МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»

першого 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 " січня 2022 р. № 1)

Освітня програма вводиться в дію з 01.09.2022 р.
Перший проректор_____ Ігор РУБАН
(наказ від " 01 " лютого 2022 р. №30)

Харків 2022

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«Безпека інформаційних і комунікаційних систем»
спеціальності 125 Кібербезпека та захисту інформації
першого (бакалаврського) рівня вищої освіти

УЗГОДЖЕНО

Перший проректор

_____ Ігор РУБАН

«_27_» _січня_ 2022_ р.

Начальник відділу ЛА та ВСЗЯО

_____ Сергій МАКАШЕВ

«_24_» _січня_ 2022_ р.

Начальник навчального відділу

_____ Аліна МІХНОВА

«_26_» _січня_ 2022_ р.

Розглянуто на засіданні Вченої ради
факультету КІУ
Протокол від «23» _12_ 2021 р. № 5
Декан факультету КІУ

_____ Олексій ЛЯШЕНКО

Розглянуто на засіданні кафедри БІТ
Протокол від «01» 12 2021 р. № 5

Завідувач кафедри БІТ

_____ Геннадій ХАЛІМОВ

Представники роботодавців

Виконавчий директор ПрАТ «ІІТ» _____ Володимир КРАВЧЕНКО_

Представник студентського самоврядування

Голова студентського сенату факультету КІУ _____ Юлія ІВАНКО_

РОЗРОБЛЕНО
Проектна група:

керівник проектної групи:

Гріненко Тетяна Олексіївна, к.т.н.,
доц., доцент кафедри БІТ ХНУРЕ _____

члени проектної групи:

Ликов Юрій Володимирович, к.т.н.,
доц., доцент кафедри КРіСТЗІ ХНУРЕ _____

Снігуров Аркадій Владиславович, к.т.н.,
доц., декан факультету ІК ХНУРЕ _____

Ляшенко Олексій Сергійович, к.т.н.,
доц., декан факультету КІУ ХНУРЕ _____

ПЕРЕДМОВА

Розроблено проектною групою у складі:

Керівник проектної групи:

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

Члени проектної групи:

2. Ликов Юрій Володимирович - кандидат технічних наук, доцент, доцент кафедри КРіСТЗІ факультету ІРТЗІ ХНУРЕ;

3. Снігуров Аркадій Владиславович - кандидат технічних наук, доцент, декан факультету ІК, доцент кафедри ІКІ факультету ІК ХНУРЕ;

4. Ляшенко Олексій Сергійович - кандидат технічних наук, доцент, декан факультету КІУ, доцент кафедри БІТ факультету КІУ ХНУРЕ.

1. Профіль освітньої програми «Безпека інформаційних комунікаційних систем» за спеціальністю 125 Кібербезпека

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Харківський національний університет радіоелектроніки, факультет комп'ютерної інженерії та управління (КІУ), кафедра безпеки інформаційних технологій (БІТ).
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Бакалавр з кібербезпеки
Офіційна назва освітньої програми	Безпека інформаційних і комунікаційних систем
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 МОН України УД №21001341 від 19.03.2018 року Строк дії сертифіката до 01.07.2025 року
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, англійська для іноземних студентів
Термін дії освітньої програми:	До повного завершення періоду навчання або наступного оновлення програми.
Інтернет-адреса постійного розміщення опису освітньої програми	https://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-125-kiberbezpeka/bakalavr-125-kiberbezpeka/osvitnja-programa-bezpeka-informacijnih-i-komunikacijnih-sistem
2- Мета освітньої програми	
Забезпечити підготовку висококваліфікованих фахівців в галузі інформаційних технологій зі спеціальності 125 Кібербезпека, здатних вирішувати складні спеціалізовані задачі та практичні проблеми забезпечення інформаційної безпеки, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	12 Інформаційні технології 125 Кібербезпека
Орієнтація освітньої програми	Освітньо-професійна програма Програма зорієнтована на набуття знань, умінь, компетенцій в галузі професійної діяльності, що передбачає застосування певних теорій та методів відповідних наук і характеризується комплексністю та невизначеністю умов
Основний фокус освітньої програми та спеціалізації	Загальна вища освіта першого (бакалаврського) рівня в галузі 12 Інформаційні технології за спеціальністю 125 Кібербезпека. ***Ключові слова***: кібербезпека, інформаційна безпека, криптографічний захист інформації, технічний захист інформації, захист персональних даних, антивірусний захист, захист інформації від несанкціонованого доступу, електронний цифровий підпис, захист від технічних розвідок

Особливості освітньої 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. Підготовка висококваліфікованих фахівців на високому методичному та професійному рівні.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Назва професій згідно Національного класифікатора України: Класифікатор професій (ДК 003: 2010): 2139.2 - фахівець з питань безпеки (інформаційно-комунікаційні технології); 2139.2 - фахівець з криптографічного захисту інформації; 2139.2 - фахівець з технічного захисту інформації; 2139.2 - фахівець сфери захисту інформації; 2139.2 - фахівець з підтримки інфраструктури кіберзахисту; 3439 – фахівець із організації інформаційної безпеки, 3439 – фахівець із організації захисту інформації з обмеженим доступом
Подальше навчання	Продовження навчання за програмою другого (магістерського) рівня вищої освіти
5 - Викладання та оцінювання	
Викладання та навчання	Лекції, практичні та лабораторні заняття, самонавчання, проектно-орієнтоване навчання, консультації із науково-педагогічними співробітниками, проведення наукових досліджень, підготовка кваліфікаційної роботи
Оцінювання	Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано) та 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F)
6 – Перелік компетентностей випускника	
Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки та захисту інформації, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (КЗ)	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. КЗ 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 (КФ)	КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

	КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
6 – Кінцеві, підсумкові та інтегративні результати навчання	
Результати навчання (РН)	РН 1 - застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 - організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 - використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 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; РН 5 - адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 - критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7- діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 - готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 - впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

	РН 10 - виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 - виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 - розробляти моделі загроз та порушника; РН 13 - аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 - вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 - використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 - реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 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; РН 18 - використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 - застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 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; РН 22 - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 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); РН 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; РН 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;

	РН 27 - вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 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; РН 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; РН 30 - здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 - застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 - вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 - вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 - приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 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; РН 36 - виявляти небезпечні сигнали технічних засобів; РН 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 технічного захисту інформації; РН 38 - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 - проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 - забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 - впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 - застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 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;

	РН 45 - застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 - здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН 47 - вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 - виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 - забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 - забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 - підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 - використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН 53 - вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 - усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	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.
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. 6.Забезпеченість комп'ютерною технікою, контрольно-вимірювальними приладами, програмно-технічними засобами автоматизації та системами автоматизації проектування. Засоби обчислювальної техніки з прикладним та спеціалізованим програмним забезпеченням, спеціальні радіовимірювальні пристрої, засоби технічного захисту інформації, спеціалізовані апаратно-програмні комплекси. Високий рівень практичної підготовки фахівців забезпечується розвиненою міжнародною співпрацею в науковій і освітніх сферах, наявністю спеціалізованих лабораторій: основ захисту інформації, технічних і програмно-апаратних засобів захисту і обробки інформації в інформаційно-комунікаційних системах, аналізу захищених децентралізованих блокчейн систем, моніторингу та виявлення каналів витоку інформації.

	В 2020 році в рамках програми Tempus (Trans-European Mobility Programme for University Studies) закуплено обладнання та створено програмно-апаратний комплекс для вивчення, дослідження та супроводження об'єктів інформаційної діяльності у галузі кібербезпеки.
Інформаційне та навчально-методичне забезпечення	1. Забезпеченість вітчизняними та закордонними фаховими періодичними виданнями в галузі інформаційної безпеки та кібербезпеки, 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 (http://nure.ua/) та кафедри (http://its.nure.ua/), на якому розміщена основна інформація про 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, також надання доступу до правової БД "Ліга: Закон"; електронних версій підручників видавництва «Центр учбової літератури»; електронних журналів: «Захист інформації. INSIDE»; «Information Security»; online-журнали з наукової бібліотеки eLIBRARY. Специфічними характеристиками інформаційного та навчально-методичного забезпечення є: - використання методів, моделей, методик та технологій створення, обробки, передачі, приймання, знищення, відображення та кіберзахисту інформаційних ресурсів; - використання методів та моделей розробки прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та кібербезпеки; - використання сукупності нормативно-правових (національні та міжнародні стандарти) та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та закладами вищої освіти України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та закладами вищої освіти зарубіжних країн-партнерів.
Навчання іноземних здобувачів вищої освіти	На основі договорів (угод) між Харківським національним університетом радіоелектроніки та закладами вищої освіти іноземних країн.

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

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проекти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОП			
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Гуманітарні та соціально-економічні дисципліни			
ОК 1	Українське фахове мовлення	4	залік
ОК 2	Іноземна мова	8	екзамен
ОК 3*	Українська мова як іноземна	12	екзамен
ОК 4	Філософія	4	екзамен
ОК 5	Основи права	2	залік
ОК 6	Фізичне виховання (за рахунок вільного часу студентів)		залік
ОК 7*	Українська мова як іноземна		залік
Загальний обсяг обов'язкових компонентів за циклом		**18**	
Природничо-наукові (фундаментальні) дисципліни			
ОК 8	Вища математика	12	екзамен
ОК 9	Фізика	6	екзамен
Загальний обсяг обов'язкових компонентів за циклом		**18**	
Дисципліни базової (професійної) підготовки за спеціальністю			
ОК 10	Безпека життєдіяльності	3	залік
ОК 11	Економіка та бізнес	3	залік
ОК 12	Введення в спеціальність	4	залік
ОК 13	Вища математика (спец. розділи)	4	залік
ОК 14	Програмування	18	екзамен
ОК 15	Основи теорії кіл	4	екзамен
ОК 16	Схемотехніка	4	залік
ОК 17	Електрорадіовимірювання	4	залік
ОК 18	Теорія інформації і кодування	5	екзамен
ОК 19	Інформаційні технології	4	залік
ОК 20	Архітектура комп'ютерних систем	4	залік
ОК 21	Організація та управління захистом інформації	4	екзамен
ОК 22	Інформаційно-комунікаційні системи	9	екзамен
ОК 23	Нормативно-правове забезпечення інформаційної безпеки	4	залік
ОК 24	Операційні системи	4	залік
Загальний обсяг обов'язкових компонентів за циклом		**78**	

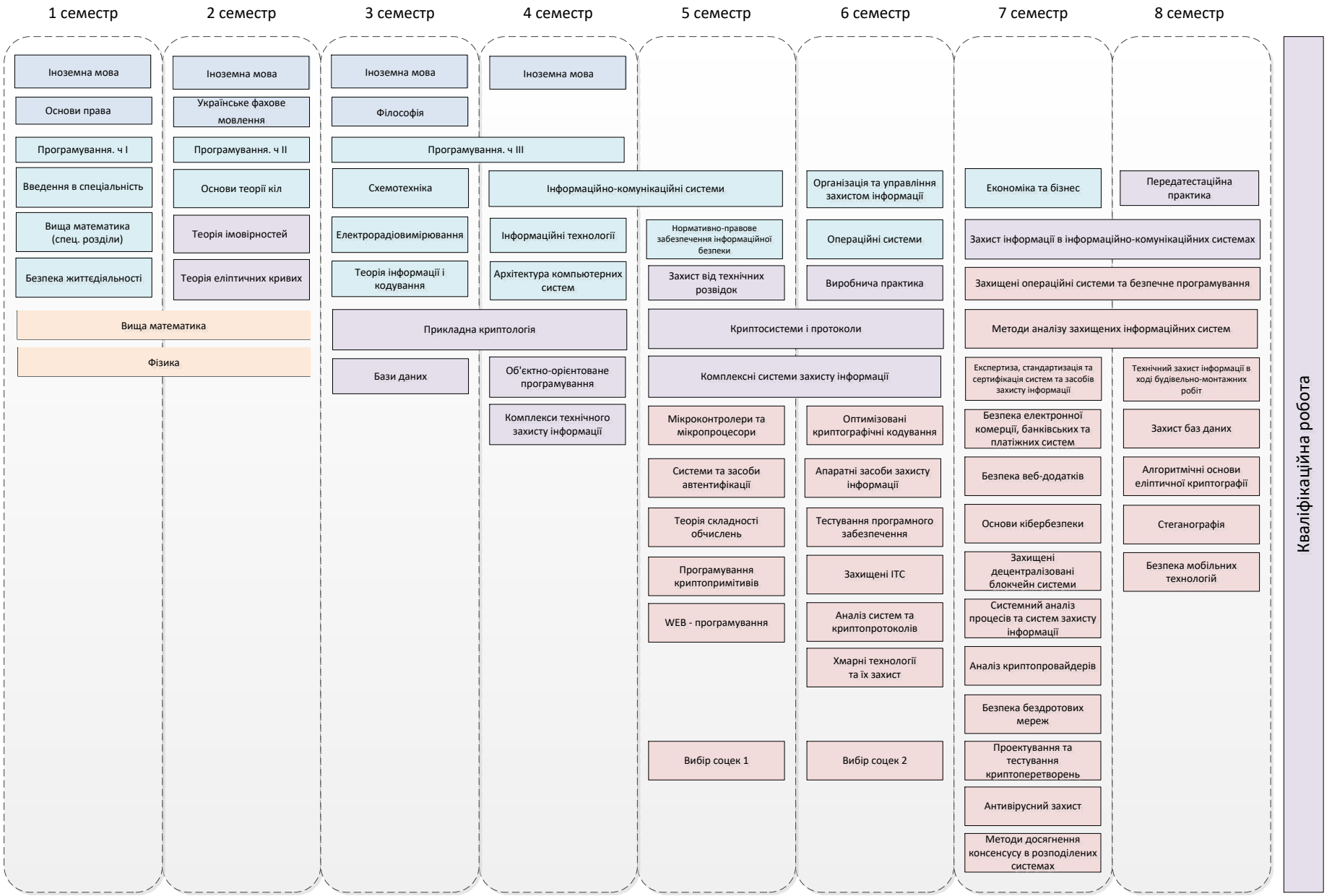
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проекти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
Дисципліни професійної та практичної підготовки за освітньою програмою «Безпека інформаційних і комунікаційних систем»			
ОК 25	Теорія ймовірностей	4	залік
ОК 26	Теорія еліптичних кривих	3	залік
ОК 27	Бази даних	3	залік
ОК 28	Прикладна криптологія	8,5	екзамен
ОК 29	Захист від технічних розвідок	3,5	екзамен
ОК 30	Об'єктно-орієнтоване програмування	3	залік
ОК 31	Криптосистеми і протоколи	6	екзамен
ОК 32	Комплекси технічного захисту інформації	4	залік
ОК 33	Комплексні системи захисту інформації	7	екзамен
ОК 34	Захист інформації в інформаційно-комунікаційних системах	6	екзамен
ОК 35	Виробнича практика	4,5	залік
ОК 36	Передатестаційна практика	4,5	залік
ОК 37	Кваліфікаційна робота	9	екзамен
Загальний обсяг обов'язкових компонентів за циклом		**66**	
ВИБІРКОВІ КОМПОНЕНТИ ОП			
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Гуманітарні та соціально-економічні дисципліни **			
Загальний обсяг вибіркових компонентів за циклом		**6**	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
Дисципліни професійної та практичної підготовки за освітньою програмою «Безпека інформаційних і комунікаційних систем»			
ВК 1	Мікроконтролери та мікропроцесори	4,5	залік
ВК 2	Системи та засоби автентифікації	4,5	залік
ВК 3	Теорія складності обчислень	4	залік
ВК 4	Програмування криптопримітивів	4	залік
ВК 5	WEB - програмування	4	залік
ВК 6	Оптимізовані криптографічні кодування	4	залік
ВК 7	Апаратні засоби захисту інформації	4	залік
ВК 8	Тестування програмного забезпечення	4	залік
ВК 9	Захищені ІТС	4	залік
ВК 10	Аналіз систем та криптопротоколів	4	залік
ВК 11	Хмарні технології та їх захист	4	залік
ВК 12	Експертиза, стандартизація та сертифікація систем та засобів захисту інформації	4	екзамен
ВК 13	Безпека електронної комерції, банківських та платіжних систем	4	екзамен
ВК 14	Безпека веб-додатків	4	екзамен
ВК 15	Основи кібербезпеки	4	залік

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проекти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ВК 16	Захищені децентралізовані блокчейн системи	4	залік
ВК 17	Системний аналіз процесів та систем захисту інформації	4	екзамен
ВК 18	Аналіз криптопровайдерів	4	екзамен
ВК 19	Безпека бездротових мереж	4	екзамен
ВК 20	Проектування та тестування криптоперетворень	4	екзамен
ВК 21	Антивірусний захист	4	залік
ВК 22	Методи досягнення консенсусу в розподілених системах	4	залік
ВК 23	Захищені операційні системи та безпечне програмування	7,5	екзамен
ВК 24	Методи аналізу захищених інформаційних систем	7,5	екзамен
ВК 25	Технічний захист інформації в ході будівельно-монтажних робіт	5	залік
ВК 26	Захист баз даних	5	залік
ВК 27	Алгоритмічні основи еліптичної криптографії	5	залік
ВК 28	Стеганографія	5	залік
ВК 29	Безпека мобільних технологій	5	залік
Загальний обсяг вибіркових компонентів за циклом		**54**	
Загальний обсяг вибіркових компонентів		**60**	
Загальний обсяг обов'язкових компонентів		**180**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

* – для іноземних здобувачів вищої освіти;
** – 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 наведена на рисунку 1.

Структурно-логічна схема освітньо-професійної програми



3. Форма атестації здобувачів вищої освіти

Форма атестації здобувачів вищої освіти за освітньою програмою «Безпека інформаційних і комунікаційних систем» спеціальності 125 Кібербезпека - захист кваліфікаційної роботи з видачою документу встановленого зразка про присудження здобувачеві ступеня бакалавра із присвоєнням освітньої кваліфікації: Бакалавр з кібербезпеки, Безпека інформаційних і комунікаційних систем.

Атестація здійснюється у формі публічного захисту кваліфікаційної роботи. Кваліфікаційна робота має продемонструвати здатність випускника розв'язувати складні спеціалізовані задачі та практичні проблеми в галузі забезпечення інформаційної безпеки і\або кібербезпеки та захисту інформації, що характеризується комплексністю та неповною визначеністю 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

Складається з двох частин у таблицях:

4.1. Матриця відповідності компетентностей обов'язковим компонентам освітньої програми. Може корегуватися за рішенням Вченої ради факультету КІУ.

4.2. Матриця відповідності компетентностей варіативним компонентам освітньої програми. Може корегуватися за рішенням кафедри БІТ.

5. Матриця забезпечення результатів навчання компонентам освітньої програми

Складається з двох частин у таблицях:

5.1. Матриця забезпечення результатів навчання обов'язковими компонентами освітньої програми. Може корегуватися за рішенням Вченої ради факультету КІУ.

5.2. Матриця забезпечення результатів навчання вибірковими компонентами освітньої програми. Може корегуватися за рішенням кафедри БІТ.

4.1. Матриця відповідності компетентностей обов'язковим компонентам освітньої програми

	ОК1	ОК2	ОК*3	ОК4	ОК5	ОК6	ОК*7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37
КЗ 1								+	+		+		+		+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+
КЗ 2												+	+	+					+	+	+		+			+	+	+	+	+	+	+	+	+	+	+	+
КЗ 3	+	+	+				+																														
КЗ 4					+			+	+	+	+					+									+										+	+	
КЗ 5				+										+	+			+	+	+	+	+		+	+		+	+		+					+	+	+
КЗ 6		+		+	+																																
КЗ 7		+		+	+	+																															
КФ 1	+											+	+								+		+					+			+		+		+	+	+
КФ 2																		+	+	+	+	+				+	+	+		+		+		+	+	+	+
КФ 3															+					+				+				+	+				+	+			+
КФ 4											+																				+	+	+	+			
КФ 5																		+			+	+		+				+				+	+	+	+	+	+
КФ 6																								+								+	+	+			
КФ 7																												+					+				+
КФ 8																					+							+					+				
КФ 9																					+							+									
КФ 10																					+								+		+	+		+			
КФ 11																					+	+												+			
КФ 12																					+												+				+

4.2. Матриця відповідності компетентностей варіативним компонентам освітньої програми

	ВК 1	ВК 2	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8	ВК 9	ВК 10	ВК 11	ВК 12	ВК 13	ВК 14	ВК 15	ВК 16	ВК 17	ВК 18	ВК 19	ВК 20	ВК 21	ВК 22	ВК 23	ВК 24	ВК 25	ВК 26	ВК 27	ВК 28	ВК 29
КЗ 1		+	+	+	+	+	+	+	+	+		+		+		+		+	+	+	+	+		+	+	+	+		+
КЗ 2	+	+						+		+	+		+		+	+			+		+	+	+	+	+			+	
КЗ 3							+		+			+					+						+	+					
КЗ 4			+	+	+	+			+				+			+	+				+				+	+		+	
КЗ 5	+	+			+			+		+	+	+	+						+			+	+			+	+		
КЗ 6															+														
КЗ 7																	+							+					
КФ 1		+					+		+			+	+								+				+				
КФ 2	+	+			+			+	+	+	+		+	+	+	+		+	+	+	+	+	+			+			+
КФ 3			+				+		+	+					+						+								
КФ 4																+	+												
КФ 5										+							+		+			+		+						
КФ 6															+						+		+			+			
КФ 7									+															+					
КФ 8													+								+								
КФ 9									+				+																
КФ 10		+												+		+					+								+
КФ 11																+			+			+		+					
КФ 12										+			+	+					+				+	+		+			+

5.1. Матриця забезпечення результатів навчання обов'язковими компонентами освітньої програми

	ОК1	ОК2	ОК*3	ОК4	ОК5	ОК6	ОК*7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37
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															+																	+	+				
РН 26																					+								+					+			
РН 27													+															+						+	+	+	
РН 28																					+								+				+	+		+	

	ОК1	ОК2	ОК*3	ОК4	ОК5	ОК6	ОК*7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37
РН 29																					+								+				+	+			
РН 30																								+	+				+				+	+			
РН 31														+													+			+	+						+
РН 32																								+								+	+				
РН 33																					+				+									+			
РН 34																		+			+		+													+	+
РН35																																	+		+	+	
РН36																	+												+			+					
РН 37																	+												+			+				+	
РН 38																	+												+			+	+				
РН 39																																	+				
РН 40																	+												+			+	+				
РН 41																						+		+								+					
РН 42																					+								+			+		+			
РН 43												+							+		+		+						+								+
РН 44											+										+		+											+			
РН 45																													+				+				+
РН 46																		+			+				+								+	+			
РН 47														+												+		+	+	+			+	+		+	
РН 48																																		+			
РН 49															+									+							+			+			
РН 50																																	+	+			
РН 51																																	+	+			
РН 52															+							+		+										+			
РН 53														+																+							
РН 54				+	+						+	+																									

5.2. Матриця забезпечення результатів навчання вибірковими компонентами освітньої програми

	ВК 1	ВК 2	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8	ВК 9	ВК 10	ВК 11	ВК 12	ВК 13	ВК 14	ВК 15	ВК 16	ВК 17	ВК 18	ВК 19	ВК 20	ВК 21	ВК 22	ВК 23	ВК 24	ВК 25	ВК 26	ВК 27	ВК 28	ВК 29
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									+														+						
РН 26									+				+										+		+				
РН 27		+	+	+					+						+	+		+	+		+							+	
РН 28										+		+							+										

	ВК 1	ВК 2	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8	ВК 9	ВК 10	ВК 11	ВК 12	ВК 13	ВК 14	ВК 15	ВК 16	ВК 17	ВК 18	ВК 19	ВК 20	ВК 21	ВК 22	ВК 23	ВК 24	ВК 25	ВК 26	ВК 27	ВК 28	ВК 29
РН 29									+	+		+	+	+				+	+						+				+
РН 30								+	+	+		+	+	+				+							+				+
РН 31		+				+													+									+	
РН 32																+													
РН 33													+		+														
РН 34										+		+	+																
РН 35												+																	
РН 36																									+				
РН 37																									+				
РН 38																									+				
РН 39												+																	
РН 40												+													+				
РН 41																							+						
РН 42						+							+					+			+		+						
РН 43																		+	+										
РН 44													+		+				+						+				
РН 45															+				+										
РН 46									+			+							+										
РН 47		+	+	+		+	+		+	+						+		+		+		+		+			+		
РН 48			+			+				+	+							+		+				+			+		
РН 49																													
РН 50									+										+		+								
РН 51							+		+																				
РН 52					+		+		+																	+		+	
РН 53								+		+													+						
РН 54													+																