ПРОЄКТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ОСВІТНЬО-НАУКОВА ПРОГРАМА

КІБЕРБЕЗПЕКА

третього (освітньо-наукового) рівня вищої освіти
(оновлена)

Спеціальність **125 Кібербезпека та захист інформації**

Галузь знань **12 Інформаційні технології**

Кваліфікація: **Доктор філософії з кібербезпеки та захисту інформації**

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Протокол № ___ від ___ _____ 2025 р.
Наказ № ___ від ___ _____ 2025 р.

Ректор _____ Володимир ШУЛЬГА

Освітня програма вводиться в дію з ___ _____ 2025 р.

Київ-2025

ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬОЇ ПРОГРАМИ
ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

спеціальність	125 Кібербезпека та захист інформації
галузь знань	12 Інформаційні технології
рівень вищої освіти	третій (освітньо-науковий)
кваліфікація	доктор філософії з кібербезпеки та захисту інформації

1. Перший проректор Олександр КОРЧЕНКО
2. Проректор з навчальної роботи Артур ГУДМАНЯН
3. Т.в.о. начальника навчально-методичного відділу Вадим ВЛАСЕНКО
4. Вчена Рада Навчально-наукового інституту кібербезпеки та захисту інформації

   Протокол № ___ від ___ _____ 2025 р.

Голова Вченої Ради ННІКБЗІ Євгенія ІВАНЧЕНКО

5. Кафедра систем та технологій кібербезпеки

   Протокол № ___ від ___ _____ 2025 р.

Завідувач кафедри систем та технологій кібербезпеки Галина ГАЙДУР

Рецензії від зовнішніх стейкхолдерів (компаній-партнерів):

1. _____
2. _____
3. _____

ПЕРЕДМОВА

Розроблено робочою групою складі:

Гарант освітньої програми –

Савченко Віталій Анатолійович – доктор технічних наук, професор, професор кафедри Управління кібербезпекою та захистом інформації.

Члени робочої групи:

Гайдур Галина Іванівна – доктор технічних наук, професор, завідувач кафедри Систем та технологій кібербезпеки.

Казмірчук Світлана Володимирівна – доктор технічних наук, професор, професор кафедри Систем та технологій кібербезпеки.

Чабан Богдан Валентинович – аспірант кафедри Технічних систем кіберзахисту.

_____ – представник компанії-партнера.

ВІДОМОСТІ ПРО ПЕРЕГЛЯД ОСВІТНЬОЇ ПРОГРАМИ

Оновлення освітньої програми здійснено відповідно до:

- стандарту вищої освіти спеціальності 125 Кібербезпека та захист інформації для третього (освітньо-наукового) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 29.10.2024 № 1543.
- рекомендацій акредитаційної комісії від ___ _____ 2025 р. та акредитаційних комісій суміжних освітніх програм;
- рекомендацій роботодавців, здобувачів вищої освіти та інших стейкхолдерів.

Затверджено рішенням кафедри Систем та технологій кібербезпеки,
протокол № ___ від ___ _____ 2025 р.

Введено в дію наказом ректора № ___ від ___ _____ 2025 р.

1. **Профіль освітньої програми**

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Державний університет інформаційно-комунікаційних технологій, Навчально-науковий інститут кібербезпеки та захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Доктор філософії. Освітня кваліфікація – Доктор філософії з кібербезпеки та захисту інформації
Кваліфікація в дипломі	Ступінь вищої освіти – Доктор філософії Галузь знань – 12 Інформаційні технології Спеціальність – 125 Кібербезпека та захист інформації
Офіційна назва освітньої програми	«Кібербезпека»
Тип диплому та обсяг освітньої програми	Диплом доктора філософії, одиничний Обсяг освітньої складової освітньо-наукової програми – 36 кредитів ЄКТС; термін навчання в аспірантурі – 4 роки; термін освоєння освітньої складової – 2 роки
Наявність акредитації	Акредитовано
Цикл/рівень	НРК України – 8 рівень / доктор філософії, QF-EHEA – третій цикл, EQF-LLL – 8 рівень
Передумови	Наявність освітнього ступеня «магістр» або освітньо-кваліфікаційного рівня «спеціаліст» за спеціальністю 125 Кібербезпека та захист інформації (125 Кібербезпека). Дозволяється вступ на ОНП з інших галузей знань за умови складання додаткового іспиту за спеціальністю за спеціальністю 125 Кібербезпека та захист інформації
Мова(и) викладання	українська, англійська
Термін дії освітньої програми	Програма започаткована у 2016 році. Останнє оновлення відбулося у 2024 році відповідно до: – Закону України від 16.12.2020 № 1089-IX «Про електронні комунікації»; – постанови Кабінету Міністрів України від 16.12.2022 № 1392 «Про внесення змін до переліку

	галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти»; – рекомендацій акредитаційних комісій Університету; – пропозицій роботодавців та побажань здобувачів вищої освіти.
Інтернет - адреса постійного розміщення опису освітньо-наукової програми	http://www.dut.edu.ua/ua/1822-osvitno-profesiyni-programi-kafedra-informaciynoi-ta-kibernetichnoi-bezpeki
2 – Мета освітньої програми	
Здобуття теоретичних знань, умінь, навичок та інших компетентностей з кібербезпеки та захисту інформації, достатніх для продукування нових ідей, розв'язання комплексних проблем у галузі професійної та/або дослідницько-інноваційної діяльності, оволодіння методологією наукової та педагогічної діяльності, а також проведення власного наукового дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.	
3 – Характеристика освітньої 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).
Академічні права випускників	Доктор філософії має право на здобуття наукового ступеня доктора наук та додаткових кваліфікацій у системі освіти дорослих.
Орієнтація освітньої програми	Освітньо-наукова програма підготовки докторів філософії спрямована на забезпечення зазальних та спеціальних (фахових) компетентностей за спеціальністю 125 Кібербезпека та захист інформації, в тому числі, визначених на основі аналізу сучасного стану ринку праці та вимог до вакансій потенційних роботодавців у сфері дослідження, проектування, розробки, впровадження та супроводу сучасних систем кібербезпеки та захисту інформації. Програма грунтується на загальновідомих та інноваційних наукових результатах із врахуванням сучасного та перспективного стану інформаційних технологій. Також, програма містить наукову та педагогічну складові. 75% обсягу освітньої програми спрямовано на забезпечення загальних та спеціальних компетентностей за спеціальністю 125 Кібербезпека та

	захист інформації, 25% спрямовано на вивчення дисциплін вільного вибору.
Основний фокус освітньої програми та спеціальності	Підготовка конкурентноспроможних фахівців, що володіють сучасними методами дослідження в області науки та практики кібербезпеки та захисту інформації, організації та забезпечення кібербезпеки інформаційно-комунікаційних систем, технічного захисту інформації, управління кібербезпекою та захистом інформації. Ключові слова: ІНФОРМАЦІЯ, ІНФОРМАЦІЙНІ СИСТЕМИ, ІНФОРМАЦІЙНІ МЕРЕЖІ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ЗАГРОЗИ, ВРАЗЛИВОСТІ, ЗАХИЩЕНІСТЬ, КІБЕРБЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ.
Особливості програми	Програма передбачає: – активне застосування інтерактивних, проблемно-орієнтованих технологій навчання, де здобувачу освіти надається право самостійно генерувати ідеї та пропонувати їх рішення; – підвищена увага розвитку дослідницьких якостей здобувача освіти через практико-орієнтований характер освітнього процесу; – вивчення базових теоретичних основ у поєднанні інноваційними рішеннями світового рівня; – інтернаціоналізація наукового обміну інформацією шляхом реалізації спільних науково-дослідних проектів разом з закордонними науковцями; – широке залучення здобувачів освіти до участі у грантових проектах та стипендіальних програмах.
4 – Викладання та оцінювання	
Викладання та навчання	**Стиль навчання:** – поєднання репродуктивного та творчого стилів навчання як взаємодоповнюючих з домінуючим творчим компонентом; – емоційно-ціннісний стиль навчання з поєднанням емоційно-імпровізаційного та емоційно-методичного стилів; – проблемно-орієнтовані лекційні курси, семінари, групові та індивідуальні консультації, самопідготовка у бібліотеці та з використанням технологій дистанційного навчання, інформації з мережі Інтернет. **Методика навчання:** – узгодження декількох навчальних технологій – інформаційної, моделюючої, розвивальної та активізуючої технологій, технології виробничого,

	випереджаючого та дистанційного навчання; – інтерактивне співробітництво здобувача освіти з науковим керівником, колегами із наукової групи та науково-педагогічними працівниками університету. **Організація навчального процесу:** – формування і дотримання дослідницького портфоліо.
Оцінювання	Оцінювання сформованих компетентностей проводиться під час контрольних заходів, які передбачені цією освітньою програмою та зазначені у навчальному плані. Критерії оцінювання компетентностей здобувачів освіти розробляються відповідно до Положення про організацію освітнього процесу Державного університету інформаційно-комунікаційних технологій та зазначаються у силабусах навчальних дисциплін. У якості форм оцінювання застосовуються: усні та письмові екзамени, заліки, наукові звіти із оцінюванням досягнутого, усні презентації, поточний контроль, публікації результатів досліджень. Написання та привселюдний захист наукових досягнень, виконаних у формі кваліфікаційної (дисертаційної) роботи.
5 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Доктор філософії з кібербезпеки та захисту інформації здатен обіймати посади в дослідницьких групах в університетах та наукових установах інформаційно-комунікаційної галузі (наукові дослідження і сфера управління), у промисловості та комерції. Самостійне працевлаштування. Доктор філософії з кібербезпеки та захисту інформації (випускник) придатний до професійної діяльності за Державним класифікатором професій ДК 003: 2010: **Основна:** 2131.1 Науковий співробітник (обчислювальні системи) **Додаткова:** 2139.1 Науковий співробітник (галузь обчислень) 2144.1 Науковий співробітник (електроніка, комунікації) 2310.2 Викладач вищого навчального закладу 2310.1 Доцент

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	ЗК1. Здатність до абстрактного мислення, аналізу і синтезу. ЗК2. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК3. Здатність працювати в міжнародному контексті. ЗК4. 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	СК1. 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. СК2. Здатність ініціювати, розробляти і реалізовувати комплексні наукові та інноваційні проєкти в сфері кібербезпеки та захисту інформації. СК3. Здатність розв'язувати значущі проблеми у сфері кібербезпеки та захисту інформації, розширювати та переоцінювати наявні знання і професійні практики. СК4. 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. СК5. 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. СК6. Здатність вільно спілкуватися з питань, що стосуються сфери кібербезпеки та захисту інформації, з колегами, широкою науковою спільнотою,

	суспільством у цілому українською та англійською мовами. СК7. Здатність здійснювати та організовувати наукову та освітню науково-педагогічну діяльність у закладах вищої освіти. СК8. *Здатність до виробничо-технологічної діяльності щодо удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення кібербезпеки та захисту інформації.*
7 – Програмні результати навчання	
Програмні результати навчання	РН1. 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. РН2. 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. РН3. Критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми. РН4. 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. РН5. Формулювати і перевіряти гіпотези; використовувати для обгрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані. РН6. 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. РН7. 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. РН8. 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. РН9. 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. РН10. 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. РН11. *Визначати проблематику, ставити наукові завдання, пропонувати нові інноваційні рішення у сфері безпеки інформаційно-комунікаційних технологій, криптографічного захисту інформації, захисту мережевих ресурсів та кінцевих точок.* РН12. *Розробляти та досліджувати нові підходи у сфері технічного захисту інформації, контролю доступу до об'єктів інформаційної діяльності, розробки комплексних систем захисту інформації.* РН13. *Досліджувати існуючі та генерувати нові методи управління у сфері кібербезпеки та захисту інформації на основі поєднання наукових методів та кращих практик теорії управління.*
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Всі науково-педагогічні працівники, залучені до реалізації освітньої складової освітньо-наукової програми є штатними співробітниками Державного університету інформаційно-комунікаційних технологій, мають підтверджений рівень наукової і професійної активності. Кількісний та якісний склад Групи забезпечення спеціальності 125 Кібербезпека та захист інформації відповідає Ліцензійним вимогам.

Матеріально-технічне забезпечення	Теоретичні заняття проводяться в сучасних комп'ютерних класах та спеціалізованих лабораторіях, які оснащені спеціалізованими апаратно-програмними засобами. Для проведення досліджень, практичних та лабораторних занять з метою формування професійних компетентностей зі спеціальності 125 Кібербезпека та захист інформації використовуються 6 спеціалізованих лабораторій, які оснащенні сучасними комп'ютерами, програмно-апаратними комплексами та мультимедійними системами, а саме: **Навчальна лабораторія мережевої безпеки** Лабораторія призначена для вивчення технологій мережевої безпеки CISCO, проведення тренінгів з впровадження технології HoneyPot щодо протидії кібератакам зловмисників на корпоративні інформаційні системи та сертифікаційних курсів від компанії-партнера CISCO: Introduction to Cybersecurity, CCNA Security, CCNA Cybersecurity Operations. **Навчальна лабораторія реагування на кіберінциденти** Лабораторія призначена для проведення практичних занять з використанням програмно-апаратних комплексів: IBM QRadar SIEM, IBM Security AppScan, IBM i2 Analyst's Notebook Premium, Tenable Nessus Professional. Дозволяє відпрацьовувати навички роботи у Центрі забезпечення кібербезпеки (Security Operation Center) з використанням технологій моніторингу, виявлення, аналізу та реагування на кіберінциденти в корпоративних інформаційних системах. **Навчальна лабораторія захисту кінцевих точок** Лабораторія використовується для вивчення спеціалізованих засобів захисту на базі продуктів компанії ESET – ESET PROTECT Enterprise On-Prem. Крім того, у лабораторії проводяться тренінги з використанням криптографічних засобів захисту інформації в інформаційно-комунікаційних системах, віртуальних приватних мереж VPN, електронного цифрового підпису та інфраструктури відкритих ключів. Дозволяє моделювати кіберінциденти з використанням платформи JupyterLab, вивчати та застосовувати засоби криптографічного захисту IP-шифратор CryptoIP-448, електронні ключі "SecureToken-337, програмний IP-шифратор «CryptoIP-VPN Client», безконтактні кард-рідери КР-382, USB.

	Навчальна лабораторія засобів контролю доступу – забезпечує проведення практичних занять та досліджень з питань контролю та управління доступом, використання автономних біометричних терміналів, мережевих контролерів, програмно-апаратних комплексів систем відеоспостереження. Обладнана автоматизованим комплексом відеоспо-стереження та охорони об'єктів інформаційної діяльності (Harbor), програмно-апаратними комплексами контролю доступу, сповіщувачами інфрачервоними (SRP 600) та магніто-контактними (СОМК-10). Дозволяє вивчати питання застосування програмних комплексів захисту інформації. **Навчальна лабораторія технічного захисту інформації** – забезпечує проведення практичних занять з питань технічного захисту конфіденційної інформації на об'єктах інформаційної діяльності від витоку акустичним, віброакустичним та електромагнітним каналами з використанням широкосмугових генераторів акустичного та електромагнітного шуму (Ріас-2ГС, ГШ 1000). Крім того, у лабораторії досліджуються питання застосування пошукового програмно-апаратного комплексу DigiSkan EX; методів виявлення випромінювань за допомогою індикаторів поля типу PROTEKT; порядку застосування скануючих приймачів AR 8200, IC-R5, IC-R2500 та локатора нелінійностей NR-900 EM. **Навчальна лабораторія Security Operation Center** Лабораторія призначена для проведення занять з питань аналізу, обробки та аудиту інформаційної безпеки за допомогою SIEM-систем (AlienVault) та програмних сканерів типу Nessus та Kali Linux. Крім того, дозволяє вивчати методи управління ризиками на основі методологій CRAMM, OCTAVE та RiskWatch у відповідності до вимог міжнародних стандартів з інформаційної та кібербезпеки. Дозволяє працювати з програмними засобами підтримки прийняття рішень у сфері інформаційної безпеки (LibreOffice Calc, OpenSolver, SciPy, NumPy (Python)).
Інформаційне та навчально-методичне забезпечення	Інформація про освітньо-наукову програму, її освітні компоненти та вимоги до осіб, які можуть здобувати вищу освіту за цією програмою розміщена на офіційному сайті Державного університету інформаційно-комунікаційних технологій. Усі освітні компоненти освітньої програми забезпечені інформаційними та навчально-

	методичними матеріалами, є у вільному доступі у якості ресурсів бібліотеки, електронної бібліотеки Університету та системи дистанційного навчання GWE.
9 – Академічна мобільність	
Національна кредитна мобільність	Наявність двосторонніх договорів між Державним університетом інформаційно-комунікаційних технологій та закладами вищої освіти України забезпечує національну кредитну мобільність
Міжнародна кредитна мобільність	Зміст освітньо-наукової програми відповідає стандартам вищої освіти, що дозволяє приймати участь у програмах подвійних дипломів та бути конкурентоспроможним на світовому ринку праці
Навчання іноземних здобувачів вищої освіти	Передбачає навчання іноземців та осіб без громадянства

2. Перелік компонент освітньої програми та їх логічна послідовність

2.1. Зміст підготовки за освітньою програмою, компетентності та результатами навчання

№ п.п.	Дисципліна	Шифр	Компетентність	Результат навчання
1. Цикл обов'язкових компонент освітньо-наукової програми				
1.1. Оволодіння загальнонауковими (філософськими) компетентностями, спрямованими на формування системного наукового світогляду, професійної етики та загального культурного кругозору				
1.	Філософські проблеми наукового пізнання	ОК11.1.1.01	ЗК1, ЗК4	РН3, РН4,
2.	Основи наукових досліджень та організація науки	ОК11.1.1.02	ЗК2, ЗК4, СК1, СК7	РН2, РН5,
1.2. Набуття універсальних навичок дослідника				
3.	Патентознавство та авторське право	ОК11.1.2.01	ЗК2, СК7	РН9
4.	Сучасні методи викладання у вищій школі	ОК11.1.2.02	СК6, СК7	РН10
5.	Науково-педагогічна практика	ОК11.1.2.03	СК7, СК8	РН2, РН6, РН10
1.3. Здобуття мовних компетентностей				
6.	Англійська мова наукового спрямування *	ОК11.1.3.01	ЗК3, СК1, СК6	РН6
1.4. Здобуття глибинних знань зі спеціальності				
7.	Методологія наукових досліджень у кібербезпеці	ОК11.1.4.01	СК2, СК3, СК4, СК5, СК8	РН1, РН7, РН8, РН11
8.	Теоретичні та практичні проблеми технічного захисту інформації	ОК11.1.4.02	СК2, СК3, СК4, СК5, СК8	РН1, РН7, РН8, РН12
9.	Сучасні методи управління інформаційною та кібербезпекою	ОК11.1.4.03	СК2, СК3, СК4, СК5, СК8	РН1, РН7, РН8, РН13
2. Цикл вибіркових компонент освітньо-наукової програми				
10.	*Дисципліна 1***			
11.	*Дисципліна 2***			
12.	*Дисципліна 3***			

** Дисципліна «Англійська мова наукового спрямування» для підготовки іноземців та осіб без громадянства замінюється на дисципліну «Українська мова як іноземна».*

*** Дисципліни вільного вибору обираються аспірантами самостійно на початку навчального року з Каталогу вибіркових освітніх компонент, при цьому загальний обсяг таких дисциплін повинен складати 9 кредитів ЄКТС.*

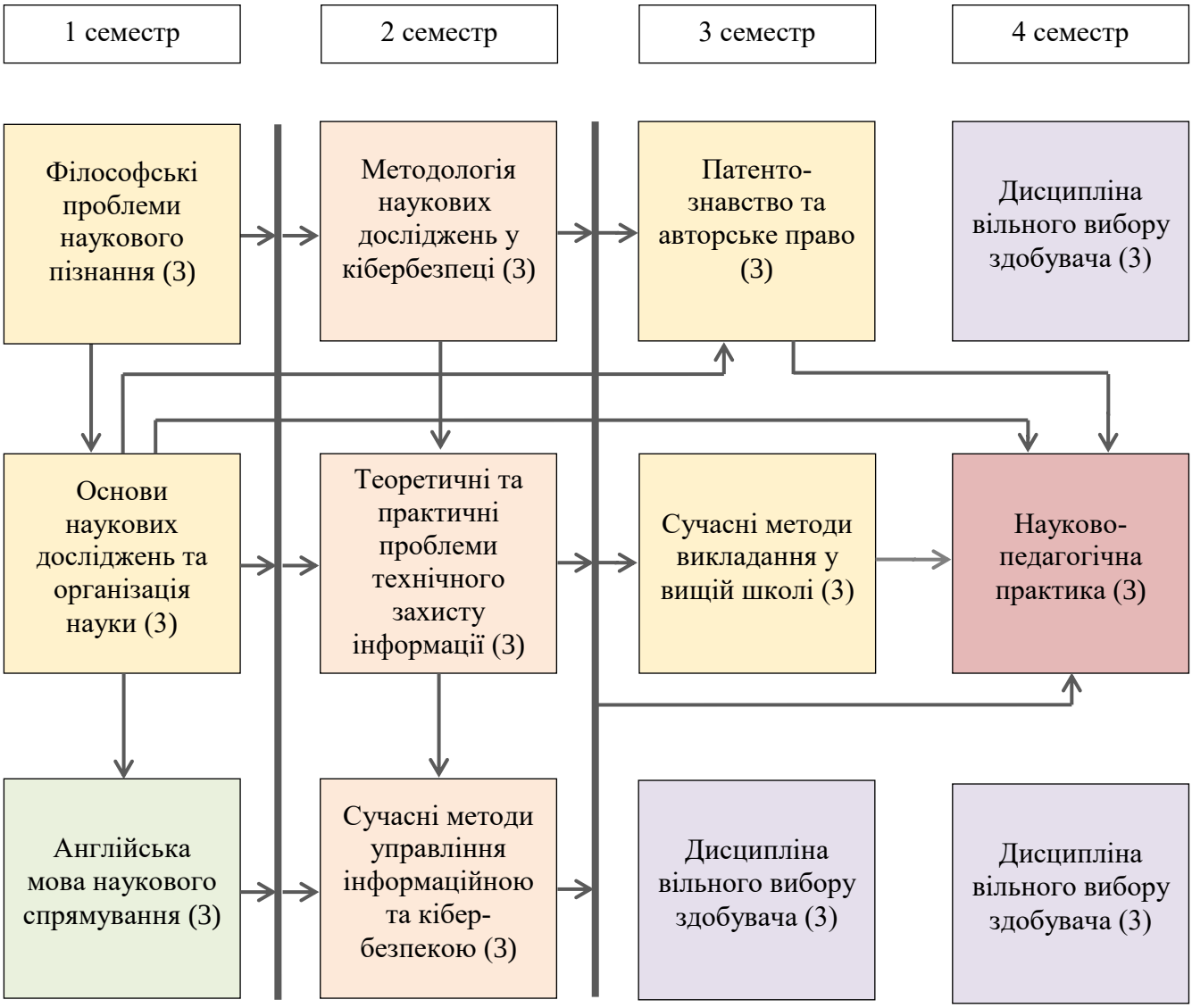
2.2. Перелік компонент освітньої програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти освітньо-наукової програми			
ОК11.1.1.01	Філософські проблеми наукового пізнання	3	Залік
ОК11.1.1.02	Основи наукових досліджень та організація науки	3	Залік
ОК11.1.2.01	Патентознавство та авторське право	3	Залік
ОК11.1.2.02	Сучасні методи викладання у вищій школі	3	Залік
ОК11.1.2.03	Науково-педагогічна практика	3	Залік
ОК11.1.3.01	Англійська мова наукового спрямування *	3	Іспит
ОК11.1.4.01	Методологія наукових досліджень у кібербезпеці	3	Іспит
ОК11.1.4.02	Теоретичні та практичні проблеми технічного захисту інформації	3	Іспит
ОК11.1.4.03	Сучасні методи управління інформаційною та кібербезпекою	3	Іспит
Загальний обсяг обов'язкових компонент:		**27**	
Вибіркові компоненти освітньо-наукової програми			
	*Дисципліна 1***	9	Залік
	*Дисципліна 2***		Залік
	*Дисципліна 3***		Залік
Загальний обсяг вибіркових компонент:		**9**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ		**36**	

** Дисципліна «Англійська мова наукового спрямування» для підготовки іноземців та осіб без громадянства замінюється на дисципліну «Українська мова як іноземна».*

*** Дисципліни вільного вибору обираються аспірантами самостійно на початку навчального року з Каталогу вибіркових освітніх компонент, при цьому загальний обсяг таких дисциплін повинен складати 9 кредитів ЄКТС.*

2.3. Структурно-логічна схема освітньої програми



3. Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів освітнього рівня 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 комплексної проблеми в сфері кібербезпеки та захисту інформації, результати якого мають наукову новизну, теоретичне та практичне значення. Дисертація не повинна містити академічного плагіату, фальсифікації, фабрикації. Дисертація має бути розміщена на сайті Університету (окрім робіт, які містять інформацію з обмеженим доступом).

4. Матриця відповідності визначених Стандартом компетентностей дескрипторам НРК

	Класифікація компетентностей за НРК	**Знання** **Зн1.** Концептуальні та методологічні знання в галузі чи на межі галузей знань або професійної діяльності	**Уміння/Навички** **Ум1.** Спеціалізовані уміння/навички і методи, необхідні для розв'язання значущих проблем у сфері професійної діяльності, науки та/або інновацій, розширення та переоцінки вже існуючих знань і професійної практики **Ум2.** Започаткування, планування, реалізація та коригування послідовного процесу ґрунтовного наукового дослідження з дотриманням належної академічної доброчесності **Ум3.** Критичний аналіз, оцінка і синтез нових та комплексних ідей	**Комунікація** **К1.** Вільне спілкування з питань, що стосуються сфери наукових та експертних знань, з колегами, широкою науковою спільнотою, суспільством у цілому **К2.** Використання академічної української та іноземної мови у професійній діяльності та дослідженнях	**Автономія та відповідальність** **АВ1.** Демонстрація значної авторитетності, інноваційність, високий ступінь самостійності, академічна та професійна доброчесність, постійна відданість розвитку нових ідей або процесів у передових контекстах професійної та наукової діяльності **АВ2.** здатність до безперервного саморозвитку та самовдосконалення
Загальні компетентності					
ЗК1	Здатність до абстрактного мислення, аналізу і синтезу.		Ум1		АВ1, АВ2
ЗК2	Здатність до пошуку, оброблення та аналізу інформації з різних джерел.	Зн1.	Ум1, Ум3	К1	АВ2
ЗК3	Здатність працювати в міжнародному контексті.			К1, К2	АВ1, АВ2
ЗК4	Здатність розв'язувати комплексні проблеми предметної області на основі системного наукового	Зн1.	Ум2	К2	АВ1, АВ2

	світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.				
Спеціальні (фахові) компетентності					
СК1	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.	Зн1	Ум1, Ум2, Ум3	К1, К2	АВ1, АВ2
СК2	Здатність ініціювати, розробляти і реалізовувати комплексні наукові та інноваційні проєкти в сфері кібербезпеки та захисту інформації.			К1, К2	АВ1, АВ2
СК3	Здатність розв’язувати значущі проблеми у сфері кібербезпеки та захисту інформації, розширювати та переоцінювати наявні знання і професійні практики.			К1	АВ2
СК4	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	Зн1	Ум1, Ум2, Ум3		

	інформації.				
СК5	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.	Зн1	Ум1, Ум2, Ум3		АВ2
СК6	Здатність вільно спілкуватися з питань, що стосуються сфери кібербезпеки та захисту інформації, з колегами, широкою науковою спільнотою, суспільством у цілому українською та англійською мовами.		Ум2, Ум3	К1	АВ1
СК7	Здатність здійснювати та організовувати наукову та освітню науково-педагогічну діяльність у закладах вищої освіти.		Ум1, Ум2, Ум3	К1, К2	АВ2
СК8	*Здатність до виробничо-технологічної діяльності щодо удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення кібербезпеки та захисту інформації.*	Зн1	Ум1, Ум3	К2	АВ1, АВ2

5. Матриця відповідності визначених Стандартом результатів навчання та компетентностей

Результати навчання	Компетентності											
	Інтегральна компетентність: Здатність розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики											
	Загальні компетентності				**Спеціальні (фахові) компетентності**							
	ЗК1	ЗК2	ЗК3	ЗК4	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8
1	3	4	5	6	7	8	9	10	11	12	13	14
РН1. 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.			+		+					+		
РН2. Планувати і виконувати експериментальні та/або теоретичні дослідження з кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики.	+	+		+	+	+	+			+	+	
РН3. Критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми.			+	+	+			+				
РН4. 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.		+				+		+			+	+
РН5. Формулювати і перевіряти гіпотези; використовувати для обгрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані.	+			+		+						

1	3	4	5	6	7	8	9	10	11	12	13	14
РН6. 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.	+		+		+		+		+	+	+	
РН7. 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.				+		+			+			
РН8. 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.	+	+			+		+				+	
РН9. 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.	+	+	+					+	+			
РН10. 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.	+		+					+				
РН11. *Визначати проблематику, ставити наукові завдання, пропонувати нові інноваційні рішення у сфері безпеки інформаційно-комунікаційних технологій, криптографічного захисту інформації, захисту мережевих ресурсів та кінцевих точок.*				+	+	+	+	+	+			+
РН12. *Розробляти та досліджувати нові підходи у сфері технічного захисту інформації, контролю доступу до об'єктів інформаційної діяльності, розробки комплексних систем захисту інформації.*				+	+	+	+	+	+			+
РН13. *Досліджувати існуючі та генерувати нові методи управління у сфері кібербезпеки та захисту інформації на основі поєднання наукових методів та кращих практик теорії управління.*				+	+	+	+	+	+			+

6. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК11.1.1.01	ОК11.1.1.02	ОК11.1.2.01	ОК11.1.2.02	ОК11.1.2.03	ОК11.1.3.01	ОК11.1.4.01	ОК11.1.4.02	ОК11.1.4.03
ЗК 1	+								
ЗК 2		+	+						
ЗК 3						+			
ЗК 4	+	+							
СК 1		+				+			
СК 2							+	+	+
СК 3							+	+	+
СК 4							+	+	+
СК 5							+	+	+
СК 6				+		+			
СК 7		+	+	+	+				
СК 8					+		+	+	+

7. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми

	ОК11.1.1.01	ОК11.1.1.02	ОК11.1.2.01	ОК11.1.2.02	ОК11.1.2.03	ОК11.1.3.01	ОК11.1.4.01	ОК11.1.4.02	ОК11.1.4.03
ПРН 1							+	+	+
ПРН 2		+			+				
ПРН 3	+								
ПРН 4	+								
ПРН 5		+							
ПРН 6					+	+			
ПРН 7							+	+	+
ПРН 8							+	+	+
ПРН 9			+						
ПРН 10				+	+				
ПРН 11							+		
ПРН 12								+	
ПРН 13									+

Гарант освітньо-наукової програми «Кібербезпека»
Професор кафедри управління кібербезпекою та захистом інформації
Державного університету інформаційно-комунікаційних технологій

доктор технічних наук, професор **Віталій САВЧЕНКО**