МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря Сікорського»

ЗАТВЕРДЖЕНО
Вченою радою
КПІ ім. Ігоря Сікорського
(протокол № 6 від 29.06 2021 р.)
Голова Вченої ради
_____ Михайло ІЛЬЧЕНКО

СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

SYSTEMS OF TECHNICAL PROTECTION OF INFORMATION

ОСВІТНЬО-НАУКОВА ПРОГРАМА

другого (магістерського) рівня вищої освіти

за спеціальністю	**125 Кібербезпека**
галузі знань	**12 Інформаційні технології**
кваліфікація	**Магістр з кібербезпеки**

Введено в дію з 2021/2022 навч. року
наказом ректора
КПІ ім. Ігоря Сікорського
від 13.07 2021 р. № МОН/194/2021

Київ – 2021

ПРЕАМБУЛА

РОЗРОБЛЕНО проєктною групою:

Керівник проєктної групи:
Новіков Олексій Миколайович,
директор Фізико-технічного інституту, д.т.н., професор

Члени проєктної групи:
Мачуський Євген Андрійович,
В.о. завідувача кафедри фізико-технічних засобів
захисту інформації, д.т.н., професор

Земляк Олександр Михайлович,
професор кафедри фізико-технічних засобів захисту інформації,
д.т.н., професор

Луценко Володимир Миколайович,
доцент кафедри фізико-технічних засобів захисту інформації,
к.т.н., доцент

Прогонов Дмитро Олександрович,
доцент кафедри фізико-технічних засобів захисту інформації,
к.т.н., доцент

За підготовку здобувачів вищої освіти за освітньою програмою відповідає кафедра фізико-технічних засобів захисту інформації

ПОГОДЖЕНО:

Науково-методичною комісією КПІ ім. Ігоря Сікорського зі спеціальності

125 Кібербезпека

Голова НМКУ зі спеціальності 125 Кібербезпека

_____ Олексій НОВІКОВ
(протокол № 2/2021 від «05» 05 20 21 р.)

Методичною радою КПІ ім. Ігоря Сікорського

Голова Методичної ради

_____ Юрій ЯКИМЕНКО
(протокол № 8 від «24» 06 2021 р.)

ВРАХОВАНО:
фахову експертизу стейкхолдерів:

Представники роботодавців:
Мохонько Олексій Анатолійович, к.ф.-м.н.,
R&D директор з інформаційної безпеки,
ТОВ "Самсунг Електронікс Україна Компані",
український центр досліджень та розробок Samsung

Соловйов Євгеній Валерійович,
Начальник Управління інформаційними технологіями
Служби зовнішньої розвідки України

Авдєєв Ігор Володимирович,
полковник служби цивільного захисту,
Начальник Центру оперативного зв'язку,
телекомунікаційних систем та інформаційних технологій
Державної служби з надзвичайних ситуацій

Представники студентських організацій:
Ракович Дарина,
голова Профбюро студентів

Михалко Дмитро,
голова Студради ФТІ

Мазурок Валентин,
виборний представник студентів

Назаров Олександр,
виборний представник студентів

Рецензії-відгуки стейкхолдерів додаються.

Освітню програму оновлено у зв'язку з виходом стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти від 18.03.2021 № 332, та внесені наступні зміни: доповнено перелік загальних/фахових компетентностей та програмних результатів навчання, змінено кількість кредитів щодо практики. Оновлена освітня програма відповідає вимогам стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти від 18.03.2021 № 332.Програму обговорено після надходження всіх побажань та пропозицій від роботодавців, здобувачів і випускників освітньої програми. Схвалено на розширеному засіданні кафедри фізико-технічних засобів захисту інформації (протокол № 10-а від «25» березня 2021 р.).

ЗМІСТ

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

«Системи технічного захисту інформації»
зі спеціальності 125 Кібербезпека

1 – Загальна інформація	
Повна ЗВО та інституту/ факультету	Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського” Фізико-технічний інститут
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь – магістр Кваліфікація – магістр з кібербезпеки
Рівень з НРК	НРК України – 7 рівень QF-EHEA – другий цикл EQF-LLL – 7 рівень
Офіційна назва освітньої програми	Системи технічного захисту інформації
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 120 кредитів, термін навчання 1 рік 9 місяців
Наявність акредитації	Сертифікат акредитації освітньої програми УД 11008908, дійсний до 01.07.2024
Передумови	Наявність ступеня бакалавра
Мова(и) викладання	Українська
Термін дії освітньої програми	До наступної акредитації
Інтернет-адреса постійного розміщення освітньої програми	http://ptmip.ipt.kpi.ua/ http://ipt.kpi.ua/ https://osvita.kpi.ua/op
2 – Мета освітньої програми	
Підготовка фахівця, здатного аналізувати, формулювати, вирішувати науково-практичні проблеми та розв’язувати складні фізико-технічні та логіко-організаційні задачі кібернетичної безпеки в умовах комплексності та недостатньої визначеності технологічних, екологічних, соціально-економічних та політичних загроз, проводити дослідницьку та науково-інноваційну діяльність в галузі інформаційної та/або кібербезпеки, всебічного професійного, інтелектуального, соціального та творчого розвитку особистості на найвищих рівнях досконалості в освітньо-науковому середовищі	

3 – Характеристика освітньої програми	
Предметна область	**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. **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. **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. • 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.
Орієнтація освітньої програми	Освітньо-наукова
Основний фокус освітньої програми	Спеціальна освіта в галузі кібербезпеки за освітньою програмою «Системи технічного захисту інформації». Основні фокуси програми: 1. Посилена підготовка в галузі новітніх методів отримання, обробки та передавання сигналів різної фізичної природи; 2. Фундаментальна підготовка щодо проектування, розробки, впровадження та супроводу комплексних систем захисту інформації, що циркулює на об'єктах інформаційної діяльності державної та приватної форми власності; 3. Посилена підготовка в галузі міждисциплінарного системного аналізу з метою створення комплексних систем захисту інформаційних потоків у комунікаційних мережах; 4. Посилена підготовка щодо проведення дослідницьких та інноваційних проектів; 5. Робочі плани підготовки здобувачів вищої освіти щорічно переглядаються з метою включення розділів, пов'язаних з розвитком знань у галузі кібернетичної безпеки на основі аналізу нових науково-технологічних здобутків; 6. Розвиток дуальної освіти та міжуніверситетських програм з провідними установами світу, участь у міжнародних конференціях; 7. Проведення щорічних конференцій та олімпіад з нових напрямків кібернетичної безпеки з метою навчання здобувачів вищої освіти розробці індивідуальних стартапів на етапі підготовки кваліфікаційної роботи. Ключові слова: кібернетична безпека, технічні засоби захисту інформації, технічний аудит, проектування та створення комплексів технічного захисту інформації

Особливості програми	1. Посилена підготовка в галузі технічних наук (програмування, обробки сигналів різної фізичної природи, розробка та оптимізація пристроїв захисту інформації); 2. Фундаментальна підготовка щодо проектування, розробки, впровадження та супроводу комплексних систем захисту інформації, що циркулює на об'єктах інформаційної діяльності державної та приватної форми власності; 3. Посилена підготовка до проведення дослідницьких та інноваційних проектів, розробки наукоємних технологій на замовлення вітчизняних та закордонних організацій різної форми власності; 4. Використання елементів дуальної освіти, зокрема міжуніверситетських програм з провідними установами світу та проходження практик на провідних підприємствах галузі захисту інформації; 5. Участь у виконанні спільних проектів на замовлення державних установ, науково-дослідних організацій та приватних компаній.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Відповідно до Державного класифікатору професій ДК 003:2010 випускники можуть працювати на посадах, що відповідають класифікаційним угрупованням: 213 Професіонали в галузі обчислень 2131 Професіонали в галузі обчислювальних систем 2131.2 Розробники обчислювальних систем, адміністратор системи інженер з програмного забезпечення комп'ютерів 2132.2 Розробники комп'ютерних програм, Інженер –програміст, Програміст (бази даних), Програміст прикладний 2149.2 Професіонали із організації інформаційної безпеки Можуть працювати фахівцями із захисту інформації в складі інформаційних департаментів підприємств та банків, розробниками та тестувальниками застосунків, що потребують виконання особливих вимог щодо інформаційної та кібернетичної безпеки; керівниками та співробітниками служб захисту інформації; аудиторами інформаційної та кібернетичної безпеки, адміністраторами інформаційної та кібернетичної безпеки, проектувальниками систем захисту інформації в кіберпросторі; розробниками програмних та програмно-апаратних засобів захисту інформації в кіберпросторі, консультантами-інструкторами з кібербезпеки, аналітиками кібербезпеки в установах державної та інших форм власності, спеціалістами в галузі кібербезпеки в складі кіберполіції, спеціалістами з забезпечення кібербезпеки в кіберпросторі (зокрема, в соціальних мережах; об'єктах з використанням "інтернету речей", об'єктах критичної інфраструктури (електростанції, водо-, газопостачання тощо)); науковими співробітниками.
Подальше навчання	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти

5 – Викладання та оцінювання	
Викладання та навчання	Програмою передбачено студентоцентроване навчання. Викладання проводиться у таких формах: лекції, практичні та семінарські заняття, комп'ютерні практикуми і лабораторні роботи; курсові проекти і роботи; технологія змішаного навчання, практики; виконання дипломного проекту і дипломної роботи (магістерської дисертації)
Оцінювання	Оцінювання знань студентів здійснюється у відповідності до Положення про рейтингову систему оцінювання результатів навчання студентів КПІ ім. Ігоря Сікорського за усіма видами аудиторної та позааудиторної роботи (вхідний, поточний, рубіжний, підсумковий контроль); екзамени, заліки, індивідуальні завдання тощо.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (ЗК)	
ЗК 1	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
ЗК 2	Здатність проведення досліджень на відповідному рівні.
ЗК 3	Здатність до абстрактного мислення, аналізу та синтезу.
ЗК 4	Здатність оцінювати та забезпечувати якість виконуваних робіт.
ЗК 5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові компетентності (ФК)	
ФК 1	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, науково-технічні розробки, фізичні та математичні фундаментальні знання і моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у галузі інформаційної безпеки та/або кібербезпеки.
ФК 2	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
ФК 3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
ФК 4	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
ФК 5	Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення уразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
ФК 6	Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ФК 7	Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
ФК 8	Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи й засоби захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/ або кібербезпеки організації
ФК 9	Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
ФК 10	Здатність проводити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також здійснювати наукові дослідження в сфері безпеки інформаційних систем і технологій, відповідно вітчизняним та світовим стандартам і вимогам.
ФК 11	Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, критично оцінювати результати досліджень та інновацій, презентувати результати досліджень та формувати науково-технічну звітність.
ФК 12	Здатність виявляти та локалізувати джерела небезпечних сигналів в умовах обмеженості апріорних даних щодо їх фізичної природи і характеристик на фоні сильних завадових сигналів
ФК 13	Здатність проводити комплексний аналіз ефективності технічних засобів, пристроїв та систем захисту інформації, розробляти методи підвищення їх ефективності
ФК 14	Здатність аналізувати існуючі методики проведення спеціальних досліджень об’єктів інформаційної діяльності та розробляти рекомендації щодо їх вдосконалення
ФК 15	Здатність виявляти та протидіяти роботі прихованих каналів несанкціонованої передачі інформації з обмеженим доступом при передачі повідомлень в локальних та глобальних інформаційно-комунікаційних системах
7 – Програмні результати навчання	
ПРН 1	Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки
ПРН 2	Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах
ПРН 3	Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі
ПРН 4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки

ПРН 5	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення
ПРН 6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення
ПРН 7	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки
ПРН 8	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури
ПРН 9	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки
ПРН 10	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації
ПРН 11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації
ПРН 12	Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому
ПРН 13	Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури
ПРН 14	Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
ПРН 15	Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
ПРН 16	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
ПРН 17	Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання
ПРН 18	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки

ПРН 19	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
ПРН 20	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик
ПРН 21	Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки
ПРН 22	Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки
ПРН 23	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації
ПРН 24	Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.
ПРН 25	Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.
ПРН 26	Вирішувати задачі розробки, впровадження та супроводу систем виявлення і протидії поширенню небезпечних сигналів різної фізичної природи
ПРН 27	Проводити аналіз та обробку сигналів різної фізичної природи з використанням новітніх методів статистичного, спектрального та структурного аналізу
ПРН 28	Обирати, аналізувати і розробляти методи виявлення та деструкції повідомлень, вбудованих до повідомлень, що поширюються в локальних та глобальних інформаційно-комунікаційних системах
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності у сфері вищої та післядипломної освіти (пункти 28-32 Постанови Кабінету Міністрів України № 1187 від 30.12.2015 р.) за текстом постанови Кабінету Міністрів України від 10.05.2018 р. № 347, п. 28-32)
Матеріально-технічне забезпечення	Відповідно до технологічних вимог щодо забезпечення започаткування та провадження освітньої діяльності у сфері вищої та післядипломної освіти для осіб з вищою освітою (пункти 33-38 Постанови Кабінету Міністрів України № 1187 від 30.12.2015 р.) за текстом постанови Кабінету Міністрів України від 10.05.2018 р. № 347, п. 34-35) Використання обладнання для проведення лекцій у форматі презентацій, мережевих технологій, зокрема на платформі дистанційного навчання Sikorsky.

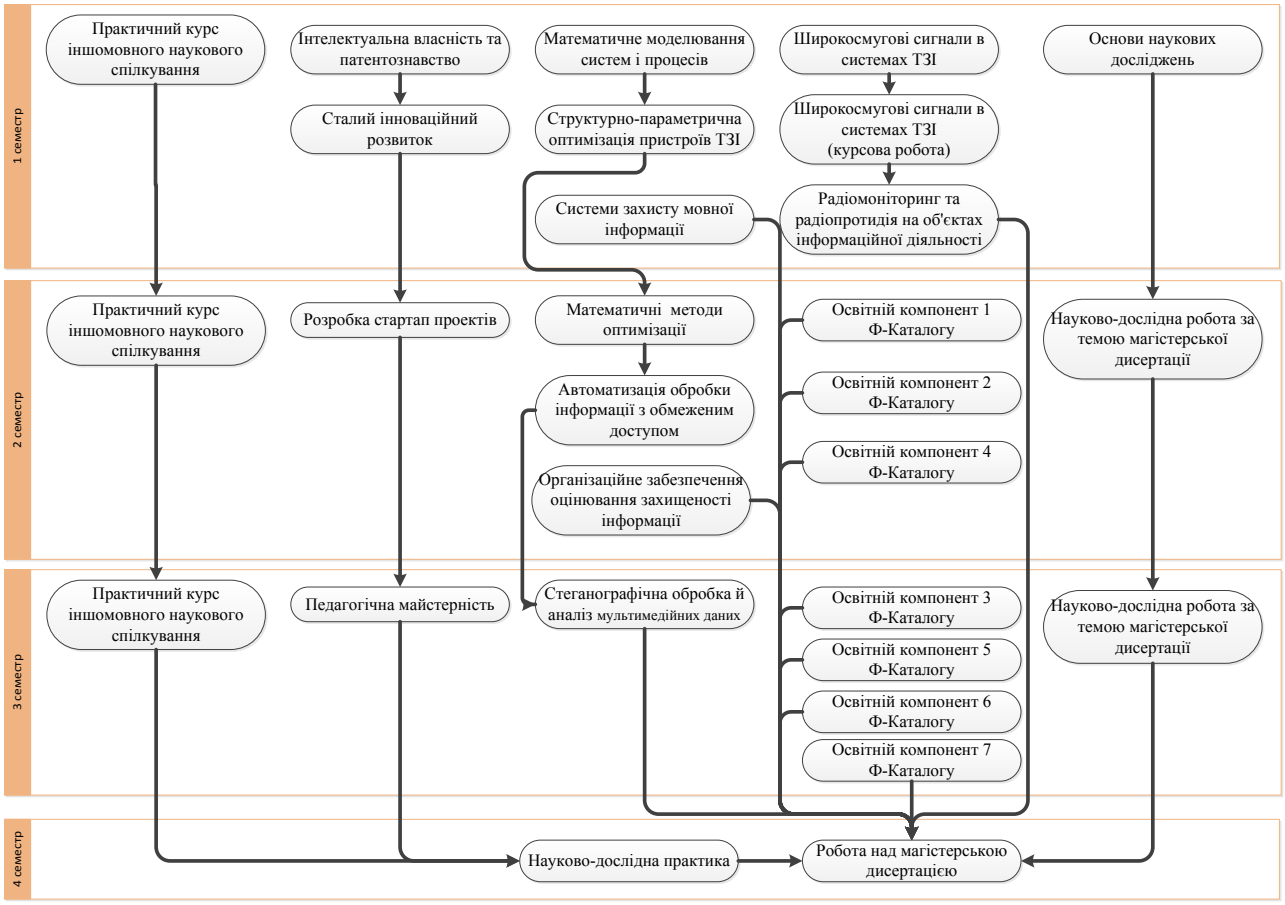
Інформаційне та навчально-методичне забезпечення	Відповідно до організаційних вимог щодо провадження освітньої діяльності у сфері вищої та післядипломної освіти для осіб з вищою освітою (пункти 39-45 Постанови Кабінету Міністрів України № 1187 від 30.12.2015 р.) , за текстом постанови Кабінету Міністрів України від 10.05.2018 р. № 347, п.36) Користування Науково-технічною бібліотекою КПІ ім. Ігоря Сікорського
9 – Академічна мобільність	
Національна кредитна мобільність	Участь студентів в програмах академічної мобільності, можливість укладення угод подвійне дипломування
Міжнародна кредитна мобільність	Можливість укладення угод про міжнародну академічну мобільність, про подвійне дипломування, про тривалі міжнародні проекти
Навчання іноземних здобувачів вищої освіти	В окремих академічних групах, при цьому українська мова вивчається як іноземна або українською мовою при навчанні у спільних академічних групах з україномовними здобувачами ВО

2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬОЇ ПРОГРАМИ

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. НОРМАТИВНІ освітні компоненти			
І.1. Цикл загальної підготовки			
ЗО 1	Інтелектуальна власність та патентознавство	3	Залік
ЗО 2	Сталий інноваційний розвиток	2	Залік
ЗО 3	Практичний курс іншомовного наукового спілкування	4,5	Залік
ЗО 4	Розробка стартап проектів	3	Залік
ЗО 5	Педагогічна майстерність	2	Залік
ЗО 6	Математичні методи оптимізації	4	Екзамен
ЗО 7	Математичне моделювання систем і процесів	4	Екзамен
І.2. Цикл професійної підготовки			
ПО 1	Широкосмугові сигнали в системах ТЗІ	5	Екзамен
ПО 2	Курсова робота з широкосмугових сигналів в системах ТЗІ	1	Залік
ПО 3	Радіомоніторинг і радіопротидія на об’єктах інформаційної діяльності	4	Екзамен
ПО 4	Системи захисту мовної інформації	3,5	Залік
ПО 5	Організаційне забезпечення оцінювання захищеності інформації	4	Екзамен
ПО 6	Автоматизація обробки інформації з обмеженим доступом	4,5	Екзамен
ПО 7	Стеганографічна обробка й аналіз мультимедійних даних	4	Екзамен
ПО 8	Структурно-параметрична оптимізація пристроїв ТЗІ	4	Залік
Дослідницький (науковий) компонент			
ПО 9	Наукова робота за темою магістерської дисертації		
ПО 9.1	Основи наукових досліджень	2	Залік
ПО 9.2	Науково-дослідна робота за темою магістерської дисертації	9,5	Залік
ПО 10	Науково-дослідна практика	15	Залік
ПО 11	Робота над магістерською дисертацією	11	Захист
2. ВИБІРКОВІ освітні компоненти			
ІІ.1. Цикл професійної підготовки (Вибіркові освітні компоненти з факультетського/кафедрального Каталогів)			
ПВ 1	Освітня компонента 1 Ф-Каталогу	4	Залік
ПВ 2	Освітня компонента 2 Ф-Каталогу	4	Залік
ПВ 3	Освітня компонента 3 Ф-Каталогу	4	Залік
ПВ 4	Освітня компонента 4 Ф-Каталогу	5	Екзамен
ПВ 5	Освітня компонента 5 Ф-Каталогу	4	Залік
ПВ 6	Освітня компонента 6 Ф-Каталогу	5	Екзамен

1	2	3	4
ПВ 7	Освітня компонента 7 Ф-Каталогу	4	Залік
Загальний обсяг **обов'язкових компонент:**		**90**	
Загальний обсяг **вибіркових компонент:**		**30**	
Загальний обсяг **освітніх компонентів, що забезпечують здобуття компетентностей визначених СВО**		**74,5**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**120**	

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ



4. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація здобувачів вищої освіти за освітньою програмою спеціальності 125 Кібербезпека проводиться у формі захисту кваліфікаційної магістерської роботи та завершується видачею документа встановленого зразка про присудження йому ступеня магістра з кібербезпеки за освітньою програмою “Системи технічного захисту інформації”.

Атестація здійснюється відкрито і публічно.

Магістерські дисертації перевіряються на ознаки порушення академічної доброчесності та після захисту публікуються в репозиторії НТБ Університету для вільного доступу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

	ЗО 1	ЗО 2	ЗО 3	ЗО 4	ЗО 5	ЗО 6	ЗО 7	ПО 1	ПО 2	ПО 3	ПО 4	ПО 5	ПО 6	ПО 7	ПО 8	ПО 9.1	ПО 9.2	ПО 10	ПО 11
ЗК1	+	+		+		+	+	+	+	+	+		+	+	+	+	+		+
ЗК2	+			+		+	+								+	+	+	+	+
ЗК3				+		+	+	+	+	+	+		+	+	+	+	+	+	+
ЗК4		+		+								+						+	+
ЗК5	+	+		+	+							+						+	
ФК 1	+	+		+		+	+	+	+	+	+		+	+	+	+	+	+	+
ФК 2	+			+								+				+	+	+	+
Ф К 3						+	+	+	+	+	+		+	+	+			+	+
ФК 4												+						+	+
ФК 5						+	+					+			+	+	+	+	+
ФК 6												+						+	+
ФК 7								+	+	+	+	+	+	+					+
ФК 8						+	+	+	+	+	+	+	+	+	+				+
ФК 9												+				+	+	+	+
ФК 10			+		+													+	
ФК 11	+	+		+				+	+	+	+		+	+		+	+	+	+
ФК 12								+	+	+	+		+					+	+
ФК 13															+			+	+
ФК 14										+	+	+						+	+
ФК 15													+	+				+	+

6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

	ЗО 1	ЗО 2	ЗО 3	ЗО 4	ЗО 5	ЗО 6	ЗО 7	ПО 1	ПО 2	ПО 3	ПО 4	ПО 5	ПО 6	ПО 7	ПО 8	ПО 9.1	ПО 9.2	ПО 10	ПО 11
ПРН 1			+															+	+
ПРН 2	+		+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН 3				+		+	+	+	+	+	+		+	+	+	+	+	+	+
ПРН 4	+		+			+	+						+				+	+	+
ПРН 5								+	+	+	+		+	+	+	+	+	+	+
ПРН 6								+	+	+	+	+		+	+	+			
ПРН 7	+	+										+	+				+	+	+
ПРН 8				+				+	+	+	+		+					+	+
ПРН 9												+	+	+				+	+
ПРН 10								+		+	+	+							
ПРН 11								+		+	+	+							
ПРН 12												+	+	+	+	+			
ПРН 13								+	+	+	+			+	+	+			
ПРН 14								+	+	+	+	+		+					
ПРН 15			+												+	+	+		
ПРН 16											+				+	+	+	+	+
ПРН 17	+					+	+								+	+	+	+	+
ПРН 18			+									+							
ПРН 19													+		+	+	+		
ПРН 20								+	+	+	+				+	+	+	+	+
ПРН 21						+	+	+	+	+	+		+						
ПРН 22						+	+	+	+	+	+		+					+	+
ПРН 23						+	+	+	+	+	+				+	+	+	+	+
ПРН 24						+	+						+			+	+	+	+
ПРН 25						+	+						+			+	+	+	+
ПРН 26								+	+	+	+							+	+
ПРН 27								+	+	+	+		+					+	+
ПРН 28													+	+				+	+