

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

ЗАТВЕРДЖЕНО

Вченою радою КПІ ім. Ігоря Сікорського
(протокол № 4 від «03» 04 2017 р.)

**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

Зміни та доповнення погоджено НМКУ 125
(протокол № 3 від «8» 06 2020 р.)

Освітню програму зі змінами та доповненнями
введено в дію з 2020/2021 навч. року
(наказ № 1/231 від «08» 07 2020 р.)

Київ - 2020

ПРЕАМБУЛА

РОЗРОБЛЕНО проєктною групою:

Керівник проєктної групи

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

Новіков

Члени проєктної групи:

Даник Юрій Григорович, професор кафедри інформаційної безпеки, професор, доктор технічних наук

Грайворонський Микола Владленович, в.о. завідувача кафедри інформаційної безпеки, доцент, кандидат фізико-математичних наук

Стьопчкіна Ірина Валеріївна, доцент кафедри інформаційної безпеки, кандидат технічних наук

За підготовку здобувачів вищої освіти за освітньою програмою відповідає кафедра інформаційної безпеки

ПОГОДЖЕНО:

Першу редакцію освітньої програми ухвалено Методичною радою КПІ ім. Ігоря Сікорського (протокол № 7 від 30.08.2017 р.)

Зміни та доповнення до освітньої програми погоджені Науково-методичною комісією університету зі спеціальності 125 Кібербезпека

(протокол № 3 від «8» 06 2020 р.)

Голова НМКУ зі спеціальності 125 Кібербезпека

Новіков Олексій НОВІКОВ

ВРАХОВАНО:

фахову експертизу 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 Дар'я, в.о. голови Профбюро ФТІ,
студентка 3 курсу бакалаврату за
спеціальністю 125 Кібербезпека

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

Рішко Катерина, студентка 1 курсу магістратури
за спеціальністю 125 Кібербезпека

Враховано такі пропозиції стейкхолдерів:

- збільшити різноманітність професійно-орієнтованих дисциплін (студенти) при збереженні насиченої фундаментальної складової (роботодавці).

В ОП було внесено також наступні зміни:

- частину дисциплін перенести до блоків вибіркових, модернізувавши їх наповнення згідно профілю 125 Кібербезпека. запропонувати список вибіркових дисциплін до Факультетського/кафедрального каталогів.

Освітню програму обговорено після надходження всіх побажань та пропозицій від здобувачів вищої освіти і випускників освітньої програми та схвалено на розширеному засіданні кафедри інформаційної безпеки (протокол № 11/2020 від 20.05.2020 р.).

ЗМІСТ

1. Профіль освітньої програми	5
2. Перелік обов'язкових компонент освітньо-професійної програми	13
3. Структурно-логічна схема освітньої програми.....	14
4. Форма випускної атестації здобувачів вищої освіти.....	14
5. Матриця відповідності програмних компетентностей нормативним компонентам освітньої програми.....	15
6. Матриця забезпечення програмних результатів навчання нормативними компонентами освітньої програми.....	16

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

зі спеціальності 125 Кібербезпека
за освітньо-професійною програмою «Системи, технології та математичні методи
кібербезпеки»

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 – 8 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 УД № 11007486 (081837) від 08.01.2019, дійсний до 01.07.2024
Передумови	Наявність ступеня бакалавра
Мова(и) викладання	Українська/англійська
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, 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 (галузь знань, спеціальність)	<p>Галузь знань – 12 Інформаційні технології Спеціальність – 125 Кібербезпека Освітня програма– Системи, технології та математичні методи кібербезпеки</p> <p>Галузь знань – 12 Інформаційні технології Спеціальність – 125 Кібербезпека Освітня програма– Системи, технології та математичні методи кібербезпеки</p> <p><u>Об’єкти професійної діяльності випускників:</u></p> <ul style="list-style-type: none"> – об’єкти інформатизації, включаючи комп’ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно- телекомунікаційні системи , інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту. <p><u>Цілі навчання</u> підготовка фахівців, здатних розробляти і впроваджувати технології інформаційної та/або кібербезпеки.</p> <p><u>Теоретичний зміст предметної області</u></p> <p><u>Знання</u></p> <ul style="list-style-type: none"> – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення – інформаційно-комунікаційних технологій; – автоматизованих систем проектування. <p><u>Методи, методики та технології:</u></p> <ul style="list-style-type: none"> – Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення – кібербезпеки. <p><u>Інструменти та обладнання:</u></p> <ul style="list-style-type: none"> – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Освітньо-професійна

Основний фокус освітньої програми та спеціалізації	<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, 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; 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; 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: 2139 Професіонали із захисту інформації в інформаційних і комунікаційних системах, професіонали із організації інформаційної безпеки. 2132.2 Розробники комп'ютерних програм. 2131.1 Наукові співробітники (обчислювальні системи) 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, рубіжний, підсумковий контроль); усних та письмових екзаменів, заліків

6 – Програмні компетентності	
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 професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
ЗК 4	Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК 5	Здатність до абстрактного мислення, аналізу та синтезу.
ЗК 6	Здатність оцінювати та забезпечувати якість виконуваних робіт.
ЗК 7	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 наукову 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.

7 – Програмні результати навчання	
ПРН 1	Розв'язувати складні науково-технічні та прикладні завдання та проблеми з інформаційної безпеки та/або кібербезпеки, що потребують оновлення та інтеграції фундаментальних знань, у тому числі в умовах неповної інформації та суперечливих вимог.
ПРН 2	Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також здійснювати наукові дослідження в сфері захисту інформації у кіберпросторі.
ПРН 3	Вільно користуватися 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 4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, науково-технічні методи і моделі, фізичні та математичні фундаментальні знання в галузі інформаційної безпеки та/або кібербезпеки.
ПРН 5	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міжпредметному рівні, зокрема з використанням інженерно-технічних і математичних наук, а також напрямів технологій створення та використання спеціалізованого програмного забезпечення.
ПРН 6	Критично оцінювати захищеність систем, комплексів та засобів кіберзахисту, технологій створення та використання спеціалізованого програмного забезпечення, зокрема з використанням сучасних програмних та програмно-апаратних рішень та сучасних підходів.
ПРН 7	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою здійснення 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	Проводити аналіз, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі концептуальних питань стратегії і політики інформаційної безпеки.
ПРН 10	Досліджувати та проводити системний аналіз забезпечення безперервності бізнес\операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, проводити аналіз ризиків та визначати оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
ПРН 11	Аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
ПРН 12	Проводити дослідження та аналіз кіберінцидентів.
ПРН 13	Проводити дослідження, розробляти, впроваджувати та використовувати методи та засоби захисту інформації, проводити аналіз та надавати оцінку ефективності їх використання в інформаційних системах та об'єктах інформаційної діяльності та критичної інфраструктури.

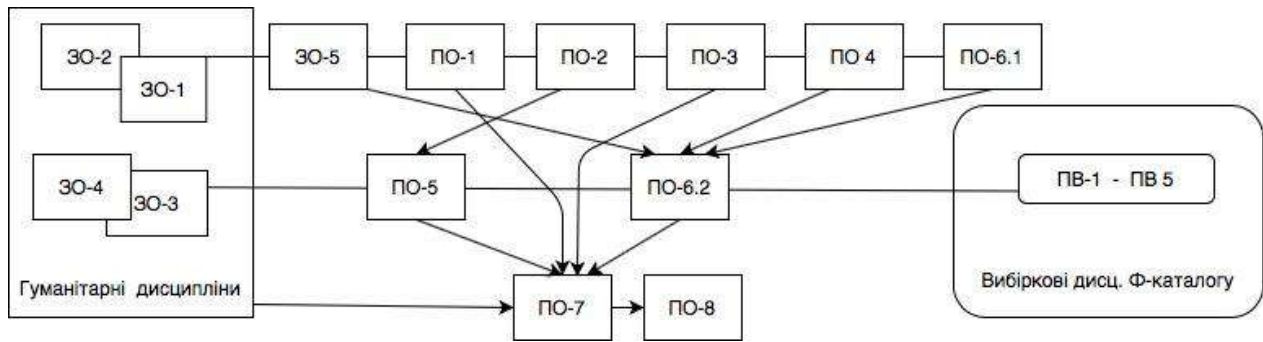
ПРН 14	Здійснювати аналіз, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів в галузі інформаційної та\або кібербезпеки в цілому.
ПРН 15	Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та\або кібербезпеки, а також знання та пояснення, що їх обґрунтовують.
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 математичних методів.
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	Проводити наукову діяльність, планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямі інформаційної безпеки та\або кібербезпеки.
ПРН 19	Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розуміти основні аспекти впровадження та супроводження проектів 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 комп'ютерного моделювання з метою детального вивчення і дослідження процесів, які стосуються інформаційної та кібербезпеки
ПРН 22	Планувати та виконувати експериментальні і теоретичні дослідження, обирати для цього придатні методи та інструменти, здійснювати обробку даних, оцінювати адекватність 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 керування, розроблення, впровадження та супроводження проектів з забезпечення інформаційної безпеки та\або кібербезпеки.

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 InstituteUkraine
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). 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	Для іноземних громадян навчання здійснюється українською або англійською мовами

2. ПЕРЕЛІК ОBOB'ЯЗKOBИХ КОМПОНЕНТ 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	Навчальна дисципліна з проблем сталого розвитку*	2	Залік
ЗО 3	Практикум іншомовного наукового спілкування	3	Залік
ЗО 4	Навчальна дисципліна з менеджменту*	3	Залік
ЗО 6	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	2	Залік
ПО 9	Наукова робота за темою магістерської дисертації:		
ПО 9.1	1. Основи наукових досліджень	2	Залік
ПО 9.2	2. Науково-дослідна робота за темою магістерської дисертації	2	Залік
ПО 10	Переддипломна практика	14	Залік
ПО 11	Робота над магістерською дисертацією	16	Захист
2. Вибіркові освітні компоненти			
2.1. Цикл професійної підготовки (Вибіркові освітні компоненти з факультетського/кафедрального Каталогів)			
ПВ 1	Освітній компонент 1 з Ф-Каталогу	4	Залік
ПВ 2	Освітній компонент 2 з Ф-Каталогу	5,5	Екзамен
ПВ 3	Освітній компонент 3 з Ф-Каталогу	5	Екзамен
ПВ 4	Освітній компонент 4 з Ф-Каталогу	4	Залік
ПВ 5	Освітній компонент 5 з Ф-Каталогу	4	Екзамен
Загальний обсяг обов'язкових компонентів		67,5	
Загальний обсяг вибіркових компонентів		22,5	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		90,0	

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ



4. ФОРМА ВИПУСКНОЇ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

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

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

5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ НОРМАТИВНИМ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ФК1	ФК2	ФК3	ФК4	ФК5	ФК6	ФК7	ФК8	ФК9	ФК10	ФК11	ФК12	ФК13
	1	2	3	4	5	6	7	1	2	3	4	5	6	7	8	9	10	11	12	13
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	301	302	303	304	305	ПО1	ПО2	ПО3	ПО4	ПО5	ПО6.1	ПО6.2	ПО7	ПО8
ПРН 1					+		+		+	+	+	+	+	+
ПРН 2					+		+	+	+	+			+	+
ПРН 3	+	+	+	+									+	+
ПРН 4					+	+	+	+	+	+	+	+	+	+
ПРН 5					+	+				+	+	+	+	+

ПРН12	ПРН11	ПРН10	ПРН9	ПРН8	ПРН7	ПРН6	ПРН
					+		301
							302
							303
							304
		+					305
	+						ПО1
							ПО2
	+	+		+		+	ПО3
+		+				+	ПО4
+		+				+	ПО5
					+		ПО6.1
+	+	+	+		+		ПО6.2
+	+	+	+	+	+	+	ПО7
+	+	+	+	+	+	+	ПО8

ПРН	ПРН 13	ПРН 14	ПРН 15	ПРН 16	ПРН 17	ПРН 18	ПРН 19	ПРН
301							+	301
302					+			302
303			+					303
304			+	+		+		304
305				+			+	305
ПО1		+					+	ПО1
ПО2							+	ПО2
ПО3	+						+	ПО3
ПО4							+	ПО4
ПО5							+	ПО5
ПО6.1			+					ПО6.1
ПО6.2	+		+		+		+	ПО6.2
ПО7	+	+	+	+	+	+	+	ПО7
ПО8	+	+	+		+		+	ПО8

ПРН 24	ПРН 23	ПРН 22	ПРН 21	ПРН 20	ПРН
				+	301
					302
					303
+					304
		+	+		305
	+				ПО1
		+			ПО2
	+				ПО3
					ПО4
					ПО5
		+		+	ПО 6.1
	+	+	+	+	ПО 6.2
+	+	+	+	+	ПО 7
	+	+	+	+	ПО 8