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 першого (бакалаврського) рівня вищої освіти

Галузь знань: 12 Інформаційні технології

Спеціальність: 125 Кібербезпека

Кваліфікація: бакалавр з кібербезпеки

3439 фахівець із організації інформаційної безпеки

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:
СЕМКО Віктор Володимирович, доктор технічних наук, доцент, доцент кафедри управління 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

МЕЛЬНИК Ірина Юріївна, кандидат технічних наук, доцент, доцент кафедри інформаційних технологій і математичних дисциплін Київського університету імені Бориса Грінченка

ЄРМОШИН Валерій Віталійович, кандидат технічних наук, доцент кафедри інформаційних технологій і математичних дисциплін Київського університету імені Бориса Грінченка (за сумісництвом)

Зовнішні рецензенти:
1. ХОРОШКО Володимир Олексійович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Київського національного авіаційного університету, м. Київ
2. РОЙ Яніна Володимирівна, кандидат технічних наук, аналітик з інформаційної безпеки ТОВ «SI Center», 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 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	бакалавр, бакалавр з кібербезпеки фахівець із організації інформаційної безпеки
Офіційна назва освітньо-професійної програми	125.00.01 Безпека інформаційних та комунікаційних систем
Тип диплому та обсяг освітньо-професійної програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	Впровадження в 2018 році
Цикл/рівень	Перший (бакалаврський) рівень / FQ-EHEA – перший цикл, EQF LLL – 6 рівень, НРК – 7 рівень
Передумови	Повна загальна середня освіта. Фахова передвища освіта за ступенем молодшого бакалавра або молодшого спеціаліста
Мова(и) викладання	Українська
Термін дії освітньо-професійної програми	2023 р.
Інтернет-адреса постійного розміщення опису освітньо-професійної програми	kubg.edu.ua
2 – Мета освітньо-професійної програми	
Забезпечити студентам якісну теоретичну та практичну підготовку у вигляді знань, умінь та навичок за спеціальністю 125 Кібербезпека для організації та забезпечення інформаційної безпеки на об'єктах інформаційної діяльності	
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 фахівців, здатних використовувати і впроваджувати технології 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 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. *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 інформаційно-комунікаційних технологій. *Співвідношення обсягів загальної і професійної складових та вибіркової частини:* Обов'язкова частина (180 кредитів, 75 %): – цикл дисциплін гуманітарної та соціально-економічної підготовки (32 кредитів ЄКТС, 960 год.); – цикл дисциплін фундаментальної та природничо-наукової підготовки (28 кредитів ЄКТС, 840 год.); – цикл дисциплін професійної та практичної підготовки за спеціальністю (73 кредити ЄКТС, 2190 год.) та фаховою спеціалізацією (30 кредитів ЄКТС, 900 год.) з написанням 2 курсових робіт у 3 та 5 семестрах та випускової бакалаврської роботи (6 кредитів ЄКТС, 180 год.). Частка виробничої (4 семестр), технологічної (6 семестр) та переддипломної практик (8 семестр): 15 кредитів ЄКТС, 450 годин. Вибіркова частина (60 кредитів, 25 %). З них спеціалізований блок навчальних дисциплін – 60 кредитів ЄКТС, 1800 год.).
Орієнтація освітньо-професійної програми	Освітньо-професійна програма з прикладною спрямованістю за напрямком - 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 на об'єктах інформаційної діяльності
Особливості програми	З метою підготовки до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації бакалавр з кібербезпеки програма передбачає надання студентам: - системних теоретичних знань в галузі IT технологій із поглибленим вивченням спеціалізації безпека інформаційних і комунікаційних систем; - сучасних компетентностей та практичних навичок з програмування, розробки та управління базами даних, формування моделей захисту інформації та політик безпеки, технічного і криптографічного захисту інформації, побудови захищених IP і TCP мереж та обслуговування сертифікатів відкритих ключів, побудови комплексних систем захисту інформації (далі – КСЗІ) на об'єктах інформаційної діяльності та захисту автоматизованих систем від несанкціонованого доступу, тестування систем захисту інформаційно-комунікаційних систем (далі – ІКС) на проникнення, реалізації управління інформаційною та кібернетичною безпекою, адміністрування захищених ІКС, проведення їх моніторингу та аудиту 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 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 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 ІКБ; адміністратор комп'ютерних систем і мереж; адміністратор інформаційної та кібербезпеки; аудитор безпеки інформаційно-комунікаційних систем; розробник засобів захисту інформації; інженер служби технічного захисту інформації тощо.	
Подальше навчання	Можливість здобуття освіти на другому (магістерському) рівні за спеціальністю 125 «кібербезпека» або іншими спорідненими (суміжними) спеціальностями галузі знань «Інформаційні технології», що узгоджуються з отриманим дипломом бакалавра, а також за іншими міждисциплінарними магістерськими програми з ІТ компонентою.	
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, бакалаврської 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, а також атестації.	
6 – Компетентності випускника		
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 (КЗ)	**ЗК-1**	Здатність застосовувати знання у практичних ситуаціях.
	ЗК-2	Знання та розуміння предметної області та розуміння професії.
	ЗК-3	Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово
	ЗК-4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням
	ЗК-5	Здатність до пошуку, оброблення та аналізу інформації.
	ЗК-6	Вміння керувати проектами та вести підприємницьку діяльність
Фахові компетентності спеціальності (КФ)	**ФК-1**	Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
	ФК -2	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.
	ФК -3	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
	ФК -4	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
	ФК -5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
	ФК -6	Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз,

		здійснення кібератак, збоїв та відмов різних класів та походження.
	ФК -7	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
	ФК -8	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку
	ФК -9	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
	ФК -10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
	ФК -11	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
	ФК -12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної та/або кібербезпеки.
7 – Результати навчання		
Знання та розуміння	**ПРН-1**	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної та/або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної та/або кібербезпеки;
	ПРН-2	- здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; - розробляти та аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; - застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем; - здійснювати захист ресурсів і процесів в ІТС на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші), а також встановлених режимів безпечного функціонування ІТС; - виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної та/або кібербезпеки в ІТС;
	ПРН-3	- забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - виконувати розробку експлуатаційної документації на КЗЗ;
	ПРН-4	- вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); - вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в ІТС;

ПРН-5	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної і кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах - проектувати та реалізувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; - вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах;
ПРН-6	- вирішувати задачі управління процесами забезпечення неперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів; - вирішувати задачі корекції цілей, стратегій, планів забезпечення неперервності бізнесу після здійснення кібератак, збоїв та відмов різних класів; - створювати і впроваджувати плани процесу забезпечення неперервності бізнесу; - виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання;
ПРН-7	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - здійснювати оцінку рівня захищеності інформації що обробляється в ІТС використовувати інструментальні засоби оцінювання наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих); - вирішувати задачі експертизи, випробування КСЗІ;
ПРН-8	- вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - проводити розслідування інцидентів інформаційної та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної та/або кібербезпеки; - забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації;
ПРН-9	- забезпечувати неперервність бізнес процесів організації на базі системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів; - забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки;
ПРН-10	- аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації; - аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації; - виявляти небезпечні сигнали технічних засобів; - вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами; - визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;

		- інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; - обґрунтовувати можливість створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; - впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами;
	ПРН-11	- забезпечувати процеси моніторингу доступу до ресурсів і процесів ІТС; - забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в ІТС;
	ПРН-12	- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних та автоматизованих системах; - аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в ІТС - аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.
8 – Ресурсне забезпечення реалізації програми		
Кадрове забезпечення	Кадрове забезпечення освітньо-професійної програми складається головним чином професорсько-викладацького складу кафедри інформаційної та кібернетичної безпеки До викладання окремих дисциплін відповідно до їх компетенції та досвіду залучені 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, які 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 кібер-полігон) 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), Лісабонський університет (Португалія) та інші.	
Навчання іноземних здобувачів вищої освіти	Згідно ліцензії передбачається підготовка іноземців та осіб без громадянства.	

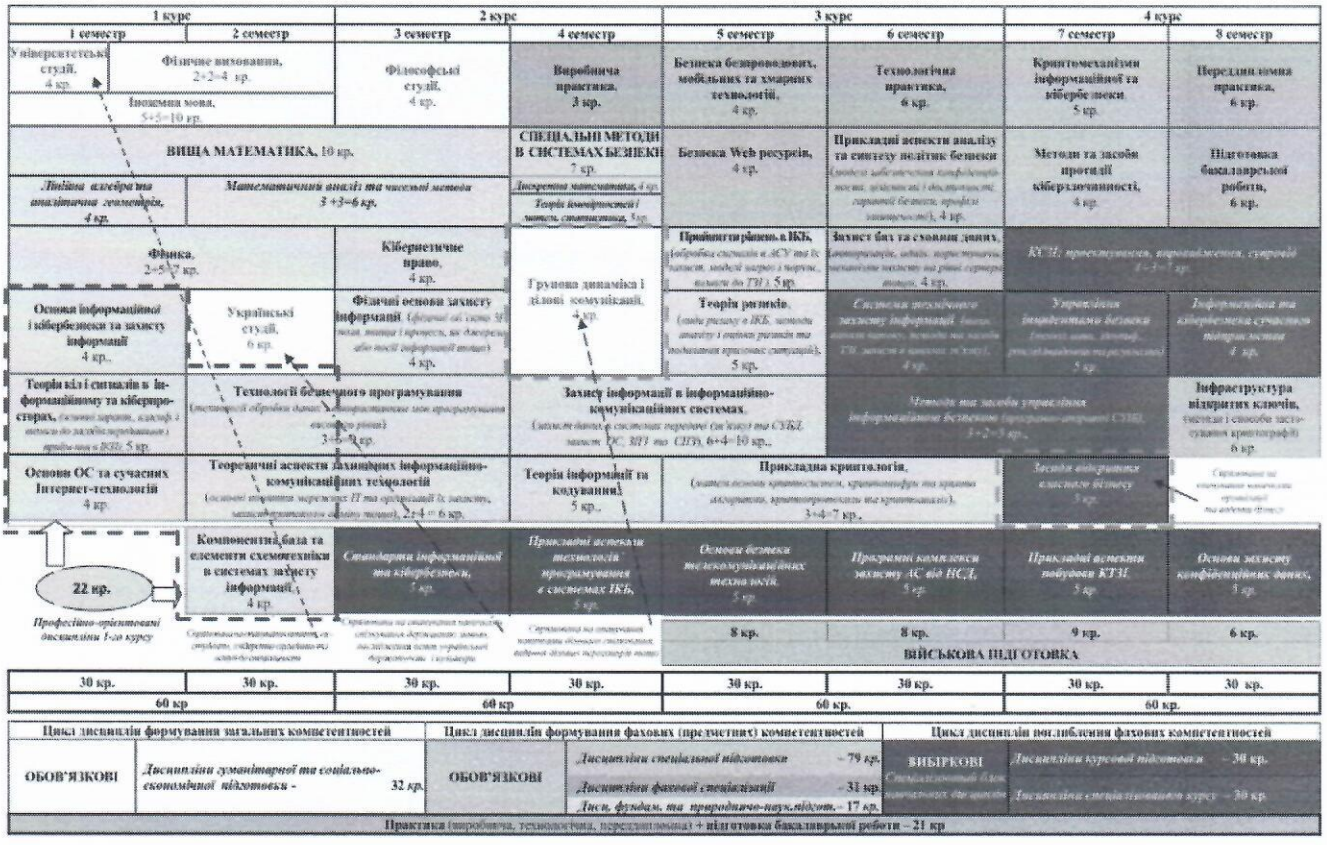
2. Перелік компонентів освітньо-професійної програми та їх логічна послідовність

2.1. Перелік та розподіл кредитних обсягів дисциплін навчального плану підготовки здобувачів першого рівня вищої освіти – бакалавр, за спеціальністю – 125 «Кібербезпека» (240 кредитів ECTS - 3 роки 10 місяців)

Код	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	кредитів	Розподіл аудиторних годин за курсами і семестрами								Форма підсумкового контролю
			1 курс		2 курс		3 курс		4 курс		
			1	2	3	4	5	6	7	8	
І. Обов'язкова частина											
1. Навчальні дисципліни											
Формування загальних компетентностей											
ОДЗ.01	Університетські студії	**4**	4								залік
	Я - студент	1	*								
	Лідерство служіння	1	*								
	Вступ до спеціальності	2	*								
ОДЗ.02	Іноземна мова	**10**	5	5							екзамен, залік
ОДЗ.03	Фізичне виховання	**4**	2	2							залік
ОДЗ.04	Українські студії	**6**		6							екзамен
ОДЗ.05	Філософські студії	**4**			4						екзамен
ОДЗ.06	Групова динаміка і ділові комунікації	**4**				4					залік
	Всього	**32**	**11**	**13**	**4**	**4**	**0**	**0**	**0**	**0**	
Формування спеціальних (фахових, предметних) компетентностей											
ОДС.01	Фізика	**7**	2	5							екзамен, залік
ОДС.02	Вища математика	**10**	4	3	3						залік. екзамен
	Лінійна алгебра та аналітична геометрія	4	*								
	Математичний аналіз та чисельні методи	6		*	*						
ОДС.03	Основи інформаційної і кібербезпеки та захисту інформації	**4**	4								залік
ОДС.04	Теорія кіл і сигналів в інформаційному та кіберпросторах	**5**	5								екзамен
ОДС.05	Основи ОС та сучасних Інтернет-технологій	**4**	4								залік
ОДС.06	Технології безпечного програмування	**9**		3	6						екзамен, залік, КР
ОДС.07	Теоретичні аспекти захищених інформаційно-комунікаційних технологій	**6**		2	4						екзамен, залік
ОДС.08	Компонентна база та елементи схемотехніки в сист.захисту інформації	**4**		4							екзамен
ОДС.09	Кібернетичне право	**4**			4						залік
ОДС.10	Фізичні основи захисту інформації	**4**			4						екзамен
ОДС.11	Спеціальні методи в системах безпеки	**7**				7					екзамен
	Дискретна математика	4				*					
	Теорія ймовірностей та математична статистика	3				*					
ОДС.12	Захист інформації в інформаційно-комунікаційних системах	**10**				6	4				екзамен, залік, КР
ОДС.13	Теорія інформації та кодування	**5**				5					екзамен
ОДС.14	Прийняття рішень в інформаційній та кібербезпеці	**5**					5				екзамен
ОДС.15	Теорія ризиків	**5**					5				залік
ОДС.16	Прикладна криптологія	**7**					3	4			екзамен, залік
ОДС.17	Безпека безпроводових, мобільних та хмарних технологій	**4**					4				екзамен
ОДС.18	Безпека Web ресурсів	**4**					4				екзамен
ОДС.19	Прикладні аспекти аналізу та синтезу політик безпеки	**4**						4			екзамен
ОДС.20	Захист баз та сховищ даних	**4**						4			екзамен
ОДС.21	Криптомеханізми інформаційної та кібербезпеки	**5**							5		екзамен
ОДС.22	Методи та засоби протидії кіберзлочинності	**4**							4		екзамен
ОДС.23	Інфраструктура відкритих ключів	**6**								6	екзамен
	Всього	**127**	**19**	**17**	**21**	**18**	**25**	**12**	**9**	**6**	
2. Практика											
ВП.2.01	Виробнича	**3**				3					залік
ВП.2.02	Виробнича (технологічна)	**6**						6			залік
ВП.2.03	Переддипломна	**6**								6	залік
	Всього	**15**	**0**	**0**	**0**	**3**	**0**	**6**	**0**	**6**	

3. Атестація											
ОА.01	Підготовка бакалаврської роботи	**4,5**								4,5	
	Захист бакалаврської роботи	**1,5**								1,5	
Всього		**6**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**6**	
Разом за обов'язковою частиною		**180**	**30**	**30**	**25**	**25**	**25**	**18**	**9**	**18**	
ІІ. Вибіркова частина											
4. Навчальні дисципліни											
4.1. Спеціалізований блок навчальних дисциплін											
ВДК.1.01	Стандарти інформаційної та кібербезпеки	**5**			5						залік
ВДК.1.02	Прикладні аспекти побудови КТЗІ	**5**				5					екзамен
ВДК.1.03	Основи безпеки телекомунікаційних технологій	**5**					5				екзамен
ВДК.1.04	Програмні комплекси захисту АС від НСД	**5**						5			екзамен
ВДК.1.05	Прикладні аспекти програмування в системах ІКБ	**5**							5		екзамен
ВДК.1.06	Основи захисту конфіденційних даних	**5**								5	екзамен
ВДК.1.07	Системи технічного захисту інформації	**4**						4			залік
ВДК.1.08	Методи та засоби управління інформаційною безпекою	**5**						3	2		залік
ВДК.1.09	КСЗІ: проектування, впровадження, супровід	**7**							4	3	екзамен .КР
ВДК.1.10	Управління інцидентами безпеки	**5**							5		залік
ВДК.1.11	Засади відкриття власного бізнесу	**5**							5		залік
ВДК.1.12	Інформаційна та кібербезпека сучасного підприємства	**4**								4	залік
Всього		**60**	**0**	**0**	**5**	**5**	**5**	**12**	**21**	**12**	
4.2. Вибір дисциплін з каталогу (студент обирає дисципліни на відповідну кількість кредитів)											
ВД 1.01	Вибір з каталогу курсів	**60**			5	5	5	12	21	12	екзамен, залік, КР
Разом за вибірковою частиною		**60**	**0**	**0**	**5**	**5**	**5**	**12**	**21**	**12**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	**30**	**30**	**30**	**30**	**30**	**30**	**30**	**30**	

2.2. Структурно-логічна схема ОПП



3. Форма атестації здобувачів вищої освіти

Атестація здобувачів вищої освіти за освітньо-професійною програмою 125.00.01 Безпека інформаційних і комунікаційних систем спеціальності 125 «Кібербезпека» проводиться екзаменаційною комісією відповідно до вимог ОПП. 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 бакалаврської роботи.

Атестація завершується видачею документу встановленого зразка про присудження особі, яка успішно виконала освітньо-професійну програму ступеня бакалавра із присвоєнням їй кваліфікації: «бакалавр з кібербезпеки».

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	ЗК-1	ЗК-2	ЗК-3	ЗК-4	ЗК-5	ЗК-6	ФК-1	ФК-2	ФК-3	ФК-4	ФК-5	ФК-6	ФК-7	ФК-8	ФК-9	ФК-10	ФК-11	ФК-12
ОДЗ.01	+	+																
ОДЗ.02			+															
ОДЗ.03					+													
ОДЗ.04			+															
ОДЗ.05	+																	
ОДЗ.06					+													
ОДС.01				+														
ОДС.02				+														
ОДС.03		+				+												
ОДС.04											+							
ОДС.05								+										
ОДС.06									+									
ОДС.07								+										
ОДС.08												+	+					
ОДС.09							+							+				
ОДС.10											+							
ОДС.11					+		+											
ОДС.12									+		+		+					
ОДС.13											+							
ОДС.14												+	+	+				
ОДС.15															+			
ОДС.16																+		
ОДС.17																	+	
ОДС.18																	+	
ОДС.19								+		+								
ОДС.20										+								
ОДС.21																+		
ОДС.22							+											
ОДС.23																		+
ВП.2.01	+	+	+	+	+	+	+	+										
ВП.2.02	+	+	+	+	+	+	+	+	+	+	+	+	+	+				

	ЗК-1	ЗК-2	ЗК-3	ЗК-4	ЗК-5	ЗК-6	ФК-1	ФК-2	ФК-3	ФК-4	ФК-5	ФК-6	ФК-7	ФК-8	ФК-9	ФК-10	ФК-11	ФК-12
ВП.2.03	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОА.01						+	+	+	+	+	+	+	+	+	+	+	+	+
ВДК.1.01							+											
ВДК.1.02													+					
ВДК.1.03											+							
ВДК.1.04										+								
ВДК.1.05									+									
ВДК.1.06																	+	+
ВДК.1.07													+			+		
ВДК.1.08															+			
ВДК.1.09													+					
ВДК.1.10														+				
ВДК.1.11						+				+								
ВДК.1.12						+												+

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	ПРН-10	ПРН-11	ПРН-12
ОДЗ.01	+	+	+	+	+	+	+	+	+	+	+	+
ОДЗ.02	+	+	+	+	+	+	+	+	+	+	+	+
ОДЗ.03	+	+	+	+	+	+	+	+	+	+	+	+
ОДЗ.04	+	+	+	+	+	+	+	+	+	+	+	+
ОДЗ.05	+								+			
ОДЗ.06	+	+	+	+	+	+	+	+	+	+	+	+
ОДС.01		+				+			+			
ОДС.02		+	+									
ОДС.03		+	+									
ОДС.04		+	+									
ОДС.05		+	+									
ОДС.06			+	+	+	+	+	+	+	+	+	+
ОДС.07		+	+								+	
ОДС.08						+					+	
ОДС.09	+					+						
ОДС.10		+									+	
ОДС.11		+	+	+						+		
ОДС.12		+	+				+				+	+
ОДС.13				+						+		
ОДС.14					+	+			+			
ОДС.15									+			+
ОДС.16										+		
ОДС.17				+		+						
ОДС.18				+		+						
ОДС.19	+			+								
ОДС.20				+	+							
ОДС.21										+		
ОДС.22										+		

	ПРН-1	ПРН-2	ПРН-3	ПРН-4	ПРН-5	ПРН-6	ПРН-7	ПРН-8	ПРН-9	ПРН-10	ПРН-11	ПРН-12
ОДС.23										+		
ВП.2.01	+	+	+	+	+	+	+	+	+	+	+	+
ВП.2.02	+	+	+	+	+	+	+	+	+	+	+	+
ВП.2.03	+	+	+	+	+	+	+	+	+	+	+	+
ОА.01	+	+	+	+	+	+	+	+	+	+	+	+
ВДК.1.01	+				+							
ВДК.1.02					+		+					
ВДК.1.03		+	+	+					+			
ВДК.1.04			+				+				+	+
ВДК.1.05			+	+	+	+	+	+	+	+	+	+
ВДК.1.06								+	+			+
ВДК.1.07			+				+					
ВДК.1.08				+					+			
ВДК.1.09					+		+					
ВДК.1.10				+				+				
ВДК.1.11						+			+			
ВДК.1.12						+				+	+	+

Керівник проектної групи (гарант освітньо-професійної програми)
доцент кафедри управління Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка,

доктор технічних наук, доцент **В.В. СЕМКО**