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

галузі знань 12 Інформаційні технології

Кваліфікація: Магістр, Кібербезпека, Системи технічного захисту інформації, автоматизація її обробки

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ
Голова вченої ради
_____ / В.В. Семенець /
(протокол № 1 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 № 46 від "02" 02 2021 р.)
зі змінами
наказ № 173 від "03" 06 2021 р.

Харків 2021 р.

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми
«Системи технічного захисту інформації, автоматизація її обробки»
другого рівня вищої освіти
за спеціальністю 125 «Кібербезпека»

УЗГОДЖЕНО
Перший проректор

_____ І.В. Рубан

«06» 06 2021 р.

В.о. начальника відділу ЛА та ВСЗЯО
_____ С.Б. Макашев

«05» 05 2021 р.

Начальник навчального відділу
_____ А.В. Міхнова

«07» 05 2021 р.

Розглянуто на засіданні Вченої Ради
факультету ІРТЗІ
протокол № 3 від 30.03. 2021 р.
декан факультету ІРТЗІ
_____ С.М. Сакало

Розглянуто на засіданні кафедри КРіСТЗІ
протокол № 8 від 23.03 .2021р.
завідувач кафедри КРіСТЗІ
_____ І.Є. Антіпов

Представник роботодавця

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 Владіславович, 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

Голова студентського сенату факультету _____ О.О. Гончаренко

ПЕРЕДМОВА

Розроблено проектною групою у складі:

1. Руженцев Віктор Ігорович	– д-р техн. наук, доцент, професор кафедри Безпеки інформаційних технологій Харківського національного університету радіоелектроніки
2. Халімов Геннадій Зайдулович	– д-р техн. наук, професор, зав. кафедри Безпеки інформаційних технологій Харківського національного університету радіоелектроніки
2. Олейніков Анатолій Миколайович	– канд. техн. наук, професор, професор кафедри Комп'ютерної радіоінженерії та систем технічного захисту інформації Харківського національного університету радіоелектроніки
3. Снігуров Аркадій Владиславович	– канд. техн. наук, доцент, декан факультету Інфокомунікацій, доцент кафедри Інфокомунікаційної інженерії ім.В.В. Поповського Харківського національного університету радіоелектроніки
4. Сєвєрінов Олександр Васильович	– канд. техн. наук, доцент, доцент кафедри Безпеки інформаційних технологій Харківського національного університету радіоелектроніки

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

1 – Загальна інформація	
Повна назва вищого навчального закладу 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, Кібербезпека, Системи технічного захисту інформації, автоматизація її обробки
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 місяці
Наявність акредитації	Сертифікат про акредитацію спеціальності МОН України НД №2190672 від 02.10.2017 року Строк дії сертифіката до 01.07.2025 року
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 мова
Термін дії освітньої програми	До повного завершення періоду навчання або наступного оновлення програми
Інтернет-адреса постійного розміщення опису освітньої програми	http://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-125-kiberbezpeka/osvitnja-programa-sistemi-tehnichnogo-zahistu-informacii
2 – Мета освітньої програми	
Мета освітньої програми полягає в оволодінні студентами знаннями, вміннями та навичками використовувати і впроваджувати технології інформаційної та/або кібербезпеки; набуття компетентностей у використанні методів дослідження і проектування систем та комплексів забезпечення інформаційної та кібербезпеки.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність,)	12 Інформаційні технології, 125 Кібербезпека
Орієнтація освіт-ньої програми	Освітньо-професійна програма Акцентована на розвиток здатності розв'язувати складні задачі і проблеми у галузі професійної діяльності, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог
Основний фокус освітньої програми та спеціалізації	Загальна вища освіта другого (магістерського) рівня в галузі інформаційної та кібербезпеки за спеціальністю Кібербезпека Ключові слова: кібербезпека, технічний захист інформації, захист від несанкціонованого доступу
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; – методів та засобів оцінювання захищеності інформації; – методів та засобів технічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; автоматизованих систем проектування. Підготовка висококваліфікованих фахівців на високому методичному та професійному рівні.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Назви професій згідно Національного класифікатора України: Класифікатор професій (ДК 003:2010) 2149.2 Професіонал із організації захисту інформації з обмеженим доступом 2149.2 Професіонал із організації інформаційної безпеки
Подальше навчання	Можливість навчання за програмою третього (освітньо-наукового) рівня вищої освіти. . Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Лекції, практичні заняття, виконання курсової роботи, лабораторні роботи, самостійна робота на основі підручників, навчальних посібників та конспектів лекцій, консультації з викладачами, науково-дослідна практика, 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 особи розв’язувати складні задачі і проблеми у 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 (ЗК)	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 (ФК)	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 вимогитехнічного 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 – Програмні результати навчання	
	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 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. 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 бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді. 2. Наявність доступу до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. 3. Наявність офіційного веб-сайту закладу освіти, на якому розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня/освітньо-наукова/ видавнича/ атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація). 4. Наявність електронного ресурсу закладу освіти, який містить навчально-методичні матеріали з дисциплін навчального плану, в тому числі в системі дистанційного навчання.
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

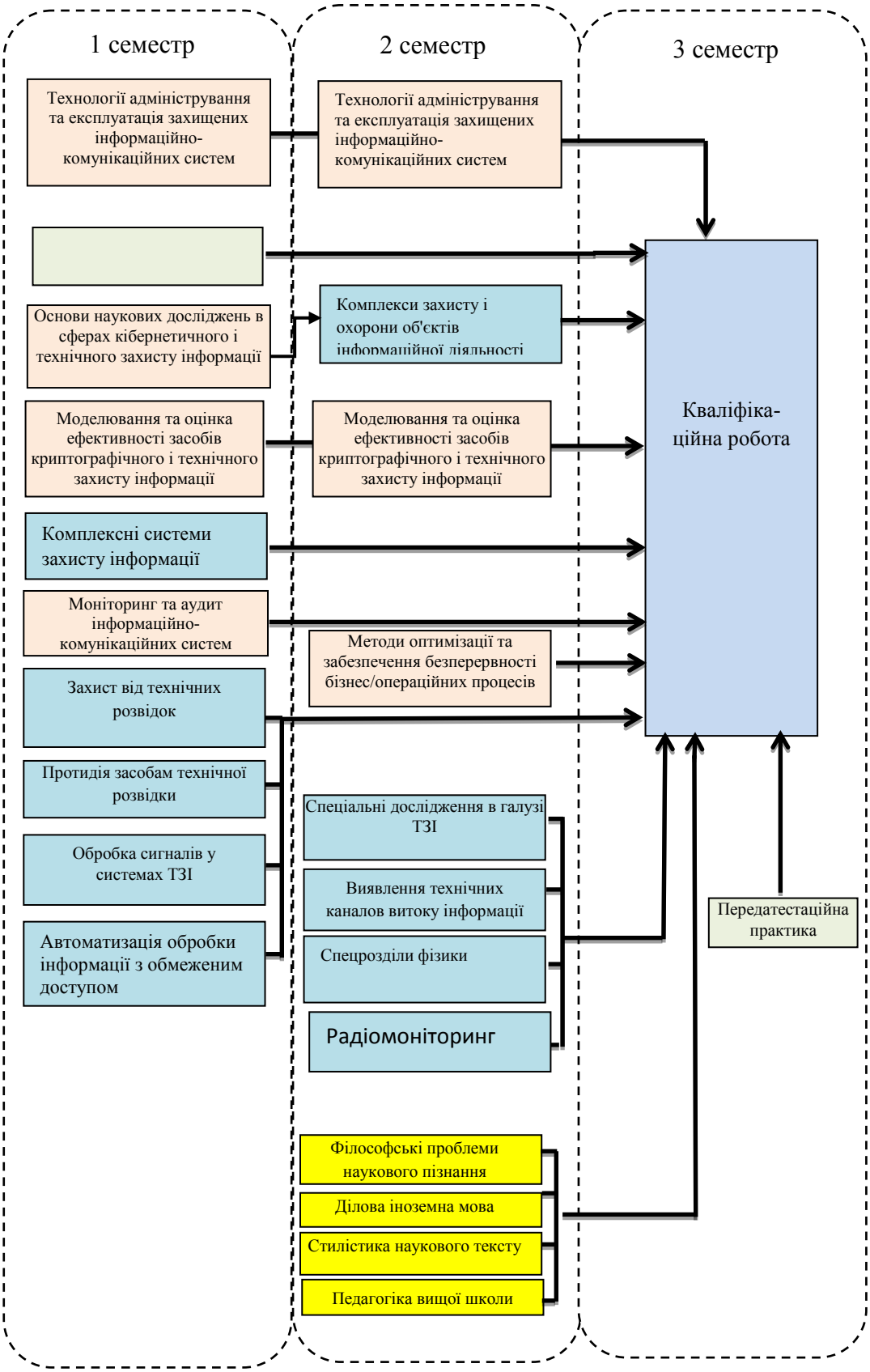
2.1. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОП			
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Гуманітарні та соціально-економічні дисципліни (обов'язкові)			
ОК * 1.1	Українська мова як іноземна	3	Зл
Дисципліни базової (професійної) підготовки за спеціальністю			
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 та 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**	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
Дисципліни професійної та практичної підготовки за освітньою програмою Системи технічного захисту інформації, автоматизація її обробки за профілем випускової кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації			
ОК 2.1	Комплекси захисту і охорони об'єктів інформаційної діяльності	4,5	Ек
ОК 2.2	Комплексні системи захисту інформації	3,5	Ек
ОК 2.3	Передатестаційна практика	15	Зл
ОК 2.4	Кваліфікаційна робота	15	Ек
Всього:		**38**	
Загальний обсяг обов'язкових компонент:		**67**	
Вибіркові компоненти ОП			
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Гуманітарні та соціально-економічні дисципліни			
ВБ 1.1	Ділова іноземна мова	3	Зл
ВБ 1.2	Філософські проблеми наукового пізнання	3	Зл
ВБ 1.3	Педагогіка вищої школи	3	Зл
ВБ 1.4	Стилістика наукового тексту	3	Зл
Всього		**3**	
Дисципліни професійної та практичної підготовки за освітньою програмою Системи технічного захисту інформації, автоматизація її обробки			
ВБ 2.1	Захист від технічних розвідок	5	Зл
ВБ 2.2	Протидія засобам технічної розвідки	5	Зл

ВБ 2.3	Обробка сигналів у системах ТЗІ	5	Зл
ВБ 2.4	Автоматизація обробки інформації з обмеженим доступом	5	Зл
ВБ 2.5	Спеціальні дослідження в галузі ТЗІ	5	Зл
ВБ 2.6	Виявлення технічних каналов витоку інформації	5	Зл
ВБ 2.7	Спецрозділи фізики	5	Зл
ВБ 2.8	Радіомоніторинг	5	Зл
Всього		**20**	
Загальний обсяг вибіркових компонент:		**23**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**90**	

* – для іноземних здобувачів вищої освіти;

2.2 Структурно-логічна схема ОПП



3 Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Системи технічного захисту інформації, автоматизація її обробки» спеціальності 125 Кібербезпека здійснюється в формі публічного захисту кваліфікаційної роботи.

Кваліфікаційна робота має передбачати розв'язання наукової або науково-технічної задачі у галузі інформаційної безпеки та/або кібербезпеки, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.

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 освітньої кваліфікації – Магістр, Кібербезпека, Системи технічного захисту інформації, автоматизація її обробки.

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 ІРТЗІ.

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

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 ІРТЗІ.

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

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				+	+	+	+		+	+					+	+			+	+			

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
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					+	+	+	+	+	+				+				+		+		+	