному сайті закладу вищої освіти або його підрозділу, або у репозитарії закладу вищої освіти.

4. Матриця відповідності компетентностей компонентам освітньої програми

4.1. Матриця відповідності загальних та фахових компетентностей обов'язковим компонентам (ОК) освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13
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 (ПРН) відповідними компонентами освітньої програми

5.1. Матриця забезпечення ПРН обов'язковими компонентами (ОК) освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13
ПРН 1												*	*
ПРН 2	*	*										*	*
ПРН 3	*	*										*	*
ПРН 4	*	*			*			*	*	*	*		*
ПРН 5	*	*		*	*	*		*	*	*	*		*
ПРН 6				*	*		*	*	*	*	*		
ПРН 7			*										*
ПРН 8			*	*	*		*	*	*	*	*		
ПРН 9			*	*		*							
ПРН10			*	*	*	*	*	*	*	*	*		
ПРН11					*		*	*			*		
ПРН12				*		*				*			
ПРН13		*						*					
ПРН14			*	*							*		
ПРН15			*									*	*
ПРН16		*	*				*	*					
ПРН17	*												
ПРН18												*	
ПРН19		*											
ПРН20	*		*		*			*				*	*
ПРН 21		*											
ПРН 22	*	*											*
ПРН 23					*	*	*	*	*	*	*		
ПРН 24	*	*										*	*
ПРН 25	*											*	*

6. Матриця відповідності визначених стандартом компетентностей 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