КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

ЗАТВЕРДЖЕНО
Рішенням Вченої ради
Київського столичного університету
імені Бориса Грінченка
27.03.2025, протокол № 3

Голова Вченої ради

_____ Наталія ВІННІКОВА
(підпис)

ОСВІТНЬО-НАУКОВА ПРОГРАМА
«Інформаційна безпека держави»
третього (освітньо-наукового) рівня вищої освіти

Галузь знань: F Інформаційні технології
Спеціальність: F5 Кібербезпека та захист інформації
Кваліфікація: доктор філософії у галузі F Інформаційні технології за спеціальністю F5 Кібербезпека та захист інформації

Введено в дію з 2025 – 2026 н. р.
(наказ від 27.03.2025 № 195)

Київ – 2025

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

ЗАТВЕРДЖЕНО
Рішенням Вченої ради
Київського столичного університету
імені Бориса Грінченка
27.03.2025, протокол № 3

Голова Вченої ради

_____ Наталія ВІННІКОВА
(підпис)

ОСВІТНЬО-НАУКОВА ПРОГРАМА
«Інформаційна безпека держави»
третього (освітньо-наукового) рівня вищої освіти

Галузь знань: 12 Інформаційні технології
Спеціальність: 125 Кібербезпека та захист інформації
Кваліфікація: доктор філософії у галузі 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Введено в дію з 2025 – 2026 н. р.
(наказ від 27.03.2025 № 195)

Київ – 2025

ЛИСТ-ПОГОДЖЕННЯ
освітньо-наукової програми

Кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 07.03.2025 р. № 3

Завідувач кафедри _____ Павло СКЛАДАННИЙ
(підпис)

Вчена рада Факультету інформаційних технологій та математики
Протокол від 19.03.2025 р. № 3

Голова Вченої ради _____ Оксана ЛИТВИН
(підпис)

Завідувач аспірантури, докторантури

_____ Ілона ТРИГУБ
(підпис)

25.03.2025

Проректор з наукової роботи та міжнародної діяльності

_____ Наталія ВІННІКОВА
(підпис)

25.03.2025

ПЕРЕДМОВА

Освітньо-наукова програма «Інформаційна безпека держави» для підготовки доктора філософії у галузі F Інформаційні технології за спеціальністю F5 Кібербезпека та захист інформації створена для продовження реалізації освітньо-наукової програми «Інформаційна безпека держави» у галузі 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації у відповідності до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти, затвердженого постановою Кабінету міністрів України від 29.04.2015 № 266 (в редакції постанови Кабінету Міністрів України від 30.08.2024 № 1021) та наказу Міністерства освіти і науки України «Про особливості запровадження змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти, затверджених постановою Кабінету Міністрів України від 30 серпня 2024 року № 1021» від 19.11.2024 № 1625, зареєстрованого в Міністерстві юстиції України 03.12.2024 за № 1833/43178, та на виконання рішення Вченої ради Київського столичного університету імені Бориса Грінченка від 27.02.2025, протокол № 2.

Освітньо-наукова програма розроблена на підставі Закону України «Про вищу освіту», Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого Постановою Кабінету міністрів України від 23.03.2016 р. № 261 (у редакції Постанови Кабінету міністрів України від 19.05.2023 р. № 502) та Стандарту вищої освіти України за спеціальністю 125 Кібербезпека та захист інформації, галузі знань 12 Інформаційні технології для третього (освітньо-наукового) рівня вищої освіти, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 29.10.2024 №1543.

Розроблено проєктною групою у складі:

Керівник проєктної групи

Бурячок Воломимир Леонідович, доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління;

Члени проєктної групи

Бессалов Анатолій Володимирович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління;

Семко Віктор Володимирович, доктор технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління;

Аносов Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління.

Зовнішні рецензенти:

Толюпа Сергій Васильович, доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації Київського національного університету ім. Т.Г. Шевченка;

Єрмошин Валерій Віталійович, кандидат технічних наук, директор Департаменту з інформаційної безпеки ДП «НЕК «Укренерго».

Переглянуто робочою групою у складі:

Керівник робочої групи:

Коршун Наталія Володимирівна, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики (гарант освітньо-наукової програми);

Члени робочої групи:

Гулак Геннадій Миколайович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики;

Крючкова Лариса Петрівна, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики;

Шевченко Віктор Леонідович, доктор технічних наук, професор, заступник директора Інституту програмних систем НАН України;

Ворохоб Максим Віталійович, випускник ОНП «Інформаційна безпека держави», період навчання з 01.09.2019 по 31.08.2023 року;

Цирканюк Діана Андріївна, здобувач ОНП «Інформаційна безпека держави» 2022 року вступу.

Освітньо-наукова програма запроваджена з 2025-2026 н.р.

Актуалізовано:

Дата перегляду ОНП	Березень 2025 р.		
Підпис			
ПІБ гаранта ОНП	Коршун Н.В.		

ОБҐРУНТУВАННЯ

Внесення змін до освітньо-наукової програми «Інформаційна безпека держави» (спеціальність 125 Кібербезпека та захист інформації) третього (освітньо-наукового) рівня вищої освіти, затвердженої рішенням Вченої ради Університету від 24.01.2019, протокол № 1 (наказ від 29.01.2019 № 37), зі змінами від 16.09.2020, протокол № 7 (наказ від 24.09.2020 № 539), нова редакція від 04.04.2022, протокол № 2 (наказ від 05.04.2022 № 146), нова редакція від 25.05.2023, протокол № 4 (наказ від 26.05.2023 № 282), нова редакція від 27.02.2025, протокол № 2 (наказ від 27.02.2025 № 110) зумовлено чинниками, які виявилися у процесі реалізації освітньо-наукової програми (навчального плану, розробки робочих програм навчальних дисциплін, проведення практичної підготовки).

Під час реалізації освітньо-наукової програми, у ході проведених опитувань, очних і дистанційних зустрічей тощо робоча група отримала відгуки від здобувачів вищої освіти, академічної спільноти, роботодавців з пропозиціями внести окремі зміни до чинної ОНП з метою її удосконалення. Відтак, провівши консультації, робочі наради, засідання, врахувавши відгуки стейкхолдерів, зміни в нормативній документації, зроблено:

• уточнення загальної інформації про освітньо-наукову програму, зокрема шифру / коду і найменувань галузі знань / спеціальності відповідно до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти, затвердженого постановою Кабінету Міністрів України від 29.04.2015 №266 (в редакції постанови Кабінету Міністрів України від 30.08.2024 №1021);

• уточнення назв окремих освітніх компонентів та оптимізація їх змісту відповідно до сучасного стану галузі і спеціальності (у блоці обов'язкових компонентів назву дисципліни «Наукова комунікація іноземною мовою» замінено на «Наукова комунікація» і виокремлено модулі «Наукова комунікація українською мовою» та «Наукова комунікація іноземною мовою» з метою удосконалення уміння здобувачів презентувати, обговорювати, оприлюднювати результати їхніх досліджень українською та іноземною мовами;

• перерозподіл кредитів у межах навчальних семестрів задля оптимізації виконання здобувачами освітньої та наукової складових ОНП з метою дотримання термінів атестації відповідно до вимог Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 23.03.2016 №261 (у редакції постанови Кабінету Міністрів України від 19.05.2023 №502).

Відповідно було внесено уточнення в такі розділи освітньо-наукової програми та її сегменти:

І. 1.1. Загальна інформація.

ІІ. 2.1. Перелік компонентів ОНП.

2.2. Структурно-логічна схема освітньо-наукової програми.

Цілі, програмні компетентності та програмні результати навчання не змінювалися.

І. Профіль освітньо-наукової програми «Інформаційна безпека держави»

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Київський столичний університет імені Бориса Грінченка Факультет інформаційних технологій та математики
Рівень вищої освіти	Третій (освітньо-науковий) рівень
Ступінь вищої освіти	Доктор філософії
Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Освітньо-наукова програма	Освітньо-наукова програма «Інформаційна безпека держави»
Кваліфікація	Доктор філософії з кібербезпеки та захисту інформації
Кваліфікація в дипломі	Ступінь вищої освіти – доктор філософії Галузь знань – F Інформаційні технології Спеціальність – F5 Кібербезпека та захист інформації
Форми здобуття вищої освіти	Інституційна (очна (денна), заочна)
Мова(и) викладання	Українська мова
Цикл/рівень	НРК України – 8 рівень, FQ-EHEA – третій цикл, EQF LLL – 8 рівень
Тип диплома та обсяг освітньо-наукової програми	Диплом доктора філософії, одиничний Обсяг освітньої складової освітньо-наукової програми доктора філософії – 60 кредитів ЄКТС. Загальний термін навчання – 4 роки
Передумови	Наявність ступеня магістра або освітньо-кваліфікаційного рівня спеціаліста
Наявність акредитації	Національне агентство забезпечення якості вищої освіти, Україна. Сертифікат про акредитацію освітньо-наукової програми «Інформаційна безпека держави» за спеціальністю 125 Кібербезпека та захист інформації, третій (освітньо-науковий) рівень: від 28.03.2024 № 7263; строк дії – до 01.07.2028.
Інтернет-адреса постійного розміщення опису освітньо-наукової програми	http://kubg.edu.ua
2 – Мета освітньо-наукової програми	
Забезпечити сучасну освітньо-наукову підготовку дослідників з галузі знань F Інформаційні технології за спеціальністю F5 Кібербезпека та захист інформації із глибинним науковим, аналітичним, дослідницьким, організаторським потенціалом задля успішної професійної самореалізації та здійснення наукових проєктів відповідно до місії Київського столичного університету імені Бориса Грінченка – «Служити людині, громаді, суспільству».	

3 – Характеристика освітньо-наукової програми	
Опис предметної області	*Об'єкти вивчення та діяльності:* – інформаційні системи і технології на об'єктах інформаційної діяльності та критичної інфраструктури сфери кібербезпеки та захисту інформації; – новітні системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення інформації (інформаційних потоків); – сучасні інформаційні ресурси різних класів (у тому числі державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – автоматизовані системи управління інформаційною безпекою, кібербезпекою та захистом інформації; – методології, технології, методи, моделі та засоби кібербезпеки та захисту інформації. *Цілі навчання:* набуття здатності продукувати нові ідеї, розв'язувати комплексні проблеми професійної та дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, та здійснювати власні наукові дослідження, результати яких мають наукову новизну, теоретичне та практичне значення. *Теоретичний зміст предметної області:* принципи, концепції, теорії захисту життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. *Методи, методики та технології:* сучасні методи, моделі, методики та технології дослідження та вдосконалення процесів створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів. у кіберпросторі, методи статистичного аналізу даних. *Інструменти та обладнання:* програмно-апаратне та програмне забезпечення, інструментальні засоби, комп'ютерна техніка, спеціальні контрольно-вимірювальні прилади, програмно-технічні засоби автоматизації та системи автоматизації проектування, виробництва, експлуатації, контролю, моніторингу, мережні, мобільні, хмарні, технології, 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).
Структура освітньо-наукової програми	Співвідношення обсягів обов'язкової та вибіркової складових ОНП: Обов'язкова частина (42 кредити ECTS, 70%): дисципліни, спрямовані на формування загальних та спеціальних (фахових, предметних) компетентностей – 36 кредитів; практики (науково-викладацька, дослідницька) – 8 кредитів. Вибіркова частина – 18 кредитів, 30%: вільний вибір освітніх компонентів.

4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Працевлаштування на посадах наукових і науково-педагогічних працівників в наукових установах і закладах вищої освіти, посадах працівників найвищої кваліфікації у дослідницьких, проєктних, конструкторських й т.п. установах і підрозділах підприємств.
Академічні права випускників	Доктор філософії має право на здобуття наукового ступеня доктора наук та додаткових кваліфікацій у системі освіти дорослих
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 та лабораторних занять. Передбачені самостійна робота (виконання індивідуальних завдань з використанням друкованих та електронних джерел); консультації з викладачами; проходження практик. Викладання здійснюється із застосуванням інноваційних, інтерактивних та інформаційних технологій на платформі дистанційного навчання Moodle у цифровому університетському кампусі, організації комунікації на платформі Google Meet, ZOOM тощо. Використання елементів неформальної освіти під час вивчення окремих модулів дисциплін на освітніх онлайн-платформах та під час участі в наукових конференціях, конгресах, вебінарах, майстер-класах тощо. Освітньо-науковою програмою передбачені освітні компоненти, спрямовані на науково-дослідницьку підготовку майбутніх докторів філософії, зокрема з орієнтацією на тематику досліджень аспірантів та врахування їх наукових інтересів.
Оцінювання	Підготовка здобувачів передбачає оцінювання всіх видів аудиторної та позааудиторної освітньої діяльності у вигляді проміжного, підсумкового (семестрового) контролю. Проміжний контроль (усне опитування, есе, письмовий експрес-контроль/комп'ютерне тестування тощо), модульний контроль, підсумковий семестровий контроль (заліки, іспити в усній, письмовій, комбінованій формах, захисти звітів з практики).
6 – Програмні компетентності	
Інтегральна компетентність	Здатність продукувати нові ідеї, розв'язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.
Загальні компетентності	ЗК 1. Здатність до абстрактного мислення, аналізу і синтезу.
	ЗК 2. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
	ЗК 3. Здатність працювати в міжнародному контексті.
	ЗК 4. Здатність розв'язувати комплексні проблеми предметної області на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.

Спеціальні (фахові, предметні) компетентності	СК 1. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у сфері кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та захисту інформації.
	СК 2. Здатність ініціювати, розробляти і реалізовувати комплексні наукові та інноваційні проєкти в сфері кібербезпеки та захисту інформації.
	СК 3. Здатність розв'язувати значущі проблеми у сфері кібербезпеки та захисту інформації, розширювати та переоцінювати наявні знання і професійні практики.
	СК 4. Здатність ефективно застосовувати методи аналізу даних, концептуального, математичного та комп'ютерного моделювання, виконувати натурні та обчислювальні експерименти при проведенні наукових і прикладних досліджень у сфері кібербезпеки та захисту інформації.
	СК 5. Здатність генерувати нові ідеї щодо розвитку теорії та практики кібербезпеки та захисту інформації, виявляти, ставити та вирішувати проблеми дослідницького характеру, оцінювати та забезпечувати якість виконуваних досліджень.
	СК 6. Здатність вільно спілкуватися з питань, що стосуються сфери кібербезпеки та захисту інформації, з колегами, широкою науковою спільнотою, суспільством у цілому українською та англійською мовами.
	СК 7. Здатність здійснювати та організовувати наукову та освітню науково-педагогічну діяльність у закладах вищої освіти.
	СКУ 8. Здатність оцінювати фізичні, технологічні, інформаційні, соціологічні, етичні та інші процеси інформаційного і кіберпросторів.
	СКУ 9. Здатність застосовувати сучасні ІТ технології при створенні систем інформаційної та/або кібербезпеки і захисту інформації, електронні інформаційні ресурси, спеціалізоване програмне забезпечення у науковій та навчальній діяльності.
	СКУ 10. Здатність проєктувати, впроваджувати і застосовувати сучасні інформаційні та безпекові технології (комплексні системи криптографічного і технічного захисту інформації, системи соціотехнічної безпеки тощо).
	СКУ 11. Здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки ІТ систем та мереж, обробки та перетворення інформації.
	СКУ 12. Здатність до планування і реалізації заходів із захисту інформації на об'єктах критичної інфраструктури, проведення моніторингу, аудиту та відновлення процесів штатного функціонування ІТ систем та мереж після збоїв та відмов різних класів і походження.
7 – Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання	
ПРН 1. Мати передові концептуальні та методологічні знання з кібербезпеки та захисту інформації і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з кібербезпеки та захисту інформації, отримання нових знань та/або здійснення інновацій. ПРН 2. Планувати і виконувати експериментальні та/або теоретичні дослідження з	

кібербезпеки та захисту інформації та дотичних міждиспиплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики.
ПРН 3. Критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми.
ПРН 4. Глибоко розуміти загальні принципи та методи кібербезпеки та захисту інформації, а також методологію наукових досліджень, застосовувати їх у власних дослідженнях у сфері інформаційних технологій та у викладацькій практиці.
ПРН 5. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані.
ПРН 6. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми кібербезпеки та захисту інформації державною та іноземною мовами усно та письмово, оприлюднювати результати досліджень у наукових публікаціях у провідних вітчизняних та міжнародних наукових виданнях.
ПРН 7. Застосовувати загальні принципи та методи математики, інформатики та інших наук, а також сучасні методи та інструменти, цифрові технології та спеціалізоване програмне забезпечення для провадження наукових досліджень у сфері кібербезпеки та захисту інформації.
ПРН 8. Розробляти та досліджувати концептуальні, математичні і комп’ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах.
ПРН 9. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи.
ПРН 10. Організовувати і здійснювати освітній процес у сфері кібербезпеки та захисту інформації, його наукове, навчально-методичне та нормативне забезпечення, розробляти і викладати спеціальні навчальні дисципліни у закладах вищої освіти.
ПРНУ 11. Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів; здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності; проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД; обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об’єктів інформаційної діяльності, а також наукових досліджень вищих рівнів, зокрема дотичних міждисциплінарних напрямів.
ПРНУ 12. Розробляти та аналізувати проєкти ІКС базуючись на стандартизованих технологіях та протоколах передачі даних; аналізувати та визначати можливість застосування технологій, методів та засобів КТЗІ в ІКС; проєктувати та реалізувати комплексні системи КТЗІ в ІКС відповідно до вимог чинних нормативно-правових документів системи захисту інформації; вирішувати задачі впровадження, супроводу та управління комплексними системами захисту інформації в ІКС, проведення їх експертизи та випробувань; забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту.
ПРНУ 13. Виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, розробляти та впроваджувати науково-дослідницькі та інноваційні проєкти в сфері захисту інформації, інформаційної та кібербезпеки; розробляти алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки;

здійснювати захист ресурсів і процесів в ІКС на основі моделей безпеки та встановлених режимів їх безпечного функціонування; забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ; забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф. ПРНУ 14. Вирішувати задачі централізованого і децентралізованого адміністрування доступом до ІР і процесів в ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них; володіти науково-організаційними основами проведення аудиту безпеки ІКС, а також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в ІТ системах та мережах.	
8 – Ресурсне забезпечення реалізації освітньо-наукової програми	
Кадрове забезпечення	Кадрове забезпечення освітньо-наукової програми складається з професорсько-викладацького складу кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики. До викладання окремих дисциплін залучений професорсько-викладацький склад кафедри філософії та релігієзнавства Факультету суспільно-гуманітарних наук, кафедри публічного права Факультету права та міжнародних відносин, кафедри комп'ютерних наук Факультету інформаційних технологій та математики, кафедри української мови Факультету української філології, культури і мистецтва, кафедри лінгвістики та перекладу Факультету романо-германської філології, кафедри освітології та психолого-педагогічних наук Факультету педагогічної освіти, кафедри психології особистості та соціальних практик Факультету психології, соціальної роботи та спеціальної освіти, відповідно до компетенції та досвіду науково-педагогічних працівників. Наукова спрямованість освітньо-наукової програми передбачає широку участь фахівців, які відповідають напряму програми, що підсилює синергетичний зв'язок теоретичної, практичної та наукової підготовки. Кадрове забезпечення освітньо-наукової програми відповідає вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності.
Матеріально-технічне забезпечення	Освітній процес здійснюється в аудиторіях загального та спеціального призначення. Приміщення оснащені стаціонарною звуко- та відеозаписуючою апаратурою, SMART-технологіями, комплексом мультимедійної апаратури, проєктувальними пристроями. В Університеті наявна достатня кількість спеціалізованих комп'ютерних класів, які оснащені комп'ютерами із відповідним програмним забезпеченням, комплексами мультимедійної апаратури, наочними та методичними матеріалами. Усі робочі місця в комп'ютерних класах під'єднано до мережі Internet. Площі приміщень, що використовуються у навчальному процесі, відповідають вимогам доступності, санітарним нормам, вимогам правил пожежної безпеки. Наявна вся необхідна соціально-побутова інфраструктура, їдальня, буфети, актові та спортивні зали, стадіон, спортивні майданчики, медичний пункт, басейн.
Інформаційне та	– офіційний вебсайт Київського столичного університету імені Бориса

навчально-методичне забезпечення	Грінченка https://kubg.edu.ua/ містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти та нормативно-правове забезпечення освітньої діяльності; – Цифровий кампус https://digita1.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 та практик.
9 – Академічна мобільність	
Національна кредитна мобільність	–
Міжнародна кредитна мобільність	На основі укладених договорів, які передбачають академічну мобільність із закордонними університетами-партнерами, у рамках програми ЄС Еразмус+ тощо.
Навчання іноземних здобувачів вищої освіти	Освітньо-науковий процес здійснюється українською мовою. Іноземці, які володіють українською мовою не нижче рівня С2, можуть навчатися за цією освітньо-науковою програмою.

ІІ. Перелік компонентів освітньо-наукової програми та їх логічна послідовність

2.1. Перелік компонентів ОНП

Код освітнього компонента	Код (№ з/п) навчальної дисципліни, практики	Компоненти освітньо-наукової програми (навчальні дисципліни, практики)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4	5
Обов'язкові компоненти (ОК) освітньо-наукової програми				
ОК 1	**ОД.01**	**Філософія і методологія наукової діяльності**	**4**	**екзамен**
		Філософія науки	2	
		Загальнонаукова методологія	1	
		Наукова етика	1	
ОК 2	**ОД.02**	**Стратегії наукових досліджень**	**6**	**залік**
		Нормативно-правова база наукових досліджень та наукової діяльності	1	
		Інтернаціоналізація науки	3	
		Сучасні технології інформаційної і кібербезпеки та захисту інформації	2	
ОК 3	**ОД.03**	**Наукова комунікація іноземною мовою**	**8**	**екзамен**
ОК 4	**ОД.04**	**Педагогіка і психологія вищої школи**	**4**	**екзамен**
		Педагогіка вищої школи	1	
		Психологія вищої школи	1	
		Технології викладання у вищій школі	2	
ОК 5	**ОД.05**	**Інформаційно-аналітичні процеси в системах безпеки державних інформаційних ресурсів**	**3**	**залік**
ОК 6	**ОД.06**	**Прикладні аспекти створення та застосування систем технічного захисту**	**3**	**залік**
ОК 7	**ОД.07**	**Прикладні аспекти створення та застосування систем криптографічного захисту**	**3**	**залік**
ОК 8	**ОД.08**	**Прикладні аспекти теорій ризиків, конфліктів і катастроф в системах безпеки**	**3**	**залік**
ОК 9	**ОП.01**	**Науково-викладацька практика**	**4**	**залік**
ОК 10	**ОП.02**	**Дослідницька практика**	**4**	**залік**
Загальний обсяг обов'язкових компонентів:			**42**	
Вибіркові компоненти (ВК)* освітньо-наукової програми (додаток 1)				
ВК 1	**ВД.01**	**Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів**	**3**	**екзамен**
		Прикладні аспекти управління інформаційною та кібербезпекою об'єктів критичної інфраструктури		
ВК 2	**ВД.02**	**Системний аналіз та прийняття рішень в інформаційній і кібербезпеці**	**4**	**залік**
		Прикладні аспекти прогнозування і моделювання в сфері інформаційної діяльності		
ВК 3	**ВД.03**	**Технології безпеки складних соціотехнічних систем**	**3**	**залік**
		Прикладні аспекти протидії кібератакам в соціотехнічних системах		
ВК 4	**ВД.04**	**Проєктування і впровадження захищених інформаційно-комунікаційних систем**	**4**	**залік**
		Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем		

ВК 5	**ВД.05**	**Організація захисту розподілених інформаційних ресурсів** Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем	**4**	**залік**
Усього:			**18**	
Вибір освітніх компонентів з каталогу курсів				
ВК	**ВД.06**	**Вибір освітніх компонентів з каталогу курсів на відповідну кількість кредитів**	**18**	заліки
Загальний обсяг вибіркових компонентів:			**18**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ			**60**	

2.2 Структурно-логічна схема освітньо-наукової програми «Інформаційна безпека держави»

<table>
<tr><td colspan="2">1 рік навчання
1 семестр</td><td colspan="2">2 семестр</td><td colspan="2">2 рік навчання
3 семестр</td><td colspan="2">4 семестр</td><td colspan="2">3 рік навчання
5 семестр</td><td colspan="2">6 семестр</td><td colspan="2">4 рік навчання
7 семестр</td><td>8 семестр</td></tr>
<tr><td colspan="2">12 кредитів</td><td colspan="2">15 кредитів</td><td colspan="2">14 кредитів</td><td colspan="2">15 кредитів</td><td colspan="2">4 кредити</td><td colspan="4">Підготовка до атестації</td></tr>
<tr><td colspan="11"></td></tr>
<tr><td colspan="2">Філософія і методологія наукової діяльності
4 кредити</td><td colspan="2">Стратегії наукових досліджень
6 кредитів</td><td colspan="2">Педагогіка і психологія вищої школи
4 кредити</td><td colspan="2">Науково-викладацька практика
4 кредити</td><td colspan="2">Дослідницька практика
4 кредити</td><td colspan="4" rowspan="4">Виконання індивідуального плану наукової роботи</td></tr>
<tr><td colspan="4">Наукова комунікація
2 кредити 2 кредити</td><td colspan="2">4 кредити</td><td colspan="2">ВД.04
4 кредити</td><td colspan="2" rowspan="3"></td></tr>
<tr><td colspan="2">Інформаційно-аналітичні процеси в системах безпеки державних інформаційних ресурсів
3 кредити</td><td colspan="2">Прикладні аспекти створення та застосування систем технічного захисту
3 кредити</td><td colspan="2">Прикладні аспекти створення та застосування систем криптографічного захисту
3 кредити</td><td colspan="2">Прикладні аспекти теорій ризиків, конфліктів і катастроф в системах безпеки
3 кредити</td></tr>
<tr><td colspan="2">ВД.01
3 кредити</td><td colspan="2">ВД.02
4 кредити</td><td colspan="2">ВД.03
3 кредити</td><td colspan="2">ВД.05
4 кредити</td></tr>
<tr><td colspan="11"></td></tr>
</table>

Наукова складова освітньо-наукової програми

Освітньо-наукова програма та навчальний план аспірантури є основою для формування аспірантом індивідуального навчального плану та індивідуального плану наукової роботи.

Наукова складова освітньо-наукової програми передбачає проведення власного наукового дослідження під керівництвом одного або двох наукових керівників та оформлення його результатів у вигляді дисертації.

Дисертація на здобуття ступеня доктора філософії є самостійним розгорнутим дослідженням, що пропонує розв'язання актуального наукового завдання зі спеціальності F5 Кібербезпека та захист інформації, результати якого характеризуються науковою новизною та практичною цінністю, становлять оригінальний внесок у суму знань відповідної галузі та оприлюднені у відповідних публікаціях.

Наукова складова освітньо-наукової програми оформлюється у вигляді індивідуального плану наукової роботи аспіранта і є невід'ємною частиною навчального плану аспірантури.

Індивідуальний план наукової роботи є обов'язковим до виконання здобувачем відповідного ступеня і використовується для оцінювання успішності запланованої наукової роботи.

III. Форма атестації здобувачів вищої освіти

Форма атестації здобувачів вищої освіти	Атестація здобувачів третього (освітньо-наукового) рівня вищої освіти на здобуття ступеня доктора філософії здійснюється у формі публічного захисту дисертації.
Вимоги до дисертації на здобуття ступеня доктора філософії	Дисертація на здобуття ступеня доктора філософії є самостійним розгорнутим дослідженням, яке пропонує розв'язання комплексної проблеми у сфері кібербезпеки та захисту інформації або на її межі з іншими спеціальностями, результати якого становлять оригінальний внесок у суму знань відповідної галузі (галузей) та оприлюднені не менше ніж у трьох наукових публікаціях, які розкривають основний зміст дисертації, мають наукову новизну, теоретичне та практичне значення. Дисертація перевіряється на плагіат. Дисертація не повинна містити академічного плагіату, фабрикації та/або фальсифікації. Дисертація та анотація до неї оприлюднюються на сайті Університету, інституційному репозиторії. Дисертація повинна мати обсяг основного тексту 6,5 – 9 авторських аркушів.

Стан готовності дисертації аспіранта до захисту визначається науковим керівником (або консенсусним рішенням двох керівників).

Обов’язковою умовою допуску до захисту є успішне виконання аспірантом його індивідуального навчального плану та індивідуального плану наукової роботи.

IV. Матриця відповідності програмних компетентностей компонентам освітньо-наукової програми

Позначки програмних компетентностей та освітніх компонентів	**ОК1**	**ОК2**	**ОК3**	**ОК4**	**ОК5**	**ОК6**	**ОК7**	**ОК8**	**ОК9**	**ОК10**
ЗК 1.	+				+					+
ЗК 2.	+	+			+					+
ЗК 3.	+	+	+							+
ЗК 4.	+	+		+	+				+	+
СК 1.	+									+
СК 2.		+			+					+
СК 3.					+	+	+	+		+
СК 4.					+					+
СК 5.		+			+	+	+	+		+
СК 6.		+	+	+						
СК 7.									+	
СКУ 8.	+	+				+	+	+		+
СКУ 9.						+	+	+	+	+
СКУ 10.					+					+
СКУ 11.						+	+	+		+
СКУ 12.					+	+	+			+

V. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньо-наукової програми

Позначки результатів навчання та освітніх компонентів	**ОК1**	**ОК2**	**ОК3**	**ОК4**	**ОК5**	**ОК6**	**ОК7**	**ОК8**	**ОК9**	**ОК10**
ПРН 1.	+	+				+	+	+		
ПРН 2.	+									+
ПРН 3.	+	+								+
ПРН 4.	+	+							+	+
ПРН 5.	+									+
ПРН 6.	+	+	+						+	+
ПРН 7.					+	+	+	+		
ПРН 8.						+	+	+		+
ПРН 9.	+	+								+
ПРН 10.				+					+	
ПРНУ 11.	+	+			+	+	+	+	+	+
ПРНУ 12.						+	+			
ПРНУ 13.					+	+	+	+		
ПРНУ 14.					+	+	+	+		

ДОДАТОК 1 – Вибіркова частина освітньо-наукової програми

Освітньо-наукова програма «Інформаційна безпека держави» забезпечує реалізацію аспірантами права на вільний вибір освітніх компонентів, передбаченого п. 15 частини 1 ст. 62 Закону України «Про вищу освіту», п. 21 Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого Постановою Кабінету міністрів України від 23.03.2016 р. № 261 (у редакції Постанови Кабінету міністрів України від 19.05.2023 р. № 502).

Для формування індивідуальної освітньої траєкторії аспірантам пропонується перелік вибіркових компонентів, які створюють умови для набуття знань і компетентностей у вузькій науковій спеціалізації, релевантній науковому напряму аспіранта, його науковим інтересам та темі дисертаційної роботи.

1. Вибіркова дисципліна «Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів» / «Прикладні аспекти управління інформаційною та кібербезпекою об'єктів критичної інфраструктури»

Дисципліна «Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів» передбачає вивчення способів формування вимог до систем безпеки об'єктів критичної інфраструктури (ОКІ); положення стандартів та нормативно-правових документів забезпечення їх захисту АСУ ОКІ від стороннього кібернетичного впливу; формування умінь та навичок з вибору стратегії дій на основі системного підходу використовуючи оброблену отриману інформацію; розробки неформалізованих моделей засобів, систем і процесів, що застосовуються в ОКІ та їх аналізу з точки зору ІКБ; забезпечення функціонування ОКІ в частині виконання вимог ІКБ; розробки планів і проведення заходів щодо організації захисту інформації (забезпечення кібербезпеки) ОКІ; побудови та перевірки моделей аналізу і синтезу інформаційно-комунікаційних систем та мереж.

Дисципліна «Прикладні аспекти управління інформаційною та кібербезпекою об'єктів критичної інфраструктури» передбачає формування у здобувачів наукового ступеня доктора філософії професійних компетенцій та здатностей щодо створення комплексних систем захисту інформації (КСЗІ) в інформаційних, комунікаційних та ІТС, здійснення комплексу заходів, спрямованих на розроблення і впровадження інформаційних технологій, які забезпечують обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими актами та нормативними документами у сфері захисту інформації. Завданнями дисципліни є формування умінь із побудови систем захисту інформації адміністрування систем захисту інформації.

Матриця відповідностей програмних компетентностей вибірковим компонентам освітньо-наукової програми (вибіркова дисципліна «Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів» / «Прикладні аспекти управління інформаційною та кібербезпекою об'єктів критичної інфраструктури»)

	ВК1
СКУ10.	+
СКУ12.	+

Матриця забезпечення програмних результатів навчання відповідними вибірковими компонентами освітньо-наукової програми (вибіркова дисципліна «Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів» / «Прикладні аспекти управління інформаційною та кібербезпекою об'єктів критичної інфраструктури»)

	ВК1
ПРНУ11.	+
ПРНУ14.	+

2. Вибіркова дисципліна «Системний аналіз та прийняття рішень в інформаційній і кібербезпеці» / «Прикладні аспекти прогнозування і моделювання в сфері інформаційної діяльності»

Дисципліна «Системний аналіз та прийняття рішень в інформаційній і кібербезпеці» передбачає вивчення основних понять, структури, основних завдань та методів системного аналізу і теорії прийняття рішень; технологій застосування системного аналізу та прийняття рішень в інформаційній безпеці; формування умінь та навичок із системного аналізу та системного підходу при прийнятті рішень достатніх для застосування і подальшого продовження самоосвіти у галузі інформаційної безпеки та захисту інформації.

Дисципліна «Прикладні аспекти прогнозування і моделювання в сфері інформаційної діяльності» передбачає формування у здобувачів наукового ступеня доктора філософії професійних компетенцій та здатностей самостійно формувати обґрунтовані судження про можливий стан систем захисту та/або систем інформаційної і кібербезпеки в майбутньому та (або) про альтернативні шляхи і терміни їх реалізації. Головними функціями прогнозування перспектив розвитку систем захисту при цьому є: науковий аналіз процесів і тенденцій; дослідження об'єктивних зв'язків явищ в розвитку; оцінка об'єкта прогнозування (базується на поєднанні аспектів детермінованості (обмеження) і невизначеності; виявлення альтернатив розвитку; накопичення наукового матеріалу для обґрунтування вибору управлінських рішень.

Матриця відповідностей програмних компетентностей вибірковим компонентам освітньо-наукової програми (вибіркова дисципліна «Системний аналіз та прийняття рішень в інформаційній і кібербезпеці» / «Прикладні аспекти прогнозування і моделювання в сфері інформаційної діяльності»)

	ВК2
ЗК1.	+
ЗК4.	+
СК4.	+
СКУ10.	+

Матриця забезпечення програмних результатів навчання відповідними вибірковими компонентами освітньо-наукової програми (вибіркова дисципліна ««Системний аналіз та прийняття рішень в інформаційній і кібербезпеці» / «Прикладні аспекти прогнозування і моделювання в сфері інформаційної діяльності»)

	ВК2
ПРНУ11.	+

3. Вибіркова дисципліна «Технології безпеки складних соціотехнічних систем» / «Прикладні аспекти протидії кібератакам в соціотехнічних системах»

Дисципліна «Технології безпеки складних соціотехнічних систем» передбачає вивчення сучасного стану проблеми безпеки в соціотехнічних системах (СТС), що є складною сукупністю взаємодій людини, інформаційної системи, навколишнього середовища в умовах впливу на них соціальних, економічних, політичних, природних, технічних та інших факторів; формування умінь та навичок з проведення оцінку безпеки СТС по заданому критерію; прогнозування можливих витоків повідомлень в СТС, моделювання систем захисту; імовірнісного аналізу помилок в повідомленні та сумарних помилок на різних рівнях інформаційного взаємодії.

Дисципліна «Прикладні аспекти протидії кібератакам в соціотехнічних системах» передбачає формування у здобувачів наукового ступеня доктора філософії професійних компетенцій та здатностей самостійної реалізації інформаційних операцій і атак в соціотехнічних системах, розробки організаційно-правових заходів захисту, необхідних для попередження атак в сфері управління ІБ. Завданнями дисципліни є формування умінь із реалізації інформаційних операцій і атак на соціотехнічні системи застосування механізмів оцінки та побудови заходів захисту від інформаційних операцій і атак в сфері управління інформаційною безпекою.

Матриця відповідностей програмних компетентностей вибірковим компонентам освітньо-наукової програми (вибіркова дисципліна «Технології безпеки складних соціотехнічних систем» / «Прикладні аспекти протидії кібератакам в соціотехнічних системах»)

	ВК3
СК3.	+
СКУ11.	+
СКУ12.	+

Матриця забезпечення програмних результатів навчання відповідними вибірковими компонентами освітньо-наукової програми (вибіркова дисципліна «Технології безпеки складних соціотехнічних систем» / «Прикладні аспекти протидії кібератакам в соціотехнічних системах»)

	ВК3
ПРНУ12.	+
ПРНУ13.	+
ПРНУ14.	+

4. Вибіркова дисципліна «Проєктування і впровадження захищених інформаційно-комунікаційних систем» / «Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем»

Дисципліна «Проєктування і впровадження захищених інформаційно-комунікаційних систем» передбачає вивчення технологій розробки захищених інформаційно-комунікаційних систем, а також проєктування відповідних комплексів засобів захисту інформації в ІКС; формування: умінь та навичок з розроблення систем захисту ІКС й визначення загальних принципів їх побудови; формування опису ІКС та середовища їх функціонування; визначення складу апаратного та програмного забезпечення; здійснення аналізу обчислювальних процесів та технологій; формування політик і правил забезпечення безпеки тощо.

Дисципліна «Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем» передбачає формування у здобувачів наукового ступеня доктора філософії професійних компетенцій та здатностей самостійно оволодіти сучасними технологіями адміністрування та захисту інформації в інформаційно-комунікаційних системах та мережах, особливостями їх реалізацій, принципами побудови та адміністрування програмних та програмно-апаратних засобів для захисту програмного забезпечення та іншої інформації в інформаційно-комунікаційних системах та мережах. Завдання дисципліни полягає у набутті аспірантами знань, умінь і здатностей (компетенцій) адміністрування в інформаційно-комунікаційних системах та мережах для ефективного вирішення завдань професійної діяльності.

Матриця відповідностей програмних компетентностей вибірковим компонентам освітньо-наукової програми (вибіркова дисципліна «Проєктування і впровадження захищених інформаційно-комунікаційних систем» / «Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем»)

	ВК4
СК3.	+
СКУ9.	+
СКУ11.	+

Матриця забезпечення програмних результатів навчання відповідними вибірковими компонентами освітньо-наукової програми (вибіркова дисципліна «Проєктування і впровадження захищених інформаційно-комунікаційних систем» / «Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем»)

	ВК4
ПРНУ11.	+
ПРНУ12.	+
ПРНУ13.	+

5. Вибіркова дисципліна «Організація захисту розподілених інформаційних ресурсів» / «Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем»

Дисципліна «Організація захисту розподілених інформаційних ресурсів» передбачає вивчення технологій створення і принципів роботи розподілених файлових систем; технологій проєктування систем захисту інформації в розподілених ІС (РІС); технологій оптимізації та пошуку і прийняття рішень при створенні систем захисту РІС; Технології обміну інформацією в РІС; формування умінь та навичок з вибору засобів ОС та програмно-апаратного забезпечення для розробки розподілених додатків; проєктування і розробки РІС та систем їх захисту; підтримки працездатності РІС в заданих функціональних характеристиках та забезпечення їх відповідності заданим критеріям якості, тощо.

Дисципліна «Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем» передбачає формування у здобувачів наукового ступеня доктора філософії професійних компетенцій та здатностей щодо створення системи моніторингу та аудиту стану інформаційної безпеки для забезпечення заданих показників захищеності інформації в розподілених обчислювальних системах. Завданнями навчальної дисципліни є формування умінь із: обґрунтування варіантів побудови автоматизованої системи моніторингу та аудиту стану інформаційної безпеки для розподіленої

обчислювальної системи та її основні складові: систему аналізу вразливостей, систему виявлення вторгнень, систему управління комплексною системою захисту інформації; застосування міждержавних та вітчизняних стандартів при створенні системи моніторингу та аудиту стану ІБ; створення перспективних систем моніторингу та аудиту стану ІБ.

Матриця відповідностей програмних компетентностей вибірковим компонентам освітньо-наукової програми (вибіркова дисципліна «Організація захисту розподілених інформаційних ресурсів» / «Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем»)

	ВК5
СК4.	+
СКУ12.	+

Матриця забезпечення програмних результатів навчання відповідними вибірковими компонентами освітньо-наукової програми (вибіркова дисципліна «Організація захисту розподілених інформаційних ресурсів» / «Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем»)

	ВК5
ПРНУ11.	+
ПРНУ14.	+

6. Вибір з каталогу курсів

Вибір дисциплін з каталогу курсів дає змогу здобувачу розширити та/або поглибити знання у вузькій науковій спеціалізації, релевантній науковому напряму аспіранта, його науковим інтересам та темі дисертаційної роботи, чи здобути додаткові знання та компетентності в межах інших спеціальностей, галузей знань.