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

ЗАТВЕРДЖЕНО
Вченою радою КПІ ім. Ігоря Сікорського
(протокол № 1 від «23» 01 2023 р.)
Голова Вченої ради
_____ Михайло ІЛЬЧЕНКО

Безпека державних інформаційних ресурсів

Security of State Information Resources

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

другого (магістерського) рівня вищої освіти

за спеціальністю	**125 Кібербезпека та захист інформації**
галузі знань	**12 Інформаційні технології**
освітня кваліфікація	**магістр з кібербезпеки та захисту інформації**

Введено в дію з 2023/2024 н.р.
Наказом ректора
КПІ ім. Ігоря Сікорського
від 17.05.2023р. № НОН/165/2023

Київ – 2023

ПРЕАМБУЛА

РОЗРОБЛЕНО проєктною групою:

Керівник проєктної групи:

Самойлов Ігор Володимирович, кандидат технічних наук, доцент, доцент Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського

Члени проєктної групи:

Іванченко Сергій Олександрович, доктор технічних наук, професор, професор Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського

Олексійчук Антон Миколайович, доктор технічних наук, доцент, професор Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського

Конотопець Микола Миколайович, кандидат технічних наук, доцент, доцент Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського

Сторчак Антон Сергійович, кандидат технічних наук, доцент Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського

За підготовку здобувачів вищої освіти за освітньо-професійною програмою відповідає Спеціальна кафедра № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського.

ПОГОДЖЕНО:

Науково-методична комісія КПІ ім. Ігоря Сікорського зі спеціальності 125

Голова НМКУ 125 (для ІСЗЗІ) _____ Сергій ІВАНЧЕНКО

протокол № 1 від «12» 01 2023 р.)

Методична рада КПІ ім. Ігоря Сікорського

Голова Методичної ради _____ Анатолій Мельниченко

(протокол № 4 від «19» 01 2023 р.)

ВРАХОВАНО:

При внесенні змін та доповнень до освітньої програми враховано:

Постанову Кабінету Міністрів України від 16 грудня 2022 року № 1392 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти»;

Освітньо-професійну програму обговорено після надходження всіх пропозицій, побажань і зауважень від здобувачів вищої освіти, випускників та стейкхолдерів і схвалено на засіданні спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського (протокол № 5/1 від 05 січня 2023 року).

ЗМІСТ

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

1 – Загальна інформація	
Повна назва ЗВО та інституту/ факультету	Національний технічний університет України «Київський політехнічний інституту імені Ігоря Сікорського», Інститут спеціального зв'язку та захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь–магістр Кваліфікація – магістр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Безпека державних інформаційних ресурсів
Тип диплому та обсяг освітньої програми	Диплом магістра, 90 кредитів, термін навчання 1 рік 4 місяці
Наявність акредитації	Сертифікат про акредитацію УД № 11005377 від 20 червня 2018 року
Рівень з НРК	НРК України – 7 рівень, QF-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність освітнього ступеня бакалавра
Мова(и) викладання	Українська
Термін дії освітньої програми	До наступної акредитації
Інтернет-адреса постійного розміщення освітньої програми	https://osvita.kpi.ua/ (розділ «Освітні програми»)
2 – Мета освітньої програми	
Метою освітньо-професійної програми «Безпека державних інформаційних ресурсів» є підготовка висококваліфікованих фахівців, здатних вирішувати складні задачі і проблеми у галузі інформаційних технологій, кібербезпеки та здійснювати інноваційну професійну діяльність для проєктування, розробки, впровадження, супроводу та аудиту захищених інформаційних систем та засобів захисту. Мета освітньо-професійної програми відповідає стратегії розвитку КПІ ім. Ігоря Сікорського на 2020-2025 роки щодо формування суспільства майбутнього на засадах концепції сталого розвитку та фундаменталізації підготовки фахівців.	
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-професійна
Основний фокус освітньої програми	*Базовий фокус освітньої програми* – системи та процеси кіберпростору, сучасні методи та засоби захисту інформації. *Ключові слова:* кібербезпека, математичні методи кібербезпеки, системи і технології кібербезпеки, захист об'єктів критичної інфраструктури, розвиток засобів захисту інформації.
Особливості програми	Підготовка фахівців здійснюється у статусі курсанта. Залучення до викладання навчальних дисциплін фахівців з підрозділів Держспецзв'язку інших навчальних закладів, наукових установ. Практики проводяться відповідно до "Інструкції про порядок організації проведення практичної та військово-професійної підготовки здобувачів вищої освіти в закладі освіти Державної служби спеціального зв'язку та захисту інформації України", затвердженої наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 19 серпня 2021 року № 507 та складаються з: кібернавчань, які проводяться в першому та другому семестрах, на платформі Навчального ситуаційного центру кібербезпеки ІСЗЗІ КПІ ім. Ігоря Сікорського та платформі Тренінгового центру Кіберцентру UA30; експлуатаційної практики, яка проводиться в другому семестрі, на базі Лабораторії технічного захисту інформації ІСЗЗІ КПІ ім. Ігоря Сікорського; військового стажування в третьому семестрі яке проводиться в підрозділах Держспецзв'язку.
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: 2139.2 Аналітик безпеки інформаційно-комунікаційних систем 2132.2 Розробник систем захисту інформації 2149 Професіонали із організації інформаційної безпеки 23 Професіонали в галузі освіти і навчання Замовником фахівців зі спеціальності 125 Кібербезпека та захист інформації виступає Державна служба спеціального зв'язку та захисту інформації України.
Подальше навчання	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	Програмою передбачено проблемно-орієнтоване навчання з набуттям компетентностей, необхідних для продукування нових ідей, розв'язання комплексних проблем у професійній галузі, яке включає лекції, практичні та семінарські заняття,

	технологія змішаного навчання, підготовка та захист магістерської дисертації.
Оцінювання	Всі види навчальної діяльності та контрольні заходи (усні та письмові заліки, екзамени, тестування) оцінюються відповідно до Положення про систему оцінювання результатів навчання в КПІ ім. Ігоря Сікорського за стобальною шкалою з подальшим переведенням в оцінки університетської шкали. Навчання завершується написанням і публічним захистом магістерської дисертації.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (КЗ)	
КЗ-1	Здатність застосовувати знання у практичних ситуаціях.
КЗ-2	Здатність проводити дослідження на відповідному рівні.
КЗ-3	Здатність до абстрактного мислення, аналізу та синтезу.
КЗ-4	Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ-5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові компетентності (КФ)	
КФ1	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ2	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ4	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ5	Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів,

	аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ6	Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7	Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
КФ8	Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ9	Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ10	Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
КФ11	Здатність реалізовувати технічні вимоги на основі технік оцінки рівня захищеності інформаційних систем, технологій аналізу мережевого трафіку та принципів протидії кібератакам.
КФ12	Здатність проводити дослідження, перевірку, аналіз, оцінювання об'єктів інформаційної діяльності щодо їх відповідності вимогам нормативних документів із технічного захисту інформації.
КФ13	Здатність аналізувати, інтегрувати і використовувати кращі світові практики, міжнародні стандарти при розробці криптографічних систем захисту спеціальних інформаційно-комунікаційних систем.
КФ14	Здатність застосовувати комплекс фізичної підготовки військовослужбовців для розвитку загальних і спеціальних фізичних якостей, формування військово-прикладних навичок та виховання вольових і психічних якостей.
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.

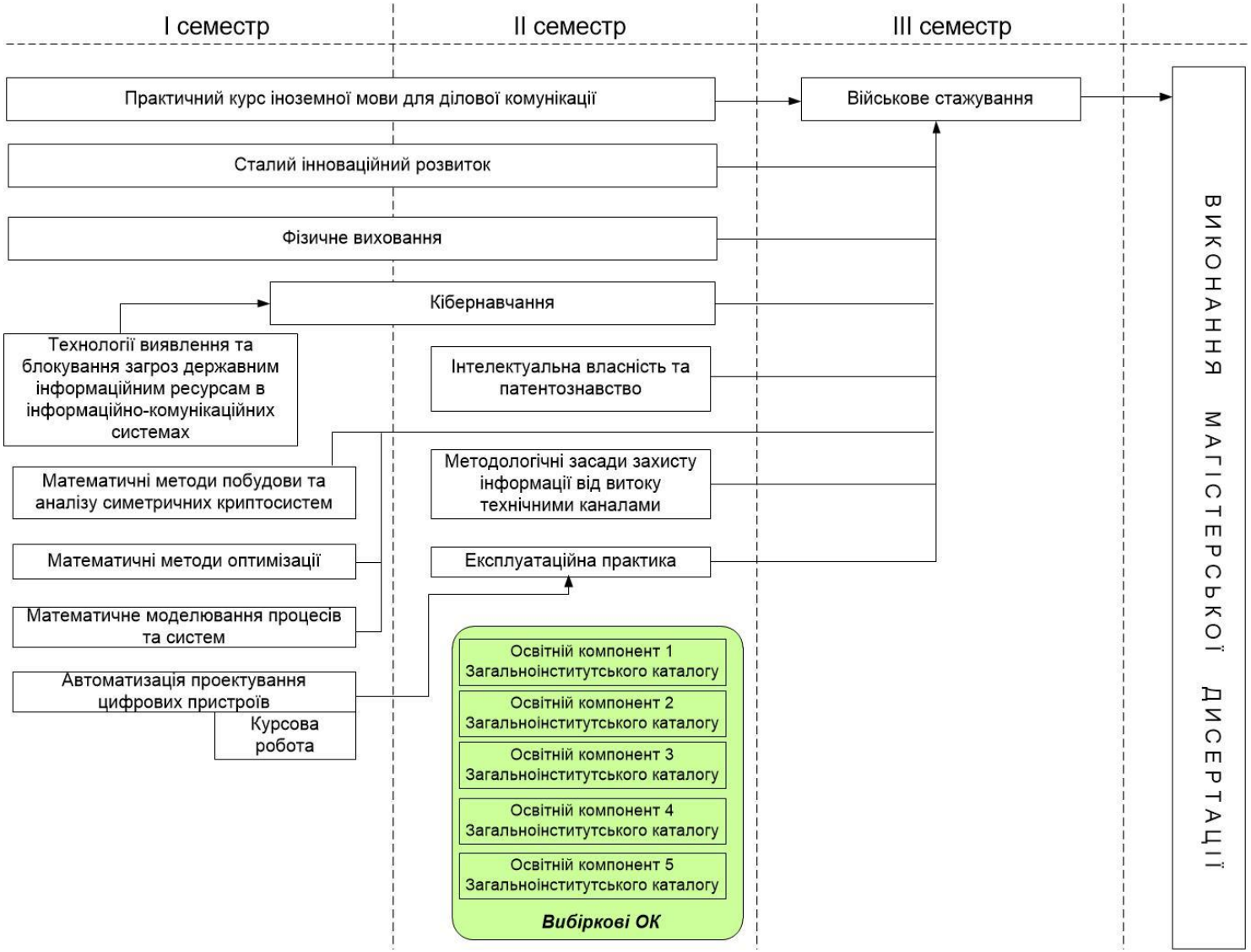
РН13	Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.
РН14	Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\абокібербезпеки в цілому.
РН15	Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН17	Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.
РН18	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19	Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21	Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22	Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у

	суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
РН24	Оцінювати стан інформаційних систем, розподіляти послуги безпеки і обирати механізми безпеки, впроваджувати технологічні рішення інноваційного характеру щодо виявлення та блокування загроз інформаційним ресурсам.
РН25	Застосовувати методики щодо оцінювання захищеності об'єктів інформаційної діяльності та державних інформаційних ресурсів від несанкціонованого доступу.
РН26	Проводити аналіз та синтез криптографічних алгоритмів та криптографічних протоколів; розробляти рекомендації впровадження інноваційних проектів, використовуючи базові методи дослідницької діяльності.
РН27	Застосовувати спеціальні фізичні якості та військово-прикладні навички при виконанні бойових завдань.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності для відповідного рівня вищої освіти, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 в чинній редакції. Залучення до викладання професійно-орієнтованих дисциплін фахівців-практиків в галузі кібербезпеки та захисту інформації.
Матеріально-технічне забезпечення	Відповідно до технологічних вимог щодо матеріально-технічного забезпечення освітньої діяльності відповідного рівня вищої освіти, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 в чинній редакції. Використання сучасних засобів та комплексів для дослідження оцінки захищеності інформації, вимога щодо захисту якої передбачена законодавством України, орієнтованих на здійснення освітнього процесу.
Інформаційне та навчально-методичне забезпечення	Відповідно до вимог щодо інформаційного та навчально-методичного забезпечення освітньої діяльності відповідного рівня вищої освіти, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 в чинній редакції. Користування Науково-технічною бібліотекою ті іншими інформаційними ресурсами КПІ ім. Ігоря Сікорського.
9 – Академічна мобільність	
Національна кредитна мобільність	Можливість укладання угод про академічну мобільність.
Міжнародна кредитна мобільність	Можливість укладання угод про академічну мобільність, про тривалі міжнародні проєкти, які передбачають включене навчання здобувачів вищої освіти (за рішенням Голови Держспецзв’язку).
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти за даною освітньо-професійною програмою не передбачено.

2. ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬОЇ СКЛАДОВОЇ ОСВІТНЬОЇ ПРОГРАМИ

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики)	Кількість кредитів ЄКТС	Форма підсумкового контролю
1. НОРМАТИВНІ освітні компоненти			
1.1. Цикл загальної підготовки			
ЗП 1	Інтелектуальна власність та патентознавство	3	залік
ЗП 2	Сталий інноваційний розвиток	4	залік
ЗП 3	Практичний курс іноземної мови для ділової комунікації	3	залік
1.2. Цикл професійної підготовки			
ПП 1.1	Фізичне виховання. Частина 1	3	залік
ПП 1.2	Фізичне виховання. Частина 2	3,5	залік
ПП 2	Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах	4	екзамен
ПП 3	Математичні методи побудови та аналізу симетричних криптосистем	3	залік
ПП 4	Математичні методи оптимізації	3	залік
ПП 5	Математичне моделювання процесів та систем	3	залік
ПП 6	Автоматизація проектування цифрових пристроїв	4	екзамен
ПП 7	Автоматизація проектування цифрових пристроїв Курсова робота	1	залік
ПП 8	Методологічні засади захисту інформації від витоку технічними каналами	4	екзамен
ПП 9	Виконання магістерської дисертації	13,5	захист
Практики			
ПП 10	Кібернавчання	3	залік
ПП 11	Експлуатаційна практика	3	залік
ПП 12	Військове стажування	9	залік
2. ВИБІРКОВІ освітні компоненти			
Вибіркові освітні компоненти із Загальноінститутського Каталогу			
ПВ 1	Освітній компонент 1 Загальноінститутського Каталогу	4	залік
ПВ 2	Освітній компонент 2 Загальноінститутського Каталогу	5	залік
ПВ 3	Освітній компонент 3 Загальноінститутського Каталогу	4	залік
ПВ 4	Освітній компонент 4 Загальноінститутського Каталогу	5	залік
ПВ 5	Освітній компонент 5 Загальноінститутського Каталогу	5	екзамен
Загальний обсяг нормативних компонент		**67**	
Загальний обсяг вибіркових компонент		**23**	
Обсяг освітніх компонентів, що забезпечують здобуття компетентностей, визначених СВО		**60,5**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**90**	

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ



4. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація здобувачів вищої освіти за освітньо-професійною програмою «Безпека державних інформаційних ресурсів» здійснюється у формі публічного захисту кваліфікаційної роботи, що забезпечує оцінювання досягнення результатів навчання, визначених освітньою програмою та завершується видачею документа встановленого зразка про присудження йому ступеня магістра з присвоєнням освітньої кваліфікації: магістр з кібербезпеки та захисту інформації, за освітньо-професійною програмою «Безпека державних інформаційних ресурсів».

Кваліфікаційна робота має передбачати розв’язання складної задачі дослідницького та/або інноваційного характеру у сфері кібербезпеки та захисту інформації. Кваліфікаційна робота не повинна містити академічного плагіату, фальсифікації, фабрикації.

Кваліфікаційна робота перевіряється на плагіат та після захисту розміщується в навчальній бібліотеці ІСЗЗІ КПІ ім. Ігоря Сікорського в архіві наукових та освітніх матеріалів для вільного доступу.

Атестація здійснюється відкрито і публічно. Але, якщо кваліфікаційна робота містить інформацію з обмеженим доступом, то захист проводиться в закритому режимі з неухильним дотриманням і виконанням вимог чинного законодавства щодо збереження службової та державної таємниці.

5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

	ЗП 1	ЗП 2	ЗП 3	ПП 1	ПП 2	ПП 3	ПП 4	ПП 5	ПП 6	ПП 7	ПП 8	ПП 9	ПП 10	ПП 11	ПП 12
КЗ-1	+	+	+		+	+	+		+	+	+	+	+	+	+
КЗ-2		+	+		+		+	+	+	+	+	+		+	+
КЗ-3		+				+	+	+		+		+	+		+
КЗ-4	+	+							+	+		+		+	+
КЗ-5	+	+	+		+		+	+				+	+	+	+
КФ 1						+	+	+	+	+		+	+		+
КФ 2	+	+				+					+	+		+	+
КФ 3					+				+			+		+	+
КФ 4					+							+	+		+
КФ 5					+		+	+				+	+		+
КФ 6						+						+	+		+
КФ 7					+							+	+		+
КФ 8						+	+		+	+	+	+		+	+
КФ 9					+							+	+		+
КФ 10	+	+										+			+
КФ 11					+							+	+		+
КФ 12											+	+		+	+
КФ 13						+						+	+		+
КФ 14				+											+

6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

	ЗП 1	ЗП 2	ЗП 3	ПП 1	ПП 2	ПП 3	ПП 4	ПП 5	ПП 6	ПП 7	ПП 8	ПП 9	ПП 10	ПП 11	ПП 12
РН1	+	+	+				+					+	+		+
РН2	+	+			+	+	+	+	+	+	+	+	+		+
РН3		+				+	+		+	+		+		+	+
РН4	+					+	+	+	+	+		+	+	+	+
РН5	+	+	+				+	+	+			+			+
РН6					+	+						+	+	+	+
РН7			+				+		+			+		+	+
РН8					+					+		+	+		+
РН9					+							+	+		+
РН10					+							+	+	+	+
РН11					+							+	+		+
РН12					+							+	+		+
РН13	+					+	+		+	+		+		+	+
РН14					+							+			+
РН15	+	+	+				+					+			+
РН16							+	+	+		+	+	+		+
РН17	+	+					+		+			+	+		+
РН18	+	+										+		+	+
РН19							+			+		+		+	+
РН20			+			+	+			+		+			+
РН21					+		+	+	+	+		+	+	+	+
РН22	+	+				+		+			+	+		+	+
РН23							+		+	+		+			+
РН24					+							+	+		+
РН25											+	+		+	+
РН26						+						+	+		+
РН27				+											+