КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА

ЗАТВЕРДЖЕНО
Протокол засідання Вченої ради
Київського університету імені Бориса Грінченка
від 17.06.2021 р., протокол №6

ЗМІНИ ЗАТВЕРДЖЕНО
Протокол засідання Вченої ради
Факультету інформаційних технологій та
Київського університету столичного
імені Бориса Грінченка
від 27.08.2024 р., протокол №6

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
125.00.01 Безпека інформаційних і комунікаційних систем

другого (магістерського) рівня вищої освіти

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

(нова редакція зі змінами)

Введено в дію з 01.09.2024 р.
(наказ від 29.08.2024 р. № 632)

Київ – 2024 р.

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

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА

ЗАТВЕРДЖЕНО
Рішенням Вченої ради
Факультету інформаційних
технологій та математики
від 27.08.2024 р., протокол № 6

Голова Вченої ради
_____ Оксана ЛИТВИН

ЗМІНИ ДО ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМи

125.00.01 Безпека інформаційних і комунікаційних систем

другого (магістерського) рівня вищої освіти

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

Введено в дію з 01.09.2024 р.
(наказ від 29.08.2024 р. №632)

Київ – 2024 р.

Освітньо-професійна програма розроблено на підставі основі Закону України «Про вищу освіту» з урахуванням Проекту Стандарту вищої освіти зі спеціальності 125 Кібербезпека та захист інформації другого (магістерського) рівня вищої освіти.

Голова робочої групи (гарант освітньої програми) – Володимир СОКОЛОВ, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка

Члени робочої групи:

Геннадій ГУЛАК, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка

Юлія ЖДАНОВА, кандидат фізико-математичних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка

Віктор ШЕВЧЕНКО, доктор технічних наук, професор, заступник директора з наукової роботи Інституту програмних систем НАН України, (представник роботодавця)

Валерій ЄРМОШИН, кандидат технічних наук, начальник Департаменту інформаційної безпеки НЕК «УКРЕНЕРГО», (представник роботодавця)

Діана ЦИРКАНЮК, випускниця освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти

Леонід ПОДРІЗ, здобувач І курсу освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти.

Зовнішні рецензенти:

Трофимчук Олександр Миколайович – член-кореспондент НАН України, доктор технічних наук, професор, директор інституту телекомунікацій та глобального інформаційного просто НАН України.

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

Освітня програма запроваджена 1 вересня 2021р.

Термін перегляду освітньої програми1 раз на 2 роки.

Актуалізовано:

Дата перегляду ОП/ Внесення змін до ОП	28.04.2024	
Підпис		
ПІБ гаранта ОП		

ПЕРЕДМОВА

Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» розроблена у відповідності до Стандарту вищої освіти України зі спеціальності 125 Кібербезпека другого (магістерського) рівня, затвердженого наказом Міністерства освіти і науки України від 18.03.2021 р. № 332

Ураховуючи побажання всіх зацікавлених груп було уточнено назви освітніх компонентів:

- ОК 7 «Технології розслідування інцидентів безпеки» на «Технології розслідування інцидентів безпеки критичної інфраструктури;
- ОК 4 «Технології безпеки безпроводових і мобільних мереж» на «Технології безпеки та управління критичними інфраструктурами».

Виокремлено в окрему компетентність щодо дотримання норм академічної доброчесності та етичної поведінки у розділ І (підрозділ 6. Програмні компетентності) ОП додано загальну компетентність **ЗК 7** «Розуміти, виконувати та дотримуватися принципів академічної доброчесності, зокрема, усвідомлювати важливість інтелектуальної чесності у всіх видах навчальної та дослідницької роботи, дотримуватися правил і обмежень, пов'язаних з плагіатом, шахрайством, підробкою даних та іншими формами недопустимої поведінки».

І. Профіль освітньої програми

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Київський столичний університет імені Бориса Грінченка Факультет інформаційних технологій та математики Кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр з кібербезпеки
Офіційна назва освітньої програми	125.00.01 Безпека інформаційних та комунікаційних систем
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці
Наявність акредитації	Національне агенство 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
Цикл/рівень	Другий (магістерський) рівень / FQ-EHEA – другий цикл, QF LLL – 7 рівень, НРК – 8 рівень
Передумови	Ступінь бакалавра
Мова(и) викладання	Українська
Термін дії освітньої програми	
Інтернет-адреса постійного розміщення опису освітньої програми	kubg.edu.ua
2 – Мета освітньої програми	
Забезпечити студентам фундаментальну підготовку у вигляді поглиблених теоретичних і практичних знань, умінь та навичок за спеціальністю 125 Кібербезпека та захист інформації, достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузях телекомунікацій та інформаційних технологій, педагогіки та методики вищої освіти.	
3 - Характеристика освітньої програми	
Предметна область	Об’єкти професійної діяльності випускників: – 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; – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології кібербезпеки та захисту інформації; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту; – методи застосування уразливостей в телекомунікаційних технологіях і *SMART-інфраструктури* та способи боротьби з ними, методи організації захищеної передачі даних у незахищеному *SMART-середовищі,* засоби спеціального мережевого обладнання для забезпечення безпеки корпоративних мереж; – концепції проєктування, побудови та експлуатації захищених проводових і *безпроводових телекомунікаційних та SMART-систем.* *Цілі навчання:* підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки використовувати і впроваджувати технології та застосовувати засоби інформаційної та/або кібербезпеки. *Теоретичний зміст предметної діяльності*. Знання: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до 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 проєктування. Теоретичні засади наукових 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: м*етоди, методики та технології забезпечення інформаційної та/або кібербезпеки.

	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:* – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проєктування, 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. *Співвідношення обсягів загальної і професійної складових та вибіркової частини:* Обов'язкова частина (63 кредити, 70 %): – цикл дисциплін професійно орієнтованої гуманітарної, соціально-економічної та природничо-наукової підготовки (13 кредитів ЄКТС, 390 год.); – цикл дисциплін спеціальної підготовки (20 кредитів ЄКТС, 600 год.) та фахової спеціалізації (12 кредитів ЄКТС, 360 год.) з написанням 1 курсової роботи у 9 семестрі та випускової магістерської роботи (6 кредитів ЄКТС, 180 год.). Частка науково-дослідницької (11 семестр), виробничої (технологічної) (11 семестр) та переддипломної практик (11 семестр): 12 кредитів ЄКТС, 13 %, 360 годин. Вибіркова частина (27 кредитів, 30 %). З них в спеціалізованому блоці навчальних дисциплін: – дисципліни курсової підготовки (8 кредитів ЄКТС, 240 год.); – дисципліни спеціалізованого курсу (19 кредитів ЄКТС, 510 год.).
Орієнтація освітньої програми	Освітньо-професійна програма з прикладною спрямованістю за спеціалізацією безпека інформаційних і комунікаційних систем.
Основний фокус освітньої програми та спеціалізації	Загальна: дослідження в області практики та науки захисту інформації, організації та забезпечення інформаційної та/або кібербезпеки об'єктів, що підлягають захисту.
Особливості програми	З метою підготовки до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації магістр з кібербезпеки, програма забезпечує підготовку професіоналів, здатних: – виявляти та оцінювати ознаки стороннього кібернетичного впливу;

	– моделювати можливі ситуації стороннього кібернетичного впливу та прогнозувати їх можливі наслідки; – організовувати і підтримувати комплекс заходів щодо забезпечення інформаційної та/або кібербезпеки; – проводити дослідження у напрямах забезпечення інформаційної та/або кібербезпеки національних інтересів України й обґрунтовувати шляхи підвищення їх ефективності; – протидіяти несанкціонованому проникненню протиборчих сторін до власних ІТ систем і мереж, забезпечити стійкість їх роботи, а також відновлення їх нормального функціонування після здійснення кібернападів; – забезпечити криптозахист власного інформаційного ресурсу тощо. З метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу програма передбачає: − реалізацію процесного підходу при конструюванні змісту профільно-орієнтованих навчальних дисциплін, студентської мобільності, академічної співпраці та молодіжних обмінів; − залучення до викладацької діяльності керівників та професіоналів, які працюють як в системі професійної освіти, так й на виробництві в галузі інформаційних технологій та телекомунікацій, а також представників бізнесу.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники можуть працювати в державному та приватному секторах Києва, України та Європейського Союзу у таких сферах діяльності: 1) адміністрування ОС сімейства Windows/Linux, мережевого обладнання і технологій TCP/IP, DNS, DHCP, SSL/TLS, etc.; 2) застосування засобів антивірусного захисту (ESET, McAfee, Zilly, etc.), програмних, клієнт-серверних та хмарних технологій захисту інформації (систем веб фільтрації, систем запобігання вторгнень, систем захисту пошти від вірусів і спаму, etc.); 3) створення технічної, проектної та експлуатаційної документації 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 інформаційної та кібербезпеки; – адміністратор комп'ютерних систем і мереж; – адміністратор інформаційної та кібербезпеки; – аудитор/пентестер безпеки інформаційно-комунікаційних систем;

	– розробник засобів захисту інформації; – провідний спеціаліст/керівник служби технічного захисту інформації тощо.
Подальше навчання	Можливість здобуття освіти на другому (магістерському) рівні за спеціальністю 125 «Кібербезпека та захист інформації» 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, кваліфікаційної магістерської роботи.
Оцінювання	Накопичувальна бально-рейтингова система, що передбачає оцінювання студентів за усі види аудиторної та позааудиторної освітньої діяльності у вигляді вхідного, поточного, рубіжного та/або семестрового контролю та атестації.
6 - 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 (КЗ)	**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. **ЗК 7.** Розуміти та дотримуватися принципів академічної доброчесності, зокрема, усвідомлювати важливість інтелектуальної чесності у всіх видах навчальної та дослідницької роботи, дотримуватися правил і обмежень, пов'язаних з плагіатом, шахрайством, підробкою даних та іншими формами недопустимої поведінки.
Фахові компетентності спеціальності (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	
ПРН 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.	
ПРН 2 Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	
ПРН 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.	
ПРН 4 Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	

ПРН 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.
ПРН 6 Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
ПРН 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.
ПРН 8 Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
ПРН 9 Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
ПРН 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.
ПРН 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.
ПРН 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.
ПРН 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.
ПРН 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.
ПРН 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.
ПРН 16 Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
ПРН 17 Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

ПРН 18 Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
ПРН 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
ПРН 20 Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
ПРН 21 Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
ПРН 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.
ПРН 23 Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
ПРН(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, 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 імені професора Володимира Бурячка. До викладання окремих дисциплін відповідно до їх компетенції та досвіду залучений професорсько-викладацький склад кафедри іноземних мов Університету. Практико-орієнтований характер ОПП передбачає широку участь фахівців практиків, що відповідають напряму програм, що підсилює синергетичний зв'язок теоретичної та практичної підготовки. Кадрове забезпечення ОПП відповідає вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності. Всі розробники є співробітниками Київського столичного університету імені Бориса Грінченка. До реалізації програми залучаються науково-педагогічні працівники з науковими ступенями та/або вченими званнями, а також висококваліфіковані спеціалісти. З метою підвищення фахового рівня всі науково-педагогічні працівники один раз на п'ять років проходять стажування.
Матеріально-технічне забезпечення	Викладання навчальних дисциплін здійснюється в аудиторіях загального та спеціального призначення. Спеціально обладнані апаратно-програмним забезпечення, наочними та методичними матеріалами центри розвитку компетентностей, а саме: 1) «Центр дослідження технологій функціонування й захисту інформаційно-комунікаційних систем та мереж» з: навчальною «Лабораторією комп'ютерних мереж та кібербезпеки», навчальною

	«Лабораторією безпеки інформаційно-комунікаційних систем» та навчальною «Лабораторією антивірусного захисту»; 2) «Центр дослідження технологій захисту інформаційних ресурсів» з: навчальною «Лабораторією безпеки інформаційних активів» (навчальний кіберполігон) та навчальною «Лабораторією систем технічного та криптографічного захисту інформації»; 3) «Центр моделювання та програмування»; 4) «Лабораторія вбудованих систем і 3Д моделювання» тощо.
Інформаційне та навчально-методичне забезпечення	Бібліотечні електронні ресурси, електронні наукові видання, електронні навчальні курси із можливістю дистанційного навчання та самостійної роботи, хмарні сервіси Microsoft.
9 - Академічна мобільність	
Національна кредитна мобільність	
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.

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 та управління критичними інфраструктурами	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 критичної інфраструктури	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

<table>
<tr><th colspan="2">1 курс</th><th>2 курс</th></tr>
<tr><th>1 семестр
30 кр.</th><th>2 семестр
34,5 кр.</th><th>3 семестр
25,5 кр.</th></tr>
<tr><td>Іноземна мова професійного спрямування,
4 кр.</td><td></td><td></td></tr>
<tr><td>Організація науки і наукових досліджень,
4 кр.</td><td></td><td></td></tr>
<tr><td>Прикладна загальна теорія систем безпеки,
4 кр.</td><td>Прикладні аспекти тестувань на проникнення та етичного хакінгу, 5 кр.</td><td>Науково-дослідницька практика,
4,5 кр.</td></tr>
<tr><td>Технології безпеки та управління критичними інфраструктурами, 7 кр.</td><td>Технології безпеки Web-ресурсів,
6 кр.</td><td rowspan="2">Виробнича практика (технологічна),
4,5 кр.</td></tr>
<tr><td>Технології безпеки безпроводових і мобільних мереж, 7 кр.</td><td>Технології розслідування інцидентів безпеки критичної інфраструктури,
6 кр.</td></tr>
<tr><td>Вибіркові компоненти,
4 кр.</td><td>Вибіркові компоненти,
13 кр.</td><td>Вибіркові компоненти,
9 кр.</td></tr>
<tr><td></td><td></td><td>Переддипломна практика, 6 кр.</td></tr>
<tr><td></td><td colspan="2">Написання і захист кваліфікаційної магістерської роботи,
6 кр.</td></tr>
</table>

<table>
<tr><td colspan="3">Вибірковий блок 1</td></tr>
<tr><td colspan="2">Моніторинг, аудит та адміністрування захищених ІТ систем і мереж,
7 кр.</td><td></td></tr>
<tr><td></td><td>Технології розробки і тестування ПЗ мережевої безпеки, 6 кр.</td><td>Технології протидії злоякісному програмному коду, 5 кр.</td></tr>
<tr><td></td><td>Математичні методи криптографії
4 кр.</td><td>Методи побудови і аналізу криптосистем,
4 кр.</td></tr>
<tr><td colspan="3">Вибірковий блок 2 – Вибір дисциплін з Каталогу</td></tr>
<tr><td>Вибіркові компоненти,
4 кр.</td><td>Вибіркові компоненти,
13 кр.</td><td>Вибіркові компоненти,
9 кр.</td></tr>
</table>

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 та захист інформації» 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	+								+	+	+	+
ЗК 7		+								+	+	+
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
ПРН 1	+											+
ПРН 2		+										+
ПРН 3		+	+							+	+	+
ПРН 4			+						+	+	+	+
ПРН 5		+					+	+	+	+	+	+
ПРН 6				+			+	+	+	+	+	+
ПРН 7		+	+						+	+	+	+
ПРН 8				+	+	+			+	+	+	+
ПРН 9				+	+	+			+	+	+	+
ПРН 10				+			+		+	+	+	+
ПРН 11					+	+			+	+	+	+
ПРН 12							+		+	+	+	+
ПРН 13			+		+		+		+	+	+	+
ПРН 14				+	+	+			+	+	+	+
ПРН 15	+	+							+	+	+	+
ПРН 16			+						+	+	+	+
ПРН 17	+	+	+						+	+	+	+
ПРН 18		+							+		+	+
ПРН 19		+	+	+	+	+			+		+	+
ПРН 20			+	+	+	+	+	+		+	+	+
ПРН 21		+	+				+	+		+	+	+
ПРН 22		+	+							+	+	+
ПРН 23			+	+		+	+	+	+	+	+	+
ПРН(У) 24				+	+		+		+	+	+	+

ДОДАТОК 1 – ВИБІРКОВА ЧАСТИНА ОСВІТНЬОЇ ПРОГРАМИ

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.