МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Управління інформаційною безпекою»

першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: «Бакалавр з кібербезпеки»

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ

Заступник голови Вченої ради_____ Олександр ФИЛИПЕНКО
протокол від "31 " 01 2022 р. № 1)

Освітня програма вводиться в дію з 01.09. 2022 р.

Перший проректор_____ Ігор РУБАН
наказ від " 01 " 02 2022 р. № 30)

Харків 2022 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«Управління інформаційною безпекою»
спеціальності 125 Кібербезпека
першого (бакалаврського) рівня вищої освіти

УЗГОДЖЕНО
Перший проректор
_____ Ігор РУБАН
«_27_» ___01___ 20_22_р.

В.о. начальника відділу ЛА та ВСЗЯО
_____ Сергій МАКАШЕВ
«_26_» ___01___ 20_22_р.

Начальник навчального відділу
_____ Аліна МІХНОВА
«_26_» ___01___ 20_22_р.

Розглянуто на засіданні Вченої ради
Факультету ІК
Протокол від «13» 01. 2022 № 1
Декан факультету ІК
_____ Аркадій СНІГУРОВ

Розглянуто на засіданні кафедри ІКІ
Протокол від «28» 12. 2021 № 12
Завідувач кафедри ІКІ
_____ 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:
Гріненко Тетяна Олексіївна,
кандидат технічних наук, доцент,
доцент кафедри БІТ ХНУРЕ _____

члени проектної групи:
Ликов Юрій Володимирович,
кандидат технічних наук, доцент,
доцент кафедри КРСТЗІ ХНУРЕ _____
Снігуров Аркадій Владиславович,
кандидат технічних наук, доцент,
декан факультету ІК ХНУРЕ _____
Ляшенко Олексій Сергійович,
кандидат технічних наук, доцент,
декан факультету КІУ ХНУРЕ _____

ПЕРЕДМОВА

Розроблено проектною групою у складі:

Керівник проектної групи:

Гріненко Тетяна Олексіївна, кандидат технічних наук, доцент, доцент кафедри БІТ, факультету КІУ ХНУРЕ.

Члени проектної групи:

Ликов Юрій Володимирович, кандидат технічних наук, доцент, доцент кафедри КРСТЗІ, факультету ІРТЗІ ХНУРЕ.

Снігуров Аркадій Владиславович, кандидат технічних наук, доцент, декан факультету ІК ХНУРЕ.

Ляшенко Олексій Сергійович, кандидат технічних наук, доцент, декан факультету КІУ ХНУРЕ.

Керівник проектної групи  Тетяна ГРІНЕНКО

1. Профіль освітньої програми «Управління інформаційною безпекою» за спеціальністю 125 Кібербезпека

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	Бакалавр Бакалавр з кібербезпеки
Офіційна назва освітньої програми	Управління інформаційною безпекою
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців, 2 роки 10 місяців
Наявність акредитації	Сертифікат про акредитацію спеціальності УД 21001341 від 19.03.2018. Строк дії сертифікату: до 01.07.2025.
Цикл/рівень	НРК України –6 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, 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/bakalavr-125-kiberbezpeka/osvitnja-programa-upravlinnja-informacijnoju-bezpekoju
2 - Мета освітньої програми	
– підготовка висококваліфікованих та конкурентоспроможних фахівців здатних використовувати та впроваджувати технології інформаційної та/або кібербезпеки; – надання ґрунтовної освіти з інформаційної та/або кібербезпеки із широким доступом до працевлаштування або продовження навчання за другим (освітньо-професійним або 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 професійної діяльності, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.
Основний фокус освітньої програми	Загальна вища освіта першого (бакалаврського) рівня в галузі 12 Інформаційні технології за спеціальністю 125 Кібербезпека. Акцент на здатності організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної та/або кібербезпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізації, економічної доцільності,

	можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації. Ключові слова: кібербезпека, інформаційна безпека, кібератаки, криптографічні методи захисту інформації, технічні методи захисту інформації, безпека інформаційно-комунікаційних систем, захист операційних систем, захист систем електронної комерції та банківських систем, кібербезпека проводових та безпроводових мереж, система менеджменту інформаційної безпеки, ідентифікація та аутентифікація користувачів
Особливості програми	Інтеграція програмно-апаратних засобів виявлення, моніторингу та забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності.
4 - Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Назва професій згідно Національного класифікатора України: Класифікатор професій (ДК 003: 2010) 2132.2 Розробник систем захисту інформації 2139.2 Аналітик загроз безпеки 2139.2 Аналітик з безпеки інформаційно-комунікаційних систем 2139.2 Дізнавач (сфера кібербезпеки та захисту інформації) 2139.2 Експерт криміналіст (сфера кібербезпеки та захисту інформації) 2139.2 Експерт криміналіст судової експертизи (сфера кібербезпеки та захисту інформації) 2139.2 Фахівець з криптографічного захисту інформації 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології) 2139.2 Фахівець з підтримки інфраструктури кіберзахисту 2139.2 Фахівець з реагування на інциденти кібербезпеки 2139.2 Фахівець з тестування систем захисту інформації 2139.2 Фахівець з технічного захисту інформації 2139.2 Фахівець сфери захисту інформації
Подальше навчання	Можливість навчання за програмою другого (магістерського) 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, виробнича та передатестаційна практика, підготовка кваліфікаційної роботи.
Оцінювання	Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано); 100-бальною шкалою та шкалою ЄКТС (A, B, C, D, E, FX, F)
6 - Програмні компетентності	
Інтегральна компетентність	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)	1. Здатність застосовувати знання у практичних ситуаціях. 2. Знання та розуміння предметної області та розуміння професії. 3. Здатність професійно спілкуватися державною та іноземною мовою як усно, так і письмово (українською мовою для іноземних студентів). 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. 5. Здатність до пошуку, оброблення та аналізу інформації. 6. Здатність реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Фахові компетентності спеціальності (ФК)	1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики та стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. 3. Здатність до використання програмних та програмно-апаратних комплексів захисту інформації в інформаційно-комунікаційних (автоматизованих) системах 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку 9.Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності 11. Здатність виконувати моніторинг процесів функціонування

	інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленою політикою інформаційної та/або кібербезпеки
7 - Програмні результати навчання	
	1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації (української мови для іноземних студентів). 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. 4. 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. 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. 12. Розробляти моделі загроз та порушника. 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

	17. Забезпечувати процеси захисту та функціонування інформаційно- телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах. 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки. 23. Реалізувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах. 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту. 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем. 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання

	комплексів засобів захисту в умовах реалізації загроз різних класів. 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем. 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. 36. Виявляти небезпечні сигнали технічних засобів. 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи захисту інформації. 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної, і/або кібербезпеки. 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

	45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-комунікаційних системах. 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-комунікаційних системах. 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. 54. Усвідомлювати цінності громадського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина України.
8 - Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями або вченими званнями, які мають досвід навчально-методичної, науково-дослідницької роботи та відповідають кваліфікації відповідно до спеціальності згідно ліцензійних умов
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.
9 - Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів (угод) між Харківським національним університетом радіоелектроніки та закладами вищої освіти України
Міжнародна кредитна мобільність	На основі двосторонніх договорів (угод) між Харківським національним університетом радіоелектроніки та закладами вищої іноземних країн
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

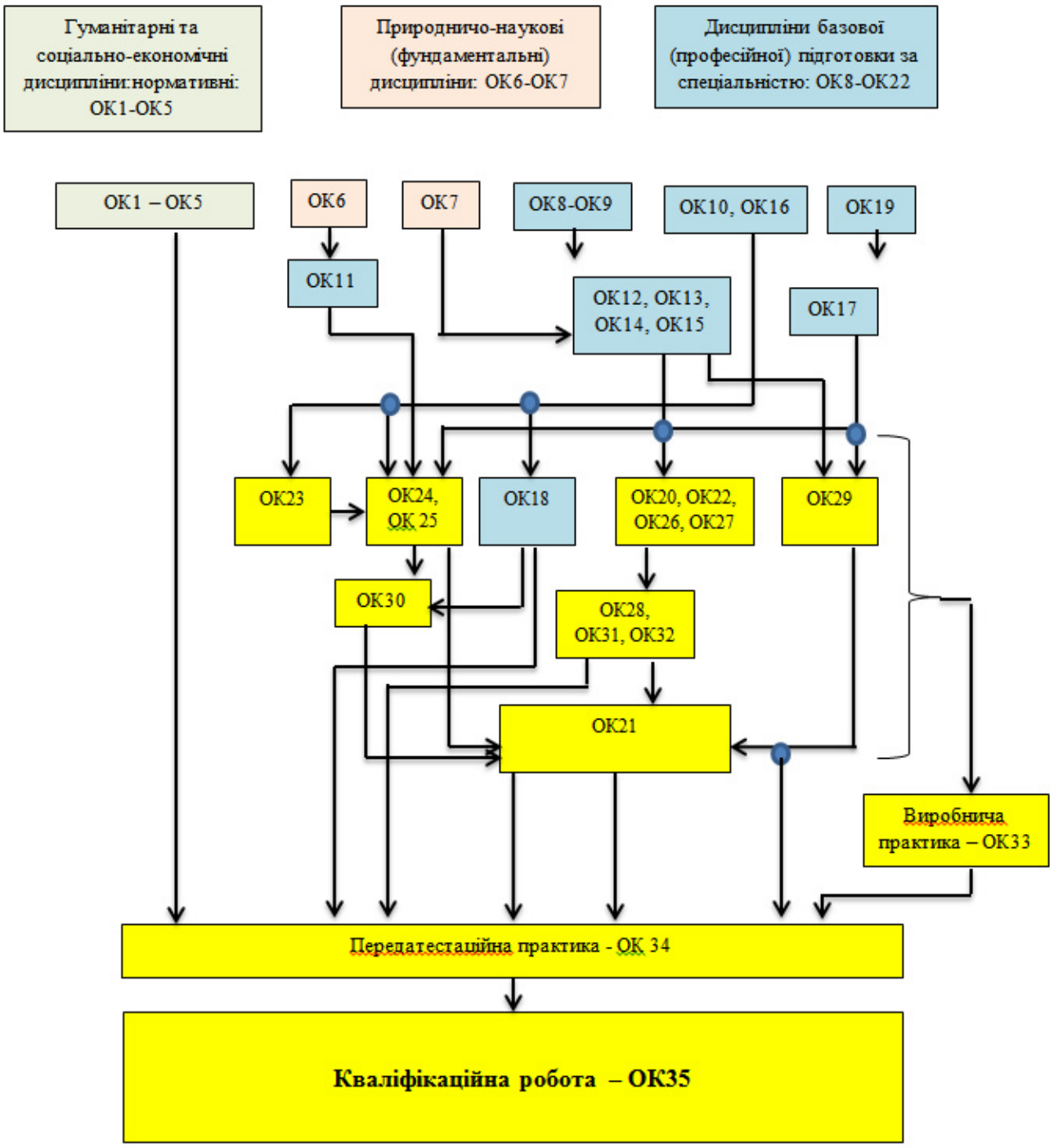
2.1. Перелік компонент ОП

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		
	Гуманітарні та соціально-економічні дисципліни (обов'язкові)		
ОК 1	Українське фахове мовлення	4	залік
ОК 2	Філософія	4	екзамен
ОК 3	Іноземна мова	8	екзамен
ОК3*	Українська мова як іноземна	12	залік
ОК 4	Основи права	2	залік
ОК 5	Фізичне виховання (за рахунок вільного часу студентів)	0	залік
ОК 5*	Українська мова як іноземна (за рахунок вільного часу студентів)	0	залік
	Всього:	18	
	*-для іноземних здобувачів вищої освіти		
	Дисципліни природничо-наукової (фундаментальної) підготовки за спеціальністю (обов'язкові)		
ОК 6	Вища математика	12	екзамен
ОК 7	Фізика	6	екзамен
	Всього:	18	
	Дисципліни базової (професійної) підготовки за спеціальністю (обов'язкові)		
ОК 8	Безпека життєдіяльності	3	залік
ОК 9	Економіка та бізнес	3	залік
ОК 10	Інформаційні технології	4	залік
ОК 11	Вища математика (спец. розділи)	4	залік
ОК 12	Архітектура комп'ютерних систем	4	екзамен
ОК 13	Схемотехніка	4	залік
ОК 14	Основи теорії кіл	4	екзамен
ОК 15	Електрорадіовимірювання	4	залік
ОК 16	Програмування	18	екзамен
ОК 17	Нормативно-правове забезпечення інф. безпеки	4	залік
ОК 18	Операційні системи	4	залік
ОК 19	Введення в спеціальність	4	залік
ОК 20	Теорія інформації та кодування	5	екзамен
ОК 21	Управління інформаційною безпекою	4	екзамен
ОК 22	Інформаційно-комунікаційні системи	9	екзамен
	Всього:	78	
	ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ		
	Дисципліни професійної та практичної підготовки за освітньою програмою «Управління інформаційною безпекою» (обов'язкові)		
ОК 23	Основи комп'ютерного моделювання	3	залік
ОК 24	Математичні основи криптології	4	екзамен
ОК 25	Основи криптографічного захисту інформації	6	екзамен
ОК 26	Основи IP-мереж	4	екзамен
ОК 27	Локальні мережі	5,5	залік

ОК 28	Безпека інформації в інформаційно-комунікаційних системах	5	екзамен
ОК 29	Основи технічного захисту інформації. Ч.1.	6	екзамен
ОК 30	Основи захисту сучасних операційних систем	3,5	залік
ОК 31	Ідентифікація об’єктів та користувачів	4	залік
ОК 32	Безпека та аудит безпроводових мереж	6	екзамен
ОК 33	Виробнича практика	4,5	залік
ОК 34	Передатестаційна практика	4,5	залік
ОК 35	Кваліфікаційна робота	9	Екзамен
	Всього:	65	
	Загальний обсяг обов'язкових компонентів	**179**	
	ВИБІРКОВІ КОМПОНЕНТИ ОП*		
	ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ		
	Гуманітарні та соціально-економічні дисципліни	6	
	Загальний обсяг вибіркових компонентів за циклом	6	
	ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ		
	Дисципліни професійної та практичної підготовки за освітньою програмою «Управління інформаційною безпекою»		
ВБ 1	Організація та інформаційне забезпечення управлінської діяльності	4	залік
ВБ 2	Організаційне забезпечення захисту інформації	4	залік
ВБ 3	Прогнозування та моделювання в соціальній сфері	3	залік
ВБ 4	Інтернет-технології	3	залік
ВБ 5	Основи планування та адміністрування служб доступу до інформаційних ресурсів	4	екзамен
ВБ 6	Основи технічного захисту інформації. Ч.2.	4	залік
ВБ 7	Системи виявлення та протидії атакам	4	екзамен
ВБ 8	Основи побудови безпроводових мереж	4	екзамен
ВБ 9	Захист систем електронної комерції та мультисервісних систем	5	екзамен
ВБ 10	Системи управління базами даних	4	залік
ВБ 11	Мережне програмування	5	екзамен
ВБ 12	Інформаційна безпека в операційних системах Unix	4	залік
ВБ 13	Методи машинного навчання	4	екзамен
ВБ 14	Безпека банківських систем	4	залік
ВБ 15	Технології транзакцій на основі Blockchain	4	екзамен
ВБ 16	Методи моніторингу частотного ресурсу	5	екзамен
ВБ 17	Основи цифрової криміналістики	5	залік
ВБ 18	Основи аналізу вразливостей та етичного хакінгу	5	залік
ВБ 19	Основи Web-безпеки	5	екзамен
ВБ 20	Безпека кіберінформаційної структури	4	екзамен
ВБ 21	Стеганографія	4	залік
ВБ 22	Основи інформаційної безпеки телекомунікаційних та хмарних технологій	4	екзамен
	Загальний обсяг вибіркових компонентів за циклом	**55**	
	Загальний обсяг вибіркових компонентів	61	
	ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ	**240**	

* 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 «Управління інформаційною безпекою» спеціальності 125 Кібербезпека – захист кваліфікаційної роботи з видачею документу встановленого зразка про присудження здобувачеві ступеня магістра із присвоєнням освітньої кваліфікації: «Бакалавр з кібербезпеки»).

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 у сфері 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 5	ОК 6, ОК 7, ОК 9	ОК 8, ОК 9	ОК 10, ОК 16, ОК 23	ОК 12 – ОК 15	ОК 17, ОК 21	ОК 33, ОК 34, ОК 35	ОК 24, ОК 25	ОК 20, ОК 26, ОК 27	ОК 28, ОК 30, ОК 31, ОК 32, ОК 22, ОК 18	ОК 29
ЗК-1							*				
ЗК-2						*	*	*		*	*
ЗК-3	*						*				
ЗК-4						*	*	*		*	*
ЗК-5	*										
ЗК-6	*										
ЗК-7	*	*	*								
ФК-1						*					
ФК-2				*	*			*	*	*	
ФК-3				*						*	
ФК-4						*	*				
ФК-5										*	
ФК-6										*	
ФК-7						*		*		*	*
ФК-8						*				*	
ФК-9						*					
ФК-10								*			
ФК-11										*	
ФК-12										*	*

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 5	ОК 6, ОК 7, ОК 9	ОК 8, ОК 9	ОК 10, ОК 16, ОК 23	ОК 12 – ОК 15	ОК 17, ОК 21	ОК 33, ОК 34, ОК 35	ОК 24, ОК 25	ОК 20, ОК 26, ОК 27	ОК 28, ОК 30, ОК 31, ОК 32, ОК 22, ОК 18	ОК 29
ПРН – 1	*										
ПРН – 2	*						*				
ПРН – 3	*	*	*								
ПРН – 4	*	*									
ПРН – 5		*		*	*				*		
ПРН – 6	*	*									
ПРН – 7						*	*				
ПРН – 8						*	*				
ПРН – 9						*	*			*	
ПРН – 10							*		*		
ПРН – 11				*			*		*		
ПРН – 12						*	*			*	
ПРН – 13							*		*		
ПРН – 14							*			*	
ПРН – 15				*			*		*	*	
ПРН – 16						*	*			*	*
ПРН – 17							*		*	*	
ПРН – 18				*	*		*		*	*	
ПРН – 19							*			*	
ПРН – 20		*		*	*		*		*	*	
ПРН – 21							*			*	
ПРН – 22							*		*	*	
ПРН – 23							*		*	*	
ПРН – 24							*			*	
ПРН – 25							*			*	
ПРН – 26							*			*	

ПРН – 27							*		*	*	
ПРН – 28							*			*	
ПРН – 29						*	*			*	
ПРН – 30							*			*	
ПРН – 31							*		*	*	
ПРН – 32							*		*	*	
ПРН – 33						*	*				
ПРН – 34						*	*				
ПРН – 35						*	*			*	
ПРН – 36					*		*				*
ПРН – 37					*		*				*
ПРН – 38					*		*				*
ПРН – 39						*	*				*
ПРН – 40						*	*				*
ПРН – 41						*	*			*	
ПРН – 42						*	*			*	
ПРН – 43						*	*			*	
ПРН – 44						*	*				
ПРН – 45						*	*			*	
ПРН – 46						*	*			*	
ПРН – 47							*	*			
ПРН – 48							*	*			
ПРН – 49							*			*	
ПРН – 50							*			*	
ПРН – 51							*			*	
ПРН – 52							*			*	
ПРН – 53				*			*			*	
ПРН – 54	*										