КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

ЗАТВЕРДЖЕНО
Рішенням Вченої ради Київського
університету імені Бориса Грінченка
00 лютого 2022 р., протокол № 00

Голова Вченої ради, ректор

_____ Віктор ОГНЕВ'ЮК

ОСВІТНЬО-НАУКОВА ПРОГРАМА

«Інформаційна безпека держави»

третього (освітньо-наукового) рівня вищої освіти

Галузь знань:	12 Інформаційні технології
Спеціальність:	125 Кібербезпека
Ступінь вищої освіти:	Доктор філософії

(нова редакція)

Введено в дію з 00.02.2022
(наказ від 00.02.2022 № 00)

Київ – 2022

ЛИСТ-ПОГОДЖЕННЯ
нової редакції освітньо-наукової програми
«Інформаційна безпека держави»

Кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Протокол від 00.02.2022 № 00
Завідувач кафедри _____ Павло СКЛАДАННИЙ

Вчена рада Факультету інформаційних технологій та управління
Протокол від 00.02.2022 № 00
Голова Вченої ради _____ Алла МИХАЦЬКА

Завідувач аспірантури, докторантури
_____ Ілона ТРИГУБ
___.___.2022

Проректор з наукової роботи
_____ Наталія ВІННІКОВА
___.___.2022

ПЕРЕДМОВА

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 Кабінетів міністрів України від 23.03.2016 р. № 261 (зі змінами). Стандарт вищої освіти України відсутній.

Розроблено 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 управління (гарант освітньо-наукової програми);
Члени робочої групи:
Бессалов Анатолій Володимирович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та управління;
Козачок Валерій Анатолійович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та управління;
Устименко Василь Олександрович, доктор фізико-математичних наук, професор, завідувач відділу інформаційної безпеки Інституту телекомунікацій і глобального інформаційного простору НАН України;
Ворохоб Максим Віталійович, аспірант ОНП «Інформаційна безпека держави».

Зовнішні рецензенти:
Лукова-Чуйко Наталія Вікторівна, доктор технічних наук, професор, завідувач кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій Київського національного університету імені Тараса Шевченка;
Опірський Іван Романович, доктор технічних наук, професор, професор кафедри захисту інформації Національного університету «Львівська політехніка».

Відгуки представників професійних асоціацій / роботодавців:
Скітер Ігор Семенович, кандидат фізико-математичних наук, доцент, старший науковий співробітник Інституту проблем безпеки атомних електростанцій.

Освітньо-наукова програма запроваджена з 01.09.2019.

Актуалізовано:

Дата перегляду ОНП			
Підпис			
ПІБ гаранта ОНП			

ОБҐРУНТУВАННЯ

Оновлення освітньо-наукової програми «Інформаційна безпека держави» третього (освітньо-наукового) рівня вищої освіти, затвердженої рішенням Вченої ради Київського університету імені Бориса Грінченка 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) зумовлене чинниками, які виявилися у процесі реалізації освітньо-наукової програми (навчального плану, розробки робочих програм навчальних дисциплін та проведення практичної підготовки здобувачів третього (освітньо-наукового) рівня вищої освіти) протягом 2019-2021 років. Під час реалізації освітньо-наукової програми, у ході проведених опитувань, очних і дистанційних зустрічей та ін. робоча група отримала відгуки від здобувачів вищої освіти, академічної спільноти, роботодавців з побажаннями внести окремі зміни та уточнення до діючої освітньо-наукової програми.

При оновленні освітньо-наукової програми враховано лист Національного агентства із забезпечення якості вищої освіти від 03.09.2021 № 672 «Про забезпечення володіння випускниками освітньо-наукових програм доктора філософії методологією педагогічної діяльності», п. 25 Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого Постановою Кабінету Міністрів від 23.03.2016 № 261 (зі змінами)) та Методичні рекомендації з розроблення та оновлення освітніх програм (нова редакція) Київського університету імені Бориса Грінченка від 09.06.2021 № 406).

Провівши консультації, робочі наради, засідання, врахувавши відгуки стейкхолдерів, внесено зміни, уточнення та доповнення до освітньо-наукової програми, які стосуються:

- уточнення загальної інформації про освітньо-наукову програму;
- уточнення назв окремих освітніх компонентів та оптимізації їх структури відповідно до сучасного стану галузі і спеціальності (у блок обов’язкових компонентів ОНП введено навчальну дисципліну «Педагогіка і психологія викладання у вищій школі»);
- перерозподілу кредитів між освітніми компонентами для посилення теоретично-методологічної складової викладацької діяльності.

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

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Київський університет імені Бориса Грінченка Факультет інформаційних технологій та управління
Рівень вищої освіти	Третій (освітньо-науковий) рівень
Ступінь вищої освіти	Доктор філософії
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітньо-наукова програма	Освітньо-наукова програма «Інформаційна безпека держави»
Кваліфікація	Доктор філософії з кібербезпеки
Кваліфікація в дипломі	Ступінь вищої освіти – доктор філософії Галузь знань – 12 Інформаційні технології Спеціальність – 125 Кібербезпека
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. Термін подання програми на акредитацію – 2022 р.
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 12 Інформаційні технології за спеціальністю 125 Кібербезпека із глибинним науковим, аналітичним, дослідницьким, організаторським потенціалом задля успішної професійної самореалізації та здійснення наукових проєктів відповідно до місії Київського університету імені Бориса Грінченка – «Служити людині, громаді, суспільству».	
3 – Характеристика освітньо-наукової програми	
Опис предметної області	*Об'єкти вивчення:* об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації; процеси управління інформаційною та/або кібербезпекою об'єктів,

	що підлягають захисту. *Цілі навчання:* підготовка фахівців з кібербезпеки, здатних продукувати нові ідеї, розв'язувати комплексні проблеми у професійній та дослідницько-інноваційній діяльності, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення. *Теоретичний зміст предметної області:* знання законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; теорії, моделей та принципів управління доступом до ІР; теорії систем управління інформаційною та/або кібербезпекою; методів та засобів виявлення, управління та ідентифікації ризиків; методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; методів та засобів технічного та криптографічного захисту інформації; сучасних інформаційно-комунікаційних технологій; сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; автоматизованих систем проєктування. *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. *Інструментарій та обладнання:* системи розробки, забезпечення, моніторингу та контролю інформаційної та/або кібербезпеки; сучасні інформаційні системи та програмне забезпечення, мультимедійні засоби; системи електронних бібліотек та архівів; системи опрацювання текстової та графічної інформації.
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	Заклади освіти, наукові та науково-дослідні установи; державні та неурядові організації, установи та підприємства орієнтовані на викладацьку, дослідницьку, експертну діяльність, підвищення кваліфікації.
Академічні права	Здобуття наукового ступеня доктора наук та додаткових кваліфікацій у системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання	Освітній процес побудований на принципах: студентоцентрованого,

та навчання	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 у професійній та/або дослідницько-інноваційній діяльності, 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 оволодіння різними комунікаційними стилями спілкування (неофіційним, офіційним та науковим) державною та іноземною мовами; вільного спілкування іноземною мовою, як усно (участь у міжнародних наукових проєктах, виступи на наукових заходах, комунікація з іноземними представниками наукової спільноти тощо), так і письмово (використання іншомовних інформаційних ресурсів, підготовка наукових публікацій до друку у зарубіжних виданнях, індивідуальних та колективних грантових заявок (аплікаційних форм) тощо); застосування іноземної мови у самоосвітній діяльності.
	ЗК 2 Здатність до накопичення нових професійно профільованих знань і практичних навичок та застосування їх у професійній діяльності.
	ЗК 3 Здатність до виявлення проблемних аспектів у галузі забезпечення інформаційної та/або кібербезпеки, їх аналізу, оцінювання та вирішення; виявлення та розв'язування комплексних задач дослідницького характеру із дотриманням принципів професійної етики та академічної доброчесності; досягнення наукових результатів, які створюють нові знання, зокрема у міждисциплінарних напрямах.

	ЗК 4 Здатність до синтезу нових ідей, проведення наукових досліджень та реалізації технічних розробок за професійним спрямуванням на відповідному рівні; працювати у міжнародному контексті; розробляти проєкти та управляти ними.
Спеціальні (фахові, предметні) компетентності	СК 1 Здатність оцінювати фізичні, технологічні, інформаційні, соціологічні, етичні та інші процеси інформаційного і кіберпросторів.
	СК 2 Здатність застосовувати математичні навички, навички системного аналізу та синтезу для вирішення нагальних проблем в системах інформаційної та/або кібербезпеки і захисту інформації.
	СК 3 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; здійснювати проєктну діяльність на засадах лідерства.
	СК 4 Здатність проєктувати, впроваджувати і застосовувати сучасні інформаційні та безпекові технології (комплексні системи криптографічного і технічного захисту інформації, системи соціотехнічної безпеки тощо).
	СК 5 Здатність робити оцінки та в умовах припущень і обмежень знаходити відповідні рішення щодо систем інформаційної та/або кібербезпеки і захисту інформації.
	СК 6 Здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки ІТ систем та мереж, обробки та перетворення інформації.
	СК 7 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.
	СК 8 Здатність здійснювати науково-педагогічну діяльність у вищій освіті.
7 – Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання	
РН 1 Презентувати та обговорювати результати наукових досліджень державною та іноземною мовами. РН 2 Здійснювати інформаційний пошук; аналізувати потреби, пов’язані з науковими дослідженнями, з розвитком загальних компетентностей фахівців і професіоналів із захисту інформації, інформаційної та/або кібербезпеки. РН 3 Виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією; РН 4 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. РН 5 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; використовувати для обґрунтування висновків належні докази, наявні літературні дані. РН 6 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. РН 7 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. РН 8 Здатність здійснювати педагогічну та/або науково-педагогічну діяльність у закладах фахової передвищої та/або вищої освіти.	
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 управління. До викладання окремих дисциплін залучений професорсько-викладацький склад кафедри філософії Історико-філософського факультету, кафедри публічного та приватного права Факультету права та міжнародних відносин, кафедри комп'ютерних наук і математики Факультету інформаційних технологій та управління, кафедри лінгвістики та перекладу Інституту філології, кафедри теорії та історії педагогіки Педагогічного інституту, кафедри психології особистості та соціальних практик Інституту людини, 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 навчально-методичне забезпечення	– офіційний веб-сайт Київського університету імені Бориса 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	-

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		
ОК 3	**ОД.03**	**Наукова комунікація іноземною мовою**	**8**	**екзамен**
ОК 4	**ОД.04**	**Педагогіка і психологія викладання у вищій школі**	**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**	**Системний аналіз та прийняття рішень в інформаційній і кібербезпеці**	**4**	**залік**
		Прикладні аспекти прогнозування і моделювання в сфері інформаційної діяльності		
ВК 2	**ВД.02**	**Проєктування і впровадження захищених інформаційно-комунікаційних систем**	**4**	**залік**
		Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем		
ВК 3	**ВД.03**	**Організація захисту розподілених інформаційних ресурсів**	**4**	**залік**
		Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем		
ВК 4	**ВД.04**	**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 5	**ВД.05**	**Технології безпеки складних соціотехнічних систем** Прикладні аспекти протидії кібератакам в соціотехнічних системах	**3**	**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

<table>
<tr><td colspan="2">1 рік</td><td colspan="2">2 рік</td><td colspan="2">3 рік</td><td colspan="2">4 рік</td></tr>
<tr><td>1 семестр
8 кредитів</td><td>2 семестр
10 кредитів</td><td>3 семестр
10 кредитів</td><td>4 семестр
12 кредитів</td><td>5 семестр
11 кредитів</td><td>6 семестр
9 кредитів</td><td>7 семестр</td><td>8 семестр</td></tr>
<tr><td colspan="6">Наукова складова ОНП</td><td colspan="2" rowspan="9">Завершення виконання наукової складової ОНП</td></tr>
<tr><td colspan="6">Освітня складова ОНП – 60 кредитів</td></tr>
<tr><td colspan="2">Філософія і методологія наукової діяльності
4 кредити</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Стратегії наукових досліджень
6 кредитів</td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Наукова комунікація іноземною мовою
8 кредитів</td><td></td><td></td><td></td></tr>
<tr><td colspan="6">Вибіркові компоненти 18 кредитів</td></tr>
<tr><td></td><td></td><td>Інформаційно-аналітичні процеси в системах безпеки державних інформаційних ресурсів
3 кредити</td><td>Педагогіка і психологія викладання у вищій школі
4 кредити</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td>Прикладні аспекти створення та застосування систем технічного захисту
3 кредити</td><td></td><td></td></tr>
</table>

			Прикладні аспекти створення та застосування систем криптографічного захисту *3 кредити*	Науково-викладацька практика *4 кредити*	Дослідницька практика *4 кредити*	
			Прикладні аспекти теорій ризиків, конфліктів і катастроф в системах безпеки *3 кредити*			

Структурно-логічна схема вибіркової частини освітньо-наукової програми

<table>
<tr><td colspan="2">1 рік</td><td colspan="2">2 рік</td><td colspan="2">3 рік</td><td colspan="2">4 рік</td></tr>
<tr><td>1 семестр
2 кредити</td><td>2 семестр
2 кредити</td><td>3 семестр
3 кредити</td><td>4 семестр
0 кредитів</td><td>5 семестр,
6 кредитів</td><td>6 семестр,
5 кредитів</td><td>7 семестр</td><td>8 семестр</td></tr>
<tr><td colspan="6">Вибіркова частина освітньої складової ОНП – 18 кредитів</td><td colspan="2" rowspan="5">Завершення виконання наукової складової ОНП</td></tr>
<tr><td colspan="2">Системний аналіз та прийняття рішень в інформаційній та кібербезпеці / Прикладні аспекти прогнозування і моделювання в сфері інформаційної діяльності
4 кредити</td><td colspan="2">Технології безпеки складних соціотехнічних систем/ прикладні аспекти протидії кібератакам в соціотехнічних системах
3 кредити</td><td>Проєктування і впровадження захищених інформаційно-комунікаційних систем / Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем
4 кредити</td><td>Забезпечення безпеки об’єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів / Прикладні аспекти управління інформаційною та кібербезпекою об’єктів критичної інфраструктури
3 кредити</td></tr>
<tr><td colspan="3"></td><td></td><td colspan="2">Організація захисту розподілених інформаційних ресурсів / Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем
4 кредити</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6">Вибір освітніх компонентів з каталогу курсів 18 кредитів</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 125 Кібербезпека, 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.

ІІІ. Форма атестації здобувачів вищої освіти

Форма атестації здобувачів вищої освіти	Атестація здобувачів третього (освітньо-наукового) рівня 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, що пропонує розв'язання складної спеціалізованої задачі та практичної проблеми у напрямі кібербезпеки 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. Дисертація перевіряється на плагіат. Дисертація не повинна містити академічний плагіат, 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					+	+	+			+
СК 8				+					+	

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

Позначки результатів навчання та освітніх компонентів	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10
РН 1	+	+	+						+	+
РН 2	+	+								+
РН 3	+	+	+		+				+	+
РН 4	+	+			+	+	+	+	+	+
РН 5						+	+			
РН 6					+	+	+	+		
РН 7					+	+	+	+		
РН 8				+					+	

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. 26 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 (зі змінами).

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 «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; отримання кваліфікації як аналітика даних, спеціаліста аналізу даних, бізнес-аналітика ІКТ, Web-аналітика тощо (відповідно до «Проекту реєстру кваліфікацій: сфера ІТ та цифрові професії» від 03.09.2020 р.).

Дисципліна «Прикладні аспекти прогнозування і моделювання в сфері інформаційної діяльності» передбачає формування у здобувачів наукового ступеня «доктор 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»)

	ВК1
ЗК 3	+
ЗК 4	+
СК 2	+
СК 4	+

Матриця забезпечення 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»)

	ВК1
РН 4	+

2. 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; отримання: кваліфікації як фахівця з питань обслуговування мереж, фахівця з ІКТ безпеки, консультанта з питань ІКТ безпеки, тестувальника систем безпеки, експерта з кібернетики, тощо (відповідно до «Проекту реєстру кваліфікацій: сфера ІТ та цифрові професії» від 03.09.2020 року).

Дисципліна «Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем» передбачає формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно оволодіти студентами 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 студентами 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»)

	ВК2
СК 3	+
СК 5	+
СК 6	+

Матриця забезпечення 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»)

	ВК2
РН 4	+
РН 5	+
РН 6	+

3. 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; отримання кваліфікації як фахівця з питань обслуговування мереж, розробника та інтегратора БД; адміністратора мережі ІКТ; директора з ІКТ безпеки; адміністратора Web-сайту; менеджера з розвитку Web-бізнесу; адміністратора безпеки ІКТ, тощо (відповідно до «Проекту реєстру кваліфікацій: сфера ІТ та цифрові професії» від 03.09.2020 року).

Дисципліна «Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем» передбачає формування у здобувачів наукового ступеня «доктор 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»)

	ВКЗ
СК 2	+
СК 7	+

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

	ВКЗ
РН 4	+
РН 7	+

4. 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; отримання кваліфікації як аналітика даних, Web-аналітика, ризик-менеджера, менеджера соціальних мереж, консультанта з питань ІКТ безпеки, експерта з кібернетики, директора з ІКТ безпеки; адміністратора безпеки ІКТ, тощо (відповідно до «Проекту реєстру кваліфікацій: сфера ІТ та цифрові професії» від 03.09.2020 року).

Дисципліна «Прикладні аспекти управління інформаційною та кібербезпекою об'єктів критичної інфраструктури» передбачає формування у здобувачів наукового ступеня «доктор 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»)

	ВК4
СК 4	+
СК 7	+

Матриця забезпечення 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»)

	ВК4
РН 4	+
РН 7	+

5. 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; отримання кваліфікації як аналітика клієнтського досвіду, менеджера з оптимізації пошукових систем, Web-розробника, ризик-менеджера, менеджера соціальних мереж, тощо (відповідно до «Проекту реєстру кваліфікацій: сфера ІТ та цифрові професії» від 03.09.2020 року).

Дисципліна «Прикладні аспекти протидії кібератакам в соціотехнічних системах» передбачає формування у здобувачів наукового ступеня «доктор 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»)

	ВК5
СК 5	+
СК 6	+
СК 7	+

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

	ВК5
РН 5	+
РН 6	+
РН 7	+

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.