МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації, автоматизація її обробки»

другого рівня вищої освіти

за спеціальністю 125 Кібербезпека та захист інформації

галузі знань 12 Інформаційні технології

Кваліфікація: Магістр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ

Заступник голови Вченої ради_____ Олександр ФИЛИПЕНКО

(протокол від "31"01 2024 р. № 2)

Освітня програма вводиться в дію з 01.09. 2024 р.

В.о. ректора_____ Ігор РУБАН

(наказ від "___"_____ 20__ р. № ___)

Харків 2024 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«Системи технічного захисту інформації, автоматизація її обробки»
спеціальності 125 Кібербезпека та захист інформації
другого (магістерського) рівня вищої освіти

УЗГОДЖЕНО

Перший проректор
_____ Ігор РУБАН
«___» _____ 2024р.

Начальник відділу ЛА та ВСЗЯО

Сергій МАКАШЕВ

«___» _____ 20__ р.

Начальник навчального відділу

_____ Аліна МІХНОВА

«___» _____ 20__ р.

Розглянуто на засіданні Вченої Ради факультету ІРТЗІ
протокол № 1 від 16.01.2024 р.
декан факультету ІРТЗІ

_____ _ Сергій САКАЛО

Розглянуто на засіданні кафедри КРіСТЗІ
протокол № 4 від 11.01. 2024 р.
завідувач кафедри КРіСТЗІ

_____Іван АНТІПОВ

Представники роботодавців

Виконавчий директор ПрАТ «ІІТ» Володимир КРАВЧЕНКО_

Експерт відділу досліджень у сфері ІТ
ХНДЕКЦ МВС України Ігор НОСУЛЬКО

Представник студентського самоврядування
Голова студентського сенату факультету ІРТЗІ Катерина БУРЦЕВА

РОЗРОБЛЕНО
Проектна група:
керівник проектної групи:

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

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

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

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

Сєвєрінов Олександр Васильович, к.т.н.,
доц., доцент кафедри БІТ ХНУРЕ _____

ПЕРЕДМОВА

Розроблено проєктною групою у складі:

1. Руженцев Віктор Ігорович (керівник проектної групи)	– доктор технічних наук, доцент, професор кафедри БІТ факультету КІУ ХНУРЕ.
Члени проектної групи:	
2. Халімов Геннадій Зайдулович	– доктор технічних наук, професор, завідувач кафедри БІТ факультету КІУ ХНУРЕ;
3. Олейніков Анатолій Миколайович	– кандидат технічних наук, професор, професор кафедри КРіСТЗІ факультету ІРТЗІ ХНУРЕ;
4. Снігуров Аркадій Владиславович	– кандидат технічних наук, доцент, декан факультету ІК, доцент кафедри ІКІ факультету ІК ХНУРЕ;
5. Сєвєрінов Олександр Васильович	– кандидат технічних наук, доцент, доцент кафедри БІТ факультету КІУ ХНУРЕ.

Гарант освітньої програми
«Системи технічного захисту інформації,
автоматизація її обробки» спеціальності
125 Кібербезпека та захист інформації
другого (магістерського) рівня вищої освіти  Анатолій ОЛЕЙНІКОВ

1 Профіль освітньої програми « Системи технічного захисту інформації, автоматизація її обробки » за спеціальністю 125 Кібербезпека та захист інформації

1 - Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Харківський національний університет радіоелектроніки Факультет Інформаційних радіотехнологій та технічного захисту інформації Кафедра комп'ютерної радіоінженерії та систем технічного захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Магістр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Системи технічного захисту інформації, автоматизація її обробки
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 міс.
Наявність акредитації	Сертифікат про акредитацію спеціальності НД 21016833 від 24.07.2015. Строк дії сертифікату до 01.07.2025.
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра (або освітньо-кваліфікаційний рівень спеціаліста)
Мова(и) викладання	Українська, англійська для іноземних студентів
Термін дії освітньої програми	До повного завершення періоду навчання або наступного оновлення програми
Інтернет-адреса постійного розміщення опису освітньої програми	http://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-125-kiberbezpeka/osvitnja-programa-sistemi-tehnichnogo-zahistu-informacii
2 - Мета освітньої програми	
Мета освітньої програми полягає в оволодінні студентами знаннями, вміннями та навичками щодо впровадження та застосування технологій кібербезпеки та технічного захисту інформації; набуття компетентностей у використанні методів дослідження та проектування систем й комплексів забезпечення кібербезпеки.та технічного захисту інформації	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	12 Інформаційні технології 125 Кібербезпека та захист інформації **Об'єкти вивчення:** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології;

	– інфраструктура об’єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. **Цілі навчання:** Підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки та технічного захисту інформації. **Теоретичний зміст предметної області** Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки та технічного захисту інформації.. **Методи, методики та технології** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки та технічного захисту інформації.. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання**. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об’єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки та технічного захисту 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 та спеціалізації	Загальна вища освіта другого (магістерського) рівня в галузі інформаційної та кібербезпеки за спеціальністю «Кібербезпека та захист інформації» Освітньо професійна програма орієнтована на підготовку фахівців, здатних:

	- розв'язувати складні задачі і проблеми у галузі кібербезпеки та у сфері проведення спеціальних досліджень з виявлення технічних каналів витоку інформації, а також запобігання витоку, блокування та порушення цілісності інформації шляхом розробки, впровадження та супроводу комплексів технічного захисту інформації у складі комплексної системи захисту на об'єктах інформаційної діяльності. - проводити всебічний аналіз ефективності заходів з кібербезпеки та систем технічного захисту інформації, розробляти методи та засоби підвищення їх ефективності. Ключові слова: кібербезпека, технічні канали витоку інформації, технічний захист інформації, комплексні системи захисту.
Особливості програми	Програма передбачає вивчення: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – принципів розробки, впровадженню, супроводу комплексних систем захисту інформації; – методів та засобів оцінювання захищеності інформації; – методів та засобів технічного захисту інформації сучасних інформаційно-комунікаційних технологій. 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 – аналітик систем захисту інформації та оцінки вразливостей; 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, проектно-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).
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. КФ 11 Здатність виявляти та локалізувати джерела небезпечних сигналів в умовах обмеженості апріорних даних щодо їх фізичної природи і характеристик на фоні сильних завадових сигналів КФ 12 Здатність проводити комплексний аналіз ефективності технічних засобів, пристроїв та систем захисту інформації, розробляти методи підвищення їх ефективності

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. РН24 Вирішувати задачі розробки, впровадження та супроводу систем виявлення і протидії поширенню небезпечних сигналів різної фізичної природи. РН25 Проводити аналіз та обробку сигналів різної фізичної природи з використанням новітніх методів статистичного та спектрального аналізу.

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. Високий рівень практичної підготовки фахівців забезпечується наявністю спеціалізованих лабораторій: систем технічного захисту інформації, спеціальних досліджень у галузі технічного захисту інформації, систем охорони об'єктів, а також значним парком лабораторної і вимірювальної техніки: скануючі комп'ютерні радіоприймачі IC-PCR-100, IC-PCR-1000 (фірма ICOM, Японія), AOR-5001D, радіочастотовимірювач 3000A Plus (фірма Optoelectronics, США), лазерна система акустичної розвідки, апаратно-програмні комплекси «ОРТ», «Восток», маскувачі телефонних розмов та ін.
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 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 інформації.
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

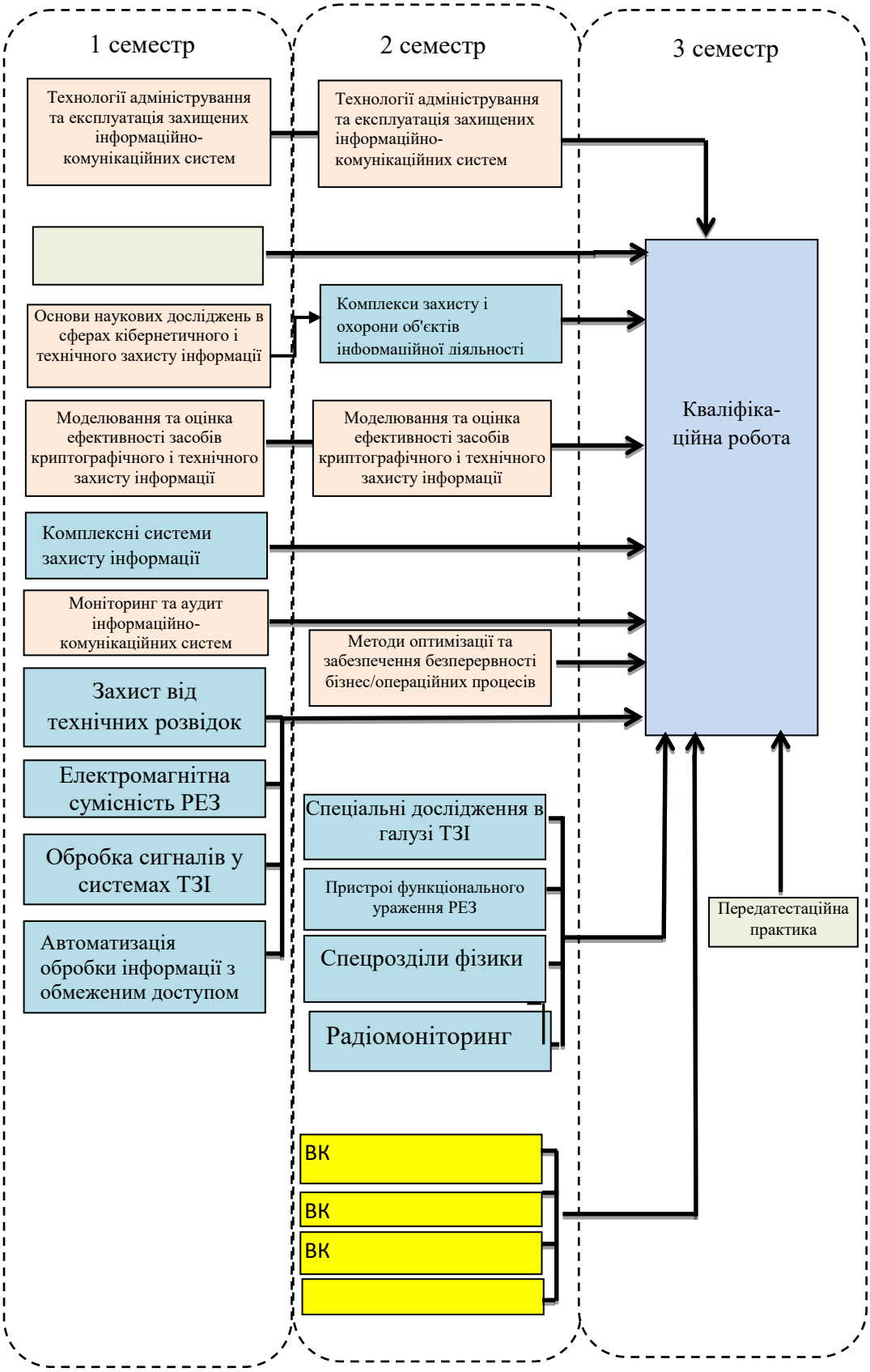
2.1. Перелік компонент ОП

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 (обов'язкові)			
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 «Системи технічного захисту інформації, автоматизація її обробки» (обов'язкові)			
ОК 6	Комплекси захисту і охорони об'єктів інформаційної діяльності	5	Екзамен
ОК 7	Комплексні системи захисту інформації	3	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			
		3	Залік
Загальний обсяг вибіркових компонентів за циклом		3	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
Дисципліни професійної та практичної підготовки за освітньою програмою «Системи технічного захисту інформації, автоматизація її обробки»			
ВК1	Захист від технічних розвідок	5	Залік
ВК 2	Радіомоніторинг	5	Залік
ВК 3	Спеціальні дослідження в галузі ТЗІ	5	Залік
ВК4	Автоматизація обробки інформації з обмеженим доступом	5	Залік
ВК5	Електромагнітна сумісність РЕЗ	5	Залік
ВК6	Обробка сигналів у системах ТЗІ	5	Залік
ВК7	Спецрозділи фізики	5	Залік
ВК8	Пристрої функціонального ураження РЕЗ	5	Залік
Загальний обсяг вибіркових компонентів за циклом		20	
Загальний обсяг вибіркових компонентів		23	
Загальний обсяг обов'язкових компонентів		67	

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
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

2.1 Структурно-логічна схема ОПП



3 Форма атестації здобувачів вищої освіти

Атестація здобувачів вищої освіти за освітньою програмою «Системи технічного захисту інформації, автоматизація її обробки» спеціальності 125 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

Компетентності	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6	ВК7	ВК8
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	+		+					+	+				+				
КФ -11								+	+	+	+	+		+			+
КФ -12								+	+	+	+	+		+			+

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

Результати навчання	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6	ВК7	ВК8
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								+	+	+					+		+

6. Матриця відповідності визначених Стандартом компетентностей дескрипторам НРК

Класифікація компетентностей (результатів навчання) за НРК	**Знання** **Зн1** Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та на межі галузей знань	**Уміння/Навички** **Ум1** Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур **Ум2** Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах **Ум3** Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	**Комунікація** **К1** Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	**Відповідальність і автономія** **АВ1** Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів **АВ2** Відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів **АВ3** Здатність продовжувати навчання з високим ступенем автономії
Загальні компетентності				
КЗ1	Зн1	Ум1, Ум3	К1	АВ1, АВ2
КЗ2	Зн1	Ум1, Ум2, Ум3		АВ2, АВ3
КЗ3	Зн1	Ум2, Ум3		АВ1
КЗ4	Зн1	Ум3		АВ1, АВ2
КЗ5	Зн1	Ум2	К1	АВ1
Спеціальні (фахові) компетентності				
КФ1	Зн1	Ум2		АВ2
КФ2	Зн1	Ум2		АВ2
КФ3	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
КФ4	Зн1	Ум1, Ум2	К1	АВ1, АВ2
КФ5	Зн1	Ум1, Ум2	К1	АВ1, АВ2
КФ6	Зн1	Ум1, Ум2	К1	АВ1
КФ7	Зн1	Ум1, Ум2	К1	АВ1
КФ8	Зн1	Ум1, Ум2	К1	АВ1
КФ9	Зн1	Ум1, Ум2	К1	АВ1
КФ10	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2

7. Матриця відповідності визначених Стандартом результатів навчання та компетентностей

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