КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

«ЗАТВЕРДЖЕНО»
Рішенням Вченої ради Київського
університету імені Бориса Грінченка
від 17 червня 2021 р., протокол № 6

Голова Вченої ради, ректор
_____ Віктор ОГНЕВ'ЮК

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

125.00.01 Безпека інформаційних і комунікаційних систем

другого (магістерського) рівня вищої освіти

Галузь знань:	12 Інформаційні технології
Спеціальність:	125 Кібербезпека
Кваліфікація:	Магістр з кібербезпеки

(нова редакція)

Введено в дію з 01.09.2021
(наказ від 17.06.2021 № 432)

Київ – 2021

ЛИСТ-ПОГОДЖЕННЯ
нової редакції освітньо-професійної програми
«Безпека інформаційних і комунікаційних систем»
другого (магістерського) рівня вищої освіти

Програма була переглянута й оновлена в 2021 році.

Кафедра інформаційної та кібернетичної безпеки
Протокол від 12. 05. 2021 № 5
Завідувач кафедри _____ Павло СКЛАДАННИЙ

Вчена рада Факультету інформаційних технологій та управління
Протокол від 16. 06. 2021 № 7
Голова Вченої ради _____ Алла МИХАЦЬКА

Науково-методичний центр стандартизації та якості освіти
Завідувач _____ Ольга ЛЕОНТЬЄВА
16 .06 . 2021 р.

Проректор з науково-методичної та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
16 .06 . 2021 р.

ПЕРЕДМОВА

Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» розроблена на основі Закону України «Про вищу освіту» та Стандарту вищої освіти України за галуззю знань 12 Інформаційні технології спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, затвердженого наказом МОН України від 18.03.2021 № 332.

РОЗРОБЛЕНО робочою групою у складі:

Соколов В.Ю.– кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки (гарант освітньої програми).

Семко В.В. – доктор технічних наук, доцент, професор кафедри інформаційної та кібернетичної безпеки.

Бессалов А.В. – доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки.

Цирканюк Д.А. – студентка освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» 2020 – 2021 років Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка

ЗОВНІШНІ РЕЦЕНЗЕНТИ:

Трофімчук Олександр Миколайович – член-кореспондент НАН України, доктор технічних наук, професор, директор інституту телекомунікацій та глобального інформаційного простору НАН України

Лукова-Чуйко Наталія Вікторівна – доктор технічних наук, професор, завідувач кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка

ВІДГУКИ ПРЕДСТАВНИКІВ РОБОТОДАВЦІВ:

Єрмошин Валерій Віталійович – кандидат технічних наук, Директор департаменту інформаційної безпеки НЕК "Укренерго"

Освітня програма введена в дію 01.09.2018

Термін перегляду освітньої програми раз на рік.

Актуалізовано:

Дата перегляду	Березень 2021			
Підпис				
ПІБ гаранта ОП	Соколов В.Ю.			

Обгрунтування

Оновлення освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» зумовлене необхідністю узгодження змісту освітньо-професійної програми, затвердженої рішенням Вченої ради Київського університету імені Бориса Грінченка від 25.05.2017 протокол № 5 (наказ від 26.05.2017 № 348), зі змінами від 29.08.2019 протокол № 7 (наказ від 30.08.3019 № 509) та затвердженого стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, а також кількома чинниками, які виявилися в процесі реалізації освітньої програми впродовж 2019-2020, 2020-2021 навчальних років та пропозицій, які надійшли від стейкхолдерів (випускників та роботодавців).

Під час роботи над виконанням навчального плану, розробки робочих програм навчальних дисциплін, наповнення електронних навчальних курсів, а також під час практик та атестації, робоча група отримала відгуки від викладачів, баз практик і роботодавців із низкою побажань щодо оптимізації певних компонентів освітньо-професійної програми. Провівши консультації та робочі наради, робоча група погодила кілька змін до певних компонентів ОПП 125.00.01 «Безпека інформаційних і комунікаційних систем».

Уточнення до опису освітньо-професійної програми, з урахуванням затвердженого стандарту вищої освіти за спеціальністю 125 Кібербезпека для другого (магістерського) рівня вищої освіти (наказ Міністерства освіти і науки України від 20.06.2019 № 871), було внесено у такі розділи:

- загальна інформація;
- перелік програмних компетентностей випускника;
- результати навчання.

У навчальному плані основні зміни стосувались:

- структурно-логічної послідовності;
- перерозподіл кількості кредитів між різними освітніми компонентами;
- перепланування часових меж для проходження практик.

Нова редакція цих частин освітньо-професійної програми містяться нижче.

І. Профіль освітньої програми
125.00.01 Безпека інформаційних і комунікаційних систем

1 - Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Київський університет імені Бориса Грінченка Факультет інформаційних технологій та управління
Рівень вищої освіти	Другий (магістерський) рівень
Ступінь вищої освіти	Магістр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Освітньо-професійна програма “Безпека інформаційних і комунікаційних систем”
Кваліфікація	Магістр з кібербезпеки
Кваліфікація в дипломі	ступінь вищої освіти – Магістр спеціальність - Кібербезпека освітня програма – Безпека інформаційних і комунікаційних систем
Форма навчання	Інституційна (очна (денна))
Мова(и) викладання	Українська мова . Окремі освітні компоненти викладаються англійською мовою.
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень;
Тип диплома та обсяг освітньої програм	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці
Передумови	Наявність ступеня «бакалавр»
Наявність акредитації	Національне агентство забезпечення якості вищої освіти. Україна. Сертифікат про зразкову акредитацію освітньої програми «Безпека інформаційних і комунікаційних систем» за спеціальністю 125 Кібербезпека, за рівнем - магістр Сертифікат: № 113 від 16.01.2020 Термін дії – до 13.01.2025
Інтернет-адреса постійного розміщення опису освітньої програми	http://kubg.edu.ua/informatsiya/vstupnikam/napryami-pidgotovki/
2 - Мета освітньої програми	
Забезпечити здобувачам 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 освітньої програми	
Опис предметної області	**Об'єкти вивчення:** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. **Цілі навчання** Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. **Методи, методики та технології** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання** Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення,

	автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Структура програми	Співвідношення обсягів обов'язкової (загальної і фахової) та вибіркової складових ОП: Обов'язкова частина (64 кредити, 71 %): дисципліни, спрямовані на формування загальних та спеціальних (фахових) компетентностей (43 кредити), практика (15 кредитів), атестація (6 кредитів). Вибіркова частина (26 кредитів, 29 %): дисципліни вільного вибору
4 – Придатність випускників до працевлаштування	
Придатність до працевлаштування	Випускники можуть працювати в державному та приватному секторах міста Києва, України та Європейського Союзу у таких сферах діяльності: адміністрування ОС сімейства Windows/Linux, мережевого облад-на-ння і технологій TCP/IP, DNS, DHCP, SSL/TLS, etc.; 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.); створення технічної, проектної та експлуатаційної документації інформа-ційно-комунікаційних систем (далі – ІКС) та систем захисту інформації (далі – СЗІ); налагодження, експлуатації та проведення аналізу системних процесів функціонування мережевих, клієнт-серверних та хмарних технологій; проведення моніторингу несанкціонованої активності в обчислю-вальних системах; створення, впровадження та експлуатації комплексних систем захисту інформації (далі – КСЗІ), а також СЗІ в складі інформаційно телекомуні-каційних (далі – ІТС) та обчислювальних систем; формування політик та процесів у сфері ІТ безпеки, управління доступом до мережевих ресурсів ІТС та ризиками інформаційної безпеки; проведення розслідувань інцидентів та забезпечення аудиту процесів інформаційної безпеки; 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: 2149.2 Професіонал із організації інформаційної безпеки
Подальше навчання	Навчання на третьому (освітньо-науковому) рівні вищої освіти. Набуття додаткових кваліфікацій у системі післядипломної освіти.

5 – Викладання та оцінювання	
Викладання та навчання	Освітній процес побудований на принципах: студентоцентрованого, особистісно орієнтованого навчання, компетентнісного, системно-інтегративного підходів, навчання на основі досліджень. Викладання проводиться у вигляді: лекцій, семінарських, практичних занять, лабораторних робіт. Передбачені самостійна робота (виконання індивідуальних завдань, захист курсової роботи;); консультації з викладачами; електронне навчання за окремими освітніми компонентами, проходження практик, написання кваліфікаційної магістерської роботи. Запроваджується електронне навчання, групова проєктна робота, менторська підтримка практиків, навчання в центрах практичної підготовки. Стимулювання самонавчання здобувачів вищої освіти та організація групової роботи з метою набуття навичок командної роботи та самостійного пошуку вирішення проблеми, зокрема, під час розв'язування практичних кейсів.
Оцінювання	Накопичувальна бально-рейтингова система, що передбачає оцінювання студентів за всі види аудиторної та позааудиторної освітньої діяльності у вигляді проміжного, підсумкового (семестрового) контролю, а також атестації. Проміжний контроль (усне опитування, письмовий експрес-контроль/комп'ютерне тестування тощо), модульний контроль, підсумковий семестровий контроль (заліки, іспити в усній, письмовій (тестування), комбінованій формах, захист курсової роботи, захист звітів з практики), атестація (захист кваліфікаційної магістерської роботи). Оцінювання здобувачів вищої освіти відбувається відповідно до Уніфікованої системи оцінювання навчальних досягнень студентів Київського університету імені Бориса Грінченка
6 - Програмні компетентності	
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 (ЗК)	**ЗК 1** Здатність застосовувати знання у практичних ситуаціях.
	ЗК 2 Здатність проводити дослідження на відповідному рівні.
	ЗК 3 Здатність до абстрактного мислення, аналізу та синтезу.
	ЗК 4 Здатність оцінювати та забезпечувати якість виконуваних робіт.
	ЗК 5 Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
	ЗК 6 Здатність до професійного спілкування іноземною мовою

Спеціальні (фахові, предметні) компетентності (ФК)	**ФК 1** Здатність обгрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері 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 у професійній діяльності в сфері 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 вразливостей 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 і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

	ФК 9 Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
	ФК 10 Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
	ФК(У) 11 Здатність до застосування сучасних безпекових інформаційних та SMAR-технологій у сфері захисту інформації.
	ФК(У) 12 Здатність до виявлення уразливостей та забезпечення безпеки телекомунікаційних технологій і SMART-інфраструктури. розслідування інцидентів інформаційної та/або кібербезпеки та протидії злоякісному програмному забезпеченню
7 – Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання	
РН 1 Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	
РН 2 Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	
РН 3 Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	
РН 4 Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	
РН 5 Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	
РН 6 Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	
РН 7 Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	
РН 8 Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки	

та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН 9 Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН 10 Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН 11 Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН 12 Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН 13 Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН 14 Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН 15 Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН 16 Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН 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.
РН 18 Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН 19 Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності
РН 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.
РН 21 Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН 22 Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	
РН 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.	
РН(У) 24 Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях та SMART -інфраструктурі. Вміти проектувати захищені (з урахуванням загроз) проводові і безпроводові телекомунікаційні та SMART -системи.	
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 комп'ютерних наук та математики ФІТУ, кафедри іноземних мов ФПМВ Університету. Практико-орієнтований характер ОПП передбачає широку участь фахівців практиків, що відповідають напряму програми, що підсилює синергетичний зв'язок теоретичної та практичної підготовки. Кадрове забезпечення ОП відповідає вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності.
Матеріально-технічне забезпечення	Викладання навчальних дисциплін здійснюється в аудиторіях загального та спеціального призначення. 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», «Лабораторія вбудованих систем і 3Д моделювання» тощо. Площі приміщень, що використовуються у навчальному процесі, відповідають вимогам доступності, санітарним нормам, вимогам правил пожежної безпеки. Наявна вся необхідна соціально-побутова інфраструктура, їдальня, буфети, кількість місць в гуртожитках відповідає вимогам.
Інформаційне та навчально-методичне забезпечення	– Офіційний веб-сайт Київського університету імені Бориса Грінченка https://kubg.edu.ua/, що містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти тощо;

	– Цифровий кампус https: //digital.kubg.edu.ua/, що містить інформацію про: всі сервіси цифрової освіти, цифрову науку із доступом до різних платформ; цифрове управління нормативними базами, реєстрами, документообігом; імідж та лідерство; цифровий простір із особистими кабінетами і корпоративною поштою; інфраструктуру університету; – Система електронного навчання Університету (Moodle); – сервіси для організації онлайн-занять: Google Meet (корпоративний), Google Chat, Google Hangouts, Google Classroom; – точки бездротового доступу до мережі Інтернет; – бібліотека, читальні зали; – електронна бібліотека, репозиторій http://elibrary.kubg.edu.ua/; – доступ до електронних наукових баз Scopus, Web of Science, EBSCO та ін.; – навчальні і робочі навчальні плани; – графік освітнього процесу; – робочі програми навчальних дисциплін; – програми практик; – методичні рекомендації щодо написання та оформлення курсових робіт тощо. – методичні рекомендації щодо написання та оформлення магістерських робіт тощо.
9 – Академічна мобільність	
Національна кредитна мобільність	-
Міжнародна кредитна мобільність	Укладено угоди, які передбачають студентську мобільність із університетами європейських країн та в рамках програми Еразмус+КАІ. 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.

ІІ. Перелік компонентів освітньо-професійної програми та їхня логічна послідовність

2.1. Перелік освітніх компонентів ОП

Код компонента	Шифр компонента	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4	5
Обов'язкові компоненти ОП				
ОК 1	ОД.01	Іноземна мова професійного спрямування	4	залік
ОК 2	ОД.02	Організація науки і наукових досліджень	4	залік
ОК 3	ОД.03	Прикладна загальна теорія систем безпеки	4	екзамен
ОК 4	ОД.04	Технології безпеки мережевої та SMART інфраструктури	7	екзамен, захист курсової роботи
ОК 5	ОД.05	Технології безпеки безпроводових і мобільних мереж	7	залік
ОК 6	ОД.06	Технології безпеки Web-ресурсів	6	екзамен
ОК 7	ОД.07	Технології розслідування інцидентів безпеки	6	залік
ОК 8	ОД.08	Прикладні аспекти тестувань на проникнення та етичного хакінгу	5	екзамен
ОК 9	ОП.01	Виробнича практика (технологічна)	4,5	залік
ОК 10	ОП.02	Науково-дослідницька практика	4,5	залік
ОК 11	ОП.03	Переддипломна практика	6	залік
ОК 12	ОА.01	Підготовка і захист кваліфікаційної магістерської роботи	6	захист
Загальний обсяг обов'язкових компонентів			**64**	
Вибіркові компоненти ОП (додаток 1)				
Вибірковий блок 1				
ВК 1	ВД.1.01	Моніторинг, аудит та адміністрування захищених ІТ систем і мереж	7	екзамен
ВК 2	ВД.1.02	Технології розробки і тестування ПЗ мережевої безпеки	6	екзамен
ВК 3	ВД.1.03	Технології протидії злоякісному програмному коду	5	екзамен
ВК 4	ВД.1.04	Математичні методи криптографії	4	залік
ВК 5	ВД.1.05	Методи побудови і аналізу криптосистем	4	залік
		разом	***26***	
Вибірковий блок 2 - Вибір з каталогу курсів				
ВК 1-5	ВД 2.	студент обирає дисципліни на відповідну кількість кредитів	26	заліки, екзамени
		разом	***26***	
Загальний обсяг вибіркових компонентів			**26**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ			**90**	

2.2. Структурно-логічна схема

1 курс		2 курс
1 семестр **30 кр.**	**2 семестр** **34,5 кр.**	**3 семестр** **25,5 кр.**
Іноземна мова професійного спрямування, 4 кр.		
Організація науки і наукових досліджень, 4 кр.		
Прикладна загальна теорія систем безпеки, 4 кр.	Прикладні аспекти тестувань на проникнення та етичного хакінгу, 5 кр.	Науково-дослідницька практика, 4,5 кр.
Технології безпеки мережевої та SMART інфраструктури, 7 кр.	Технології безпеки Web-ресурсів, 6 кр.	Виробнича практика (технологічна), 4,5 кр.
Технології безпеки безпроводових і мобільних мереж, 7 кр.	Технології розслідування інцидентів безпеки, 6 кр.	
Вибіркові компоненти, 4 кр.	Вибіркові компоненти, 13 кр.	Вибіркові компоненти, 9 кр.
		Переддипломна практика, 6 кр.
	Написання і захист кваліфікаційної магістерської роботи, 6 кр.	

Вибірковий блок 1		
Моніторинг, аудит та адміністрування захищених ІТ систем і мереж, 7 кр.		
	Технології розробки і тестування ПЗ мережевої безпеки, 6 кр.	Технології протидії зловмисному програмному коду, 5 кр.
	Математичні методи криптографії 4 кр.	Методи побудови і аналізу криптосистем, 4 кр.
Вибірковий блок 2 – Вибір дисциплін з Каталогу		
Вибіркові компоненти, 4 кр.	Вибіркові компоненти, 13 кр.	Вибіркові компоненти, 9 кр.

ІІІ. Форма атестації здобувачів вищої освіти

Атестація здобувачів вищої освіти за освітньо-професійною програмою 125.00.02 «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека» здійснюється у формі ***публічного захисту кваліфікаційної магістерської роботи.***

Атестація здійснюється відкрито і публічно.

Кваліфікаційна магістерська робота спрямована на розв'язання складної задачі інформаційної безпеки та/або кібербезпеки і передбачає проведення досліджень та/або здійснення інновацій.

Кваліфікаційна магістерська робота перевіряється на плагіат. Кваліфікаційна робота не повинна містити академічний плагіат, фабрикації та/або фальсифікації.

Кваліфікаційна магістерська робота оприлюднюється на сайті Університету (у репозиторії). Оприлюднення кваліфікаційних магістерських робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

Виконання освітньо-професійної програми в повному обсязі завершується видачею випускнику документа встановленого зразка.

IV. Матриця відповідності програмних компетентностей компонентам освітньої програми

Позначки програмних компетентностей та освітніх компонентів	ОД.01	ОД.02	ОД.03	ОД.04	ОД.05	ОД.06	ОД.07	ОД.08	ОП.01	ОП.02	ОП.03	ОА.01
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(У) 11				+	+	+	+	+	+	+	+	+
ФК(У) 12				+	+	+			+	+	+	+

V. Матриця забезпечення результатів навчання відповідними компонентами освітньої програми

Позначки результатів навчання та освітніх компонентів	ОД.01	ОД.02	ОД.03	ОД.04	ОД.05	ОД.06	ОД.07	ОД.08	ОП.01	ОП.02	ОП.03	ОА.01
РН 1	+											+
РН 2		+										+
РН 3		+	+							+	+	+
РН 4			+						+	+	+	+
РН 5		+					+	+	+	+	+	+
РН 6				+			+	+	+	+	+	+
РН 7		+	+						+	+	+	+
РН 8				+	+	+			+	+	+	+
РН 9				+	+	+			+	+	+	+
РН 10				+			+		+	+	+	+
РН 11					+	+			+	+	+	+
РН 12							+		+	+	+	+
РН 13			+		+		+		+	+	+	+
РН 14				+	+	+			+	+	+	+
РН 15	+	+							+	+	+	+
РН 16			+						+	+	+	+
РН 17	+	+	+						+	+	+	+
РН 18		+							+		+	+
РН 19		+	+	+	+	+			+		+	+
РН 20			+	+	+	+	+	+		+	+	+
РН 21		+	+				+	+		+	+	+
РН 22		+	+							+	+	+
РН 23			+	+		+	+	+	+	+	+	+
РН(У) 24				+	+		+		+	+	+	+

ДОДАТОК 1 – ВИБІРКОВА ЧАСТИНА ОСВІТНЬОЇ ПРОГРАМИ

Реалізація студентами права на вільний вибір навчальних дисциплін, передбаченого пунктом 15 частини першої статті 62 Закону України «Про вищу освіту» в Київському університету імені Бориса Грінченка відбувається відповідно до Положення про порядок та умови здійснення вибору навчальних дисциплін студентами, затвердженого наказом від 25.11.2016 р. № 642.

1. Вибірковий блок 1

Для підсилення практичної спрямованості фахових компетентностей студентам пропонується блок спеціалізованих дисциплін. Цей блок включає практичні предмети з певних напрямів забезпечення інформаційної безпеки та/або кібербезпеки. Усі його компоненти вписані у фахові компетентності та описуються основними результатами навчання.

Матриця відповідності програмних компетентностей компонентам освітньої програми вибіркового блоку

Позначки програмних результатів навчання та освітніх компонентів	ВД.1.01	ВД.1.02	ВД.1.03	ВД.1.04	ВД.1.05
ЗК 1	+	+	+		
ЗК 3		+			
ФК 1		+			
ФК 2		+			
ФК 3		+			
ФК 4	+				
ФК 5	+				
ФК 6	+				
ФК 8				+	+
ФК 9	+				
ФК(У) 11	+				
ФК(У) 12	+	+			

Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми вибіркового блоку

Позначки програмних результатів навчання та освітніх компонентів	ВД.1.01	ВД.1.02	ВД.1.03	ВД.1.04	ВД.1.05
РН 3				+	+
РН 4				+	+
РН 5		+			
РН 6		+			
РН 11	+				
РН 13				+	+
РН 14	+				
РН 19	+				
РН 23		+			
РН(У) 24	+	+	+		

2. Вибірковий блок 2 - Вибір з каталогу курсів

Вибір дисциплін із переліку (каталогу курсів) з урахуванням власних потреб та інтересів щодо майбутньої фахової діяльності дозволяє студенту поглибити свої знання та здобути додаткові загальні і загально-професійні компетентності в межах споріднених спеціальностей і галузі знань та/або ознайомитись із сучасним рівнем наукових досліджень інших галузей знань та розширити або поглибити знання за загальними компетентностями.

ЛИСТ-ПОГОДЖЕННЯ
нової редакції освітньо-професійної програми
«Безпека інформаційних і комунікаційних систем»
другого (магістерського) рівня вищої освіти

Програма була переглянута й оновлена в 2021 році.

Кафедра інформаційної та кібернетичної безпеки
Протокол від 12. 05. 2021 № 5
Завідувач кафедри _____ Павло СКЛАДАННИЙ

Вчена рада Факультету інформаційних технологій та управління
Протокол від 16. 06. 2021 № 7
Голова Вченої ради _____ Алла МИХАЦЬКА

Науково-методичний центр стандартизації та якості освіти
Завідувач _____ Ольга ЛЕОНТЬЄВА
16 .06 . 2021 р.

Проректор з науково-методичної та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
16 .06 . 2021 р.

ПЕРЕДМОВА

Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» розроблена на основі Закону України «Про вищу освіту» та Стандарту вищої освіти України за галуззю знань 12 Інформаційні технології спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, затвердженого наказом МОН України від 18.03.2021 № 332.

РОЗРОБЛЕНО робочою групою у складі:

Соколов В.Ю.– кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки (гарант освітньої програми).

Семко В.В. – доктор технічних наук, доцент, професор кафедри інформаційної та кібернетичної безпеки.

Бессалов А.В. – доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки.

Цирканюк Д.А. – студентка освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» 2020 – 2021 років Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка

ЗОВНІШНІ РЕЦЕНЗЕНТИ:

Трофімчук Олександр Миколайович – член-кореспондент НАН України, доктор технічних наук, професор, директор інституту телекомунікацій та глобального інформаційного простору НАН України

Лукова-Чуйко Наталія Вікторівна – доктор технічних наук, професор, завідувач кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка

ВІДГУКИ ПРЕДСТАВНИКІВ РОБОТОДАВЦІВ:

Єрмошин Валерій Віталійович – кандидат технічних наук, Директор департаменту інформаційної безпеки НЕК "Укренерго"

Освітня програма введена в дію 01.09.2018

Термін перегляду освітньої програми раз на рік.

Актуалізовано:

Дата перегляду	Березень 2021			
Підпис				
ПІБ гаранта ОП	Соколов В.Ю.			

Обґрунтування

Оновлення освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» зумовлене необхідністю узгодження змісту освітньо-професійної програми, затвердженої рішенням Вченої ради Київського університету імені Бориса Грінченка від 25.05.2017 протокол № 5 (наказ від 26.05.2017 № 348), зі змінами від 29.08.2019 протокол № 7 (наказ від 30.08.3019 № 509) та затвердженого стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, а також кількома чинниками, які виявилися в процесі реалізації освітньої програми впродовж 2019-2020, 2020-2021 навчальних років та пропозицій, які надійшли від стейкхолдерів (випускників та роботодавців).

Під час роботи над виконанням навчального плану, розробки робочих програм навчальних дисциплін, наповнення електронних навчальних курсів, а також під час практик та атестації, робоча група отримала відгуки від викладачів, баз практик і роботодавців із низкою побажань щодо оптимізації певних компонентів освітньо-професійної програми. Провівши консультації та робочі наради, робоча група погодила кілька змін до певних компонентів ОПП 125.00.01 «Безпека інформаційних і комунікаційних систем».

Уточнення до опису освітньо-професійної програми, з урахуванням затвердженого стандарту вищої освіти за спеціальністю 125 Кібербезпека для другого (магістерського) рівня вищої освіти (наказ Міністерства освіти і науки України від 20.06.2019 № 871), було внесено у такі розділи:

- загальна інформація;
- перелік програмних компетентностей випускника;
- результати навчання.

У навчальному плані основні зміни стосувались:

- структурно-логічної послідовності;
- перерозподіл кількості кредитів між різними освітніми компонентами;
- перепланування часових меж для проходження практик.

Нова редакція цих частин освітньо-професійної програми містяться нижче.

І. Профіль освітньої програми
125.00.01 Безпека інформаційних і комунікаційних систем

1 - Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Київський університет імені Бориса Грінченка Факультет інформаційних технологій та управління
Рівень вищої освіти	Другий (магістерський) рівень
Ступінь вищої освіти	Магістр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Освітньо-професійна програма “Безпека інформаційних і комунікаційних систем”
Кваліфікація	Магістр з кібербезпеки
Кваліфікація в дипломі	ступінь вищої освіти – Магістр спеціальність - Кібербезпека освітня програма – Безпека інформаційних і комунікаційних систем
Форма навчання	Інституційна (очна (денна))
Мова(и) викладання	Українська мова . Окремі освітні компоненти викладаються англійською мовою.
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень;
Тип диплома та обсяг освітньої програм	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці
Передумови	Наявність ступеня «бакалавр»
Наявність акредитації	Національне агентство забезпечення якості вищої освіти. Україна. Сертифікат про зразкову акредитацію освітньої програми «Безпека інформаційних і комунікаційних систем» за спеціальністю 125 Кібербезпека, за рівнем - магістр Сертифікат: № 113 від 16.01.2020 Термін дії – до 13.01.2025
Інтернет-адреса постійного розміщення опису освітньої програми	http://kubg.edu.ua/informatsiya/vstupnikam/napryami-pidgotovki/
2 - Мета освітньої програми	
Забезпечити здобувачам 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 освітньої програми	
Опис предметної області	**Об'єкти вивчення:** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. **Цілі навчання** Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. **Методи, методики та технології** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання** Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення,

	автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Структура програми	Співвідношення обсягів обов'язкової (загальної і фахової) та вибіркової складових ОП: Обов'язкова частина (64 кредити, 71 %): дисципліни, спрямовані на формування загальних та спеціальних (фахових) компетентностей (43 кредити), практика (15 кредитів), атестація (6 кредитів). Вибіркова частина (26 кредитів, 29 %): дисципліни вільного вибору
4 – Придатність випускників до працевлаштування	
Придатність до працевлаштування	Випускники можуть працювати в державному та приватному секторах міста Києва, України та Європейського Союзу у таких сферах діяльності: адміністрування ОС сімейства Windows/Linux, мережевого облад-на-ння і технологій TCP/IP, DNS, DHCP, SSL/TLS, etc.; 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.); створення технічної, проектної та експлуатаційної документації інформа-ційно-комунікаційних систем (далі – ІКС) та систем захисту інформації (далі – СЗІ); налагодження, експлуатації та проведення аналізу системних процесів функціонування мережевих, клієнт-серверних та хмарних технологій; проведення моніторингу несанкціонованої активності в обчислю-вальних системах; створення, впровадження та експлуатації комплексних систем захисту інформації (далі – КСЗІ), а також СЗІ в складі інформаційно телекомуні-каційних (далі – ІТС) та обчислювальних систем; формування політик та процесів у сфері ІТ безпеки, управління доступом до мережевих ресурсів ІТС та ризиками інформаційної безпеки; проведення розслідувань інцидентів та забезпечення аудиту процесів інформаційної безпеки; 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: 2149.2 Професіонал із організації інформаційної безпеки
Подальше навчання	Навчання на третьому (освітньо-науковому) рівні вищої освіти. Набуття додаткових кваліфікацій у системі післядипломної освіти.

5 – Викладання та оцінювання	
Викладання та навчання	Освітній процес побудований на принципах: студентоцентрованого, особистісно орієнтованого навчання, компетентнісного, системно-інтегративного підходів, навчання на основі досліджень. Викладання проводиться у вигляді: лекцій, семінарських, практичних занять, лабораторних робіт. Передбачені самостійна робота (виконання індивідуальних завдань, захист курсової роботи;); консультації з викладачами; електронне навчання за окремими освітніми компонентами, проходження практик, написання кваліфікаційної магістерської роботи. Запроваджується електронне навчання, групова проєктна робота, менторська підтримка практиків, навчання в центрах практичної підготовки. Стимулювання самонавчання здобувачів вищої освіти та організація групової роботи з метою набуття навичок командної роботи та самостійного пошуку вирішення проблеми, зокрема, під час розв'язування практичних кейсів.
Оцінювання	Накопичувальна бально-рейтингова система, що передбачає оцінювання студентів за всі види аудиторної та позааудиторної освітньої діяльності у вигляді проміжного, підсумкового (семестрового) контролю, а також атестації. Проміжний контроль (усне опитування, письмовий експрес-контроль/комп'ютерне тестування тощо), модульний контроль, підсумковий семестровий контроль (заліки, іспити в усній, письмовій (тестування), комбінованій формах, захист курсової роботи, захист звітів з практики), атестація (захист кваліфікаційної магістерської роботи). Оцінювання здобувачів вищої освіти відбувається відповідно до Уніфікованої системи оцінювання навчальних досягнень студентів Київського університету імені Бориса Грінченка
6 - Програмні компетентності	
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 (ЗК)	**ЗК 1** Здатність застосовувати знання у практичних ситуаціях.
	ЗК 2 Здатність проводити дослідження на відповідному рівні.
	ЗК 3 Здатність до абстрактного мислення, аналізу та синтезу.
	ЗК 4 Здатність оцінювати та забезпечувати якість виконуваних робіт.
	ЗК 5 Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
	ЗК 6 Здатність до професійного спілкування іноземною мовою

Спеціальні (фахові, предметні) компетентності (ФК)	**ФК 1** Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері 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 у професійній діяльності в сфері 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 вразливостей 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 і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

	ФК 9 Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
	ФК 10 Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
	ФК(У) 11 Здатність до застосування сучасних безпекових інформаційних та SMAR-технологій у сфері захисту інформації.
	ФК(У) 12 Здатність до виявлення уразливостей та забезпечення безпеки телекомунікаційних технологій і SMART-інфраструктури. розслідування інцидентів інформаційної та/або кібербезпеки та протидії злоякісному програмному забезпеченню
7 – Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання	
РН 1 Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	
РН 2 Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	
РН 3 Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	
РН 4 Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	
РН 5 Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	
РН 6 Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	
РН 7 Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	
РН 8 Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки	

та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН 9 Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН 10 Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН 11 Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН 12 Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН 13 Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН 14 Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН 15 Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН 16 Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН 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.
РН 18 Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН 19 Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності
РН 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.
РН 21 Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН 22 Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	
РН 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.	
РН(У) 24 Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях та SMART -інфраструктурі. Вміти проектувати захищені (з урахуванням загроз) проводові і безпроводові телекомунікаційні та SMART -системи.	
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 комп'ютерних наук та математики ФІТУ, кафедри іноземних мов ФПМВ Університету. Практико-орієнтований характер ОПП передбачає широку участь фахівців практиків, що відповідають напряму програми, що підсилює синергетичний зв'язок теоретичної та практичної підготовки. Кадрове забезпечення ОП відповідає вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності.
Матеріально-технічне забезпечення	Викладання навчальних дисциплін здійснюється в аудиторіях загального та спеціального призначення. 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», «Лабораторія вбудованих систем і ЗД моделювання» тощо. Площі приміщень, що використовуються у навчальному процесі, відповідають вимогам доступності, санітарним нормам, вимогам правил пожежної безпеки. Наявна вся необхідна соціально-побутова інфраструктура, їдальня, буфети, кількість місць в гуртожитках відповідає вимогам.
Інформаційне та навчально-методичне забезпечення	– Офіційний веб-сайт Київського університету імені Бориса Грінченка https://kubg.edu.ua/, що містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти тощо;

	– Цифровий кампус https: //digital.kubg.edu.ua/, що містить інформацію про: всі сервіси цифрової освіти, цифрову науку із доступом до різних платформ; цифрове управління нормативними базами, реєстрами, документообігом; імідж та лідерство; цифровий простір із особистими кабінетами і корпоративною поштою; інфраструктуру університету; – Система електронного навчання Університету (Moodle); – сервіси для організації онлайн-занять: Google Meet (корпоративний), Google Chat, Google Hangouts, Google Classroom; – точки бездротового доступу до мережі Інтернет; – бібліотека, читальні зали; – електронна бібліотека, репозиторій http://elibrary.kubg.edu.ua/; – доступ до електронних наукових баз Scopus, Web of Science, EBSCO та ін.; – навчальні і робочі навчальні плани; – графік освітнього процесу; – робочі програми навчальних дисциплін; – програми практик; – методичні рекомендації щодо написання та оформлення курсових робіт тощо. – методичні рекомендації щодо написання та оформлення магістерських робіт тощо.
9 – Академічна мобільність	
Національна кредитна мобільність	-
Міжнародна кредитна мобільність	Укладено угоди, які передбачають студентську мобільність із університетами європейських країн та в рамках програми Еразмус+КАІ. 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.

ІІ. Перелік компонентів освітньо-професійної програми та їхня логічна послідовність

2.1. Перелік освітніх компонентів ОП

Код компонента	Шифр компонента	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4	5
Обов'язкові компоненти ОП				
ОК 1	ОД.01	Іноземна мова професійного спрямування	4	залік
ОК 2	ОД.02	Організація науки і наукових досліджень	4	залік
ОК 3	ОД.03	Прикладна загальна теорія систем безпеки	4	екзамен
ОК 4	ОД.04	Технології безпеки мережевої та SMART інфраструктури	7	екзамен, захист курсової роботи
ОК 5	ОД.05	Технології безпеки безпроводових і мобільних мереж	7	залік
ОК 6	ОД.06	Технології безпеки Web-ресурсів	6	екзамен
ОК 7	ОД.07	Технології розслідування інцидентів безпеки	6	залік
ОК 8	ОД.08	Прикладні аспекти тестувань на проникнення та етичного хакінгу	5	екзамен
ОК 9	ОП.01	Виробнича практика (технологічна)	4,5	залік
ОК 10	ОП.02	Науково-дослідницька практика	4,5	залік
ОК 11	ОП.03	Переддипломна практика	6	залік
ОК 12	ОА.01	Підготовка і захист кваліфікаційної магістерської роботи	6	захист
Загальний обсяг обов'язкових компонентів			**64**	
Вибіркові компоненти ОП (додаток 1)				
Вибірковий блок 1				
ВК 1	ВД.1.01	Моніторинг, аудит та адміністрування захищених ІТ систем і мереж	7	екзамен
ВК 2	ВД.1.02	Технології розробки і тестування ПЗ мережевої безпеки	6	екзамен
ВК 3	ВД.1.03	Технології протидії злоякісному програмному коду	5	екзамен
ВК 4	ВД.1.04	Математичні методи криптографії	4	залік
ВК 5	ВД.1.05	Методи побудови і аналізу криптосистем	4	залік
		разом	***26***	
Вибірковий блок 2 - Вибір з каталогу курсів				
ВК 1-5	ВД 2.	студент обирає дисципліни на відповідну кількість кредитів	26	заліки, екзамени
		разом	***26***	
Загальний обсяг вибіркових компонентів			**26**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ			**90**	

2.2. Структурно-логічна схема

1 курс		2 курс
1 семестр **30 кр.**	**2 семестр** **34,5 кр.**	**3 семестр** **25,5 кр.**
Іноземна мова професійного спрямування, 4 кр.		
Організація науки і наукових досліджень, 4 кр.		
Прикладна загальна теорія систем безпеки, 4 кр.	Прикладні аспекти тестувань на проникнення та етичного хакінгу, 5 кр.	Науково-дослідницька практика, 4,5 кр.
Технології безпеки мережевої та SMART інфраструктури, 7 кр.	Технології безпеки Web-ресурсів, 6 кр.	Виробнича практика (технологічна), 4,5 кр.
Технології безпеки безпроводових і мобільних мереж, 7 кр.	Технології розслідування інцидентів безпеки, 6 кр.	
Вибіркові компоненти, 4 кр.	Вибіркові компоненти, 13 кр.	Вибіркові компоненти, 9 кр.
		Переддипломна практика, 6 кр.
	Написання і захист кваліфікаційної магістерської роботи, 6 кр.	

Вибірковий блок 1		
Моніторинг, аудит та адміністрування захищених ІТ систем і мереж, 7 кр.		
	Технології розробки і тестування ПЗ мережевої безпеки, 6 кр.	Технології протидії злоякісному програмному коду, 5 кр.
	Математичні методи криптографії 4 кр.	Методи побудови і аналізу криптосистем, 4 кр.
Вибірковий блок 2 – Вибір дисциплін з Каталогу		
Вибіркові компоненти, 4 кр.	Вибіркові компоненти, 13 кр.	Вибіркові компоненти, 9 кр.

ІІІ. Форма атестації здобувачів вищої освіти

Атестація здобувачів вищої освіти за освітньо-професійною програмою 125.00.02 «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека» здійснюється у формі ***публічного захисту кваліфікаційної магістерської роботи.***

Атестація здійснюється відкрито і публічно.

Кваліфікаційна магістерська робота спрямована на розв'язання складної задачі інформаційної безпеки та/або кібербезпеки і передбачає проведення досліджень та/або здійснення інновацій.

Кваліфікаційна магістерська робота перевіряється на плагіат. Кваліфікаційна робота не повинна містити академічний плагіат, фабрикації та/або фальсифікації.

Кваліфікаційна магістерська робота оприлюднюється на сайті Університету (у репозиторії). Оприлюднення кваліфікаційних магістерських робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

Виконання освітньо-професійної програми в повному обсязі завершується видачею випускнику документа встановленого зразка.

IV. Матриця відповідності програмних компетентностей компонентам освітньої програми

Позначки програмних компетентностей та освітніх компонентів	ОД.01	ОД.02	ОД.03	ОД.04	ОД.05	ОД.06	ОД.07	ОД.08	ОП.01	ОП.02	ОП.03	ОА.01
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(У) 11				+	+	+	+	+	+	+	+	+
ФК(У) 12				+	+	+			+	+	+	+

V. Матриця забезпечення результатів навчання відповідними компонентами освітньої програми

Позначки результатів навчання та освітніх компонентів	ОД.01	ОД.02	ОД.03	ОД.04	ОД.05	ОД.06	ОД.07	ОД.08	ОП.01	ОП.02	ОП.03	ОА.01
РН 1	+											+
РН 2		+										+
РН 3		+	+							+	+	+
РН 4			+						+	+	+	+
РН 5		+					+	+	+	+	+	+
РН 6				+			+	+	+	+	+	+
РН 7		+	+						+	+	+	+
РН 8				+	+	+			+	+	+	+
РН 9				+	+	+			+	+	+	+
РН 10				+			+		+	+	+	+
РН 11					+	+			+	+	+	+
РН 12							+		+	+	+	+
РН 13			+		+		+		+	+	+	+
РН 14				+	+	+			+	+	+	+
РН 15	+	+							+	+	+	+
РН 16			+						+	+	+	+
РН 17	+	+	+						+	+	+	+
РН 18		+							+		+	+
РН 19		+	+	+	+	+			+		+	+
РН 20			+	+	+	+	+	+		+	+	+
РН 21		+	+				+	+		+	+	+
РН 22		+	+							+	+	+
РН 23			+	+		+	+	+	+	+	+	+
РН(У) 24				+	+		+		+	+	+	+

ДОДАТОК 1 – ВИБІРКОВА ЧАСТИНА ОСВІТНЬОЇ ПРОГРАМИ

Реалізація студентами права на вільний вибір навчальних дисциплін, передбаченого пунктом 15 частини першої статті 62 Закону України «Про вищу освіту» в Київському університету імені Бориса Грінченка відбувається відповідно до Положення про порядок та умови здійснення вибору навчальних дисциплін студентами, затвердженого наказом від 25.11.2016 р. № 642.

1. Вибірковий блок 1

Для підсилення практичної спрямованості фахових компетентностей студентам пропонується блок спеціалізованих дисциплін. Цей блок включає практичні предмети з певних напрямів забезпечення інформаційної безпеки та/або кібербезпеки. Усі його компоненти вписані у фахові компетентності та описуються основними результатами навчання.

Матриця відповідності програмних компетентностей компонентам освітньої програми вибіркового блоку

Позначки програмних результатів навчання та освітніх компонентів	ВД.1.01	ВД.1.02	ВД.1.03	ВД.1.04	ВД.1.05
ЗК 1	+	+	+		
ЗК 3		+			
ФК 1		+			
ФК 2		+			
ФК 3		+			
ФК 4	+				
ФК 5	+				
ФК 6	+				
ФК 8				+	+
ФК 9	+				
ФК(У) 11	+				
ФК(У) 12	+	+			

Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми вибіркового блоку

Позначки програмних результатів навчання та освітніх компонентів	ВД.1.01	ВД.1.02	ВД.1.03	ВД.1.04	ВД.1.05
РН 3				+	+
РН 4				+	+
РН 5		+			
РН 6		+			
РН 11	+				
РН 13				+	+
РН 14	+				
РН 19	+				
РН 23		+			
РН(У) 24	+	+	+		

2. Вибірковий блок 2 - Вибір з каталогу курсів

Вибір дисциплін із переліку (каталогу курсів) з урахуванням власних потреб та інтересів щодо майбутньої фахової діяльності дозволяє студенту поглибити свої знання та здобути додаткові загальні і загально-професійні компетентності в межах споріднених спеціальностей і галузі знань та/або ознайомитись із сучасним рівнем наукових досліджень інших галузей знань та розширити або поглибити знання за загальними компетентностями.