

## ВІДОМОСТІ ПРО ПЕРЕГЛЯД ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ

Оновлення освітніх компонент освітньо-наукової програми відповідно до рекомендацій акредитаційних комісій Університету, пропозицій роботодавців, побажань здобувачів вищої освіти та з урахуванням вимог стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти (Наказ МОН України від 18.03.2021 № 332)

Затверджено рішенням кафедри Інформаційної та кібернетичної безпеки протокол № 9 від «26» березня 2021 р.

Затверджено рішенням Вченої Ради Навчально-наукового інституту захисту інформації протокол № \_\_\_\_\_ від «\_\_\_\_\_» \_\_\_\_\_ 2021 р.

Затверджено рішенням Вченої Ради Університету протокол № \_\_\_\_\_ від «\_\_\_\_\_» \_\_\_\_\_ 2021 р.

Введено в дію наказом ректора № \_\_\_\_\_ від «\_\_\_\_\_» \_\_\_\_\_ 2021 р.

<b>6- Програмні компетентності</b>	
<b>Інтегральна компетентність</b>	Здатність розв'язувати комплексні проблеми в галузі кібербезпеки, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики.
<b>Загальні компетентності (ЗК)</b>	<b>ЗК-1. Уміння критичної самооцінки</b> – здатність визначати та задовольняти потреби особистого та наукового розвитку, бути критичним і самокритичним. <b>ЗК-2. Навички творчого спілкування</b> – здатність спілкуватися результативно в усній і письмовій формах з фахівцями та нефахівцями, здатність спілкуватися другою мовою. <b>ЗК-3. Знання інформаційних технологій</b> – здатність використовувати інформаційні і комунікаційні технології для впровадження проєктів в інформаційній та безпековій сферах. <b>ЗК-4. Навички керування проєктами</b> – здатність демонструвати своєчасність та спланованість у дослідженні, здатність до адаптації та дії в новій ситуації, здатність розробляти та управляти проєктами. <b>ЗК-5. Уміння підтримати інших</b> – здатність допомагати через викладання, наставництво та наочні приклади (демонстрацію). <b>ЗК-6. Уміння працювати етично</b> – здатність визначати,

	<p>поважати та керувати етичними, культурними та іншими питаннями, пов'язаними з наявністю тих чи інших відмінностей.</p> <p><b>ЗК-7. Навички підприємництва</b> – здатність визначати підприємницькі можливості чи вид діяльності або громадського впливу, здатність приймати обґрунтовані рішення, здатність оцінювати та забезпечувати якість виконуваних робіт.</p> <p><b>ЗК-8. Уміння командної роботи</b> – знання про стимули та бар'єри в ефективній командній роботі, вміння виявляти, ставити та вирішувати проблеми.</p>
<p><b>Фахові компетентності (ФК)</b></p>	<p><b>ФК-1. Інтегративна компетентність</b> – здатність до інтеграції знань, умінь і навичок та їх ефективного використання в умовах швидкої адаптації організацій до вимог зовнішнього середовища, що забезпечують виконання завдань науково-дослідної, науково-педагогічної, управлінської та інноваційної діяльності в інформаційній та безпековій сфері тощо.</p> <p><b>ФК-2. Соціально-психологічна компетентність</b> (емоційні, перцептивні, концептуальні, поведінкові) – здатність особистості орієнтуватися у різних життєвих ситуаціях, ефективно працювати в умовах ринкової економіки; уміння реалізувати стратегії і плани; здатність до розуміння поведінки людей, мотивації та організації їх спільної діяльності тощо.</p> <p><b>ФК-3. Організаційно-комунікативна компетентність</b> (у специфічних сферах управлінської діяльності) – здатність до лідерства та новаторської діяльності, до формування високого рівня комунікативної культури; здатність переконувати оточуючих, стверджувати свою позицію; володіння державною мовою, грамотним усним та писемним діловим мовленням, ораторським мистецтвом, професійним етикетом, а також навичками публічної презентації результатів роботи, вміннями обирати відповідні форми і методи презентації; володіння іноземними мовами, уміння правильно розмовляти та писати різними комунікативними стилями, а саме неофіційним, офіційним та науковим тощо.</p> <p><b>ФК-4. Професійна компетентність</b> – стан теоретичної та практичної підготовленості, що забезпечує ефективність вирішення професійних проблем і типових професійних завдань; стан володіння інформаційними технологіями та технологіями захисту інформації; здатність до удосконалення та впровадження у практику інновацій у сфері</p>

інформаційної та кібербезпеки; ступінь використання наукової літератури та інших джерел інформації для реалізації інноваційних технологій; здатність до здійснення ефективного пошуку та структурування інформації, до кваліфікованої роботи з різними ІР тощо.

**ФК-5. Загальнонаукова компетентність** – здатність до накопичення професійних вмінь та навичок (діагностування й інтерпретування ситуацій, планування та здійснення наукових досліджень, викладання у вищому навчальному закладі предметів, що відносяться до галузі інформаційних технологій та захисту інформації); здатність до генерування нових знань з теорії захисту інформації та інформаційної безпеки, з проблем алгоритмізації та програмування процесів в системах кібербезпеки; здатність до застосування нових знань у професійній діяльності (проектній, винахідницькій та раціоналізаторській роботі) тощо.

**ФК-6. Політехнічна компетентність** – знання загальних (методологічних, історичних, економічних, ергономічних тощо) питань безпекової сфери, принципів дії і будови основних функціональних органів інформаційних систем; здатність до оволодіння спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та безпечними технологіями; здатність до застосування різноманітних, професійно профільованих знань і практичних навичок у сфері захисту інформації.

**ФК-7. Інженерна компетентність** – здатність до виробничо-технологічної діяльності (розробки та впровадження інноваційних технологій інформаційної безпеки, вибору технології ІБ, устаткування та засобів, використання інформаційних технологій; розробки програм і методик випробувань систем інформаційної та кібербезпеки); здатність до організаційно-управлінської діяльності (організації процесу створення та надання інфокомунікаційних послуг); здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем, до обробки та перетворення інформації тощо.

**ФК-8. Ділова компетентність** – здатність і готовність здійснювати ефективну професійну діяльність у відповідній галузі, надавати інфокомунікаційні послуги

	<p>та послуги безпеки; здатність до планування й реалізації заходів із захисту інформації в ІКС, створення та забезпечення функціонування систем інформаційної та кібербезпеки; здатність до формування правильних висновків, оперативного приймання та реалізації нестандартних рішень тощо.</p>
<b>7 – Програмні результати навчання</b>	
<p><b>Програмні результати навчання (ПРН)</b></p>	<p><b>ПРН-1. Уміти</b> формувати і аргументовано відстоювати власну позицію з різних проблем філософії науки та методології наукового пізнання.</p> <p><b>ПРН-2. Уміти</b> визначати та задовольняти потреби особистого та наукового розвитку, бути критичним і самокритичним.</p> <p><b>ПРН-3. Уміти вести</b> дискусії і полеміки, здійснювати публічні промови, робити повідомлення і доповіді з питань дисертаційного дослідження, аргументовано викладати власну точку зору державною та іноземною мовою.</p> <p><b>ПРН-4. Уміти читати</b> оригінальну наукову літературу на іноземній мові, опрацьовувати та оформляти інформацію.</p> <p><b>ПРН-5. Уміти розробляти</b> логічні схеми, складати план-проспекти та технічні завдання на виконання наукових досліджень.</p> <p><b>ПРН-6. Уміти здійснювати</b> бібліографічний пошук і відбір літературних джерел, складати їх бібліографічний опис.</p> <p><b>ПРН-7. Уміти моделювати</b> структуру наукового дослідження, формулювати мету, об'єкт, предмет та наукові задачі, упорядковувати та систематизувати результати дослідження, обґрунтовувати їх достовірність та проводити їх апробацію.</p> <p><b>ПРН-8. Уміти обґрунтовувати</b> та формулювати висновки щодо проведених наукових досліджень та рекомендації щодо їх наукового і практичного використання.</p> <p><b>ПРН-9. Володіти вмінням</b> робити наукові доповіді щодо захисту результатів дослідження, аргументувати і захищати теоретичну позицію на основі емпіричної роботи.</p> <p><b>ПРН-10. Уміти узагальнювати</b> і критично оцінювати результати, отримані вітчизняними і зарубіжними дослідниками.</p> <p><b>ПРН-11. Уміти характеризувати</b> основні елементи системи та змісту вищої освіти в Україні, приймати</p>

рішення щодо критеріїв якості навчання та діагностики знань.

**ПРН-12. Уміти визначати основні параметри інформаційних ресурсів наукового дослідження (навчального процесу), планувати структуру, зміст та процес організації його проведення (лекцій, практично-семінарських занять).**

**ПРН-13. Уміти 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.**

**ПРН-14. Володіти навиками роботи із спеціалізованими системами криптозахисту та криптоаналізу, управляти змінами при роботі з існуючими системами криптографічного захисту.**

**ПРН-15. Уміти орієнтуватися у сучасних концепціях і моделях, методах та засобах управління інцидентами інформаційної безпеки.**

**ПРН-16. Уміти розробляти та проектувати нові, вдосконалювати існуючі системи управління інформаційною безпекою.**

**ПРН-17. Уміти підтримувати комплексні системи інформаційної та кібербезпеки в стані, необхідному для вирішення завдань захисту інформації.**

**ПРН-18. Уміти аналізувати існуючі технології, методи і засоби застосування шкідливого програмного забезпечення, нівелювання уразливостей мережевих та Web-ресурсів.**

**ПРН-19. Уміти проектувати перспективні технології виявлення шкідливого програмного забезпечення, а також уразливостей мережевих та Web-ресурсів й застосовувати їх на практиці.**

**ПРН-20. Уміти визначати і вирішувати етичні питання при проведенні досліджень та пошуку відмінностей у шкідливому програмному забезпечення, уразливостях мережевих та Web-ресурсів.**

**ПРН-21. Уміти аналізувати та розробляти алгоритми, методики, моделі та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки.**

**ПРН-22. Уміти розробляти та впроваджувати дослідницькі проекти в галузі знань «інформаційні технології» спеціальності «кібербезпека» для забезпечення безпеки мережевої інфраструктури.**

**ПРН-23. Бути здатним** генерувати нові знання з теорії захисту інформації та інформаційної безпеки, з проблем алгоритмізації та програмування процесів в системах кібербезпеки.

**ПРН-24. Уміти** здійснювати науково-технічне супроводження заходів з формування і коригування програмних комплексів забезпечення безпеки та захисту інформації на об'єктах інформаційної діяльності.

**ПРН-25. Уміти** визначати можливості для підприємницької та громадської діяльності за напрямом захисту інформації, організації й забезпечення інформаційної та кібербезпеки об'єктів інформаційної діяльності.

**ПРН-26. Уміти** 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.

**ПРН-27. Бути здатним** оволодіти спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та безпековими технологіями.

**ПРН-28. Бути здатним** до застосування різноманітних, професійно профільованих знань і практичних навичок у сфері захисту інформації.

**ПРН-29. Уміти розробляти та впроваджувати** раціональні технології інформаційної безпеки, програми і методики випробувань систем інформаційної та кібербезпеки

**ПРН-30. Бути здатним** до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем, до обробки та перетворення інформації тощо.

**ПРН-31. Уміти** проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та кібербезпеки об'єктів інформаційної діяльності.

**ПРН-32. Уміти** обґрунтовувати раціональні шляхи щодо захисту інформації на об'єктах інформаційної діяльності та інформації, що циркулює в ІТ системах та мережах.

## 8 – Ресурсне забезпечення реалізації програми

Кадрове забезпечення

Група забезпечення спеціальності 125 Кібербезпека

	сформована у відповідності до Ліцензійних вимог
<b>Матеріально-технічне забезпечення</b>	<p>Теоретичні заняття проводяться в сучасних комп'ютерних класах та спеціалізованих лабораторіях, які оснащені спеціалізованими апаратно-програмними засобами.</p> <p>Для проведення досліджень, практичних та лабораторних занять з метою формування професійних компетентностей зі спеціальності 125 Кібербезпека використовуються 6 спеціалізованих лабораторій, які оснащені сучасними комп'ютерами, програмно-апаратними комплексами та мультимедійними системами, а саме:</p> <p><b>НАВЧАЛЬНА ЛАБОРАТОРІЯ АКАДЕМІЧНИЙ ЦЕНТР КОМПЕТЕНЦІЙ ІВМ «КІБЕРПОЛІГОН»</b></p> <p>Лабораторія призначена для проведення практичних занять з використанням програмно-апаратних комплексів: IBM QRadar SIEM, IBM i2 Analyze 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.</p> <p><b>НАВЧАЛЬНА ЛАБОРАТОРІЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ НА БАЗІ ТЕХНОЛОГІЙ «АВТОР»</b></p> <p>Лабораторія використовується для вивчення спеціалізованих засобів криптографічного захисту на базі продуктів компанії АВТОР – партнера кафедри Інформаційної та кібернетичної безпеки. 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 вивчати та застосовувати програмно-технічний комплекс «Центр сертифікації ключів», засоби криптографічного захисту IP-шифратор CryptoIP-448, електронні ключі “SecureToken-337, програмний IP-шифратор «CryptoIP-VPN Client», безконтактні карт-рідери КР-382, USB.</p> <p><b>НАВЧАЛЬНА ЛАБОРАТОРІЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ CISCO</b></p> <p>Лабораторія призначена для вивчення технологій мережевої безпеки CISCO, проведення тренінгів з</p>

впровадження технології HoneyPot щодо протидії кібератакам зловмисників на корпоративні інформаційні системи та сертифікаційних курсів від партнера кафедри Інформаційної та кібернетичної безпеки – компанії CISCO: Introduction to Cybersecurity, CCNA Security, CCNA Cybersecurity Operations.

**НАВЧАЛЬНА ЛАБОРАТОРІЯ ЦЕНТР УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ (SECURITY OPERATION CENTER)**

Лабораторія призначена для проведення занять з питань аналізу, обробки та аудиту інформаційної безпеки за допомогою SIEM-систем та програмних сканерів типу Nessus та Kali Linux. Крім того, дозволяє вивчати методи управління ризиками на основі методологій CRAMM, OSTATE та RiskWatch у відповідності до вимог міжнародних стандартів з інформаційної та кібербезпеки. Дозволяє працювати з програмними засобами підтримки прийняття рішень у сфері інформаційної безпеки («Вибір», Mpriority 1.0).

**НАВЧАЛЬНА ЛАБОРАТОРІЯ ЗАСОБІВ КОНТРОЛЮ ДОСТУПУ «HIKVISION»** – забезпечує проведення практичних занять та досліджень з питань контролю та управління доступом, використання автономних біометричних терміналів, мережевих контролерів, програмно-апаратного комплексу системи відеоспостереження HikVision. Обладнана автоматизованим комплексом відеоспо-стереження та охорони об'єктів інформаційної діяльності (Harbor), програмно-апаратними комплексами контролю доступу (HikVision), сповіщувачами інфрачервоними (SRP 600) та магніто-контактними (СОМК-10). Дозволяє вивчати питання застосування програмних комплексів захисту інформації («Лоза», «Гриф», «Рубіж»).

**НАВЧАЛЬНА ЛАБОРАТОРІЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ «РІАС»** – забезпечує проведення практичних занять з питань технічного захисту конфіденційної інформації на об'єктах інформаційної діяльності від витоку акустичним, віброакустичним та електромагнітним каналами з використанням ширококутових генераторів акустичного та електромагнітного шуму (Ріас-2ГС, ГШ 1000, «Беркут»). Крім того, у лабораторії досліджуються питання застосування пошукового програмно-апаратного комплексу DigiSkan EX; методів виявлення випромінювань за допомогою індикаторів поля типу ПРОТЕКТ; порядку застосування скануючих



	приймачів AR 8200, IC-R5, IC-R2500 та локатора нелінійностей NR-900 EM.
<b>Інформаційне та навчально-методичне забезпечення</b>	Всі дисципліни навчального плану забезпечені інформаційними та навчально-методичними матеріалами, засобами системи дистанційного навчання Moodle у т.ч. доступом до електронної бібліотеки Державного університету телекомунікацій.
<b>9 – Академічна мобільність</b>	
<b>Національна кредитна мобільність</b>	Наявність двосторонніх договорів між Державним університетом телекомунікацій та закладами вищої освіти України забезпечує національну кредитну мобільність
<b>Міжнародна кредитна мобільність</b>	Зміст освітньо-наукової програми відповідає стандартам вищої освіти, що дозволяє приймати участь у програмах подвійних дипломів та бути конкурентоспроможним на світовому ринку праці
<b>Навчання іноземних здобувачів вищої освіти</b>	Передбачає навчання іноземців та осіб без громадянства після акредитації освітньо-наукової програми

## 2. Перелік компонент освітньо-наукової програми та їх логічна послідовність

### 2.1. Зміст підготовки за освітньо-науковою програмою, компетентності та результатами навчання

№ п.п.	Дисципліна	Шифр	Компетентність	Результат навчання
<b>1. Цикл обов'язкових компонент освітньо-наукової програми</b>				
<b>1.1. Здобуття глибоких знань зі спеціальності</b>				
1.	Методологія наукових досліджень у кібербезпеці	OK11.1.1.01	ФК3, ФК4, ФК5, ФК6, ФК7	ПРН14, ПРН18, ПРН19, ПРН20, ПРН22, ПРН23, ПРН26, ПРН27, ПРН30
2.	Теоретичні та практичні проблеми технічного захисту інформації	OK11.1.1.02	ФК1, ФК4, ФК5, ФК6, ФК7	ПРН5, ПРН13, ПРН17, ПРН21, ПРН24, ПРН25, ПРН31, ПРН32
3.	Сучасні методи управління інформаційною та кібербезпекою	OK11.1.1.03	ФК1, ФК2, ФК6, ФК7, ФК8	ПРН12, ПРН15, ПРН16, ПРН21, ПРН25, ПРН28, ПРН29, ПРН30
<b>1.2. Оволодіння загальнонауковими (філософськими) компетентностями</b>				
4.	Філософія	OK11.1.2.01	ЗК1, ЗК5, ЗК6	ПРН1, ПРН2, ПРН3, ПРН9, ПРН10
5.	Основи наукових досліджень та організація науки	OK11.1.2.02	ФК1, ФК5, ФК7	ПРН5, ПРН6, ПРН7, ПРН8, ПРН10, ПРН12, ПРН13, ПРН29
<b>1.3. Набуття універсальних навичок дослідника</b>				
6.	Патентознавство та авторське право	OK11.1.3.01	ЗК4, ЗК7	ПРН3, ПРН6, ПРН10, ПРН24
7.	Сучасні методи викладання у вищій школі	OK11.1.3.02	ФК2, ФК3	ПРН1, ПРН11, ПРН13, ПРН28
8.	Педагогічна практика	OK11.1.3.03	ФК3, ФК4, ФК8	ПРН1, ПРН9, ПРН11, ПРН28
<b>1.4. Здобуття мовних компетентностей</b>				
9.	Англійська мова наукового спрямування *	OK11.1.4.01	ЗК2, ЗК3, ЗК8, ФК3	ПРН3, ПРН4, ПРН10, ПРН13
<b>2. Цикл вибірових компонент освітньо-наукової програми</b>				
10.	Дисципліна 1**			
11.	Дисципліна 2**			
12.	Дисципліна 3**			
13.	Дисципліна 4**			
14.	Дисципліна 5**			

\* Дисципліна «Іноземна мова» 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 вибірових освітніх компонентів, при цьому загальний обсяг таких дисциплін повинен складати 15 кредитів ЄКТС.

## 2.2. Перелік компонент освітньо-наукової програми

Код н/д	Компоненти освітньо-наукової програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
<b>Обов'язкові компоненти освітньо-наукової програми</b>			
OK11.1.1.01	Методологія наукових досліджень у кібербезпеці	4	Іспит
OK11.1.1.02	Теоретичні та практичні проблеми технічного захисту інформації	4	Іспит
OK11.1.1.03	Сучасні методи управління інформаційною та кібербезпекою	4	Іспит
OK11.1.2.01	Філософія	3	Іспит
OK11.1.2.02	Основи наукових досліджень та організація науки	3	Залік
OK11.1.3.01	Патентознавство та авторське право	3	Залік
OK11.1.3.02	Сучасні методи викладання у вищій школі	3	Залік
OK11.1.3.03	Педагогічна практика	6	Залік
OK11.1.4.01	Англійська мова наукового спрямування *	15	Іспит
<b>Загальний обсяг обов'язкових компонент:</b>		<b>45</b>	
<b>Вибіркові компоненти освітньо-наукової програми</b>			
	<i>Дисципліна 1**</i>	15	Залік
	<i>Дисципліна 2**</i>		Залік
	<i>Дисципліна 3**</i>		Залік
	<i>Дисципліна 4**</i>		Залік
	<i>Дисципліна 5**</i>		Залік
<b>Загальний обсяг вибіркового компонент:</b>		<b>15</b>	
<b>ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ</b>		<b>60</b>	

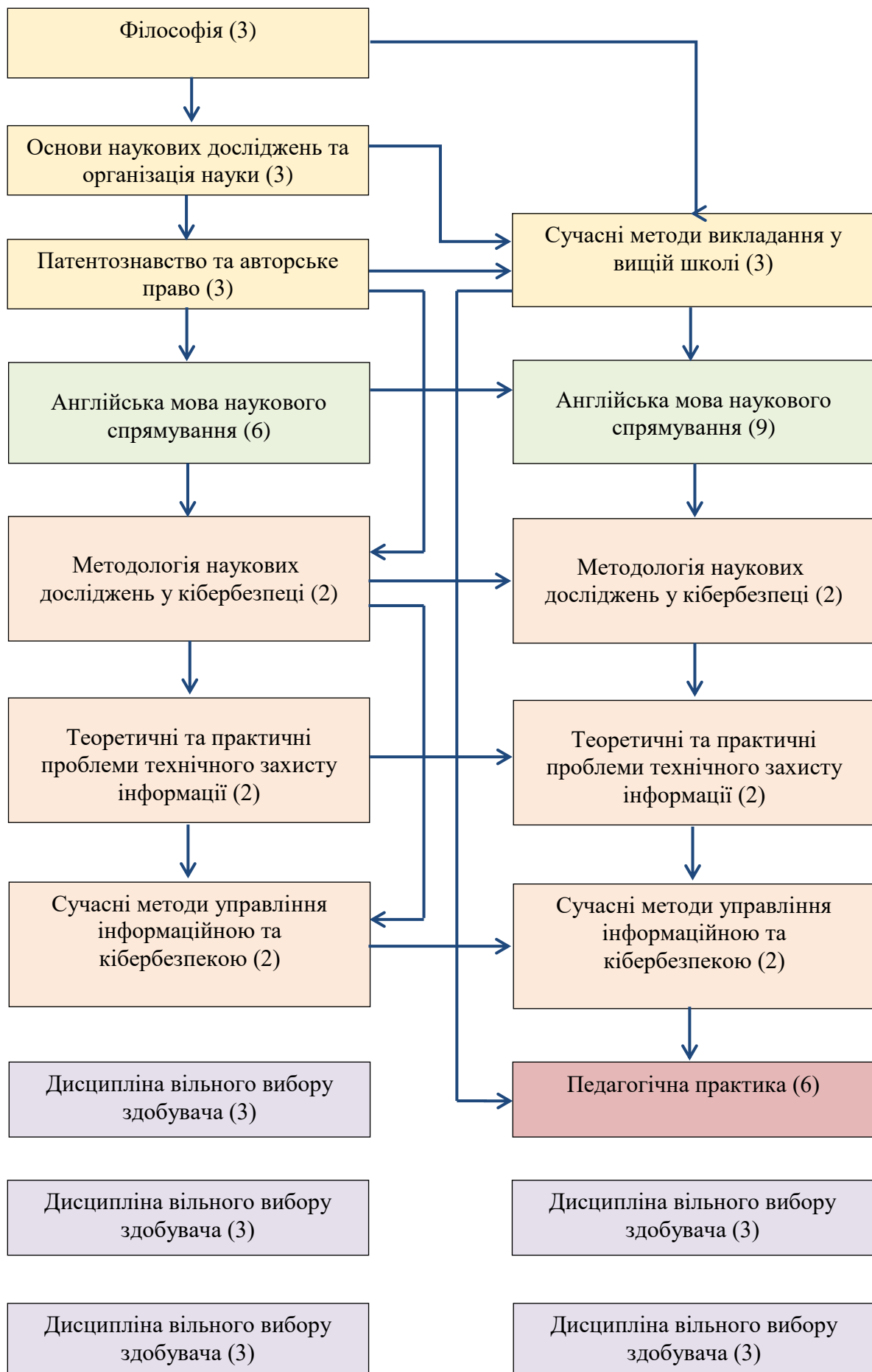
\* Дисципліна «Іноземна мова» для підготовки іноземців та осіб без громадянства замінюється на дисципліну «Українська мова як іноземна».

\*\* Дисципліни вільного вибору обираються аспірантами самостійно на початку навчального року з Каталогу вибіркового освітніх компонентів, при цьому загальний обсяг таких дисциплін повинен складати 15 кредитів ЄКТС.

### 2.3. Структурно-логічна схема освітньо-наукової програми (частина 1)

Цикл	I курс				Всього	
	1 семестр		2 семестр		Кр.	%
Здобуття глибоких знань зі спеціальності	Методологія наукових досліджень у кібербезпеці	2	Методологія наукових досліджень у кібербезпеці	2		
	Теоретичні та практичні проблеми технічного захисту інформації	2	Теоретичні та практичні проблеми технічного захисту інформації	2		
	Сучасні методи управління інформаційною та кібербезпекою	2	Сучасні методи управління інформаційною та кібербезпекою	2		
	<b>Всього</b>	<b>6</b>	<b>Всього</b>	<b>6</b>	<b>12</b>	<b>20%</b>
Оволодіння загальнонауковими (філософськими) компетентностями	Філософія	3				
	Основи наукових досліджень та організація науки	3				
	<b>Всього</b>	<b>6</b>	<b>Всього</b>	<b>0</b>	<b>6</b>	<b>10%</b>
Набуття універсальних навичок дослідника	Патентознавство та авторське право	3	Сучасні методи викладання у вищій школі	3		
			Педагогічна практика	6		
	<b>Всього</b>	<b>3</b>	<b>Всього</b>	<b>9</b>	<b>12</b>	<b>20%</b>
Здобуття мовних компетентностей	Англійська мова наукового спрямування	6	Англійська мова наукового спрямування	9		
	<b>Всього</b>	<b>6</b>	<b>Всього</b>	<b>9</b>	<b>15</b>	<b>25%</b>
Цикл вибірових компонент	<i>Дисципліна 1</i>	3	<i>Дисципліна 4</i>	3		
	<i>Дисципліна 2</i>	3	<i>Дисципліна 5</i>	3		
	<i>Дисципліна 3</i>	3				
	<b>Всього</b>	<b>9</b>	<b>Всього</b>	<b>6</b>	<b>15</b>	<b>25%</b>
	<b>Всього за I курс</b>	<b>30</b>		<b>30</b>	<b>60</b>	<b>100%</b>

## Структурно-логічна схема освітньо-наукової програми (частина 2)



### 3. Форма атестації здобувачів вищої освіти

<b>Форми атестації здобувачів вищої освіти</b>	Атестація докторів філософії із кібербезпеки здійснюється у формі публічного захисту дисертаційної роботи на спеціалізованій вченій раді після успішного складання іспитів і заліків освітньої складової програми.
<b>Вимоги до кваліфікаційної роботи</b>	Дисертація на здобуття наукового ступеня є кваліфікаційною науковою працею, виконаною особисто здобувачем у вигляді спеціально підготовленого рукопису або опублікованої монографії. Підготовлена до захисту дисертація повинна містити висунуті здобувачем науково обґрунтовані теоретичні або експериментальні результати а також характеризуватися єдністю змісту і свідчити про особистий внесок здобувача в науку у галузі інформаційної та кібербезпеки. Робота має бути перевірена на плагіат відповідно до «Кодексу академічної доброчесності Державного університету телекомунікацій» та оприлюднена у репозитарії Університету.

#### 4. Матриця відповідності програмних компетентностей компонентам освітньо-наукової програми

	OK11.1.1.01	OK11.1.1.02	OK11.1.1.03	OK11.1.2.01	OK11.1.2.02	OK11.1.3.01	OK11.1.3.02	OK11.1.3.03	OK11.1.4.01
ЗК 1				•					
ЗК 2									•
ЗК 3									•
ЗК 4						•			
ЗК 5				•					
ЗК 6				•					
ЗК 7						•			
ЗК 8									•
ФК 1		•	•		•				
ФК 2			•				•		
ФК 3	•						•	•	•
ФК 4	•	•						•	
ФК 5	•	•			•				
ФК 6	•	•	•						
ФК 7	•	•	•		•				
ФК 8			•					•	

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

	ОК11.1.1.01	ОК11.1.1.02	ОК11.1.1.03	ОК11.1.2.01	ОК11.1.2.02	ОК11.1.3.01	ОК11.1.3.02	ОК11.1.3.03	ОК11.1.4.01
ПРН 1				•			•	•	
ПРН 2				•					
ПРН 3				•		•			•
ПРН 4									•
ПРН 5		•			•				
ПРН 6					•	•			
ПРН 7					•				
ПРН 8					•				
ПРН 9				•				•	
ПРН 10				•	•	•			•
ПРН 11							•	•	
ПРН 12			•		•				
ПРН 13		•			•		•		•
ПРН 14	•								
ПРН 15			•						
ПРН 16			•						
ПРН 17		•							
ПРН 18	•								
ПРН 19	•								
ПРН 20	•								
ПРН 21		•	•						
ПРН 22	•								
ПРН 23	•								
ПРН 24		•				•			
ПРН 25		•	•						
ПРН 26	•								
ПРН 27	•								
ПРН 28			•				•	•	
ПРН 29			•		•				
ПРН 30	•		•						
ПРН 31		•							
ПРН 32		•							

**Гарант освітньо-наукової програми**

Директор Навчально-наукового інституту захисту інформації  
Державного університету телекомунікацій

доктор технічних наук, професор

**В.А. Савченко**