МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»

другого рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: Магістр, Кібербезпека,

Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ

Голова вченої ради

_____ / В.В. Семенець /

(протокол № 7 від "28" 01 2021 р.)

зі змінами

протокол № 5 від «28» 05 2021р.

Освітня програма вводиться в дію з 01.09. 2021 р.

Ректор_____ / В.В. Семенець /

(наказ № 16 від "02" 02 2021 р.)

зі змінами

наказ №173 від "03" 06 2021 р.

Харків 2021 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«Безпека інформаційних і комунікаційних систем»
другого рівня вищої освіти
за спеціальністю 125 Кібербезпека

УЗГОДЖЕНО

Перший проректор
_____ І.В. Рубан
«__» ____ 2021 р.

В.о. начальника відділу ЛА та ВСЗЯО
_____ С.Б. Макашев
«27» 05 2021 р.

Начальник навчального відділу
_____ А.В. Міхнова
«21» 05 2021 р.

Розглянуто на засіданні Вченої ради
факультету КІУ
Протокол № 9 від 26.05.2021 р.
Декан факультету КІУ
_____ О.С. Ляшенко

Розглянуто на засіданні кафедри БІТ
Протокол № 11 від 12.05.2021 р.
Завідувач кафедри БІТ
_____ Г.З. Халімов

Представники роботодавців
Кравченко Володимир Дмитрович
Виконавчий директор ПрАТ «ІІТ»
_____ В.Д. Кравченко

РОЗРОБЛЕНО
Проектна група:

керівник проектної групи:

Руженцев Віктор Ігорович, д.т.н., доц.,
проф. кафедри БІТ, ХНУРЕ
_____ В.І. Руженцев

члени проектної групи:
Халімов Геннадій Зайдулович, д.т.н., проф.,
зав. каф. БІТ, ХНУРЕ
_____ Г.З. Халімов

Олейніков Анатолій Миколайович, к.т.н., проф.,
професор каф. КРіСТЗІ, ХНУРЕ
_____ А.М. Олейніков

Снігуров Аркадій Владиславович, к.т.н., доц.,
доц. каф. ІКІ, декан факультету ІК, ХНУРЕ
_____ А.В. Снігуров

Сєвєрінов Олександр Васильович, к.т.н., доц.,
доц. каф. БІТ, ХНУРЕ
_____ О.В. Сєвєрінов

Представник студентського самоврядування
Голова студентського сенату факультету КІУ
_____ М.Е. Бондаренко

ПЕРЕДМОВА

Розроблено проектною групою у складі:

1. Руженцев Віктор Ігорович (керівник проектної групи)	– доктор технічних наук, доцент, професор кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки
2. Халімов Геннадій Зайдулович	– доктор технічних наук, професор, зав. кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки
2. Олейніков Анатолій Миколайович	– кандидат технічних наук, професор, професор кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації Харківського національного університету радіоелектроніки
3. Снігуров Аркадій Владиславович	– кандидат технічних наук, доцент, декан факультету інфокомунікацій, доцент кафедри Інфокомунікаційної інженерії ім. В.В. Поповського Харківського національного університету радіоелектроніки
4. Сєвєрінов Олександр Васильович	– кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки

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

1 - Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Харківський національний університет радіоелектроніки Факультет комп'ютерної інженерії та управління Кафедра безпеки інформаційних технологій
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Магістр, Кібербезпека, Безпека інформаційних і комунікаційних систем
Офіційна назва освітньої програми	Безпека інформаційних і комунікаційних систем
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 міс.
Наявність акредитації	Сертифікат про акредитацію спеціальності МОН України НД №2190672 від 24.07.2015 р. Строк дії сертифіката до 01.07.2025 р.
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра (або освітньо-кваліфікаційний рівень спеціаліста)
Мова(и) викладання	Українська, англійська для іноземних студентів
Термін дії освітньої програми	До повного завершення періоду навчання або наступного оновлення програми
Інтернет-адреса постійного розміщення опису освітньої програми	https://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-125-kiberbezpeka/magistr-125-kiberbezpeka/osvitnja-programa-bezpeka-informacijnih-i-komunikacijnih-sistem
2 - Мета освітньої програми	
Мета освітньої програми полягає в оволодінні студентами знаннями, вміннями та навичками щодо впровадження та застосування технологій кібербезпеки; набуття компетентностей у використанні методів дослідження та проектування систем й комплексів забезпечення кібербезпеки.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	12 Інформаційні технології 125 Кібербезпека
Орієнтація освітньої програми	Освітньо-професійна програма Акцент програми зроблений на підготовку фахівців, здатних 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 та спеціалізації	Загальна спеціальна освіта другого (магістерського) рівня вищої освіти в галузі інформаційних технологій за спеціальністю 125 Кібербезпека.

	Ключові слова: кібербезпека, інформаційна безпека, криптографічний захист інформації, захист персональних даних, антивірусний захист, захист інформації, захист від несанкціонованого доступу, електронний цифровий підпис
Особливості програми	Програма передбачає вивчення: - законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; - принципів розробки, впровадженню, супроводу комплексних систем захисту інформації; - методів та засобів оцінювання захищеності інформації; - технології, методи, моделі та засоби кібербезпеки; - методів та засобів криптографічного захисту інформації; - технології, методи, моделі та засоби захисту сучасних інформаційно-комунікаційних технологій; - системи управління кібербезпекою.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники підготовлені до роботи за національним класифікатором України: Класифікатор професій (ДК 003:2010): 2149.2- професіонал із організації інформаційної безпеки; 2149.2- професіонал із організації захисту інформації з обмеженим доступом.
Подальше навчання	Можливість навчатися за програмою третього (освітньо-наукового) рівня вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
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 атестаційної роботи
Оцінювання	Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано); 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F)
6 - Програмні компетентності	
Інтегральна компетентність	Здатність розв’язувати складні задачі і проблеми в галузі інформаційної безпеки та/або кібербезпеки, а також у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог
Загальні компетентності (КЗ)	КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
	КЗ-2. Здатність проводити дослідження на відповідному рівні.
	КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.
	КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
	КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

Фахові компетентності спеціальності (КФ)	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
	КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
	КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
	КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
	КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
	КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
	КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
	КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
	КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
	КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

7 - Кінцеві, підсумкові та інтегративні результати навчання	
Результати навчання (РН)	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
	РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
	РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
	РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
	РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
	РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
	РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
	РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
	РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
	РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
	РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
	РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
	РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх

	використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
	РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
	РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
	РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
	РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
	РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
	РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
	РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
	РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
	РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
	РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
8 – Ресурсне забезпечення реалізації	
Кадрове забезпечення	Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями та вченими званнями, які мають великий досвід навчально-методичної, науково-дослідної роботи та відповідають кваліфікації відповідно до спеціальності згідно ліцензійних умов.

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 компонент освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонент ОП

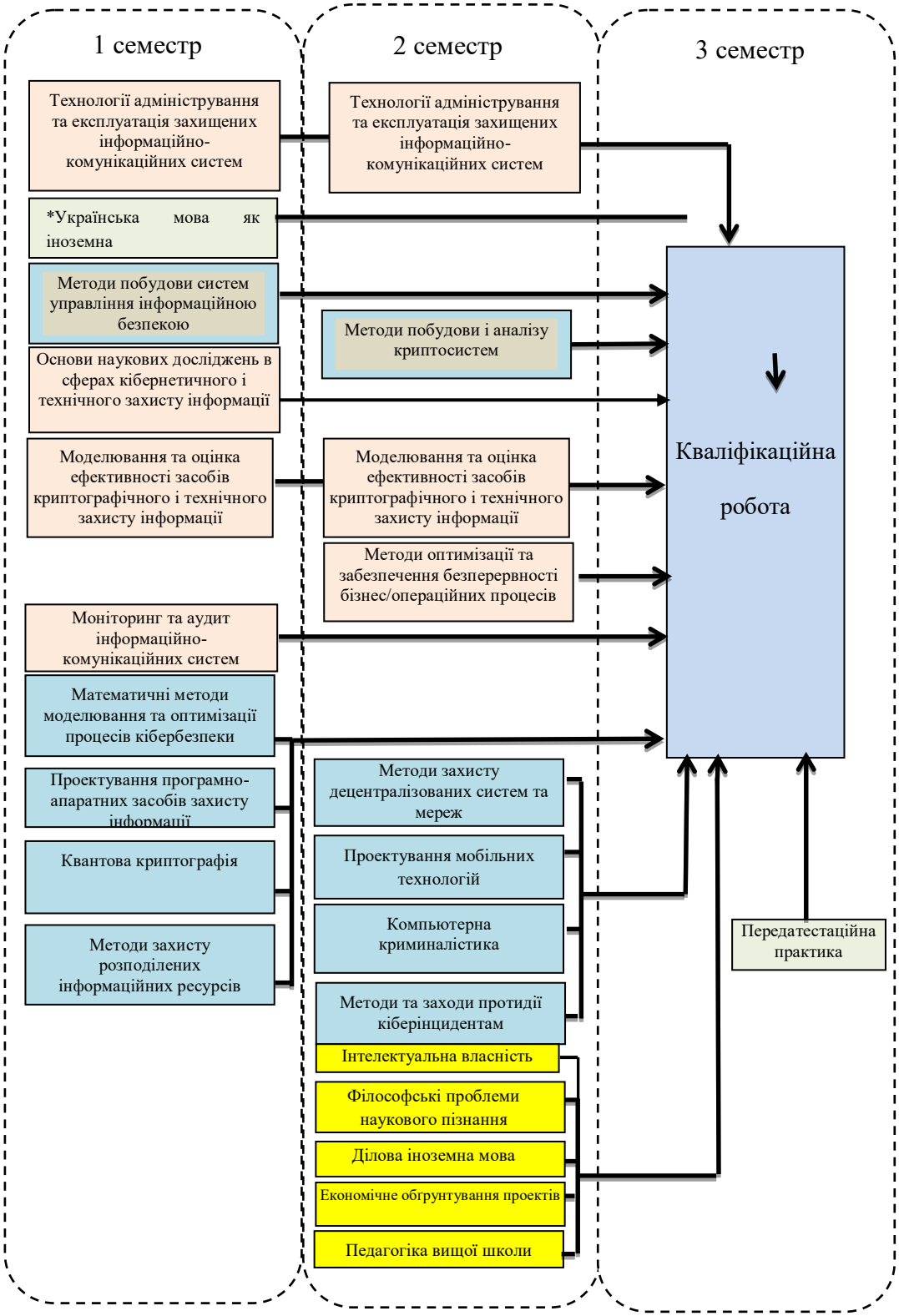
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Гуманітарні та соціально-економічні дисципліни (обов'язкові)			
ОК * 1.1	Українська мова як іноземна	3	Зл
Гуманітарні та соціально-економічні дисципліни (вибіркові)			
ВБ 1.1	Інтелектуальна власність	3	Зл
ВБ 1.2	Ділова іноземна мова (Іноземна мова за професійним спрямуванням)	3	Зл
ВБ 1.3	Філософські проблеми наукового пізнання	3	Зл
ВБ 1.4	Педагогіка вищої школи	3	Зл
ВБ 1.5	Економічне обґрунтування проектів	3	Зл
Всього:		3	
Дисципліни базової (професійної) підготовки за спеціальністю (обов'язкові)			
ОК 1.1	Основи наукових досліджень в сферах кібернетичного і технічного захисту інформації	5	Зл
ОК 1.2	Методи оптимізації та забезпечення безперервності бізнес/операційних процесів	4	Ек
ОК 1.3	Моделювання та оцінка ефективності засобів криптографічного і технічного захисту інформації	8	Ек
ОК 1.4	Моніторинг та аудит інформаційно-комунікаційних систем	5	Ек
ОК 1.5	Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	7	Ек
Всього:		29	
РАЗОМ (цикл загальної та спеціальної (фахової) підготовки):		32	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
Дисципліни професійної та практичної підготовки (обов'язкові)			
ОК 2.1	Методи побудови і аналізу криптосистем	5	Ек
ОК 2.2	Методи побудови систем управління інформаційною безпекою	3	Зл
ОК 2.3	Передатестаційна практика	15	Зл
ОК 2.4	Кваліфікаційна робота	15	Ек
Всього:		38	
Дисципліни професійної та практичної підготовки (вибіркові)			
ВБ 2.1	Проектування програмно-апаратних засобів захисту інформації	5	Зл
ВБ 2.2	Математичні методи моделювання та оптимізації процесів кібербезпеки	5	Зл
ВБ 2.3	Квантова криптографія	5	Зл
ВБ 2.4	Методи захисту розподілених інформаційних ресурсів	5	Зл
ВБ 2.5	Проектування мобільних технологій	5	Зл
ВБ 2.6	Методи захисту децентралізованих систем та мереж	5	Зл
ВБ 2.7	Комп'ютерна криміналістика	5	Зл
ВБ 2.8	Методи та заходи протидії кіберінцидентам	5	Зл
Всього		20	
РАЗОМ (цикл професійної підготовки):		58	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		90	

* – для іноземних здобувачів вищої освіти;

2.1. Структурно-логічна схема ОП

1 семестр	2 семестр	3 семестр
ОК* 1.1. ОК 1.1. ОК 1.3. ОК 1.4. ОК 1.5. ОК 2.2. ВБ 2.1., ВБ 2.2. ВБ 2.3., ВБ 2.4.	 ОК 1.2. ОК 1.3. ОК 1.5. ОК 2.1. ВБ 1.1., ВБ 1.2., ВБ 1.3., ВБ 1.4., ВБ 1.5. ВБ 2.5., ВБ 2.6. ВБ 2.7., ВБ 2.8.	ОК 2.3. ОК 2.4.

2.2 Структурно-логічна схема ОПП



3 Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Безпека інформаційних і комунікаційних систем» спеціальності 125 Кібербезпека здійснюється в формі публічного захисту кваліфікаційної роботи.

Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки, що передбачає проведення досліджень та/або здійснення інновацій.

Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Після публічного захисту кваліфікаційна робота розміщується на офіційному сайті університету (або на репозитарії кафедри).

Атестація випускників завершується видачою документу встановленого зразка про присудження йому ступеня магістра із присвоєнням кваліфікації – Магістр, Кібербезпека, Безпека інформаційних і комунікаційних систем.

4. Матриця відповідності компетентностей компонентам освітньої програми

Матриця відповідності компетентностей компонентам освітньої програми складається з двох частин: матриці відповідності компетентностей обов'язковим компонентам освітньої програми та матриці відповідності компетентностей варіативним компонентам освітньої програми.

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

Матриця забезпечення результатів навчання компонентам освітньої програми складається з двох частин: матриці забезпечення результатів навчання обов'язковими компонентами освітньої програми та матриці забезпечення результатів навчання вибірковими компонентами освітньої програми.

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 Матриця відповідності компетентностей компонентам освітньої програми

Компетентності	Обов'язкові компоненти освітньої програми										Варіативні компоненти освітньої програми											
	ОК 1.1	ОК* 1.1	ОК 1. 2	ОК 1. 3	ОК 1.4	ОК 1.5	ОК 2.1	ОК 2.2	ОК 2.3	ОК 2.4	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ВБ 1.5	ВБ 2.1	ВБ 2.2	ВБ 2.3	ВБ 2.4	ВБ 2.5	ВБ 2.6	ВБ 2.7	ВБ 2.8
КЗ-1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+
КЗ-2	+			+	+				+	+					+		+	+					
КЗ-3	+		+		+		+	+	+	+	+		+			+						+	+
КЗ-4			+	+	+	+			+	+					+		+					+	
КЗ-5	+	+	+		+		+	+	+	+		+	+	+	+	+			+		+		+
КФ-1	+		+	+	+		+	+		+						+	+	+	+	+	+	+	+
КФ-2						+		+	+	+	+	+			+							+	+
КФ -3				+	+	+	+		+	+										+			
КФ -4						+		+		+													
КФ -5			+						+	+							+		+			+	
КФ -6			+		+			+	+														
КФ -7					+	+			+	+							+					+	+
КФ -8				+		+	+		+	+						+		+			+		
КФ -9			+		+										+								
КФ -10	+			+					+	+	+			+									

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

Результати навчання	Обов'язкові компоненти освітньої програми										Варіативні компоненти освітньої програми												
	ОК 1.1	ОК* 1.1	ОК 1.2	ОК1. 3	ОК1. 4	ОК1. 5	ОК 2.1	ОК 2.2	ОК 2.3	ОК 2.4	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ВБ 1.5	ВБ 2.1	ВБ 2.2	ВБ 2.3	ВБ 2.4	ВБ 2.5	ВБ 2.6	ВБ 2.7	ВБ 2.8
РН - 1		+										+											
РН - 2	+						+	+		+						+				+			
РН - 3			+	+			+	+	+	+						+	+			+		+	
РН - 4	+		+				+	+								+	+			+		+	
РН - 5	+			+			+		+	+												+	
РН - 6				+	+		+		+	+								+				+	
РН - 7					+	+					+					+			+	+	+		
РН - 8				+		+	+			+									+		+		
РН - 9						+		+															
РН - 10			+		+					+													+
РН - 11			+					+	+														
РН - 12					+					+									+		+	+	+

Результати навчання	Обов'язкові компоненти освітньої програми										Варіативні компоненти освітньої програми												
	ОК 1.1	ОК* 1.1	ОК 1.2	ОК1. 3	ОК1. 4	ОК1. 5	ОК 2.1	ОК 2.2	ОК 2.3	ОК 2.4	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ВБ 1.5	ВБ 2.1	ВБ 2.2	ВБ 2.3	ВБ 2.4	ВБ 2.5	ВБ 2.6	ВБ 2.7	ВБ 2.8
РН - 13			+	+			+			+						+		+		+			
РН - 14				+	+			+		+							+						
РН - 15									+	+													
РН - 16			+			+	+		+								+						
РН - 17	+									+			+	+									
РН - 18	+					+								+									
РН - 19					+		+			+						+				+			
РН - 20				+			+	+		+						+				+			
РН - 21				+	+		+	+		+							+	+				+	
РН - 22	+		+				+	+		+							+	+	+	+	+	+	+
РН - 23					+	+	+	+	+	+					+			+					+