2017/2018

КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

ЗАТВЕРДЖЕНО
Рішенням Вченої ради Київського
університету імені Бориса Грінченка
«23» листопада 2017 р., протокол № 11
Голова вченої ради
_____ В. О. Огнев'юк

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
125.00.01 Безпека інформаційних і комунікаційних систем другого (магістерського) рівня вищої освіти

за спеціальністю:	**125 Кібербезпека**
галузі знань:	**12 Інформаційні технології**
освітньої кваліфікації:	**магістр з кібербезпеки**
професійної кваліфікації:	**не врегульована**

Введено в дію з «01» вересня 2018 р.
(наказ від «24» листопада 2017 р. № 762)

Київ 2018

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Кафедра інформаційних технологій і математичних дисциплін Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка
Протокол №3 від "04" 10 2017 р.
Завідувач кафедри _____ О.С.Литвин

Вчена рада Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка
Протокол №2 від "18" жовтня 2017 р.
Голова Вченої ради _____ А.В. Михацька

Науково-методичний центр стандартизації та якості освіти

Завідувач _____ О.В. Леонтьєва
22.11. 2017 р.

Проректор з науково-методичної та навчальної роботи

_____ О.Б. Жильцов
22.11. 2017 р.

НДЛ інтернаціоналізації вищої освіти

Завідувач _____ О.С. Виговська
___.___. 2017 р.

Проректор з наукової роботи

_____ Н.М. Віннікова
___.___. 2017 р.

ПЕРЕДМОВА

Освітньо-професійну програму розроблено на підставі Закону України від 01.07.2015 №1556-VII «Про вищу освіту» з урахуванням вимог проекту Стандарту вищої освіти з підготовки бакалаврів спеціальності 125 Кібербезпека від __.__.201_ №_____ робочою групою у складі:

Керівник робочої групи:
БУРЯЧОК Володимир Леонідович, доктор технічних наук, професор, професор кафедри інформаційних технологій і математичних дисциплін Київського університету імені Бориса Грінченка

Члени робочої групи:
БЕССАЛОВ Анатолій Володимирович, доктор технічних наук, професор, професор кафедри інформаційних технологій і математичних дисциплін Київського університету імені Бориса Грінченка

ТОЛЮПА Сергій Васильович, доктор технічних наук, професор, професор кафедри інформаційних технологій і математичних дисциплін Київського університету імені Бориса Грінченка (за сумісництвом)

АБРАМОВ Вадим Олексійович, кандидат технічних наук, доцент, доцент кафедри інформаційних технологій і математичних дисциплін Київського університету імені Бориса Грінченка

Рецензенти:

1. СМІРНОВ Олексій Анатолійович, доктор технічних наук, професор, завідуючий кафедрою кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, м. Кропивницький

2. ТАТЬЯНІН В'ячеслав Вікторович, кандидат технічних наук, старший науковий співробітник, директор ТОВ «АВТОР», м. Київ

Освітньо-професійна програма вводиться вперше.
Термін перегляду освітньо-професійної програми ___ раз на ___ роки

Актуалізовано:

Дата перегляду ОПП/ внесення змін до ОПП			
Підпис			
ПІБ гаранта ОПП			

1. Профіль освітньої-професійної програми зі спеціальності 125 «Кібербезпека»

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Київський університет імені Бориса Грінченка Факультет інформаційних технологій та управління
Ступінь вищої освіти та назва кваліфікації	магістр, магістр з кібербезпеки професійна кваліфікація не врегульована
Офіційна назва освітньо-професійної програми	125.00.02 Безпека інформаційних і комунікаційних систем
Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці
Наявність акредитації	Впровадження в 2018 році
Цикл/рівень	Другий (магістерський) рівень / FQ-EHEA – другий цикл, QF LLL – 7 рівень, НРК – 8 рівень
Передумови	Ступінь бакалавра
Мова(и) викладання	Українська
Термін дії освітньо-професійної програми	2021 р.
Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://kubg.edu.ua/
2 – Мета освітньо-професійної програми	
Забезпечити студентам фундаментальну підготовку у вигляді поглиблених теоретичних і практичних знань, умінь та навичок за спеціальністю 125 Кібербезпека, достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузях телекомунікацій та інформаційних технологій.	
3 - Характеристика освітньо-професійної програми	
Предметна область: 12 Інформаційні технології 125 Кібербезпека 125.00.01 Безпека інформаційних і комунікаційних систем	*Об'єкти професійної діяльності випускників:* – 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. *Цілі навчання* підготовка професіоналів, здатних використовувати і впроваджувати технології та застосовувати засоби інформаційної та/або кібербезпеки. *Теоретичний зміст предметної діяльності.* Знання: – 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 ІР; – 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-комуніка-

	ційних технологій; – автоматизованих систем проектування. *Методи, методики та технології:* методи, методики та технології забезпечення інформаційної та/або кібербезпеки. *Інструменти та обладнання:* системи розробки, забезпечення, моніторингу та контролю інформаційної та/або кібербезпеки; сучасне програмно-апаратне забезпечення інфокомунікаційних технологій. *Співвідношення обсягів загальної, професійної та вибіркової частин:* Обов'язкова частина (63 кредити, 70 %): – цикл дисциплін професійно орієнтованої гуманітарної, соціально-економічної та природничо-наукової підготовки (13 кредитів ЄКТС, 390 год.); – цикл дисциплін спеціальної підготовки (20 кредитів ЄКТС, 600 год.) та фахової спеціалізації (12 кредитів ЄКТС, 360 год.) з написанням 1 курсової роботи у 9 семестрі та випускової магістерської роботи (6 кредитів ЄКТС, 180 год.). Частка науково-дослідницької (11 семестр), виробничої (технологічної) (11 семестр) та переддипломної практик (11 семестр): 12 кредитів ЄКТС, 13 %, 360 годин. Вибіркова частина (27 кредитів, 30 %). З них в спеціалізованому блоці навчальних дисциплін: – дисципліни курсової підготовки (8 кредитів ЄКТС, 240 год.); – дисципліни спеціалізованого курсу (19 кредитів ЄКТС, 510 год.).
Орієнтація освітньо-професійної програми	Освітньо-професійна програма з прикладною спрямованістю за спеціалізацією безпека інформаційних і комунікаційних систем.
Основний фокус освітньо-професійної програми та спеціалізації	Загальна: дослідження в області практики та науки захисту інформації, організації та забезпечення інформаційної та/або кібербезпеки об'єктів, що підлягають захисту.
Особливості програми	З метою підготовки до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації магістр з кібербепеки, програма забезпечує підготовку професіоналів, здатних: – виявляти та оцінювати ознаки стороннього кібернетичного впливу; – моделювати можливі ситуації стороннього кібернетичного впливу та прогнозувати їх можливі наслідки; – організовувати і підтримувати комплекс заходів щодо забезпечення інформаційної та/або кібербезпеки; – проводити дослідження у напрямах забезпечення інформаційної та/або кібербезпеки національних інтересів України й обґрунтовувати шляхи підвищення їх ефективності; – протидіяти несанкціонованому проникненню протиборчих сторін до власних ІТ систем і мереж, забезпечити стійкість їх роботи, а також відновлення їх нормального функціонування після здійснення кібернападів; – забезпечити криптозахист власного інформаційного ресурсу тощо. З метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу програма передбачає: - реалізацію процесного підходу при конструюванні змісту профільно-орієнтованих навчальних дисциплін, студентської мобільності, академічної співпраці та молодіжних обмінів; - залучення до викладацької діяльності керівників та професіоналів, які працюють як в системі професійної освіти, так й на виробництві в галузі інформаційних технологій та телекомунікацій, а також представників бізнесу.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники можуть працювати в державному та приватному секторах Києва, України та Європейського Союзу у таких сферах діяльності: 1) адміністрування ОС сімейства Windows/Linux, мережевого обладнання і технологій TCP/IP, DNS, DHCP, SSL/TLS, etc.;

	2) застосування засобів антивірусного захисту (ESET, McAfee, Zilly , etc.), програмних, клієнт-серверних та хмарних технологій захисту інформації (систем веб фільтрації, систем запобігання вторгнень, систем захисту пошти від вірусів і спаму, etc.); 3) створення технічної, проектної та експлуатаційної документації інформаційно-комунікаційних систем (далі – ІКС) та систем захисту інформації (далі – СЗІ); 4) налагодження, експлуатації та проведення аналізу системних процесів функціонування мережевих, клієнт-серверних та хмарних технологій; 5) проведення моніторингу несанкціонованої активності в обчислювальних системах; 6) створення, впровадження та експлуатації комплексних систем захисту інформації (далі – КСЗІ), а також СЗІ в складі інформаційно телекомунікаційних (далі – ІТС) та обчислювальних систем; 7) формування політик та процесів у сфері ІТ безпеки, управління доступом до мережевих ресурсів ІТС та ризиками інформаційної безпеки; 8) проведення розслідувань інцидентів та забезпечення аудиту процесів інформаційної безпеки; 9) підтримка наукових досліджень, педагогічна діяльність тощо. Згідно з Національним класифікатором професій ДК 003:2010 фахівці, які здобули освіту за освітньою програмою «Безпека інформаційних і комунікаційних систем» можуть обіймати такі первинні посади, як: - програміст/тестувальник програмного забезпечення систем інформаційної та кібербезпеки; - адміністратор комп'ютерних систем і мереж; - адміністратор інформаційної та кібербезпеки; - аудитор/пентестер безпеки інформаційно-комунікаційних систем; - розробник засобів захисту інформації; - провідний спеціаліст/керівник служби технічного захисту інформації тощо.	
Подальше навчання	Можливість здобуття освіти на третьому (освітньо-науковому) рівні вищої освіти за спеціальністю 125 «кібербезпека» або іншими спорідненими (суміжними) спеціальностями галузі знань «Інформаційні технології», що узгоджуються з отриманим дипломом магістра, іншими міждисциплінарними магістерськими програми з ІТ компонентою. Можливість підвищення кваліфікації та отримання додаткової післядипломної освіти.	
5 – Викладання та оцінювання		
Викладання та навчання	Ґрунтуються на принципах студентоцентризму та індивідуально-особистісного підходу; реалізуються через навчання на основі досліджень, посилення практичної орієнтованості та творчої спрямованості у формі комбінації лекцій, практичних занять, самостійної навчальної і дослідницької роботи з використанням елементів дистанційного навчання, розв'язування прикладних задач, виконання проектів, навчальних та виробничих практик, курсових робіт, кваліфікаційної магістерської роботи.	
Оцінювання	Накопичувальна бально-рейтингова система, що передбачає оцінювання студентів за усі види аудиторної та позааудиторної освітньої діяльності у вигляді вхідного, поточного, рубіжного та/або семестрового контролю та атестації.	
6 – Компетентності випускника		
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.	
Загальні компетентності (КЗ)	**ЗК-1**	Здатність до професійного спілкування іноземною мовою
	ЗК-2	Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях
	ЗК-3	Здатність до виявлення, генерування, дослідження та вирішення

		проблем за професійним спрямуванням
Фахові компетентності спеціальності (КФ)	**ФК-1**	Здатність до застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації
	ФК-2	Здатність до виявлення уразливостей та забезпечення безпеки проводових і бездротових мереж, розслідування інцидентів інформаційної та/або кібербезпеки та протидії зловмисному програмному забезпеченню
	ФК-3	Здатність до забезпечення безпеки Web ресурсів, відновлення їх штатного функціонування в результаті збоїв та відмов різних класів і походження
	ФК-4	Здатність до забезпечення безпеки мережевих ресурсів та криптографічного захисту інформації в системах інформаційної та/або кібербезпеки
	ФК-5	Здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації
7 – Результати навчання		
Знання та розуміння	**ПРН-1**	- вміти застосовувати знання іноземних мов для забезпечення ефективності професійної комунікації; - вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; - вміти представляти отримані знання та навички з теорії та практики ІКБ в усній та/або письмових формах перед фаховою і нефаховою аудиторією;
	ПРН-2	- вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки; - вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні та/або безпекові технології у сфері захисту інформації; - знати уразливості й методи їх застосування в різних телекомунікаційних технологіях; - знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж; - вміти проектувати захищені (з урахуванням загроз) проводові телекомунікаційні системи; - знати методи організації захищеної передачі даних у незахищеному середовищі;
	ПРН-3	- знати уразливості й методи їх застосування в безпроводових і мобільних мережах; - вміти виявляти загрози проникнення або доступу зловмисників до таких мереж; - знати спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки безпроводових і мобільних мереж; - вміти проектувати захищені (з урахуванням загроз) безпроводові мережі;
	ПРН-4	- знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, firewalls, сніфери, сканери портів);
	ПРН-5	- вміти проводити семантичний аналіз файлів; - вміти виявляти злоякісне програмне забезпечення й файли за їх структурою та поведінкою; - вміти відновлювати пошкоджену інформацію; - вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ;

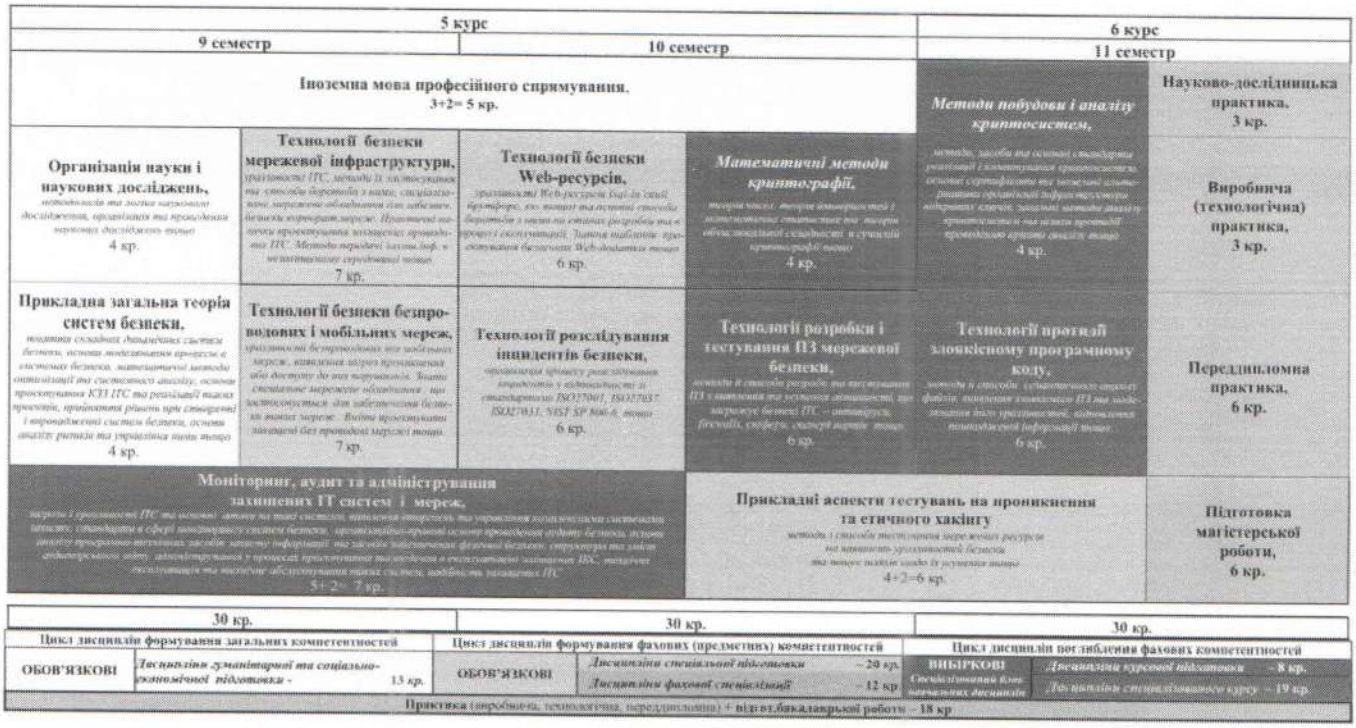
	ПРН-6	- знати існуючі уразливості Web ресурсів (sql ін'єкції, брутфорс, xss й т.д) та способи боротьби з ними на етапі розробки та в процесі експлуатації; - знати шаблони проектування безпечних Web додатків;
	ПРН-7	- знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки; - вміти знаходити шляхи для їх усунення;
	ПРН-8	- вміти організовувати процеси розслідування інцидентів у відповідності зі стандартами ISO 27001, ISO 20000, ISO/IEC TR 18044, NIST SP 800-61, CMU/SEI-2004-TR-015, ISO 27035, ISO 27037. ISO 27031;
	ПРН-9	- володіти практичними навичками проведення аудиту безпеки ІКС, їх адміністрування та експлуатації; - вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.
8 – Ресурсне забезпечення реалізації програми		
Кадрове забезпечення	Кадрове забезпечення освітньо-професійної програми складається головним чином з професорсько-викладацького складу кафедри інформаційної та кібернетичної безпеки. До викладання окремих дисциплін відповідно до їх компетенції та досвіду залучений професорсько-викладацький склад кафедри інформаційних технологій та математичних дисциплін ФІТУ Університету. Практико-орієнтований характер ОПП передбачає широку участь фахівців-практиків, що відповідають напряму програми, що підсилює синергетичний зв'язок теоретичної та практичної підготовки. Керівник проектної групи та викладацький склад, який забезпечує її реалізацію, відповідає вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності закладів освіти.	
Матеріально-технічне забезпечення	Спеціально обладнані апаратно-програмним забезпеченням, наочними та методичними матеріалами центри розвитку компетентностей, а саме: 1) «Центр дослідження технологій функціонування й захисту інформаційно-комунікаційних систем та мереж» з: навчальною «Лабораторією комп'ютерних мереж та кібербезпеки», навчальною «Лабораторією безпеки інформаційно-комунікаційних систем» та навчальною «Лабораторією антивірусного захисту»; 2) «Центр дослідження технологій захисту інформаційних ресурсів» з: навчальною «Лабораторією безпеки інформаційних активів» (навчальний кіберполігон) та навчальною «Лабораторією систем технічного та криптографічного захисту інформації»; 3) «Центр моделювання та програмування» 4) «Лабораторія вбудованих систем і 3Д моделювання» тощо.	
Інформаційне та навчально-методичне забезпечення	Бібліотечні електронні ресурси, електронні наукові видання, електронні навчальні курси із можливістю дистанційного навчання та самостійної роботи, хмарні сервіси Microsoft.	
9 – Академічна мобільність		
Національна кредитна мобільність	Положення про порядок реалізації права на академічну мобільність учасників освітнього процесу Університету введено в дію наказом від 30.09.2016 р	
Міжнародна кредитна мобільність	Укладено угоди, які передбачають студентську мобільність із університетами європейських країн та в рамках програми Еразмус+КА1. З них: Вільнюський університет (Литва), Університет Костянтина Філософа у Нітрі (Словаччина), Університет Естремадура (Іспанія), Сілезький університет в Катовіцах (Польща), Академія імені Яна Длугоша в Ченстохові (Польща), Університет Острави (Чехія), Університет Париж-Сорбонна (Франція), Ліссабонський університет (Португалія) та інші.	
Навчання іноземних здобувачів вищої освіти	Згідно ліцензії передбачається підготовка іноземців та осіб без громадянства.	

2. Перелік компонентів освітньо-професійної програми та їх логічна послідовність

2.1. Перелік та розподіл кредитних обсягів дисциплін
навчального плану підготовки здобувачів другого рівня вищої освіти – магістр,
за спеціальністю – 125 «Кібербезпека» (90 кредитів ECTS - 1 рік 4 місяці)

Шифр н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС/ %	Розподіл годин на за курсами і семестрами			Форма підсумкового контролю
			5 курс		6 курс	
			семестри			
			9	10	11	
1.	**ОБОВ'ЯЗКОВА ЧАСТИНА**					
	1. Навчальні дисципліни					
	Формування спеціальних (фахових, предметних) компетентностей					
ОДФ.01	Іноземна мова професійного спрямування	5	3	2		залік
ОДФ.02	Організація науки і наукових досліджень	4	4			залік
ОДФ.03	Прикладна загальна теорія систем безпеки	4	4			екзамен
ОДФ.04	Технології безпеки мережевої інфраструктури	7	7			екзамен, КР
ОДФ.05	Технології безпеки безпроводових і мобільних мереж	7	7			залік
ОДФ.06	Технології безпеки Web-ресурсів	6		6		екзамен
ОДФ.07	Технології розслідування інцидентів безпеки	6		6		залік
ОДФ.08	Прикладні аспекти тестувань на проникнення та етичного хакінгу	6		4	2	залік, екзамен
	Всього	**45**	**25**	**18**	**2**	
	2. Практика					
ОП.01	Виробнича (технологічна) практика	3			3	залік
ОП.02	Науково-дослідницька практика	3			3	залік
ОП.03	Переддипломна практика	6			6	залік
	Всього	**12**	**0**	**0**	**12**	
	3. Атестація					
ОА.1	Підготовка кваліфікаційної магістерської роботи	4,5		4,5		
	Захист кваліфікаційної магістерської роботи	1,5			1,5	
	Всього	**6**	**0**	**4,5**	**1,5**	
Загальний обсяг обов'язкової частини		63	**25**	**22,5**	**15,5**	
2	**ВИБІРКОВА ЧАСТИНА**					
	4. Навчальні дисципліни					
	4.1. Спеціалізований блок начальних дисциплін					
ВДС.01	Моніторинг, аудит та адміністрування захищених ІТ систем і мереж	7	5	2		залік, екзамен
ВДС.02	Технології розробки і тестування ПЗ мережевої безпеки	6		6		екзамен
ВДС.03	Технології протидії злоякісному програмному коду	6			6	екзамен
ВДС.04	Математичні методи криптографії	4		4		залік
ВДС.05	Методи побудови і аналізу криптосистем	4			4	залік
	Всього	**27**	**5**	**12**	**10**	
	4.2. Вибір дисциплін із каталогу (студент обирає дисципліни на відповідну кількість кредитів)					
ВД 1.01	Вибір з каталогу курсів	27	5	12	**10**	залік, екзамен
Загальний обсяг вибіркової частини		27				
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		90	**30**	**34,5**	**25,5**	

2.2. Суктурно-логічна схема ОПП



3. Форма атестації здобувачів вищої освіти

Атестація здобувачів вищої освіти за освітньо-професійною програмою 125.00.02 «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека» проводиться екзаменаційною комісією відповідно до вимог програми. До складу екзаменаційної комісії можуть включатися представники роботодавців та їх об'єднань, відповідно до положення про екзаменаційну комісію, затвердженого вченою радою ВНЗ.

До атестації допускаються студенти, які виконали всі вимоги програми підготовки (навчального плану). На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання. Термін проведення атестації визначається навчальним планом та графіком освітнього процесу.

Атестація здійснюється відкрито у формі публічного захисту кваліфікаційної магістерської роботи. Атестація завершується видачею документу встановленого зразка про присудження особі, яка успішно виконала освітньо-професійну програму, ступеня магістр із присвоєнням їй кваліфікації: «магістр з кібербезпеки».

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	ЗК1	ЗК2	ЗК3	ФК1	ФК2	ФК3	ФК4	ФК5
ОДФ.01	+							
ОДФ.02		+						
ОДФ.03			+					+
ОДФ.04				+				+
ОДФ.05					+			+
ОДФ.06						+		
ОДФ.07					+			+
ОДФ.08							+	+
ВДС.01								+
ВДС.02					+			
ВДС.03					+			
ВДС.04							+	
ВДС.05							+	
ОП.01	+	+	+	+				
ОП.02			+	+	+	+		
ОП.03	+	+	+	+	+	+	+	+
ОА.1	+	+	+	+	+	+	+	+

5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньо-професійної програми

	ПРН -1	ПРН -2	ПРН -3	ПРН -4	ПРН -5	ПРН -6	ПРН -7	ПРН -8	ПРН -9
ОДФ.01	+								
ОДФ.02	+	+							
ОДФ.03	+								
ОДФ.04		+	+				+		+
ОДФ.05			+						+
ОДФ.06						+			
ОДФ.07								+	+
ОДФ.08				+	+				+
ВДС.01									+
ВДС.02		+		+					
ВДС.03		+		+	+				
ВДС.04									+
ВДС.05									+
ОП.01	+	+	+	+	+	+	+	+	+
ОП.02	+	+	+	+	+	+	+	+	+
ОП.03	+	+	+	+	+	+	+	+	+
ОА.1	+	+	+	+	+	+	+	+	+

Керівник проектної групи (гарант освітньо-професійної програми)
Професор кафедри Інформаційних технологій та математичних дисциплін Факультету Інформаційних технологій та управління Київського університету імені Бориса Грінченка
доктор технічних наук, професор **В.Л. БУРЯЧОК**