**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, ТЕХНОЛОГІЇ ТА МАТЕМАТИЧНІ МЕТОДИ КІБЕРБЕЗПЕКИ

# SYSTEMS, TECHNOLOGIES AND MATHEMATICAL METHODS OF CYBER SECURITY

## ОСВІТНЬО-ПРОФЕСІЙНА 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** проектною групою:

Керівник проектної групи:

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

Члени проектної групи:

Грайворонський Микола Владленович, кандидат фізико-математичних наук, доцент, доцент кафедри інформаційної безпеки, Фізико-технічний інститут

Барановський Олексій Миколайович, кандидат технічних наук, доцент кафедри інформаційної безпеки, Фізико-технічний інститут

Лавренюк Алла Миколаївна, кандидат технічних наук, доцент, доцент кафедри інформаційної безпеки, Фізико-технічний інститут

Стьопочкіна Ірина Валеріївна, кандидат технічних наук, доцент кафедри інформаційної безпеки, Фізико-технічний інститут

**ПОГОДЖЕНО**:

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

Голова НМКУ 125

_____Олексій НОВІКОВ

(протокол № 2/2021 від «05» травня 2021 р.)

Методичною радою КПІ ім. Ігоря Сікорського

Голова Методичної ради

_____ Юрій ЯКИМЕНКО

(протокол № 8 від «24» 06 2021 р.)

**ВРАХОВАНО:**

Пропозиції стейкхолдерів

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

Жора Віктор Володимирович,
керівник ТОВ «Інфосейф»

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

**Представники студентських організацій**:

Ракович Дарина, в.о. голови Профбюро ФТІ,
студентка 4 курсу бакалаврату за
спеціальністю 125 Кібербезпека

Михалко Дмитро, голова Студради ФТІ, студент
4 курсу бакалаврату за спеціальністю 125 Кібербезпека

Колісніченко Ольга, студентка 1 курсу магістратури
за спеціальністю 125 Кібербезпека

*Внесено наступні зміни:*

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 інформаційної безпеки (протокол № 3 від «25» березня 2021 р.).

**ЗМІСТ**

## 1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

**«Системи, технології та математичні методи кібербезпеки»**
**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<br>Кваліфікація – магістр з кібербезпеки |
| 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, 90 кредитів, термін навчання 1 рік4 місяці |
| Наявність акредитації | Сертифікат акредитації освітньої програми УД № 11007486, 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»),<br><br>http://is.ipt.kpi.ua/navchalni-programi-2 |
| **2 – Мета освітньої програми** | |
| Забезпечення фундаментальної підготовки; гармонійність, багатовимірність освіти; інтеграція науково-дослідної, інноваційної діяльності і навчального процесу; орієнтація на міжнародні вимоги в сфері кібербезпеки, світові наукові досягнення; дуальна освіта, орієнтація на вимоги ринку праці.<br>Підготовка професіоналів, здатних використовувати і впроваджувати новітні технології та математичні методи, проводити науково-дослідну та інноваційну діяльність в ґалузі захисту інформації і кібернетичної безпеки;<br>Мета освітньої програми відповідає стратегії розвитку КПІ імені Ігоря Сікорського 2020-2025 років щодо формування суспільства майбутнього на засадах концепції сталого розвитку. | |

| 3 – Характеристика освітньої програми | |
|---|---|
| Предметна область | **Об’єкти вивчення:**<br>– 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;<br>– інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології;<br>– інфраструктура об’єктів інформаційної діяльності та критичних інфраструктур;<br>– системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків);<br>– інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси);<br>– програмне та програмно-апаратне забезпечення (засоби) кіберзахисту;<br>– системи управління інформаційною безпекою та/або кібербезпекою;<br>– технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки.<br><br>**Цілі навчання**:<br>Підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.<br><br>**Теоретичний зміст предметної області**<br>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**<br>Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кібер-захисту) 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.<br>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.<br>**Інструменти та обладнання**.<br>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 ОП* – системи та процеси кіберпростору, засоби та заходи захисту, які базуються на останніх досягненнях науки і техніки.<br>*Ключові слова*: кібернетична безпека, системи і технології кібербезпеки, математичні методи кібербезпеки, аналіз кіберінцидентів, аналіз вразливостей, 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;<br><br>2) проходження переддипломної практики на базі підприємств-партнерів та участь студентів у виконанні спільних науково-дослідних проектів на замовлення установ та провідних ІТ-компаній України за фахом;<br><br>3) дуальна освіта. |

| 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:<br>2139 Професіонали із захисту інформації в інформаційних і комунікаційних системах, професіонали із організації інформаційної безпеки.<br>2132.2Розробники комп'ютерних програм.<br>2131.1 Наукові співробітники (обчислювальні системи)<br>Випускники ОП можуть працювати професіоналами із захисту інформації та кібербезпеки в складі відповідних департаментів організацій, підприємств та банків, проектувальниками та розробниками застосунків, що потребують виконання особливих вимог щодо інформаційної та кібернетичної безпеки; співробітниками служб захисту інформації; адміністраторами інформаційної та кібернетичної безпеки, проектувальниками систем захисту в кіберпросторі; розробниками програмних та програмно-апаратних засобів захисту інформації в кіберпросторі, консультантами-інструкторами з кібербезпеки, спеціалістами в галузі кібербезпеки в складі правоохоронних органів, спеціалістами з забезпечення кібербезпеки в кіберпросторі (зокрема, об'єктах критичної інфраструктури). |
| 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 роботи і індивідуальні завдання; технологія змішаного навчання за окремими освітніми компонентами; практики; виконання 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, 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)** | |
| ЗК1 | Здатність застосовувати знання у практичних ситуаціях. |
| ЗК2 | Здатність проводити дослідження на відповідному рівні. |
| ЗК3 | 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 провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. |
| ФК 11 | Здатність враховувати сучасні міждисциплінарні науково-практичні контексти при прийнятті рішень в галузі інформаційної безпеки та/або кібербезпеки, зокрема, використовуючи апарат аналізу даних та враховуючи вимоги високонавантажених систем |

| **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 | Мати навички розроблення, впровадження та супроводження проектів з забезпечення інформаційної безпеки та/або кібербезпеки з урахуванням сучасних вимог та принципів побудови високонавантажених систем та аналізу даних. |

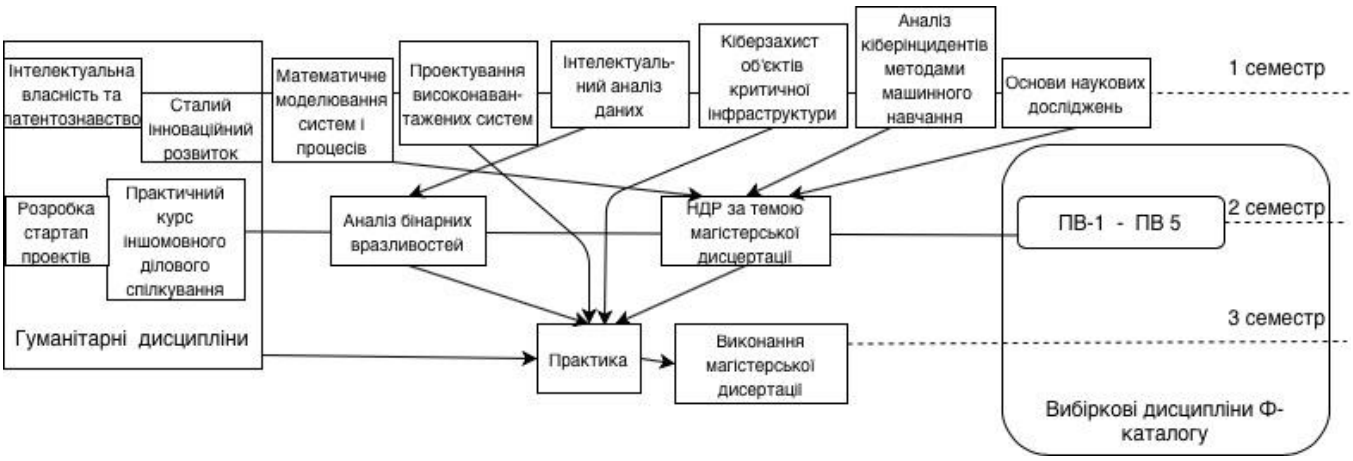
| 8 – Ресурсне забезпечення реалізації програми | |
|---|---|
| Кадрове забезпечення | Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності для відповідного рівня ВО (додаток 3 до Ліцензійних умов, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187, за текстом постанови Кабінету Міністрів України від 10.05.2018 р. № 347, п. 28-32) |
| Матеріально-технічне забезпечення | Відповідно до технологічних вимог щодо матеріально-технічного забезпечення освітньої діяльності відповідного рівня ВО (додаток 4 до Ліцензійних умов, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187, за текстом постанови Кабінету Міністрів України від 10.05.2018 р. № 347, п. 34-35), 3 комп'ютерних класи, полігон з Кібербезпеки Матеріально-технічна база Samsung R&D Institute Ukraine |
| Інформаційне та навчально-методичне забезпечення | Відповідно до вимог щодо навчально-методичного та інформаційного забезпечення освітньої діяльності відповідного рівня ВО (додаток 5 до Ліцензійних умов, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187, за текстом постанови Кабінету Міністрів України від 10.05.2018 р. № 347, п.36).<br>Ресурси науково-технічної бібліотеки КПІ імені Ігоря Сікорського,бібліотеки Фізико-технічного інституту |

| 9 – Академічна мобільність | |
|---|---|
| Національна кредитна мобільність | Участь студентів у програмах академічної мобільності |
| Міжнародна кредитна мобільність | Можливість укладення угод про міжнародну академічну мобільність, 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 КОМПОНЕНТІВ ОСВІТНЬО-ПРОФЕСІЙНОЇ 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 | Практичний курс іншомовного ділового спілкування | 3 | Залік |
| ЗО 4 | Розробка стартап проектів | 3 | Залік |
| ЗО 5 | Математичне моделювання систем і процесів | 4 | Екзамен |
| **1. 2 Цикл професійної підготовки** | | | |
| ПО 1 | Проектування високонавантажених систем | 4 | Залік |
| ПО 2 | Інтелектуальний аналіз даних | 4 | Екзамен |
| ПО 3 | Кіберзахист об'єктів критичної інфраструктури | 4 | Залік |
| ПО 4 | Аналіз кіберінцидентів методами машинного навчання | 4,5 | Екзамен |
| ПО 5 | Аналіз бінарних вразливостей | 3 | Залік |
| **Виконання магістерської дисертації** | | | |
| ПО 6 | Наукова робота за темою магістерської дисертації: | | |
| ПО 6.1 | 1. Основи наукових досліджень | 2 | Залік |
| ПО 6.2 | 2. Наукова робота за темою магістерської дисертації | 4,5 | Залік |
| ПО 7 | Практика | 15 | Залік |
| ПО 8 | 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 |
| | | | |
| **Загальний обсяг обов'язкових компонентів** | | **67** | |
| **Загальний обсяг вибіркових компонентів** | | **23** | |
| Загальний обсяг **освітніх компонентів, що забезпечують здобуття компетентностей визначених СВО** | | **59** | |
| **ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ** | | **90,0** | |

## 3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ




## 4. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

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

На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою в процесі навчання. До атестації допускаються здобувачі освіти, які виконали всі вимоги програми підготовки.

Кваліфікаційна робота-магістерська дисертація перевіряється на плагіат та після захисту розміщується в репозиторії науково-технічної бібліотеки університету для вільного доступу.

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** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| ЗО 1 | | | | + | | | + | | | | | | | | | |
| ЗО 2 | | | | | + | | | | | | | | | | | |
| ЗО 3 | | | | | + | | | | | | | | | | | |
| ЗО 4 | + | | | | | | | | | + | | | | + | + | |
| ЗО 5 | | + | + | | + | + | | | | + | | | | | | |
| ПО1 | | | | | | + | | | | | + | | | | | + |
| ПО2 | | | + | | | + | | | | | | | | | | + |
| ПО3 | | | | | | + | | + | | + | + | | + | | | |
| ПО4 | | + | | + | | | | | + | + | | + | | + | | |
| ПО5 | | | | | | + | | | | + | + | | | | | |
| ПО6.1 | + | + | + | + | + | + | | + | + | + | + | + | + | + | | + |
| ПО6.2 | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + |
| ПО7 | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + |
| ПО8 | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + |

## 6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ НОРМАТИВНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

| **ПРН** | **ЗО 1** | **ЗО 2** | **ЗО 3** | **ЗО 4** | **ЗО 5** | **ПО 1** | **ПО2** | **ПО 3** | **ПО 4** | **ПО 5** | **ПО 6.1** | **ПО 6.2** | **ПО 7** | **ПО 8** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ПРН1 | | | + | | | | | | | | + | + | + | + |
| ПРН2 | | | | | + | | | | | | + | + | + | + |
| ПРН3 | | + | | + | | | | | | | + | + | + | + |

| ПРН8 | ПРН7 | ПРН6 | ПРН5 | ПРН4 | **ПРН** |
|---|---|---|---|---|---|
| | + | | | | **ЗО 1** |
| | | | | | **ЗО 2** |
| | | | | | **ЗО 3** |
| | | | | | **ЗО 4** |
| | | | + | + | **ЗО 5** |
| | | + | + | | **ПО 1** |
| | | | | | **ПО2** |
| + | + | | | | **ПО 3** |
| | | | | | **ПО 4** |
| | | | | | **ПО 5** |
| + | + | + | + | | **ПО 6.1** |
| + | + | + | + | + | **ПО 6.2** |
| + | + | + | + | + | **ПО 7** |
| + | + | + | + | + | **ПО 8** |

| ПРН13 | ПРН12 | ПРН11 | ПРН10 | ПРН9 | **ПРН** |
|---|---|---|---|---|---|
| | | | | | **ЗО 1** |
| | | | | | **ЗО 2** |
| | | | | | **ЗО 3** |
| | | | | | **ЗО 4** |
| | | | | | **ЗО 5** |
| | | + | | | **ПО 1** |
| | + | | | | **ПО2** |
| + | | | | + | **ПО 3** |
| | + | | | | **ПО 4** |
| | | | + | | **ПО 5** |
| + | + | + | + | + | **ПО 6.1** |
| + | + | + | + | + | **ПО 6.2** |
| + | + | + | + | + | **ПО 7** |
| + | + | + | + | + | **ПО 8** |

| ПРН18 | ПРН17 | ПРН16 | ПРН15 | ПРН14 | **ПРН** |
|---|---|---|---|---|---|
| | | | | | **ЗО 1** |
| | + | | | | **ЗО 2** |
| | | | | | **ЗО 3** |
| + | | | + | | **ЗО 4** |
| | | + | | | **ЗО 5** |
| | | | | | **ПО 1** |
| | | | | | **ПО2** |
| | | | | | **ПО 3** |
| | | | | + | **ПО 4** |
| | | | | | **ПО 5** |
| | + | + | | + | **ПО 6.1** |
| + | + | + | + | + | **ПО 6.2** |
| + | + | + | + | + | **ПО 7** |
| + | + | + | + | + | **ПО 8** |

| ПРН23 | ПРН22 | ПРН21 | ПРН20 | ПРН19 | **ПРН** |
|---|---|---|---|---|---|
| + | | | + | + | **ЗО 1** |
| | | | | | **ЗО 2** |
| | | | | | **ЗО 3** |
| | | | | | **ЗО 4** |
| | + | + | | | **ЗО 5** |
| | | | | | **ПО 1** |
| | | | | | **ПО2** |
| | | | | | **ПО 3** |
| | | | | | **ПО 4** |
| | | | | | **ПО 5** |
| + | + | + | + | + | **ПО 6.1** |
| + | + | + | + | + | **ПО 6.2** |
| + | + | + | + | + | **ПО 7** |
| + | + | + | + | + | **ПО 8** |

| | |
|---|---|
| ПРН24 | **ПРН** |
| | **ЗО 1** |
| | **ЗО 2** |
| | **ЗО 3** |
| | **ЗО 4** |
| | **ЗО 5** |
| + | **ПО 1** |
| + | **ПО2** |
| | **ПО 3** |
| | **ПО 4** |
| | **ПО 5** |
| + | **ПО 6.1** |
| + | **ПО 6.2** |
| + | **ПО 7** |
| + | **ПО 8** |