

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-
КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА
другого (магістерського) рівня вищої освіти
(ПРОЄКТ)

Спеціальність **F5 Кібербезпека та захист інформації**

Галузь знань **F Інформаційні технології**

Кваліфікація: **Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою інформаційна та кібернетична безпека**

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Протокол № _____ від _____ 2026 р.

Наказ № _____ від _____ 2026 р.

Ректор _____ Володимир ШУЛЬГА

Освітня програма вводиться в дію з 01 вересня 2026 р.

**ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА»
ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ**

спеціальність	<i>F5 Кібербезпека та захист інформації</i>
галузь знань	<i>F Інформаційні технології</i>
рівень вищої освіти	<i>другий (магістерський)</i>
освітня кваліфікація	<i>Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою інформаційна та кібернетична безпека</i>

1. Перший проректор _____ Олександр КОРЧЕНКО

2. Проректор з навчальної роботи _____ Артур ГУДМАНЯН

3. Начальника навчально-методичного відділу _____ Вадим ВЛАСЕНКО

4. Вчена рада Навчально-наукового інституту кібербезпеки та захисту інформації

Протокол № _____ від « _____ » _____ 20 _____ р.

Голова Вченої Ради ННІЗІ _____ Євгенія ІВАНЧЕНКО

5. Кафедра систем та технологій кібербезпеки

Протокол № _____ від « _____ » _____ 20 _____ р.

Завідувач кафедри систем та технологій
кібербезпеки _____ Галина ГАЙДУР

Рецензії від зовнішніх стейкхолдерів:

Рецензії на освітньо-професійну програму підготовки здобувачів вищої освіти:

1. ТОВ «ЄВРОТЕЛЕКОМ».

2. Київський національний університет ім. Тараса Шевченка.

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Гарант освітньої програми (голова робочої групи)

Галина ГАЙДУР – доктор технічних наук, професор, завідувач кафедри систем та технологій кібербезпеки;

Члени робочої групи:

Сергій ЗИБІН – доктор технічних наук, професор, професор кафедри систем та технологій кібербезпеки;

Сергій ГАХОВ – кандидат військових наук, доцент, доцент кафедри систем та технологій кібербезпеки;

Віталій МАРЧЕНКО – кандидат технічних наук, доцент, доцент кафедри систем та технологій кібербезпеки;

Павло БУЛАВІН –директор ТОВ "ЄВРОТЕЛЕКОМ.

ВІДОМОСТІ ПРО ПЕРЕГЛЯД ОСВІТНЬОЇ ПРОГРАМИ

Оновлення (змісту освітніх компонентів та освітньої програми) відповідно до:

пропозицій та побажань стейкхолдерів (здобувачів вищої освіти, науково-педагогічних працівників, випускників, роботодавців, громадської організації) та з урахуванням тенденцій розвитку спеціальності, ринку праці, галузевого контексту, а також досвіду аналогічних вітчизняних та іноземних освітніх програм.

Державного стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти (Наказ МОН України від 18.03.2021 № 332);

Професійного стандарту на групу професій «Викладачі закладів вищої освіти» (Наказ Міністерства економіки від 23.03.2021 № 610);

Постанови Кабінету Міністрів України «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 16.12.2022 №1392;

Наказу Міністерства економіки України «Про затвердження зміни № 11 до національного класифікатора ДК 003:2010» «Класифікатор професій» від 29.12.2022 № 5573;

рекомендацій акредитаційних комісій Університету; пропозицій роботодавців; побажань здобувачів вищої освіти.

Затверджено рішенням кафедри систем та технологій кібербезпеки

протокол № _____ від « ____ » _____ 2026 р.

Введено в дію наказом ректора № ____ від _____ 20__ року.

1. Профіль освітньої програми

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Державний університет інформаційно-комунікаційних технологій, Навчально-науковий інститут захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Освітня кваліфікація – Магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека
Офіційна назва освітньої програми	Освітньо-професійна програма «Інформаційна та кібернетична безпека»
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний Обсяг освітньої програми-90 кредитів ЄКТС; термін навчання 1 рік 5 місяців (денна), 1 рік 10 місяців (заочна)
Наявність акредитації	
Цикл/рівень	НРК України – 7 рівень/ Магістр, QF-EHEA- другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра, освітнього ступеня магістра (освітньо-кваліфікаційного рівня спеціаліста) іншої спеціальності.
Мова(и) викладання	Українська, англійська
Термін дії освітньої програми	Введена в дію з 01.09.2017 року
Інтернет - адреса постійного розміщення опису освітньої програми	https://duikt.edu.ua/ua/1822-osvitno-profesiyni-programi-kafedra-informaciynoi-ta-kibernetichnoi-bezpeki

2 – Мета освітньої програми

Метою освітньо-наукової програми є підготовка висококваліфікованих фахівців з кібербезпеки та захисту інформації в інформаційних і комунікаційних системах, які здатні:

- розв'язувати задачі дослідницького та інноваційного характеру;
- описувати та роз'яснювати процеси, що відбуваються у сфері інформаційної та/або кібернетичної безпеки;
- здійснювати апробацію та практичне впровадження наукових результатів;
- володіти інноваційними способами мислення та мати компетентності, необхідні для проведення досліджень сучасних процесів, аналізу, створення та захисту інформаційних систем і технологій на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки;
- проводити розслідування кіберінцидентів;

- підтримувати інфраструктуру кіберзахисту;
- володіти навичками аналітичної роботи з інформацією.

Набуті компетентності можуть бути застосовані в дослідницькій, управлінській, освітній, бізнесовій та інших дисциплінарно-професійних полях.

3 – Характеристика освітньої програми

Опис предметної області

Об'єкти вивчення:

- сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки;
- інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології;
- інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур;
- системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків);
- інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси);
- програмне та програмно-апаратне забезпечення (засоби) кіберзахисту;
- системи управління інформаційною безпекою та/або кібербезпекою;
- технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки.

Цілі навчання:

Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.

Теоретичний зміст предметної області

Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки.

Методи, методики та технології

Методи, моделі, методики та технології створення,

	<p>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.</p> <p>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.</p> <p>Інструменти та обладнання.</p> <p>Засоби, пристрої, 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), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.</p>
<p>Орієнтація освітньої програми</p>	<p>Освітньо-професійна програма підготовки розроблена для студентів, які прагнуть стати професіоналами у сфері кібербезпеки, наукової та інноваційної діяльності забезпечення безпеки інформаційних систем та технологій. Програма ґрунтується на загальновідомих наукових результатах з врахуванням сьогоdnішнього стану сфери кібербезпеки, має прикладний характер, спрямована на забезпечення потреб ринку праці при вирішенні професійних задач в галузі кібербезпеки та захисту інформації.</p>
<p>Основний фокус освітньої програми та спеціалізації</p>	<p>Дослідження в галузі кібербезпеки.</p> <p>Акцент на впровадженні інноваційних методів та технологій в процесі захисту інформації в інформаційних і кібернетичних системах на підприємствах, в установах і організаціях.</p> <p>Ключові слова: ІНФОРМАЦІЯ, ЗАГРОЗИ, ІНЦИДЕНТ, ВРАЗЛИВОСТІ, ІНФРАСТРУКТУРА, КІБЕРБЕЗПЕКА.</p>
<p>Особливості програми</p>	<p>Програма реалізується науковими групами, передбачає застосування широкого кола загальнонаукових і спеціальних аналітичних методів, принципів і прийомів наукових досліджень, з врахуванням сучасного світового досвіду в галузі кібербезпеки та захисту інформації.</p>

	<p>Передбачено проведення лекційних курсів, семінарських та практичних занять, тренінгів, з залученням фахівців з інформаційної безпеки та самостійної науково-дослідної роботи.</p> <p><i>В програму впроваджені результати проекту Європейського союзу Tempus №544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR «Освіта експертів наступного покоління в галузі кібербезпеки: нова програма магістерської програми ЄС».</i></p> <p><i>В програму впроваджені результати академічної співпраці з компанією IBM «SkillsBuild».</i></p>
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	<p>Магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека (випускник) здатний виконувати професійні роботи за Державним класифікатором професій ДК 003: 2010:</p> <p>Основна: 2139.2 Фахівець з реагування на інциденти кібербезпеки Фахівець з підтримки інфраструктури кіберзахисту 2310.2 – викладач закладу вищої освіти</p>
Академічні права випускників	<p>Продовжити освіту за третім (освітньо-науковим) рівнем вищої освіти.</p> <p>Набуття додаткових кваліфікацій в системі дорослої освіти.</p>
5 – Викладання та оцінювання	
Викладання та навчання	<p>Студентоцентроване навчання і викладання. Викладання проводиться державною мовою. Іноземною мовою (англійською) проводиться викладання окремих дисциплін, які формують професійні компетентності. Викладання спрямовано на засвоєння знань, умінь і навичок для подальшого застосування у практиці, яке доповнюється практичними складовими компаніями партнерами.</p> <p>Основними способами передачі змісту освітньої програми є проведення лекцій, практичних, лабораторних і індивідуальних занять, консультацій, розв'язання ситуативних завдань, тестування, презентацій, змістовні кейси від партнерів кафедри науково-дослідна, науково-педагогічна, переддипломна практики.</p>

Оцінювання	<p>Накопичувальна бально-рейтингова система, що передбачає оцінювання студентів за усі види аудиторної та позааудиторної навчальної діяльності, спрямовані на опанування навчального навантаження з освітньої програми: поточний, модульний, підсумковий контроль, екзамени, заліки, заліки з практик.</p> <p>Також, з метою отримання додаткових балів в межах дисциплін зараховуються здобуті студентами сертифікати відомих компаній за тематикою дисциплін.</p>
6- Програмні компетенції	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (ЗК)	<p>КЗ1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КЗ2. Здатність проводити дослідження на відповідному рівні.</p> <p>КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.</p> <p>КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.</p> <p>КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).</p> <p><i>КЗ6. Знання та розуміння предметної області і професійної діяльності.</i></p> <p><i>КЗ7. Володіння навичками критичного мислення.</i></p> <p><i>КЗ8. Здатність використовувати інформаційні та комунікаційні технології.</i></p> <p><i>КЗ9. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.</i></p> <p><i>КЗ10. Здатність застосовувати кращі практики у професійній діяльності.</i></p> <p><i>КЗ11. Здатність проявляти толерантність та повагу до культурної різноманітності.</i></p>

<p>Фахові компетентності спеціальності (КФ)</p>	<p>КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.</p> <p>КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.</p> <p>КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.</p> <p>КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.</p> <p>КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.</p> <p>КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.</p> <p>КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.</p> <p>КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної</p>
--	---

	<p>інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.</p> <p>КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.</p> <p>КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.</p>
--	--

7 – Програмні результати навчання

	<p>РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.</p> <p>РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.</p> <p>РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.</p> <p>РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.</p> <p>РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.</p> <p>РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології</p>
--	---

створення та використання спеціалізованого програмного забезпечення.

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

РН16. Приймати обґрунтовані рішення з організаційно-

	<p>технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.</p> <p>РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.</p> <p>РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.</p> <p>РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.</p> <p>РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.</p> <p>РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.</p> <p>РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.</p> <p>РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.</p>
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	<p>Всі науково-педагогічні працівники, залучені до реалізації освітньої складової освітньо-професійної програми є штатними співробітниками Державного університету інформаційно-комунікаційних технологій, мають підтверджений рівень наукової і професійної</p>

	<p>активності. Група забезпечення спеціальності F5 Кібербезпека та захист інформації, сформована з числа науково-педагогічних працівників Державного університету інформаційно-комунікаційних технологій. Кількісний та якісний склад групи відповідають Ліцензійним вимогам.</p>
Матеріально-технічне забезпечення	<p>Для проведення практичних та лабораторних занять з метою формування спеціальних компетентностей зі спеціальності F5 Кібербезпека та захист інформації освітньої програми Інформаційна та кібернетична безпека використовуються спеціалізовані лабораторії університету, які оснащені сучасними комп'ютерами та програмно-апаратними комплексами.</p> <p>НАВЧАЛЬНА ЛАБОРАТОРІЯ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ Лабораторія призначена для проведення практичних занять з використанням програмно-апаратних комплексів: IBM QRadar SIEM, IBM i2 Analyze Notebook, 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>НАВЧАЛЬНА ЛАБОРАТОРІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК Лабораторія використовується для вивчення спеціалізованих засобів криптографічного захисту, захисту кінцевих точок на базі рішення Eset Protect яке відстежує та захищає від загроз. Продукт містить безпечне шифрування, мультифакторну ідентифікацію, що дає змогу захистити конфіденційні дані. Програма блокує листи фішингу, захищає електронну пошту завдяки багаторівневій технології.</p> <p>НАВЧАЛЬНА ЛАБОРАТОРІЯ МЕРЕЖЕВОЇ БЕЗПЕКИ Лабораторія призначена для вивчення технологій мережевої безпеки CISCO та Huawei, проведення тренінгів щодо протидії кібератакам зловмисників на корпоративні інформаційні системи та сертифікаційних курсів від партнерів кафедри – Introduction to Cybersecurity, CCNA Security, CCNA Cybersecurity Operations, HCIA Security V4. 0.</p>
Інформаційне та навчально-методичне забезпечення	<p>Інформація про освітню програму, її освітні компоненти та вимоги до осіб, які можуть здобувати вищу освіту за цією програмою розміщена на</p>

	офіційному сайті Державного університету інформаційно-комунікаційних технологій. Усі освітні компоненти освітньої програми забезпечені навчально-методичними матеріалами, є у вільному доступі у якості ресурсів бібліотеки, системи дистанційного навчання (електронної бібліотеки) університету.
9 – Академічна мобільність	
Національна кредитна мобільність	Наявність двосторонніх договорів між ДУІКТ та вищими навчальними закладами України забезпечує національну кредитну мобільність.
Міжнародна кредитна мобільність	Зміст навчання відповідає світовим освітнім стандартам, що дозволяє приймати участь у програмах подвійних дипломів та бути конкурентоспроможним на світовому ринку праці.
Навчання іноземних здобувачів вищої освіти	Дозволяє можливість навчання іноземним громадянам.

2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1. Зміст підготовки за освітньою програмою компетентності та результатами навчання

№ п.п.	Дисципліна	Шифр	Компетентність	Результат навчання
Цикл дисциплін загальної підготовки				
1.	Корпоративна та професійна етика в кібербезпеці	OK1	ІК, К31, К32, К33, К34, К35, КФ1, КФ3, КФ4, КФ5, КФ6, КФ7, КФ9, КФ10	РН1, РН15, РН16, РН17, РН18
2.	Педагогіка та психологія у вищій школі	OK2	ІК, К31, К32, К33, К34, К35, К36, К36, К37, К38, К39, К310, К311, КФ1, КФ2, КФ3, КФ10	РН2, РН17, РН18
3.	Проведення наукових досліджень в кібербезпеці	OK3	ІК, К31, К32, К33, К34, К35, К37, К38, К39, К310, КФ1, КФ2, КФ3, КФ4, КФ6, КФ7, КФ8, КФ9, КФ10	РН3, РН17, РН19, РН20, РН23
4.	Науково-технічний переклад	OK4	ІК, К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ6, КФ7, КФ8, КФ9, КФ10	РН1, РН2, РН17, РН20, РН23
Цикл дисциплін професійної підготовки				
1.	Прикладна загальна теорія систем кібербезпеки	OK5	ІК, К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	РН3, РН5, РН6, РН7, РН11, РН16, РН17, РН23
2.	Управління проектами інформаційної безпеки	OK6	ІК, К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ4, КФ9, КФ10	РН4, РН8, РН9, РН14, РН17, РН20
3.	Технології забезпечення безпеки мережевої інфраструктури	OK7	ІК, К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21
4.	Технології виявлення уразливостей мережевих ресурсів	OK8	ІК, К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21

5.	Науково-педагогічна практика	OK9	IK, K31, K32, K33, K34, K35, K36, K37, K38, K39, K310, K311, KФ1, KФ2, KФ3, KФ10	PH1, PH2, PH15, PH17, PH18
6.	Науково-дослідна практика	OK10	IK, K31, K32, K33, K34, K35, KФ1, KФ2, KФ3, KФ4, KФ5, KФ6, KФ7, KФ8, KФ9, KФ10	PH3, PH4, PH5, PH8, PH11, PH12, PH13, PH17, PH19, PH20, PH21, PH22, PH23
7.	Переддипломна практика	OK11	IK, K31, K32, K33, K34, K35, KФ1, KФ2, KФ3, KФ4, KФ5, KФ6, KФ7, KФ8, KФ9, KФ10	PH3, PH4, PH5, PH8, PH10, PH11, PH12, PH13, PH17, PH19, PH20, PH22, PH23
8.	Кваліфікаційна робота	OK12	IK, K31, K32, K33, K34, K35, KФ1, KФ2, KФ3, KФ4, KФ5, KФ6, KФ7, KФ8, KФ9, KФ10	PH3, PH4, PH5, PH8, PH10, PH11, PH12, PH13, PH17, PH19, PH20, PH21, PH22, PH23
Дисципліни вільного вибору студента				
9.	Дисципліни вільного вибору здобувача			
10.	Дисципліни вільного вибору здобувача			
11.	Дисципліни вільного вибору здобувача			
12.	Дисципліни вільного вибору студента			
13.	Дисципліни вільного вибору здобувача			

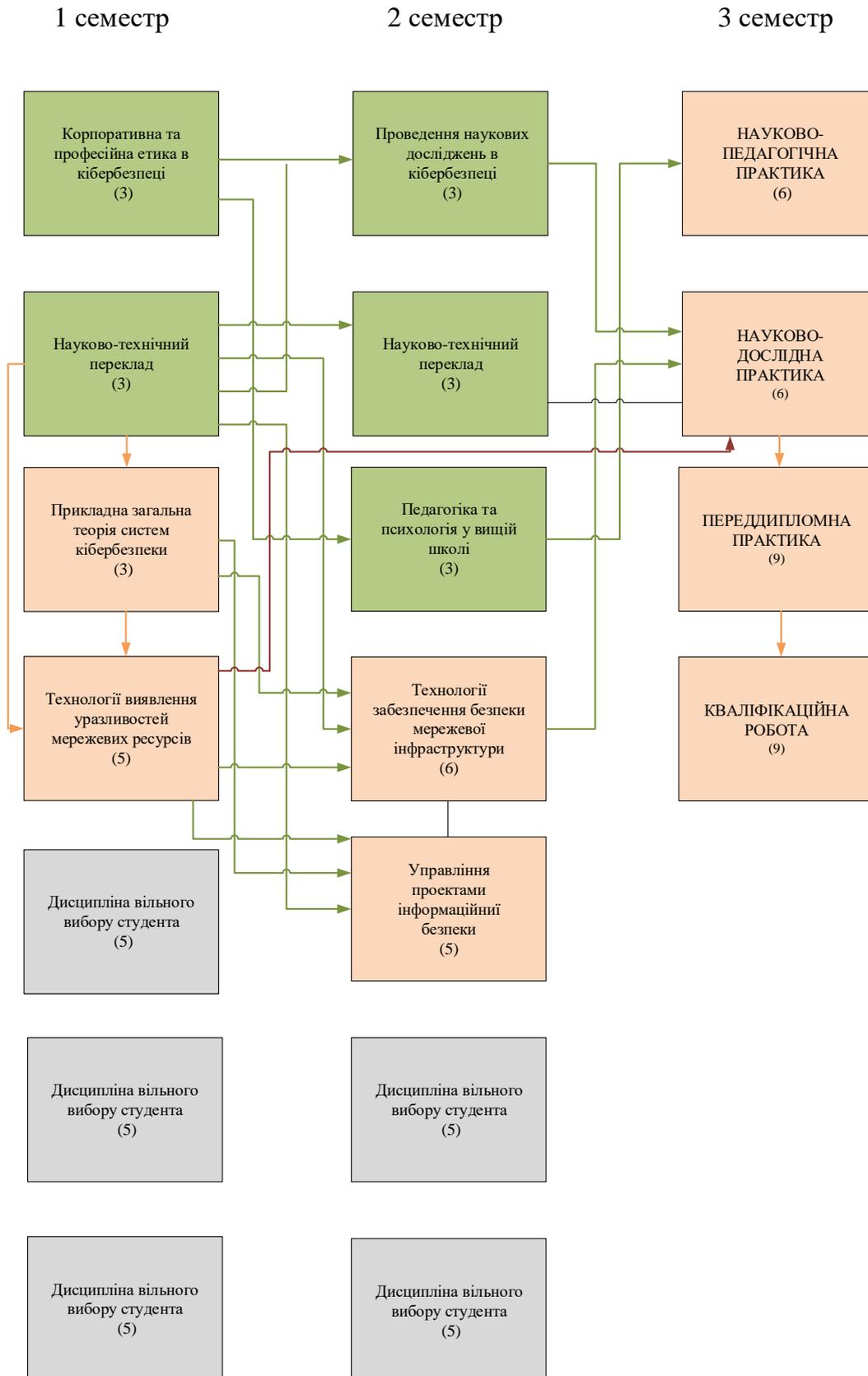
2.2. Перелік компонент ОП

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 ОПШ			
Цикл загальної підготовки			
OK1	Корпоративна та професійна етика в кібербезпеці	3	Іспит
OK2	Педагогіка та психологія у вищій школі	3	Залік
OK3	Проведення наукових досліджень в кібербезпеці	3	Залік
OK4	Науково-технічний переклад	6	Залік, Іспит
Цикл професійної та практичної підготовки			

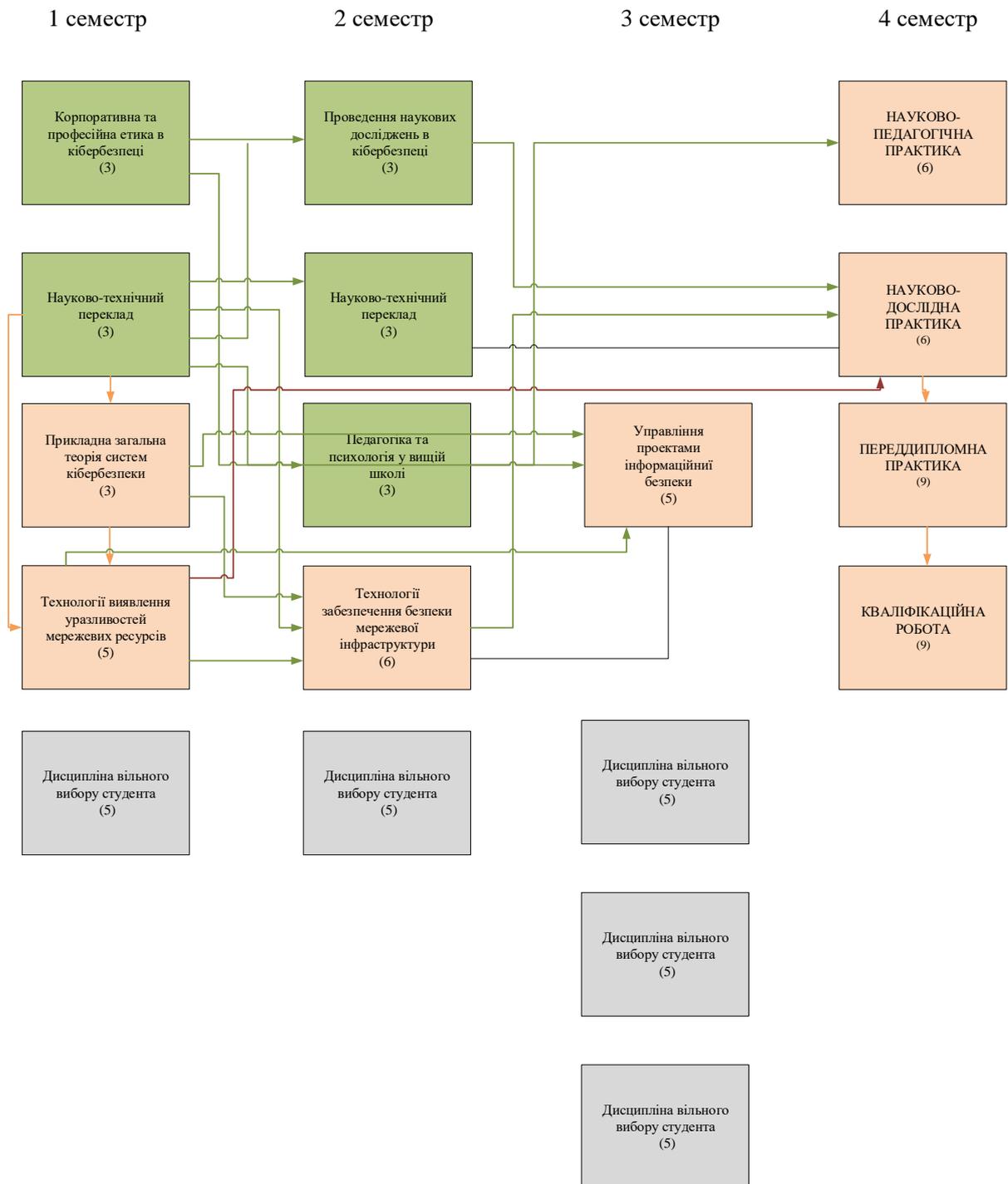
OK5	Прикладна загальна теорія систем кібербезпеки	4	Іспит
OK6	Управління проектами інформаційної безпеки	5	Іспит
OK7	Технології забезпечення безпеки мережевої інфраструктури	6	Іспит
OK8	Технології виявлення уразливостей мережевих ресурсів	5	Іспит
OK9	Науково-педагогічна практика	6	Залік
OK10	Науково-дослідна практика	6	Залік
OK11	Переддипломна практика	9	Залік
OK12	Кваліфікаційна робота	9	
Загальний обсяг обов'язкових компонент:		65	
Вибіркові компоненти ОП			
ВК 1	Дисципліни вільного вибору здобувача	5	Залік
ВК 2	Дисципліни вільного вибору здобувача	5	Залік
ВК 3	Дисципліни вільного вибору здобувача	5	Залік
ВК 4	Дисципліни вільного вибору здобувача	5	Залік
ВК 5	Дисципліни вільного вибору здобувача	5	Залік
Загальний обсяг вибірових компонент:		25	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		90	

2.3. Структурно-логічна схема ОПШ

Денна



Заочна



3. Форма атестації здобувачів вищої освіти

<i>Форми атестації здобувачів вищої освіти</i>	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
<i>Вимоги до кваліфікаційної роботи</i>	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації згідно «Положення про запобігання академічному плагіату у Державному університеті інформаційно-комунікаційних технологій». Атестація здійснюється відкрито і гласно.

**5. Матриця забезпечення програмних результатів навчання (ПРН)
відповідними компонентами освітньої програми**

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12
РН1	•			•					•			
РН2		•		•					•			
РН3			•		•					•	•	•
РН4						•	•	•		•	•	•
РН5					•		•	•		•	•	•
РН6					•		•	•				
РН7					•							
РН8						•	•	•		•	•	•
РН9						•						
РН10											•	•
РН11					•		•	•		•	•	•
РН12										•	•	•
РН13							•	•		•	•	•
РН14						•						
РН15	•								•			
РН16	•				•							
РН17	•	•	•	•	•	•	•	•	•	•	•	•
РН18	•	•							•			
РН19			•							•	•	•
РН20			•	•		•				•	•	•
РН21							•	•		•		•
РН22										•	•	•
РН23			•	•	•					•	•	•

Гарант освітньої програми

Завідувач кафедри інформаційної та кібернетичної безпеки

Навчально-наукового інституту захисту інформації

Державного університету інформаційно-комунікаційних технологій

доктор технічних наук, професор

Галина ГАЙДУР