МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет радіоелектроніки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

"Безпека інформаційних і комунікаційних систем"

другого рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: Магістр, Кібербезпека,

Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ

Голова вченої ради

_____ / В.В. Семенець /

(протокол № 4 від " 28 " березня 2019р.)

Освітня програма вводиться в дію з _____2019 р.

Ректор_____ / В.В. Семенець /

(наказ № 178 від " 03 " квітня 2019 р.)

Харків 2019 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«Безпека інформаційних і комунікаційних систем»
другого рівня вищої освіти
за спеціальністю 125 «Кібербезпека»

УЗГОДЖЕНО
Перший проректор

_____ І.В. Рубан

«___» _____ 2019 р.

В.о. начальника відділу ДА та ВСЗЯО
_____ Макашев С.Б.

«12» 04 2019 р.

Розглянуто на засіданні Вченої Ради
факультету КІУ
протокол № 7 від 13.03.2019 р
Декан факультету КІУ
_____ О.С. Ляшенко

Розглянуто на засіданні кафедри БІТ
Протокол №10 від 07.03.2019 р.
Завідувач кафедри БІТ
_____ Г.З.Халімов

Представник роботодавця

КравченкоВолодимир Дмитрович
Виконавчий директор ПрАТ «ІІТ» _____ В.Д.Кравченко

РОЗРОБЛЕНО

Проектна група:
Керівник проектної групи:
Руженцев Віктор Ігоревич, д.т.н.,доц.,
проф. кафедри БІТ, ХНУРЕ _____ В.І.Руженцев

члени проектної групи:
Халімов Геннадій Зайдулович, д.т.н., проф.,
зав. каф. БІТ, ХНУРЕ _____ Г.З.Халімов

Олейніков Анатолій Миколайович, к.т.н., доц.,
професор каф. КРіСТЗІ, ХНУРЕ _____ А.М.Олейніков

Снігуров Аркадій Владіславович, к.т.н., доц.,
доц. каф. ІКІ, декан факультету ІК, ХНУРЕ _____ А.В.Снігуров

Заболотний Володимир Ілліч, к.т.н., доц.,
професор каф. БІТ, ХНУРЕ _____ В.І.Заболотний

ПЕРЕДМОВА

Розроблено проектною групою у складі:

1. Руженцев Віктор Ігоревич	– д-р техн. наук, доцент, професор кафедри Безпеки інформаційних технологій Харківського національного університету радіоелектроніки
2. Халімов Геннадій Зайдулович	– д-р техн. наук, професор, зав. кафедри Безпеки інформаційних технологій Харківського національного університету радіоелектроніки
2. Олейніков Анатолій Миколайович	– канд. техн. наук, доцент, професор кафедри Комп'ютерної радіоінженерії та систем технічного захисту інформації Харківського національного університету радіоелектроніки
3. Снігуров Аркадій Владиславович	– канд. техн. наук, доцент, декан факультету Інфокомунікацій, доцент кафедри Інфокомунікаційної інженерії Харківського національного університету радіоелектроніки
4. Заболотний Володимир Ілліч	– канд. техн. наук, доцент, професор кафедри Безпеки інформаційних технологій Харківського національного університету радіоелектроніки

1 Профіль освітньої програми
«Безпека інформаційних і комунікаційних систем»
за спеціальністю 125 Кібербезпека

1 - Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Харківський національний університет радіоелектроніки Факультет Комп'ютерної інженерії та управління Кафедра Безпеки інформаційних технологій
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Магістр, Кібербезпека, Безпека інформаційних і комунікаційних систем
Офіційна назва освітньої програми	Безпека інформаційних і комунікаційних систем
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1рік 4 міс.
Наявність акредитації	
Цикл/рівень	НРК України – 8 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра (або освітньо-кваліфікаційний рівень спеціаліста)
Мова(и) викладання	Українська
Термін дії освітньої програми	До повного завершення періоду навчання або наступного оновлення програми
Інтернет-адреса постійного розміщення опису освітньої програми	http://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-125-kiberbezpeka/magistr-125-kiberbezpeka
2 - Мета освітньої програми	
Мета освітньої програми полягає в оволодінні студентами знаннями, вміннями та навичками використовувати і впроваджувати технології інформаційної та/або кібербезпеки; набуття компетентностей у використанні методів дослідження і проектування систем та комплексів забезпечення інформаційної та кібербезпеки.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	12 Інформаційні технології 125 Кібербезпека
Орієнтація освітньої програми	Освітньо-професійна програма Акцент програми зроблений на розвиток здатності розв'язувати складні задачі і проблеми у галузі професійної діяльності, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог
Основний фокус освітньої програми та спеціалізації	Загальна спеціальна освіта другого (магістерського) рівня в галузі інформаційних технологій за спеціальністю «Кібербезпека». ***Ключові слова***: кібербезпека, інформаційна безпека,

	криптографічний захист інформації, захист персональних даних, антивірусний захист, захист інформації, захист від несанкціонованого доступу, електронний цифровий підпис
Особливості програми	Програма передбачає вивчення: - законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; - принципів розробки, впровадженню, супроводу комплексних систем захисту інформації; - способів та засобів забезпечення кібербезпеки; - теорії, моделей та принципів управління доступом до інформаційних ресурсів; - методів та засобів оцінювання захищеності інформації; - методів та засобів криптографічного захисту інформації; - сучасних інформаційно-комунікаційних технологій; - організації електронного цифрового підпису в Україні і світі
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники підготовлені до роботи за національним класифікатором України: - професіонал із організації інформаційної безпеки; - професіонал із організації захисту інформації з обмеженим доступом; - науковий співробітник (інформаційна безпека); - фахівець з режиму секретності; - фахівець з досліджень та розробок; - інспектор з організації захисту секретної інформації
Подальше навчання	Можливість навчатися за програмою третього (освітньо-наукового) рівня вищої освіти
5 - Викладання та оцінювання	
Викладання та навчання	Лекції, практичні та лабораторні заняття, самонавчання, проектно-орієнтоване навчання, консультації із науково-педагогічними співробітниками, проведення наукових досліджень, підготовка атестаційної роботи
Оцінювання	Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано); 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F)
6 - Програмні компетентності	
Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	ЗК-1 Здатність застосовувати знання у практичних ситуаціях. ЗК-2 Здатність спілкуватися державною та іноземною мовою. ЗК-3 Навички використання інформаційних і телекомунікаційних технологій. ЗК-4 Здатність проведення досліджень на відповідному рівні. ЗК-5 Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК-6 Вміння виявляти, ставити та вирішувати проблеми. ЗК-7 Здатність приймати обґрунтовані рішення.

Фахові компетентності спеціальності (ФК)	ФК-1 Здатність застосовувати відповідні математичні, наукові і технічні методи, а також комп'ютерне програмне забезпечення для вирішення завдань в сфері інформаційної та кібербезпеки; ФК-2 Здатність продемонструвати практичні навички в сфері інформаційної та кібербезпеки; ФК-3 Здатність продемонструвати знання і розуміння наукових фактів, концепцій, теорій, принципів і методів, необхідних для підтримки спеціалізацій з інформаційної та кібербезпеки; ФК-4 Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному/кібернетичному простору та інформаційним ресурсам. ФК-5 Здатність продемонструвати розуміння проблем інформаційної та кібербезпеки; ФК-6 Здатність продемонструвати розуміння питань використання технічної літератури та інших джерел інформації ФК-7 Здатність виявляти і описувати ефективність рішень в сфері інформаційної та кібербезпеки на основі використання аналітичних методів і методів моделювання; ФК-8 Здатність продемонструвати знання і розуміння математичних принципів і методів, необхідних для підтримки спеціалізацій з інформаційної та кібербезпеки; ФК-9 Здатність розробляти плани і проекти для забезпечення досягнення поставленої певної мети з урахуванням всіх аспектів вирішуваної проблеми ФК-10 Здатність продемонструвати розуміння вимог до діяльності в сфері інформаційної та кібербезпеки; ФК-11 Здатність продемонструвати обізнаність з питань авторського права.
7 - Програмні результати навчання	
	ПРН - 1 Знання і розуміння сучасних методів ведення науково-дослідних робіт, організації та планування експерименту, фізико-математичних методів, що застосовуються в інженерній і дослідницькій практиці, на рівні, необхідному для досягнення інших результатів освітньої програми
	ПРН - 2 Здатність аналізувати складні інженерні продукти, процеси і системи відповідно до спеціалізації; обирати і застосовувати придатні типові аналітичні, розрахункові та експериментальні методи; правильно інтерпретувати результати таких досліджень
	ПРН – 3 Здатність виявляти, формулювати і вирішувати завдання в сфері інформаційної та кібербезпеки відповідно до спеціалізації; обирати і застосовувати адекватні аналітичні, розрахункові та експериментальні методи
	ПРН – 4 Здатність розробляти і проектувати, відповідно до спеціалізації, складні вироби, процеси і системи, які задовольняють встановлені вимоги
	ПРН – 5 Здатність виявляти, формулювати і вирішувати незнайомі складні задачі в умовах технічної невизначеності, обирати і застосовувати найбільш прийнятні і відповідні методи з відомих аналітичних, обчислювальних й експериментальних, або нових і новаторських
	ПРН – 6 Здатність здійснювати пошук літератури, консультуватися і критично використовувати наукові бази даних та інші відповідні джерела інформації, здійснювати моделювання та аналіз з метою детального вивчення і дослідження питань інформаційної та кібербезпеки відповідно до спеціалізацій

	ПРН – 7 Розуміння застосовуваних методик та методів аналізу, проектування і дослідження, а також обмежень їх використання
	ПРН – 8 Практичні навички вирішення складних завдань, реалізації складних інженерних проектів і проведення досліджень в сфері інформаційної та кібербезпеки
	ПРН – 9 Розуміння технічних наслідків діяльності в сфері інформаційної та кібербезпеки
	ПРН – 10 Здатність продемонструвати мовні компетентності, достатні для представлення та обговорення своїх наукових результатів іноземною мовою (англійською або іншою, відповідно до специфіки спеціальності) в усній та письмовій формах, а також для повного розуміння іншомовних наукових текстів
	ПРН – 11 Знати та уміти застосовувати засоби сучасних інформаційних технологій для вирішення задач в сфері інформаційної та кібербезпеки
	ПРН – 12 Орієнтуватися в патентній інформації і документації, досліджувати і правильно формувати ознаки новизни в об'єктах
8 – Ресурсне забезпечення реалізації	
Кадрове забезпечення	Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями та вченими званнями, які мають великий досвід навчально-методичної, науково-дослідної роботи та відповідають кваліфікації відповідно до спеціальності згідно ліцензійних умов.
Матеріально-технічне забезпечення	1.Забезпеченість приміщеннями для проведення навчальних занять та контрольних заходів. 2. Забезпеченість мультимедійним обладнанням для одночасного використання в навчальних аудиторіях. 3. Наявність соціально-побутової інфраструктури. 4. Забезпеченість здобувачів вищої освіти гуртожитком. 5. Забезпеченість комп'ютерними робочими місцями, лабораторіями, полігонами, обладнанням, устаткуванням, необхідними для виконання навчальних планів.
Інформаційне та навчально-методичне забезпечення	1. Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді. 2. Наявність доступу до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. 3. Наявність офіційного веб-сайту закладу освіти, на якому розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня/освітньо-наукова/ видавнича/ атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація). 4. Наявність електронного ресурсу закладу освіти, який містить навчально-методичні матеріали з дисциплін навчального плану, в тому числі в системі дистанційного навчання.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та закладами вищої освіти України.
Міжнародна кредитна	На основі двосторонніх договорів між Харківським національним

мобільність	університетом радіоелектроніки та закладами вищої освіти зарубіжних країн-партнерів.
Навчання іноземних здобувачів вищої освіти	На основі договорів (угод) між Харківським національним університетом радіоелектроніки та закладами вищої освіти іноземних країн.

2 Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОП			
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Дисципліни базової (професійної) підготовки за спеціальністю			
ОК 1.1	Основи наукових досліджень, організація науки та авторське право	4	Зл
ОК* 1.1	Українська мова як іноземна	4	Зл
ОК 1.2	Математичні методи моделювання	5	Ек
ОК 1.3	Передатестаційна практика	15	Зл
ОК 1.4	Атестаційна робота (проект)	15	Ек
Всього:		**39**	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
Дисципліни професійної та практичної підготовки за освітньою програмою Безпека інформаційних та комунікаційних систем за профілем випускової кафедри Безпека інформаційних технологій			
ОК 2.1	Завадозахищені комп'ютерні системи та мережі	4	Ек
ОК 2.2	Моделювання та оцінка ефективності засобів захисту інформації	6	Ек
ОК 2.3	Методи побудови і аналізу криптосистем	7	Ек
ОК 2.4	Моніторинг та аудит інформаційно-комунікаційних систем	4	Зл
ОК 2.5	Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	7	Зл
Всього:		**28**	
Загальний обсяг обов'язкових компонент:		**67**	
Вибіркові компоненти ОП			
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Гуманітарні та соціально-економічні дисципліни			
ВБ 1.1	Інтелектуальна власність	3	Зл
ВБ 1.2	Іноземна мова за професійним спрямуванням	3	Зл
ВБ 1.3	Філософські проблеми наукового пізнання	3	Зл
ВБ 1.4	Педагогіка вищої школи	3	Зл
ВБ 1.5	Економічне обґрунтування проектів	3	Зл
Всього		**3**	

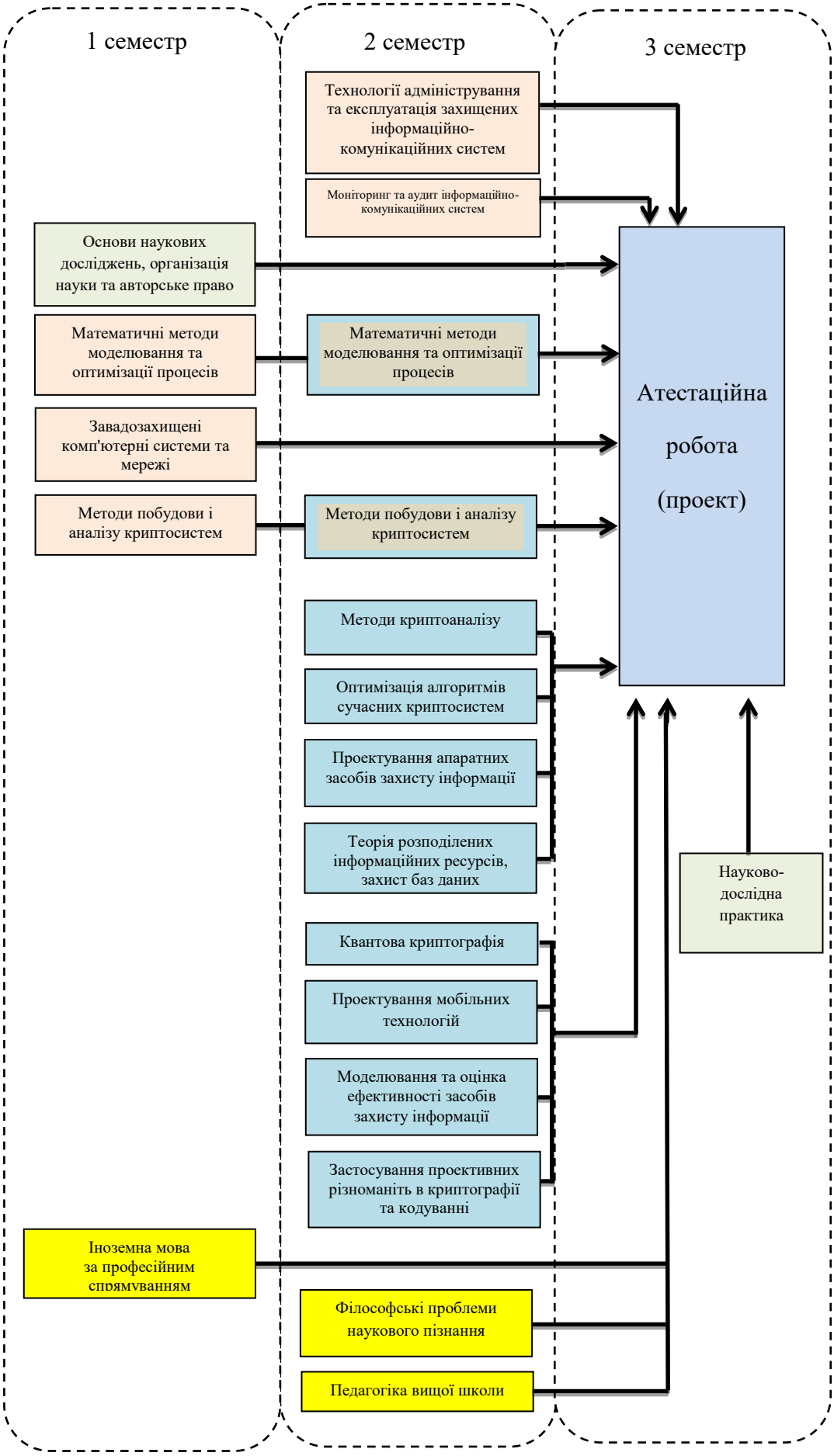
Дисципліни професійної та практичної підготовки за освітньою програмою Безпека інформаційних і комунікаційних систем			
ВБ 2.1	Оптимізація алгоритмів сучасних криптосистем	5	Зл
ВБ 2.2	Теорія розподілених інформаційних ресурсів, захист баз даних	5	Зл
ВБ 2.3	Методи криптоаналізу	5	Зл
ВБ 2.4	Квантова криптографія	5	Зл
ВБ 2.5	Проектування апаратних засобів захисту інформації	5	Зл
ВБ 2.6	Проектування мобільних технологій	5	Зл
ВБ 2.7	Методи захисту децентралізованих систем та мереж	5	Зл
ВБ 2.8	Застосування проектних різноманіть в криптографії та кодуванні	5	Зл
Всього		**20**	
Загальний обсяг вибіркових компонент:		**23**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**90**	

* – тільки для здобувачів іноземців,

2.1. Структурно-логічна схема ОП

1 семестр	2 семестр	3 семестр
ОК 1.1. ОК* 1.1. ОК 1.2. ОК 2.1. ОК 2.2. ОК 2.3. ВБ 2.1., ВБ 2.2. ВБ 2.3., ВБ 2.4.	ОК 2.4. ОК 2.5. ОК 2.2. ОК 2.3. ВБ 1.1., ВБ 1.2., ВБ 1.3., ВБ 1.4., ВБ 1.5. ВБ 2.5., ВБ 2.6. ВБ 2.7., ВБ 2.8.	ОК 1.3. ОК 1.4.

2.2 Структурно-логічна схема ОПП



3 Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Безпека інформаційних і комунікаційних систем» спеціальності 125 Кібербезпека проводиться у формі захисту атестаційної роботи та завершується видачею документу встановленого зразка про присудження йому ступеня магістра із присвоєнням кваліфікації: Магістр, Кібербезпека, Безпека інформаційних і комунікаційних систем.

Атестація здійснюється відкрито і публічно.

4 Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1.1	ОК* 1.1	ОК 1. 2	ОК 1. 3	ОК 1.4	ОК 2.1	ОК 2.2	ОК 2.3	ОК 2.4	ОК 2.5	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ВБ 1.5	ВБ 2.1	ВБ 2.2	ВБ 2.3	ВБ 2.4	ВБ 2.5	ВБ 2.6	ВБ 2.7	ВБ 2.8
ЗК-1			*	*	*				*	*	*	*		*	*	*	*	*		*	*		
ЗК-2						*				*													
ЗК-3				*	*					*												*	*
ЗК-4			*		*					*					*								
ЗК-5	*								*	*	*												
ЗК-6	*			*			*			*		*			*				*				
ЗК-7	*		*		*		*	*		*			*	*		*			*				
ФК-1	*		*					*		*													
ФК-2			*	*	*	*	*		*	*		*					*	*		*			
ФК-3	*				*					*	*			*				*					
ФК-4			*	*	*					*		*					*	*				*	
ФК-5			*	*	*					*		*											
ФК-6			*		*					*	*				*	*							
ФК-7	*		*	*	*					*													
ФК-8	*									*					*	*			*				
ФК-9				*				*		*									*			*	*
ФК-10			*	*			*			*		*											
ФК-11			*				*			*													

5 Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

	ОК 1.1	ОК* 1.1	ОК 1.2	ОК1. 3	ОК1. 4	ОК 2.1	ОК 2.2	ОК 2.3	ОК 2.4	ОК2.5	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ВБ 1.5	ВБ 2.1	ВБ 2.2	ВБ 2.3	ВБ 2.4	ВБ 2.5	ВБ 2.6	ВБ 2.7	ВБ 2.8
ПРН - 1	*				*			*							*	*			*				*
ПРН - 2			*	*	*	*				*	*	*							*		*		
ПРН - 3		*	*		*	*		*	*	*												*	
ПРН - 4			*	*			*								*	*							*
ПРН - 5	*		*	*	*					*			*	*						*	*		
ПРН - 6	*		*			*				*			*	*			*	*				*	
ПРН - 7				*	*			*		*											*		
ПРН - 8			*	*	*			*	*	*													
ПРН - 9			*	*	*		*			*	*	*			*	*							
ПРН-10			*			*		*		*					*	*	*	*	*			*	*
ПРН-11			*	*	*		*											*					
ПРН-12									*	*											*		