МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації»

першого рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: Бакалавр, Кібербезпека, Системи технічного захисту інформації

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ

Голова вченої ради

_____ / В.В. Семенець /

(протокол № 4 від "29" 04 2019 р.)

зі змінами

(протокол № 1 від "28" січня 2021 р.)

Освітня програма вводиться в дію з 01.09.2019 р.

Ректор_____ / В.В. Семенець /

(наказ № 178 від "03" 04 2019 р.)

зі змінами

(наказ № 46 від "02" 02 2021 р.)

Харків 2021 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«Системи технічного захисту інформації»»
першого рівня вищої освіти
за спеціальністю 125 Кібербезпека

УЗГОДЖЕНО

Перший проректор
_____ І.В. Рубан
«26» 01 2021 р.

В.о. начальника відділу ЛА та ВСЗЯО
_____ С.Б. Макашев
«26» 01 2021 р.

Начальник навчального відділу
_____ А.В. Міхнова
«25» 01 2021 р.

Розглянуто на засіданні Вченої ради
факультету ІРТЗІ
Протокол № 1 від 22.01.2021 р.
Декан факультету ІРТЗІ
_____ С.М. Сакало

Розглянуто на засіданні кафедри КРіСТЗІ
Протокол№ 6 від 19.01.2021 р.
Завідувач кафедри КРіСТЗІ
_____ І.Є. Антіпов

Представники роботодавців
Виконавчий директор ПрАТ «ІІТ» _____ В.Д. Кравченко_

РОЗРОБЛЕНО

Проектна група:

керівник проектної групи:

Гріненко Тетяна Олексіївна, к.т.н., доц.,
доц. кафедри БІТ, ХНУРЕ _____ Т.О. Гріненко_

члени проектної групи:

Ликов Юрій Володимирович, к.т.н., доц.,
доцент каф. КРіСТЗІ, ХНУРЕ _____ Ю.В. Ликов___

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

Ляшенко Олексій Сергійович, к.т.н., доц.,
доц. каф. ЕОМ, декан факультету КІУ, ХНУРЕ _____ О.С. Ляшенко

Представник студентського самоврядування
Голова студентського сенату факультету ІРТЗІ _____ О.О.Гончаренко

ПЕРЕДМОВА

Розроблено проектною групою у складі:

1. Гріненко Тетяна Олексіївна (керівник проектної групи) - кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки

2. Ликов Юрій Володимирович - кандидат технічних наук, доцент, доцент 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. Ляшенко Олексій Сергійович - кандидат технічних наук, доцент, декан факультету комп'ютерної інженерії та управління, доцент кафедри електронних обчислювальних машин Харківського національного університету радіоелектроніки

ЗМІСТ

1. ПЕРЕДМОВА

Розроблено робочою групою представників кафедр:

Безпеки інформаційних технологій (БІТ) факультету комп'ютерної інженерії та управління (КІУ),

Комп'ютерної радіоінженерії та систем технічного захисту інформації (КРіСТЗІ) факультету інформаційних радіотехнологій та технічного захисту інформації (ІРТЗІ),

Інфокомунікаційної інженерії (ІКІ) факультету інфокомунікацій (ІК)

ПРОЕКТНА ГРУПА

Голова проектної групи:

ГРІНЕНКО Тетяна Олексіївна, к.т.н., доц., доц. каф. БІТ, ХНУРЕ

Члени проектної групи:

ЛИКОВ Юрій Володимирович	к.т.н., доц.,	проф. каф. КРіСТЗІ, ХНУРЕ
СНІГУРОВ Аркадій Владиславович	к.т.н., доц.,	декан факультету інфокомунікацій (ІК) доц. каф. ІКІ, ХНУРЕ
ЗАБОЛОТНИЙ Володимир Ілліч	к.т.н., доц.,	проф. каф. БІТ, ХНУРЕ

1. Профіль освітньої програми «Системи технічного захисту інформації» освітньо-професійної програми 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	бакалавр Бакалавр, Кібербезпека, Системи технічного захисту інформації
Офіційна назва освітньої програми	Системи технічного захисту інформації
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Повна загальна середня освіта (або освітньо-кваліфікаційний рівень молодшого 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/bakalavr-125-kiberbezpeka/osvitnja-programa-sistemi-tehnichnogo-zahistu-informacii
2- Мета освітньої програми	
Забезпечити підготовку висококваліфікованих фахівців в галузі інформаційних технологій зі спеціальності 125 «Кібербезпека», здатних вирішувати складні спеціалізовані задачі та практичні проблеми інформаційної безпеки, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу.	
3 – Характеристика освітньої програми	
Предметна область(галузь знань, спеціальність, спеціалізація)	12 «Інформаційні технології» 125 «Кібербезпека»
Орієнтація освітньої програми	Освітньо-професійна програма прикладної орієнтації. 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	Загальна спеціальна освіта в галузі інформаційної та кібербезпеки за спеціальністю «Кібербезпека».

та спеціалізації	Акцент на здатності організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації.
Особливості освітньої програми	Інтеграція програмно-апаратних засобів виявлення, моніторингу та забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі. Програма передбачає вивчення: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – методів та засобів виявлення та локалізації каналів витоку інформації; – методів та засобів виявлення закладних пристроїв; – методів та засобів оцінювання захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – автоматизованих систем проектування.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до праце-влаштування	Назви професій згідно Національного класифікатора України: Класифікатор професій (ДК 003:2010) 3439 Фахівець з режиму секретності 3439 Фахівець із організації захисту інформації з обмеженим доступом 3439 Фахівець із організації інформаційної безпеки
Подальше навчання	Можливість навчання за програмою другого (магістерського) рівня вищої 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 розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
	ЗК 2. Знання та розуміння предметної області та розуміння професії.
	ЗК 3. Здатність спілкуватися рідною та другою іноземною мовою як усно, так і письмово
	ЗК 4. Здатність здійснювати професійну діяльність згідно з вимогами санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки
	ЗК 5. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням

	ЗК 6. Здатність до пошуку, оброблення та аналізу інформації.
	ЗК 7. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні;
	ЗК 8.Прагнення до збереження навколишнього середовища
	ЗК 9. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя
	ЗК 10. Здатність вчитися і бути сучасно навченим.
	ЗК 11. Здатність приймати обґрунтовані рішення.
	ЗК 12. Здатність до адаптації та дії в новій ситуації.
	ЗК 13. Дотримання та пропагування здорового способу життя.
	ЗК 14. Здатність бути критичним та самокритичним
Фахові компетентності спеціальності (ФК)	ФК 1. Здатність застосовувати законодавчу та нормативноправову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
	ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.
	ФК 3. Здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки
	ФК 4. Здатність до використання програмних, апаратних та програмно-апаратних комплексів засобів захисту інформації на об'єктах інформаційної діяльності.
	ФК 5. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки
	ФК 6. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
	ФК 7. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
	ФК 8. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною 8 та/або кібербезпекою.
	ФК 9. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
	ФК 10. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
	ФК 11. Здатність застосовувати методи та засоби криптографічного та стеганографічного захисту інформації на об'єктах інформаційної діяльності.
	ФК 12. Здатність виявляти та блокувати канали витоку інформації, методи несанкціонованого доступу до інформації, джерел і

	способів дестабілізуючого впливу на інформацію, здійснювати пошук закладних пристроїв.
	ФК 13. Здатність оцінювати та визначати фізичні процеси, які висвітлюють характеристики та параметри напівпровідникових активних елементів, а також проводити лінійний та нелінійний аналіз електричних схем, схемотехніки різноманітних підсилювальних каскадів, операційних підсилювачів та елементів логіки.
	ФК 14. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
	ФК 15. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
7 - Програмні результати навчання	
Програмні результати навчання, визначені стандартом вищої освіти	
Загальні результати навчання	
	ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
	ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
	ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
	ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
	ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
	ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
	ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
	ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
	ПРН 9 Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
	ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
	ПРН 11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах;
Фахові результати навчання	
	ФР 1 Розробляти моделі загроз та порушника; ФР 2. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
	ФР 3. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-

	апаратними засобами та давати оцінку результативності якості прийнятих рішень; ФР 4. Здатність застосування систем виявлення та протидії несанкціонованим вторгненням на об'єкти інформаційної діяльності, використання засобів пошуку каналів витоку інформації та закладних пристроїв. ФР 5. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; ФР 6. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
	ФР 7. Забезпечувати процеси захисту та функціонування інформаційнотелекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; ФР 8. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; ФР 9. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; ФР 10. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; ФР 11. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах; ФР 12. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційнотелекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
	ФР 13. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
	ФР 14. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); ФР 15. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;
	ФР 16. Здатність продемонструвати знання та розуміння основ схемотехніки та описати в загальних поняттях і термінах принципи дії, основні характеристики, параметри і особливості застосування електронних напівпровідникових приладів та інтегральних схем, підсилювальних каскадів, операційних підсилювачів та елементів логіки що використовуються в обчислювальній техніці, автоматичних пристроях, комп'ютерних системах та мережах.
	ФР 17. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; ФР 18. Вирішувати задачі захисту потоків даних в інформаційних,

	інформаційно-телекомунікаційних (автоматизованих) системах; ФР 19. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; ФР 20. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; ФР 21. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; ФР 22. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; ФР 23. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
	ФР 24. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; ФР 25. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; ФР 26. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; ФР 27. Виявляти небезпечні сигнали технічних засобів; ФР 28. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; ФР 29. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; ФР 30. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; ФР 31. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; ФР 32. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; ФР 33. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; ФР 34. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; ФР 35. Здатність продемонструвати знання та розуміння захисту інформації на об’єктах інформаційної діяльності та обґрунтовано обирати і застосовувати на практиці методи виявлення інформаційних загроз; програмні та програмно-апаратні засоби захисту інформації; методи протидії спробам несанкціонованого доступу до інформаційних ресурсів; організаційні та

	адміністративні заходи підвищення рівня інформаційної та/або кібербезпеки. ФР 36. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; ФР 37. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; ФР 38. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; ФР 39. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; ФР 40. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; ФР 41. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; ФР 42. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); ФР 43. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; ФР 44. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; ФР 45. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. ФР 46. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
Програмні результати навчання, визначені навчальним закладом	
	ПРЗ 1. Застосовувати національні та міжнародні стандарти для розробки систем захисту інформації; ПРЗ 2. Приймати участь у розробці, моделюванні та досліджені методів захисту даних в сучасних інформаційних системах; ПРЗ 3. Здійснювати оцінку захищеності новітніх інформаційних систем.
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.
Інформаційне та навчально-	1. Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді.

методичне забезпечення	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 компонентів освітньо-професійної програми та їх логічна послідовність наведена в навчальному плані

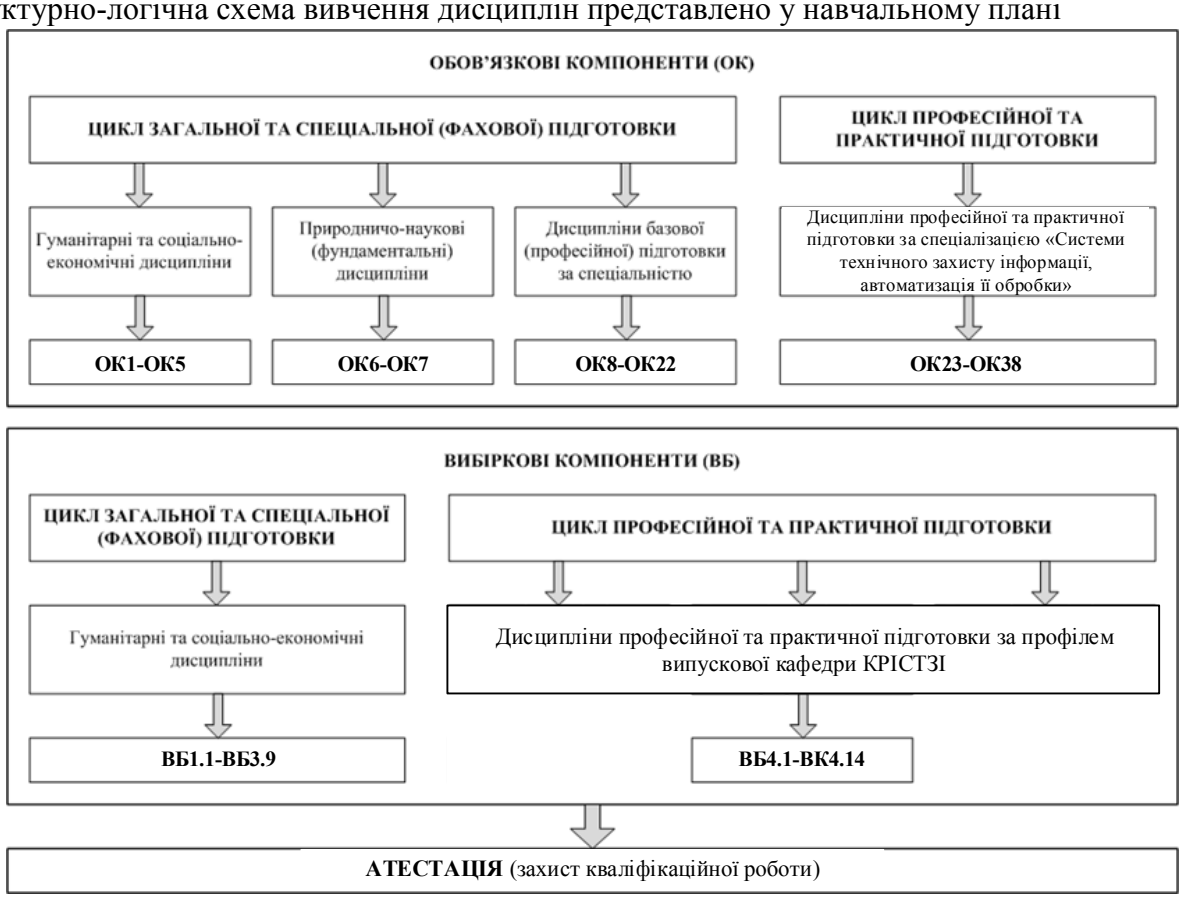
2.1. Перелік компонентів ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проекти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
Обов'язкові компоненти ОП			
Гуманітарні та соціально-економічні дисципліни			
ОК 1.	Українське фахове мовлення	4	залік
ОК 2.	Філософія	4	екзамен
ОК 3.	Іноземна мова	8	екзамен
ОК 4.	Основи права	2	залік
ОК 5.	Фізичне виховання (за рахунок вільного часу студентів)	0	залік
Природничо-наукові (фундаментальні) дисципліни			
ОК 6.	Вища математика	12	екзамен
ОК 7.	Фізика	6	екзамен
Дисципліни базової (професійної) підготовки за спеціальністю			
ОК 8.	Введення в спеціальність	4	залік
ОК 9.	Інформаційні технології	4	залік
ОК 10.	Вища математика (спец. розділи)	4	залік
ОК 11.	Архітектура КС	4	екзамен
ОК 12.	Схемотехніка	4	залік
ОК 13.	Основи теорії кіл	4	екзамен
ОК 14.	Електрорадіовимірювання	4	залік
ОК 15.	Програмування	18	екзамен
ОК 16.	Безпека життєдіяльності	3	залік
ОК 17.	Економіка та бізнес	3	залік
ОК 18.	Нормативно-правове забезпечення	4	залік
ОК 19.	Стеганографія	4	залік
ОК 20.	Виробнича практика	4,5	залік
ОК 21.	Передатестаційна практика	4,5	залік
ОК 22.	Кваліфікаційна робота	9	екзамен
Дисципліни професійної та практичної підготовки			
ОК 23.	Сигнали та процеси в ТЗІ	8	екзамен
ОК 24.	Основи теорії кіл в ТЗІ	5	екзамен
ОК 25.	Поля і хвилі в системах ТЗІ	6	екзамен
ОК 26.	Теорія інформації та кодування	4	екзамен
ОК 27.	Схемотехніка пристроїв ТЗІ 2	7	екзамен
ОК 28.	Методи та засоби захисту інф. 1	5	екзамен
ОК 29.	Методи та засоби захисту інф. 2	7	екзамен
ОК 30.	Технічні засоби охорони обєктів	4	залік
ОК 31.	Основи інформаційної безпеки	3	екзамен
ОК 32.	Організаційне забезпечення ТЗІ	4	екзамен
ОК 33.	Проектування систем захисту інф.	5	екзамен
ОК 34.	Проектування пристроїв на МК і ПЛІС. Моделюв. ЦС засобами MATLAB і VDHL	2	залік
ОК 35.	Проектування пристроїв на МК і ПЛІС. МК.	4	залік
ОК 36.	Проектування пристроїв на МК і ПЛІС. ПЛІС.	4	залік
ОК 37.	Комплексний курсовий проект	3	залік
ОК 38.	Електромагнітна сумісність СТЗІ	3,5	екзамен
	Загальний обсяг обов'язкових компонент	188,5	

Вибіркові компоненти ОП			
Гуманітарні та соціально-економічні дисципліни			
Вибірковий блок 1			
ВБ 1.1	Психологія сприйняття та переробки інформації	3	залік
ВБ 1.2	Психологія екстремальних стосунків та ефективної адаптації	3	залік
ВБ 1.3	Соціальна психологія та конфліктологія	3	залік
ВБ 1.4	Психологія управління	3	залік
ВБ 1.5	Стилістика наукового тексту	3	залік
ВБ 1.6	Україна-Європейський Союз: порівняльна характеристика ідентичності	3	залік
ВБ 1.7	Демократія: від теорії до практики	3	залік
Вибірковий блок 2			
ВБ 2.1	Логіка	3	залік
ВБ 2.2	Політичні проблеми сучасного суспільства	3	залік
ВБ 2.3	Історія науки і техніки	3	залік
ВБ 2.4	Етичні проблеми сучасного суспільства	3	залік
ВБ 2.5	Імідж сучасного спеціаліста	3	залік
ВБ 2.6	Історія української культури в контексті світової	3	залік
ВБ 2.7	Безпека праці в ІТ індустрії	3	залік
Вибірковий блок 3			
ВБ 3.1	Інформаційне суспільство	3	залік
ВБ 3.2	Соціологія та соціальні технології	3	залік
ВБ 3.3	Глобальні проблеми сучасності	3	залік
ВБ 3.4	Правові основи професійної діяльності	3	залік
ВБ 3.5	Soft scills: соціально-психологічні аспекти професійної компетентності	3	залік
ВБ 3.6	Ґендерні проблеми сучасного суспільства	3	залік
ВБ 3.7	Організація керування умовами праці	3	залік
ВБ 3.8	Екологічна безпека життєдіяльності	3	залік
ВБ 3.9	Іноземна мова для професійної комунікації	6	залік
Дисципліни професійної та практичної підготовки за спеціалізацією			
ВБ 4.1	Теоретичні основи спец. вимірювань	4	екзамен
ВБ 4.2	Системи передавання відеозображення	3	залік
ВБ 4.3	Засоби прийому та обробки інформації в СТЗІ	4	залік
ВБ 4.4	Радіопротидія	4	екзамен
ВБ 4.5	Методи адаптації в СТЗІ	3	залік
ВБ 4.6	Антенни в системах ТЗІ	4	залік
ВБ 4.7	Управління інформаційною безпекою	4	залік
ВБ 4.8	Безпека інф. та комунікаційних систем	4	залік
ВБ 4.9	Засоби передавання інф. в СТЗІ	3,5	залік
ВБ 4.10	Системи банківської безпеки	4	залік
ВБ 4.11	Засоби ТЗІ. мікрохвил.та опт.діапазонів	4	екзамен
ВБ 4.12	Мережі та системи радіодоступу	4	екзамен
ВБ 4.13	Радіомаскування	3	залік
ВБ 4.14	Біометричні технології контролю доступу	3	залік
	Загальний обсяг вибіркових компонент	51,5	
	ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ	240	

2.2. Структурно-логічна схема ОП

Структурно-логічна схема вивчення дисциплін представлено у навчальному плані



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Системи технічного захисту інформації» спеціальності 125 Кібербезпека проводиться у формі захисту кваліфікаційноїх роботи та завершується видачею документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації: Бакалавр, Кібербезпека, Системи технічного захисту інформації.

Атестація здійснюється відкрито і публічно.

4 Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37	ОК38
ЗК1	√	√	√	√	√	√			√		√	√	√	√	√	√	√	√	√		√		√	√	√	√	√	√	√	√	√	√	√				√	
ЗК2	√	√	√	√	√		√	√		√	√	√	√	√			√	√		√			√		√	√		√	√	√	√						√	
ЗК3	√	√	√	√													√	√																				
ЗК4																√																						
ЗК5		√																																			
ЗК6		√							√																												
ЗК7		√		√																																	
ЗК8																√																					
ЗК9					√											√																					
ЗК10		√					√																														
ЗК11		√				√																															
ЗК12		√				√																															
ЗК13					√											√																					
ЗК14		√																																			
ФК1				√				√										√			√	√									√	√					
ФК2									√												√	√				√											
ФК3													√								√	√	√	√			√	√	√	√	√		√				√	
ФК4															√						√	√						√	√	√				√	√	√	√	
ФК5																					√	√									√	√					√	
ФК6																					√	√									√	√					√	
ФК7														√							√	√						√	√	√	√	√						√
ФК8																				√	√	√										√					√	
ФК9																					√	√										√					√	
ФК10																					√	√										√					√	
ФК11																			√		√	√				√												
ФК12																				√	√	√						√	√	√							√	
ФК13							√					√	√								√	√	√	√			√						√					
ФК14																					√	√										√						
ФК15																					√	√											√					

Матриця відповідності програмних компетентностей компонентам освітньої програми (продовження)

	ВБ1.1	ВБ1.2	ВБ1.3	ВБ1.4	ВБ1.5	ВБ1.6	ВБ1.7	ВБ2.1	ВБ2.2	ВБ2.3	ВБ2.4	ВБ2.5	ВБ2.6	ВБ2.7	ВБ3.1	ВБ3.2	ВБ3.3	ВБ3.4	ВБ3.5	ВБ3.6	ВБ3.7	ВБ3.8	ВБ3.9	ВБ4.1	ВБ4.2	ВБ4.3	ВБ4.4	ВБ4.5	ВБ4.6	ВБ4.7	ВБ4.8	ВБ4.9	ВБ4.10	ВБ4.11	ВБ4.12	ВБ4.13	ВБ4.14
ЗК1	√		√		√	√						√	√	√	√	√	√	√	√	√				√	√	√	√	√		√							
ЗК2	√	√	√					√	√		√	√	√	√	√			√	√		√			√		√	√			√							
ЗК3	√	√	√		√	√				√	√	√	√	√	√	√	√	√	√	√	√	√														
ЗК4														√							√	√															
ЗК5	√	√	√	√	√			√							√						√		√														
ЗК6	√														√																						
ЗК7							√		√		√		√				√	√		√																	
ЗК8														√								√															
ЗК9														√								√															
ЗК10	√							√													√																
ЗК11	√							√													√																
ЗК12	√	√	√	√				√													√																
ЗК13														√							√	√															
ЗК14	√																																				
ФК1																																					
ФК2																														√				√			
ФК3																										√							√				√
ФК4																														√	√						
ФК5																													√								
ФК6																													√	√	√				√		
ФК7																									√										√	√	
ФК8																													√	√		√					
ФК9																													√	√		√					
ФК10																													√	√		√					
ФК11																														√				√			
ФК12																										√							√				√
ФК13																												√									
ФК14																																					
ФК15																													√	√		√					

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

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37	ОК38
ПР1	√		√																	√	√	√																
ПР 2						√														√	√	√																
ПР 3						√														√	√	√																
ПР 4						√	√													√	√	√																
ПР 5																				√	√	√																
ПР 6		√																		√	√	√																
ПР 7				√														√		√	√	√									√	√						
ПР 8																		√		√	√	√									√							
ПР 9																		√		√	√	√									√							
ПР10																				√	√	√				√							√					
ПР11									√	√										√	√	√																
ФР1								√												√	√	√						√			√	√						
ФР2											√									√	√	√																
ФР3																				√	√	√										√						
ФР4																				√	√	√						√	√	√		√					√	
ФР5									√						√				√	√	√	√				√												
ФР6																		√		√	√	√							√			√					√	
ФР7											√								√	√	√	√				√												
ФР8									√					√					√	√	√	√				√												
ФР9									√					√					√	√	√	√				√		√	√									
ФР10									√					√					√	√	√	√				√												
ФР11																				√	√	√								√		√	√					
ФР12																				√	√	√								√								
ФР13											√								√	√	√	√							√			√					√	
ФР14																				√	√	√																
ФР15																				√	√	√																
ФР16												√	√							√	√	√	√	√			√						√	√	√	√	√	
ФР17																				√	√	√									√							
ФР18											√									√	√	√									√							

ФР19																			√	√	√						√	√			√							
ФР20																			√	√	√										√							
ФР21																			√	√	√									√	√							
ФР22																			√	√	√						√	√									√	
ФР23																			√	√	√																	
ФР24																√			√	√	√																	
ФР25																			√	√	√									√	√							
ФР26																			√	√	√										√							
ФР27													√						√	√	√			√			√	√										√
ФР28													√						√	√	√			√			√	√										√
ФР29													√						√	√	√																	
ФР30																			√	√	√									√	√							
ФР31													√						√	√	√						√	√										
ФР32																			√	√	√																	
ФР33																			√	√	√																	
ФР34																	√		√	√	√									√	√							
ФР35																		√	√	√	√	√					√	√	√	√	√	√	√				√	
ФР36																√	√		√	√	√																	
ФР37																			√	√	√																	
ФР38																			√	√	√																	
ФР39																		√	√	√	√															√		
ФР40																		√	√	√	√															√		
ФР41																			√	√	√									√	√							
ФР42								√						√					√	√	√			√														
ФР43																			√	√	√																	
ФР44																			√	√	√																	
ФР45														√				√	√	√	√			√														
ФР46				√															√	√	√																	
ПР31																	√		√	√	√																	
ПР32																			√	√	√					√	√	√										
ПР33																			√	√	√							√		√	√							

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

	ВБ1.1	ВБ1.2	ВБ1.3	ВБ1.4	ВБ1.5	ВБ1.6	ВБ1.7	ВБ2.1	ВБ2.2	ВБ2.3	ВБ2.4	ВБ2.5	ВБ2.6	ВБ2.7	ВБ3.1	ВБ3.2	ВБ3.3	ВБ3.4	ВБ3.5	ВБ3.6	ВБ3.7	ВБ3.8	ВБ3.9	ВБ4.1	ВБ4.2	ВБ4.3	ВБ4.4	ВБ4.5	ВБ4.6	ВБ4.7	ВБ4.8	ВБ4.9	ВБ4.10	ВБ4.11	ВБ4.12	ВБ4.13	ВБ4.14
ПР 1					√	√																	√													
ПР 2							√	√								√																				
ПР 3	√		√	√				√					√		√		√		√	√		√														
ПР 4								√						√							√																
ПР 5	√	√							√	√	√	√							√																	
ПР 6	√	√																	√																	
ПР 7																		√																		
ПР 8																																				
ПР 9																													√							
ПР10																								√						√		√		√		
ПР11																														√		√		√		
ФР1																													√							
ФР2																								√	√					√	√	√		√		
ФР3																													√	√						
ФР4																							√			√									√	
ФР5																													√	√						
ФР6																													√	√						
ФР7																									√					√	√			√		
ФР8																													√	√						
ФР9																													√	√						
ФР10																													√	√						
ФР11																													√							
ФР12																																				√
ФР13																									√					√	√			√		
ФР14																													√					√		√
ФР15																													√					√		√
ФР16																																				
ФР17																																				

ФР18																																					
ФР19																														√	√						
ФР20																														√	√		√				
ФР21																							√							√	√						
ФР22																															√		√				
ФР23																														√							
ФР24																														√							
ФР25																														√							
ФР26																														√							
ФР27																							√						√								
ФР28																							√						√								
ФР29																							√														
ФР30																																					
ФР31																							√														
ФР32																														√							
ФР33																														√							
ФР34																														√							
ФР35																							√			√	√				√			√		√	
ФР36																														√							
ФР37																														√							
ФР38																														√							
ФР39																																					
ФР240																																					
ФР41																														√							
ФР42																																					√
ФР43																																					√
ФР44																															√						
ФР45																																					
ФР46						√			√										√																		
ПР31																																					
ПР32																																					
ПР33																														√	√		√				

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Реєстр суб'єктів освітньої діяльності України. Харківський національний університет радіоелектроніки. Ліцензовані спеціальності. // [Електронний ресурс]. – Режим доступу: https://www.inforesurs.gov.ua/reestr/?id=92.

2. Закон «Про вищу освіту» // [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1556 – 18.

3. Проект Європейської Комісії «Гармонізація освітніх структур в Європі» (TuningEducationalStructuresinEurope, TUNING). TUNING (для ознайомлення зі спеціальними (фаховими) компетентностями та прикладами стандартів // [Електронний ресурс]. – Режим доступу: http://www.unideusto.org/tuningeu/.

4. Постанова КМУ «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29 квітня 2015 р. №266 // [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/266- 2015-п.

5. Наказ МОН України «Про особливості запровадження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 06.11.2015 №1151. // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z1460 -15.

6. Національний глосарій 2014 // [Електронний ресурс]. – Режим доступу: http://ihed.org.ua/images/biblioteka/glossariy_Visha_osvita_2014_tempusoffice.pdf .

7. Національний класифікатор України: «Класифікатор професій» ДК 003:2010 // Видавництво «Соцінформ», – К.: 2010.