

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

ЗАТВЕРДЖЕНО
Вченою радою
КПІ ім. Ігоря Сікорського
(протокол №__ від _____ 20__ р.)
Голова Вченої ради
_____ Михайло ІЛЬЧЕНКО

**СИСТЕМИ, ТЕХНОЛОГІЇ ТА МАТЕМАТИЧНІ
МЕТОДИ КІБЕРБЕЗПЕКИ**

**SYSTEMS, TECHNOLOGIES AND MATHEMATICAL
METHODS OF CYBER SECURITY**

ОСВІТНЬО-НАУКОВА ПРОГРАМА

другого (магістерського) рівня вищої освіти

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

Введено в дію з 2024/2025 навч. року
наказом ректора
КПІ ім. Ігоря Сікорського
від _____ 20__ р. № _____

Київ – 2024

ПРЕАМБУЛА

РОЗРОБЛЕНО проектною групою:

Керівник проектної групи:

Ланде Дмитро Володимирович, доктор технічних наук, професор, завідувач кафедри інформаційної безпеки, Навчально-науковий Фізико-технічний інститут

Члени проектної групи:

Новіков Олексій Миколайович, доктор технічних наук, професор, директор Навчально-Наукового Фізико-Технічного інституту

Смирнов Сергій Анатолійович, кандидат фізико-математичних наук, старший науковий співробітник, Навчально-науковий Фізико-технічний інститут

Стьопчкіна Ірина Валеріївна, кандидат технічних наук, доцент кафедри інформаційної безпеки, Навчально-науковий Фізико-технічний інститут

ПОГОДЖЕНО:

Науково-методичною комісією КПІ ім. Ігоря Сікорського зі спеціальності 125

Голова НМКУ 125

_____ Дмитро ЛАНДЕ

(протокол №1/2023 від «10» січня 2023 р.)

Методичною радою КПІ ім. Ігоря Сікорського

Голова Методичної ради

_____ Анатолій МЕЛЬНИЧЕНКО

(протокол № ____ від «__» _____ 2023 р.)

ВРАХОВАНО:

Пропозиції стейкхолдерів.

Представники роботодавців:

Корніленко Олександр Володимирович, начальник 1 відділу 4 управління ДЦКЗ Держспецзв'язку України

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

Кудін Антон Михайлович, заступник директора департаменту, начальник управління безпеки інформації Департаменту безпеки НБУ д.т.н., професор

Представники студентських організацій:

Гуменюк Олег, студент 1 курсу магістратури за спеціальністю 125 Кібербезпека та захист інформації

Осінній Максим, студент 1 курсу магістратури за спеціальністю 125 Кібербезпека та захист інформації

Лугінін Богдан, студент 4 курсу бакалаврату за спеціальністю 125 Кібербезпека

Внесено наступні зміни:

Освітню програму оновлено у зв'язку з уточненням окремих формулювань та зміною назв деяких нормативних дисциплін. Уточнено зміст деяких ПРН, розподіл ПРН по дисциплінах.

Освітню програму обговорено на засіданнях НМКУ та ухвалено на засіданні кафедри інформаційної безпеки, протокол №10/2022 від 28.12.2022.

ЗМІСТ

| | |
|--|----|
| 1. Профіль освітньої програми..... | 5 |
| 2. Перелік компонентів освітньо-наукової програми | 14 |
| 3. Структурно-логічна схема освітньої програми | 15 |
| 4. Форма атестації здобувачів вищої освіти | 15 |
| 5. Матриця відповідності програмних компетентностей нормативним компонентам освітньої програми..... | 16 |
| 6. Матриця забезпечення програмних результатів навчання нормативними компонентами освітньої програми | 17 |

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

«Системи, технології та математичні методи кібербезпеки» зі спеціальності 125 Кібербезпека та захист інформації

| 1 – Загальна інформація | |
|---|---|
| Повна ЗВО та інституту/факультету | Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського” Навчально-науковий Фізико-технічний інститут |
| Ступінь вищої освіти та назва кваліфікації мовою оригіналу | Ступінь – магістр Кваліфікація – магістр з кібербезпеки та захисту інформації |
| Рівень з НРК | НРК України – 7 рівень, QF-EHEA – другий цикл, EQF-LLL – 7 рівень |
| Офіційна назва освітньої програми | Системи, технології та математичні методи кібербезпеки |
| Тип диплому та обсяг освітньої програми | Диплом магістра, одиничний, 120 кредитів, термін навчання 1 рік 9 місяців |
| Наявність акредитації | Сертифікат акредитації освітньої програми УД № 11008907, 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 | https://osvita.kpi.ua/node/103 , (розділ «Освітні програми»), http://is.ipt.kpi.ua/navchalni-programi-2 |
| 2 – Мета освітньої програми | |
| <p>Забезпечення фундаментальної підготовки; гармонійність, багатовимірність освіти; інтеграція науково-дослідної, інноваційної діяльності і навчального процесу; орієнтація на міжнародні вимоги в сфері кібербезпеки та захисту інформації, світові наукові досягнення; дуальна освіта, орієнтація на вимоги ринку праці.</p> <p>Підготовка професіоналів, здатних використовувати і впроваджувати новітні технології та математичні методи, проводити науково-дослідну та інноваційну діяльність в галузі захисту інформації і кібернетичної безпеки;</p> <p>Мета освітньої програми відповідає стратегії розвитку КПІ імені Ігоря Сікорського 2020-2025 років щодо формування суспільства майбутнього на засадах концепції сталого розвитку.</p> | |

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 | <i>Базовий фокус ОП</i> – системи та процеси кіберпростору, засоби та заходи захисту, які базуються на останніх досягненнях науки і техніки. <i>Ключові слова:</i> кібернетична безпека, захист інформації, системи і технології кібербезпеки, математичні методи кібербезпеки, аналіз кіберінцидентів, аналіз вразливостей, аналіз ризиків , захист об'єктів критичної інфраструктури |
| Особливості програми | 1) ґрунтовна фундаментальна підготовка у поєднанні із сучасною професійною підготовкою, яка дозволяє проводити науково-дослідну та інноваційну діяльність і працювати з наукоємними технологіями кібербезпеки; 2) проходження науково-дослідної практики на базі підприємств-партнерів та участь студентів у виконанні спільних науково-дослідних проектів на замовлення установ та провідних ІТ-компаній України за фахом; 3) наявність дуальної освіти та сертифікатної програми . |
| 4 – Придатність випускників до працевлаштування та подальшого навчання | |
| Придатність до працевлаштування | Відповідно до Державного класифікатору професій ДК 003:2010 зі Зміною №10 випускники можуть працювати на посадах, що відповідають класифікаційним угрупованням: 2139.2 Аналітик систем захисту інформації та оцінки вразливостей 2139.2 Аналітик загроз безпеки 2132.2 Розробник систем захисту інформації. 2149 Професіонали із організації інформаційної безпеки. 23 Професіонали в галузі освіти і навчання 2131.1 Наукові співробітники (обчислювальні системи) |
| 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, індивідуальні завдання; технологія змішаного навчання, практики; виконання дипломної роботи (магістерської дисертації) |

| | |
|-------------------------------------|---|
| Оцінювання | Оцінювання знань студентів здійснюється у відповідності до Положення про систему оцінювання результатів навчання КПІ ім. Ігоря Сікорського за усіма видами аудиторної та позааудиторної роботи (вхідний, поточний, календарний, підсумковий контроль); усних та письмових екзаменів, заліків |
| 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 | Здатність застосовувати знання у практичних ситуаціях. |
| 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. |
| ФК11 | 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 враховувати дослідницькі, міждисциплінарні науково-практичні контексти при прийнятті рішень в галузі інформаційної безпеки та/або кібербезпеки |
| ФК 13 | Здатність застосовувати системний підхід, теорії математичної статистики та інші міждисциплінарні теорії та практики до задач кібербезпеки. |

| 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 | Проводити 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 напрямку 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 натурального, 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 системного аналізу, теорії прийняття рішень, оптимізації процесів, математичної статистики. |
| ПРН 25 | Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій. |
| ПРН 26 | Мати навички розроблення, впровадження та супроводження проектів з забезпечення інформаційної безпеки та\або кібербезпеки з урахуванням сучасних вимог та принципів побудови високонавантажених систем, аналізу великих даних та методів машинного навчання. |

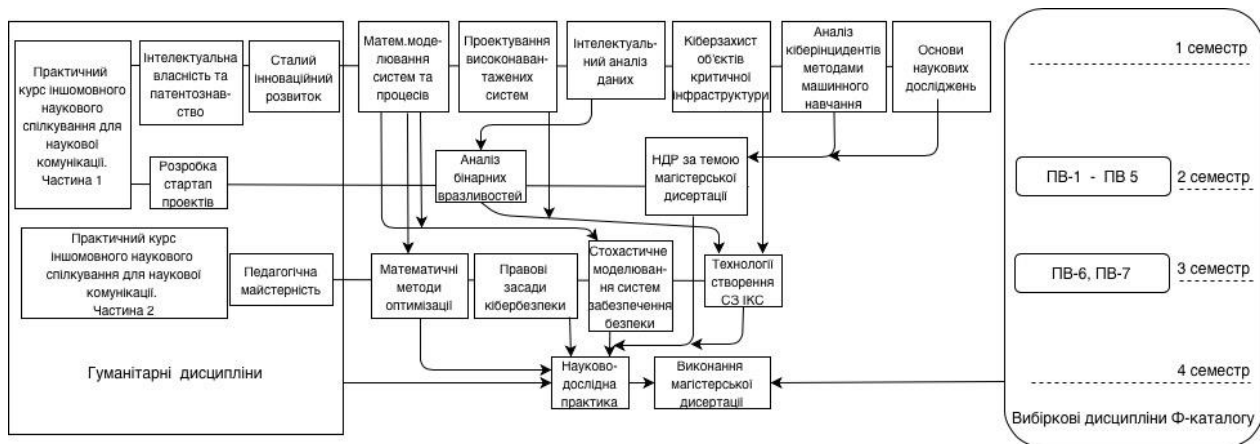
| | |
|--|---|
| ПРН27 | Застосовувати спеціалізовані концептуальні знання з інформаційної безпеки та/або кібербезпеки у професійній діяльності, у тому числі знання і розуміння новітніх досягнень, які забезпечують здатність до моделювання та дослідження сучасних систем забезпечення безпеки. |
| 8 – Ресурсне забезпечення реалізації програми | |
| Кадрове Забезпечення | Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності для відповідного рівня ВО (Постанова Кабінету Міністрів України від 30.12.2015 р. № 1187 (в чинній редакції)) |
| Матеріально-технічне забезпечення | Відповідно до технологічних вимог щодо матеріально-технічного забезпечення освітньої діяльності відповідного рівня ВО (Постанова Кабінету Міністрів України від 30.12.2015 р. № 1187 (в чинній редакції)), 3 комп'ютерних класи, полігон з Кібербезпеки. Матеріально-технічна база Samsung R&D Institute Ukraine Використання обладнання для проведення лекцій у форматі презентацій, мережевих технологій, зокрема на платформі дистанційного навчання Sikorsky |
| Інформаційне та навчально-методичне забезпечення | Відповідно до вимог щодо навчально-методичного та інформаційного забезпечення освітньої діяльності відповідного рівня ВО (Ліцензійні умови, затверджені Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 (в чинній редакції)). Ресурси науково-технічної бібліотеки КПІ імені Ігоря Сікорського, бібліотеки Навчально-наукового Фізико-технічного інституту |
| 9 – Академічна мобільність | |
| Національна кредитна мобільність | Участь студентів в програмах академічної мобільності, можливість укладення угод про подвійне дипломування |
| Міжнародна кредитна мобільність | Можливість укладення угод про міжнародну академічну мобільність, про тривалі міжнародні проекти |
| Навчання іноземних здобувачів вищої освіти | Навчання іноземних здобувачів ВО, які опановують ОП за програмами міжнародної академічної мобільності, навчання може проводитись англійською або українською мовою, за умови володіння здобувачем мовою навчання на рівні не нижче B2. |

2. ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ

| Код н/д | Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота) | Кількість кредитів | Форма підсумкового контролю |
|--|--|--------------------|-----------------------------|
| 1. Нормативні освітні компоненти | | | |
| 1.1 Цикл загальної підготовки | | | |
| ЗО 1 | Інтелектуальна власність та патентознавство | 3 | Залік |
| ЗО 2 | Сталий інноваційний розвиток | 2 | Залік |
| ЗО 3.1 | Практичний курс іноземної мови для наукової комунікації. Частина 1 | 3 | Залік |
| ЗО 3.2 | Практичний курс іноземної мови для наукової комунікації. Частина 2 | 1,5 | Залік |
| ЗО 4 | Розробка стартап проектів | 3 | Залік |
| ЗО 5 | Педагогічна майстерність | 2 | Залік |
| ЗО 6 | Математичне моделювання систем і процесів | 4 | Екзамен |
| ЗО 7 | Математичні методи оптимізації | 4 | Екзамен |
| 1. 2 Цикл професійної підготовки | | | |
| ПО 1 | Проектування високонантажених систем | 4 | Залік |
| ПО 2 | Інтелектуальний аналіз даних | 4 | Екзамен |
| ПО 3 | Кіберзахист об'єктів критичної інфраструктури | 4 | Залік |
| ПО 4 | Виявлення та аналіз кіберінцидентів методами машинного навчання | 4,5 | Екзамен |
| ПО 5 | Аналіз бінарних вразливостей | 3 | Залік |
| ПО 6 | Правові засади кібербезпеки | 2 | Залік |
| ПО 7 | Стохастичне моделювання систем кібербезпеки | 3,5 | Екзамен |
| ПО 8 | Технології забезпечення кіберзахисту інформаційно-комунікаційних систем | 4 | Екзамен |
| Дослідницький (науковий) компонент | | | |
| ПО 9.1 | Наукова робота за темою магістерської дисертації. Частина 1. Основи наукових досліджень | 2 | Залік |
| ПО 9.2 | Наукова робота за темою магістерської дисертації. Частина 2. Науково-дослідна робота за темою магістерської дисертації | 9,5 | Залік |
| ПО 10 | Науково-дослідна практика | 15 | Залік |
| ПО 11 | Виконання магістерської дисертації | 11 | Захист |
| 2. Вибіркові освітні компоненти | | | |
| 2.1. Цикл професійної підготовки (Вибіркові освітні компоненти з факультетського/кафедрального Каталогів) | | | |
| ПВ 1 | Освітній компонент 1 Ф-Каталогу | 4 | Залік |
| ПВ 2 | Освітній компонент 2 Ф-Каталогу | 5 | Екзамен |
| ПВ 3 | Освітній компонент 3 Ф-Каталогу | 5 | Екзамен |
| ПВ 4 | Освітній компонент 4 Ф-Каталогу | 4 | Залік |
| ПВ 5 | Освітній компонент 5 Ф-Каталогу | 5 | Екзамен |
| ПВ 6 | Освітній компонент 6 Ф-Каталогу | 4 | Залік |

| | | | |
|--|---------------------------------|-------------|-------|
| ПВ 7 | Освітній компонент 7 Ф-Каталогу | 4 | Залік |
| Загальний обсяг обов'язкових компонентів | | 89 | |
| Загальний обсяг вибіркових компонентів | | 31 | |
| Загальний обсяг освітніх компонентів, що забезпечують здобуття компетентностей визначених СВО | | 77,5 | |
| ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ | | 120 | |

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ



4. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація здобувачів вищої освіти за освітньо-науковою програмою спеціальності 125 Кібербезпека та захист інформації здійснюється у формі публічного захисту кваліфікаційної роботи - магістерської дисертації та завершується видачею документу встановленого зразка про присвоєння кваліфікації магістра з кібербезпеки та захисту інформації за освітньою програмою «Системи, технології та математичні методи кібербезпеки».

Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій.

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.

Атестація здійснюється відкрито і публічно.

5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ НОРМАТИВНИМ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

| | ЗК1 | ЗК2 | ЗК3 | ЗК4 | ЗК5 | ФК1 | ФК2 | ФК3 | ФК4 | ФК5 | ФК6 | ФК7 | ФК8 | ФК9 | ФК10 | ФК11 | ФК12 | ФК13 |
|--------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|------|------|------|------|
| ЗО 1 | | | | + | | | + | | | | | | | | | | | |
| ЗО 2 | | | | + | + | | | | | | | | | | | | | |
| ЗО 3.1 | | | | | + | | | | | | | | | | | | | |
| ЗО 3.2 | | | | | + | | | | | | | | | | | | | |
| ЗО 4 | + | | | | | | | | | + | | | | + | + | | | |
| ЗО 5 | + | | | | + | | | | | | | | | | + | | | |
| ЗО 6 | | + | + | | + | + | | | | | | | | | | + | | |
| ЗО 7 | | + | + | | + | + | | | | | | | | | | + | | |
| ПО1 | | | | | + | + | | | | | + | | | | | | + | + |
| ПО2 | | | | | | + | | | | | | | | | | | + | + |
| ПО3 | | | | | | + | | + | | + | + | | + | | | | | |
| ПО4 | | | | + | + | + | | | | + | + | + | | + | | | | |
| ПО5 | | | | | + | + | | | | + | + | | | + | | | | |
| ПО6 | | | | | | | + | | + | | | | | | | | | |
| ПО7 | | | | | + | + | | | | | | | | | | + | + | + |
| ПО8 | + | | | | | + | | + | + | | + | | + | + | | | | |
| ПО9.1 | + | + | + | + | + | + | | + | + | + | + | + | + | + | | + | + | + |
| ПО9.2 | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + |
| ПО10 | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + |

| | | | | | | | | | | | | | | | | | | |
|------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|------|------|------|------|
| | ЗК1 | ЗК2 | ЗК3 | ЗК4 | ЗК5 | ФК1 | ФК2 | ФК3 | ФК4 | ФК5 | ФК6 | ФК7 | ФК8 | ФК9 | ФК10 | ФК11 | ФК12 | ФК13 |
| ПО11 | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + |

6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ НОРМАТИВНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ

ПРОГРАМИ

| ПРН | ЗО 1 | ЗО 2 | ЗО 3.1 | ЗО 3.2 | 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 | |
|------|------|------|--------|--------|------|------|------|------|------|------|------|------|------|------|------|------|--------|--------|-------|-------|---|
| ПРН1 | | | + | + | | + | | | | | | | | | | | + | + | + | + | |
| ПРН2 | | | | | | | + | + | | | | | | | | | | + | + | + | + |
| ПРН3 | | + | | | + | | | | | | | | | | | | | + | + | + | + |
| ПРН4 | | | | | | | + | | | | | | | | | | | + | + | + | + |

| ПРН11 | ПРН10 | ПРН9 | ПРН8 | ПРН7 | ПРН6 | ПРН5 | ПРН |
|-------|-------|------|------|------|------|------|--------|
| | | | | + | | | 30 1 |
| | | | | | | | 30 2 |
| | | | | | | | 30 3.1 |
| | | | | | | | 30 3.2 |
| | | | | | | | 30 4 |
| | | | | | | | 30 5 |
| | | | | | | + | 30 6 |
| | | | | | | + | 30 7 |
| + | | | | | + | + | П0 1 |
| | | | | | | | П02 |
| | | | + | + | | | П0 3 |
| | | | | | | | П0 4 |
| | + | | | | | | П0 5 |
| | | | | + | | | П0 6 |
| | | | | | | | П0 7 |
| + | | + | + | | + | + | П0 8 |
| + | + | + | + | + | + | + | П0 9.1 |
| + | + | + | + | + | + | + | П0 9.2 |
| + | + | + | + | + | + | + | П0 10 |
| + | + | + | + | + | + | + | П0 11 |

| ИРН18 | ИРН17 | ИРН16 | ИРН15 | ИРН14 | ИРН13 | ИРН12 | ИРН |
|-------|-------|-------|-------|-------|-------|-------|--------|
| | | | | | | | 30 1 |
| | + | | | | | | 30 2 |
| | | | | | | | 30 3.1 |
| | | | | | | | 30 3.2 |
| + | | | + | | | | 30 4 |
| | + | + | | | | | 30 5 |
| | | | | | | | 30 6 |
| | | + | | | | | 30 7 |
| | | | | | | | ИО 1 |
| | | | | | | + | ИО2 |
| | | | | | + | | ИО 3 |
| | | | | | | + | ИО 4 |
| | | | | | | | ИО 5 |
| | | | | | | | ИО 6 |
| | | | | | | | ИО 7 |
| | | | | + | | + | ИО 8 |
| + | + | + | + | + | + | + | ИО 9.1 |
| + | + | + | + | + | + | + | ИО 9.2 |
| + | + | + | + | + | + | + | ИО 10 |
| + | + | + | + | + | + | + | ИО 11 |

| ПРН25 | ПРН24 | ПРН23 | ПРН22 | ПРН21 | ПРН20 | ПРН19 | ПРН |
|-------|-------|-------|-------|-------|-------|-------|--------|
| + | | + | | | + | + | 30 1 |
| | | | | | | | 30 2 |
| | | | | | | | 30 3.1 |
| | | | | | | | 30 3.2 |
| | | | | | | | 30 4 |
| | | | | | | | 30 5 |
| | + | | + | + | | | 30 6 |
| | + | | + | | | | 30 7 |
| | | | | | | | П0 1 |
| | | | | | | | П0 2 |
| | | | | | | | П0 3 |
| | | | | | | | П0 4 |
| | | | | | | | П0 5 |
| | | | | | + | | П0 6 |
| | | | | + | | + | П0 7 |
| | | + | | | | | П0 8 |
| + | + | + | + | + | + | + | П0 9.1 |
| + | + | + | + | + | + | + | П0 9.2 |
| + | + | + | + | + | + | + | П0 10 |
| + | + | + | + | + | + | + | П0 11 |

| ИРН27 | ИРН26 | ИРН |
|-------|-------|--------|
| | | 30 1 |
| | | 30 2 |
| | | 30 3.1 |
| | | 30 3.2 |
| | | 30 4 |
| | | 30 5 |
| | | 30 6 |
| | | 30 7 |
| + | + | ИО 1 |
| + | + | ИО 2 |
| | | ИО 3 |
| | | ИО 4 |
| | | ИО 5 |
| | | ИО 6 |
| + | + | ИО 7 |
| | | ИО 8 |
| + | + | ИО 9.1 |
| + | + | ИО 9.2 |
| + | + | ИО 10 |
| + | + | ИО 11 |