МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»

другого (магістерського) рівня вищої освіти

за спеціальністю F5 Кібербезпека та захист інформації

галузі знань F Інформаційні технології

Кваліфікація: Магістр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ
Голова Вченої ради_____ Ігор РУБАН
(протокол від "31" 03 20 26р. № 4)

Освітня програма вводиться в дію з 01вересня 2026 р.
Ректор_____ Ігор РУБАН
(наказ від "31" 03 20 26 р. № 166)

Харків 2026

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми
«Безпека інформаційних і комунікаційних систем»
спеціальності F5 Кібербезпека та захист інформації
другого (магістерського) рівня вищої освіти

ПОГОДЖЕНО

Перший проректор
_____ Андрій ЄРОХІН
« 12 » ___03___ 2026 р.

Начальник відділу ЛА та ВСЗЯО
_____ Ганна ТУГАЙ
« 09 » ___03___ 2026 р.

Начальник навчального відділу
_____ Аліна МІХНОВА
« 10 » ___03___ 2026 р.

Розглянуто на засіданні Вченої ради
факультету КБ
Протокол від «30» 03 2026 р. № 1
Декан факультету КБ
_____ Аркадій СНІГУРОВ

Розглянуто на засіданні кафедри БІТ
Протокол від « 10 » 03 2026 р. № 10
Завідувач кафедри БІТ
_____ Геннадій ХАЛІМОВ

Представники роботодавців
Виконавчий директор ПрАТ «ІІТ» _____ Володимир КРАВЧЕНКО_

Представник студентського самоврядування
Голова студентського сенату факультету КБ _____ Сергій АЛФЬОРОВ _

РОЗРОБЛЕНО
Проєктна група:
керівник проєктної групи:

Руженцев Віктор Ігорович, д.т.н.,
доц., професор кафедри БІТ ХНУРЕ _____

члени проєктної групи:
Халімов Геннадій Зайдулович, д.т.н.,
проф., завідувач кафедри БІТ ХНУРЕ _____

Радівілова Тамара Анатоліївна, д.т.н.,
проф., професор кафедри ІКІ імені В.В. Поповського _____

Олейніков Анатолій Миколайович, к.т.н.,
проф., професор кафедри ІРТЗІ ХНУРЕ _____

Євдокименко Марина Олександрівна, д.т.н.,
проф., проф. кафедри ІКІ імені В.В. Поповського _____

ПЕРЕДМОВА

Розроблено проєктною групою у складі:

Керівник проєктної групи:

1. Руженцев Віктор Ігорович	– доктор технічних наук, доцент, професор кафедри БІТ факультету КБ ХНУРЕ.

Члени проєктної групи:

2. Халімов Геннадій Зайдулович	– доктор технічних наук, професор, завідувач кафедри БІТ факультету КБ ХНУРЕ;
3. Радівілова Тамара Анатоліївна	– доктор технічних наук, професор, професор кафедри ІКІ імені В.В. Поповського факультету КБ ХНУРЕ;
4. Олейніков Анатолій Миколайович	– кандидат технічних наук, професор, професор кафедри ІРТЗІ факультету ІРТМ ХНУРЕ;
5. Євдокименко Марина Олександрівна	– доктор технічних наук, професор, професор кафедри ІКІ імені В.В. Поповського факультету КБ ХНУРЕ;

Гарант освітньої програми
«Безпека інформаційних і
комунікаційних систем» спеціальності
F5 Кібербезпека та захист інформації
другого (магістерського) рівня вищої освіти  Віктор РУЖЕНЦЕВ

1 Профіль освітньої програми «Безпека інформаційних і комунікаційних систем» за спеціальністю F5 Кібербезпека та захист інформації

1 - Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Харківський національний університет радіоелектроніки Факультет кібербезпеки (КБ) Кафедра безпеки інформаційних технологій (БІТ)
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Магістр з кібербезпеки та захисту інформації
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 УД 21019408, дійсний до 31.12.2027
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 проєктування систем й комплексів забезпечення кібербезпеки.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	F Інформаційні технології F5 Кібербезпека та захист інформації
Орієнтація освітньої програми	Освітньо-професійна програма Програма зорієнтована на підготовку фахівців, здатних розв'язувати складні задачі і проблеми у галузі професійної діяльності, передбачає проведення досліджень та/або здійснення інновацій що характеризуються невизначеністю умов і вимог
Основний фокус освітньої програми	Загальна вища освіта другого (магістерського) рівня вищої освіти в галузі F Інформаційні технології за спеціальністю F5

та спеціалізації	Кібербезпека та захист інформації. Ключові слова: кібербезпека, інформаційна безпека, криптографічний захист інформації, захист персональних даних, захист інформації, захист від несанкціонованого доступу, електронний підпис, політика безпеки, критична інфраструктура, кіберінцендент.
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	Назва професій згідно Національного класифікатора України: Класифікатор професій (ДК 003: 2010): 2139.2 – аналітик систем захисту інформації та оцінки вразливостей; 2139.2 – аналітик з безпеки інформаційно-телекомунікаційних систем; 2149.2 - професіонал із організації інформаційної безпеки; 2149.2 - професіонал із організації захисту інформації з обмеженим доступом; 231 - викладач університетів та закладів вищої освіти. Назва професій згідно International Standard Classification of Occupations 2008 (ISCO-08): 2522 System Administrators; 2529 Database and Network Professionals Not Elsewhere Classified
Подальше навчання	Продовження навчання 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, проєктно-орієнтоване навчання, консультації із науково-педагогічними співробітниками, консультації із представниками роботодавців, проведення наукових досліджень, 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 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). КЗ-6. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів не доброчесності.
Фахові компетентності спеціальності (КФ)	КФ 1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ 2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. КФ 4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ 5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ 6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ 7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ 8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно

	встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ 9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ 10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
7 - Кінцеві, підсумкові та інтегративні результати навчання	
Результати навчання (РН)	РН 1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН 2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН 3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН 4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН 5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН 6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН 7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН 9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН 10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН 11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних

	ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН 12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН 13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. РН 14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. РН 15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. РН 16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН 17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. РН 18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. РН 19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проєкти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН 20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН 21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН 22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН 23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки

	та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. РН24. Використовувати методи штучного інтелекту для аналізу ризиків та аудиту інформаційної безпеки та/або кібербезпеки в задачах захисту інформаційних систем. РН25. Аналізувати, розробляти, досліджувати криптосистеми захисту інформаційних систем в умовах нових викликів квантової революції, появи квантових комп'ютерів.
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 проєктування. 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 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

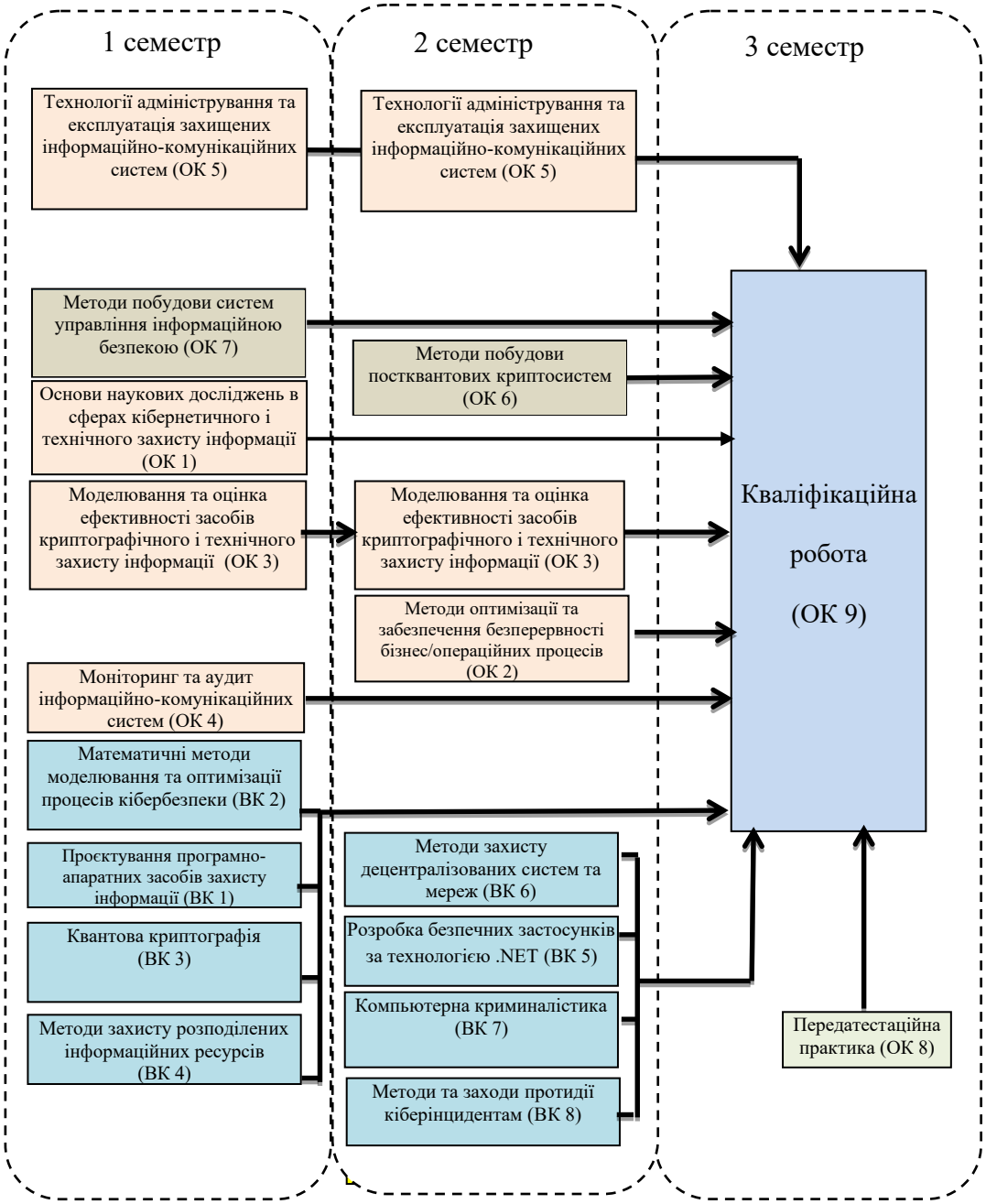
2.1. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОП			
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Дисципліни базової (професійної) підготовки за спеціальністю			
ОК 1	Основи наукових досліджень в сферах кібернетичного і технічного захисту інформації	5	Залік
ОК 2	Методи оптимізації та забезпечення безперервності бізнес/операційних процесів	4	Екзамен
ОК 3	Моделювання та оцінка ефективності засобів криптографічного і технічного захисту інформації	8	Екзамен
ОК 4	Моніторинг та аудит інформаційно-комунікаційних систем	5	Екзамен
ОК 5	Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	7	Екзамен
Загальний обсяг обов'язкових компонентів за циклом		29	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
Дисципліни професійної та практичної підготовки за освітньою програмою «Безпека інформаційних і комунікаційних систем»			
ОК 6.1	Методи побудови постквантових криптосистем	3	Екзамен
ОК 6.2	Курсова робота з дисципліни Методи побудови постквантових криптосистем	1	Захист КР
ОК 7.1	Методи побудови систем управління інформаційною безпекою	3	Залік
ОК 7.2	Курсова робота з дисципліни Методи побудови систем УІБ	1	Залік
ОК 8	Передатестаційна практика	15	Залік
ОК 9	Кваліфікаційна робота	15	Екзамен
Загальний обсяг обов'язкових компонентів за циклом		38	
ВИБІРКОВІ КОМПОНЕНТИ ОП			
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Гуманітарні та соціально-економічні дисципліни *			
Дисципліна з загального каталогу вибіркових навчальних дисциплін		3	
Загальний обсяг вибіркових компонентів за циклом		3	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
Дисципліни професійної та практичної підготовки за освітньою програмою «Безпека інформаційних і комунікаційних систем»			
ВК 1	Проєктування програмно-апаратних засобів захисту інформації	5	Залік
ВК 2	Математичні методи моделювання та оптимізації процесів кібербезпеки	5	Залік

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
ВК 3	Квантова криптографія	5	Залік
ВК 4	Методи захисту розподілених інформаційних ресурсів	5	Залік
ВК 5	Розробка безпечних застосунків за технологією .NET	5	Залік
ВК 6	Методи захисту децентралізованих систем та мереж	5	Залік
ВК 7	Комп'ютерна криміналістика	5	Залік
ВК 8	Методи та заходи протидії кіберінцидентам	5	Залік
Загальний обсяг вибіркових компонентів за циклом		20	
Загальний обсяг вибіркових компонентів		23	
Загальний обсяг обов'язкових компонентів		67	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		90	

* – 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 ОПП



3 Форма атестації здобувачів вищої освіти

Атестація здобувачів вищої освіти за освітньою програмою «Безпека інформаційних і комунікаційних систем» спеціальності F5 Кібербезпека та захист інформації - захист кваліфікаційної роботи з видачою документу встановленого зразка про присудження здобувачеві ступеня магістра із присвоєнням освітньої кваліфікації: Магістр з кібербезпеки та захисту інформації.

Кваліфікаційна робота має продемонструвати здатність випускника розв'язувати складні задачі в галузі інформаційної безпеки та/або 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

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 КБ.

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 КБ.

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

4.1 Матриця відповідності компетентностей компонентам освітньої програми

Компетентності	Обов'язкові компоненти освітньої програми									Вибіркові компоненти освітньої програми							
	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК6,ОК 6.1	ОК7,ОК 7.1	ОК 8	ОК 9	ВК1	ВК 2	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8
КЗ-1	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+
КЗ-2	+		+	+				+	+		+	+					
КЗ-3	+	+		+		+	+	+	+	+						+	+
КЗ-4		+	+	+	+			+	+		+					+	
КЗ-5	+	+		+		+	+	+	+	+			+		+		+
КЗ-6						+			+								
КФ 1	+	+	+	+		+	+		+	+	+	+	+	+	+	+	+
КФ 2					+		+	+	+							+	+
КФ 3			+	+	+	+		+	+					+			
КФ 4					+		+		+								
КФ 5		+						+	+		+		+			+	
КФ 6		+		+			+	+						+			
КФ 7				+	+			+	+		+					+	+
КФ 8			+		+	+		+	+	+		+			+		
КФ 9		+		+										+			
КФ 10	+		+					+	+								

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

Результати навчання	Обов'язкові компоненти освітньої програми									Вибіркові компоненти освітньої програми							
	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6.1,6.2	ОК 7.1,7.2	ОК 8	ОК 9	ВК 1	ВК 2	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 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				+					+				+		+	+	+
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						+											

5.1 Матриця відповідності визначених Стандартом компетентностей дескрипторам НРК

Класифікація компетентностей (результатів навчання) за НРК	**Знання** **Зн1** Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та на межі галузей знань	**Уміння/Навички** **Ум1** Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур **Ум2** Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах **Ум3** Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	**Комунікація** **К1** Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	**Відповідальність і автономія** **АВ1** Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів **АВ2** Відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів **АВ3** Здатність продовжувати навчання з високим ступенем автономії
Загальні компетентності				
КЗ-1	Зн1	Ум1, Ум3	К1	АВ1, АВ2
КЗ-2	Зн1	Ум1, Ум2, Ум3		АВ2, АВ3
КЗ-3	Зн1	Ум2, Ум3		АВ1
КЗ-4	Зн1	Ум3		АВ1, АВ2
КЗ-5	Зн1	Ум2	К1	АВ1
Спеціальні (фахові) компетентності				
КФ 1	Зн1	Ум2		АВ2
КФ 2	Зн1	Ум2		АВ2
КФ 3	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
КФ 4	Зн1	Ум1, Ум2	К1	АВ1, АВ2
КФ 5	Зн1	Ум1, Ум2	К1	АВ1, АВ2
КФ 6	Зн1	Ум1, Ум2	К1	АВ1
КФ 7	Зн1	Ум1, Ум2	К1	АВ1
КФ 8	Зн1	Ум1, Ум2	К1	АВ1
КФ 9	Зн1	Ум1, Ум2	К1	АВ1
КФ 10	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2

5.2 Матриця відповідності визначених Стандартом результатів навчання та компетентностей

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	
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	+		+	+		+	+	+			+	+	+	+		