МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА

другого (магістерського) рівня вищої освіти

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 УНІВЕРСИТЕТУ
Протокол № 3 від 17 березня 2026 р.
Наказ № 105 від 20 березня 2026 р.

Ректор _____ Володимир ШУЛЬГА

Освітня програма вводиться в дію з 01 вересня 2026 р.

Київ 2026

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

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

1. Перший проректор _____ Олександр КОРЧЕНКО

2. Проректор з навчальної роботи _____ Артур ГУДМАНЯН

3. Начальник навчально-методичного відділу _____ Вадим ВЛАСЕНКО

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

Протокол № 8 від «26» лютого 2026 р.

Голова Вченої Ради ННІЗІ _____ Євгенія ІВАНЧЕНКО

5. Кафедра систем та технологій кібербезпеки

Протокол № 7/1 від «25» лютого 2026 р.

Завідувач кафедри систем та технологій кібербезпеки _____ Галина ГАЙДУР

Голова студентської ради ННІКБЗІ _____ Станіслав ШТЕФАН

Рецензії від зовнішніх стейкхолдерів:

Рецензії на освітньо-професійну програму підготовки здобувачів вищої освіти:
1. ТОВ «СВІТ ІТ».
2. Київський національний університет ім. Тараса Шевченка.

ПЕРЕДМОВ

Розроблено робочою групою у складі:

Гарант освітньої програми (голова робочої групи)

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

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;

Максим ПОРОШИН –директор ТОВ «Світ ІТ»;

Антоніна КОРЖ – здобувач ОПП «Інформаційна та кібернетична безпека» другого (магістерського) рівня вищої освіти.

ВІДОМОСТІ ПРО ПЕРЕГЛЯД ОСВІТНЬОЇ ПРОГРАМИ

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

пропозицій та побажань стейкголдерів (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 1рік 5 місяців (денна), 1 рік 10 місяців (заочна)
Наявність акредитації	акредитовано
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,

	обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання**. 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.
Орієнтація освітньої програми	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 сьогоднішнього стану сфери кібербезпеки, має прикладний характер, спрямована на забезпечення потреб ринку праці при вирішенні професійних задач в галузі кібербезпеки та захисту інформації.
Основний фокус освітньої програми та спеціалізації	Дослідження в галузі кібербезпеки. Акцент на впровадженні інноваційних методів та технологій в процесі захисту інформації в інформаційних і кібернетичних системах на підприємствах, в установах і організаціях. Ключові слова: ІНФОРМАЦІЯ, ЗАГРОЗИ, ІНЦИДЕНТ, ВРАЗЛИВОСТІ, ІНФРАСТРУКТУРА, КІБЕРБЕЗПЕКА.
Особливості програми	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.

	Передбачено проведення лекційних курсів, семінарських та практичних занять, тренінгів, з залученням фахівців з інформаційної безпеки та самостійної науково-дослідної роботи. ***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».*** ***В програму впроваджені результати академічної співпраці з компанією IBM «SkillsBuild».***
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека (випускник) здатний виконувати професійні роботи за Державним класифікатором професій ДК 003: 2010: **Основна:** 2139.2 Фахівець з реагування на інциденти кібербезпеки Фахівець з підтримки інфраструктури кіберзахисту 2310.2 – викладач закладу вищої освіти
Академічні права випускників	Продовжити освіту за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі дорослої освіти.
5 – Викладання та оцінювання	
Викладання та навчання	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. 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.

Оцінювання	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. Також, з метою отримання додаткових балів в межах дисциплін зараховуються здобуті студентами сертифікати відомих компаній за тематикою дисциплін.
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)	КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Здатність проводити дослідження на відповідному рівні. КЗ3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). *КЗ6. Знання та розуміння предметної області і професійної діяльності.* *КЗ7. Володіння навичками критичного мислення.* *КЗ8. Здатність використовувати інформаційні та комунікаційні технології.* *КЗ9. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.* *КЗ10. Здатність застосовувати кращі практики у професійній діяльності.* *КЗ11. Здатність проявляти толерантність та повагу до культурної різноманітності.*

Фахові компетентності спеціальності (КФ)	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. 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. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. 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. 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. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. 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. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної

	інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. 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. 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.
7 – Програмні результати навчання	
	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. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. 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. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології

	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-

	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. 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. РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. 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. 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. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. 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. 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.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	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

	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.
Матеріально-технічне забезпечення	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. 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. 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. 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.
Інформаційне та навчально-методичне забезпечення	Інформація про освітню 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 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	ОК1	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	ОК2	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	ОК3	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.	Наукова комунікація та технічне документування в кібербезпеці	ОК4	ІК, К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ6, КФ7, КФ8, КФ9, КФ10	РН1, РН2, РН17, РН20, РН23
5.	Англійська мова для ділової комунікації	ОК5	ІК, К35	РН15, РН20
Цикл дисциплін професійної підготовки				
1.	Прикладна загальна теорія систем кібербезпеки	ОК6	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	ОК7	ІК, К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ4, КФ9, КФ10	РН4, РН8, РН9, РН14, РН17, РН20
3.	Технології забезпечення безпеки мережевої інфраструктури	ОК8	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	ОК9	ІК, К31, К32, К33, К34, К35, КФ1, КФ2, КФ3,	РН4, РН5, РН6, РН8, РН11, РН13, РН17,

			КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	РН21
5.	Науково-педагогічна практика	ОК10	ІК, К31, К32, К33, К34, К35, К36, К36, К37, К38, К39, К310, К311, КФ1, КФ2, КФ3, КФ10	РН1, РН2, РН15, РН17, РН18
6.	Науково-дослідна практика	ОК111	ІК, К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	РН3, РН4, РН5, РН8, РН11, РН12, РН13, РН17, РН19, РН20, РН21, РН22, РН23
7.	Переддипломна практика	ОК12	ІК, К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	РН3, РН4, РН5, РН8, РН10, РН11, РН12, РН13, РН17, РН19, РН20, РН22, РН23
8.	Кваліфікаційна робота	ОК13	ІК, К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	РН3, РН4, РН5, РН8, РН10, РН11, РН12, РН13, РН17, РН19, РН20, РН21, РН22, РН23
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			

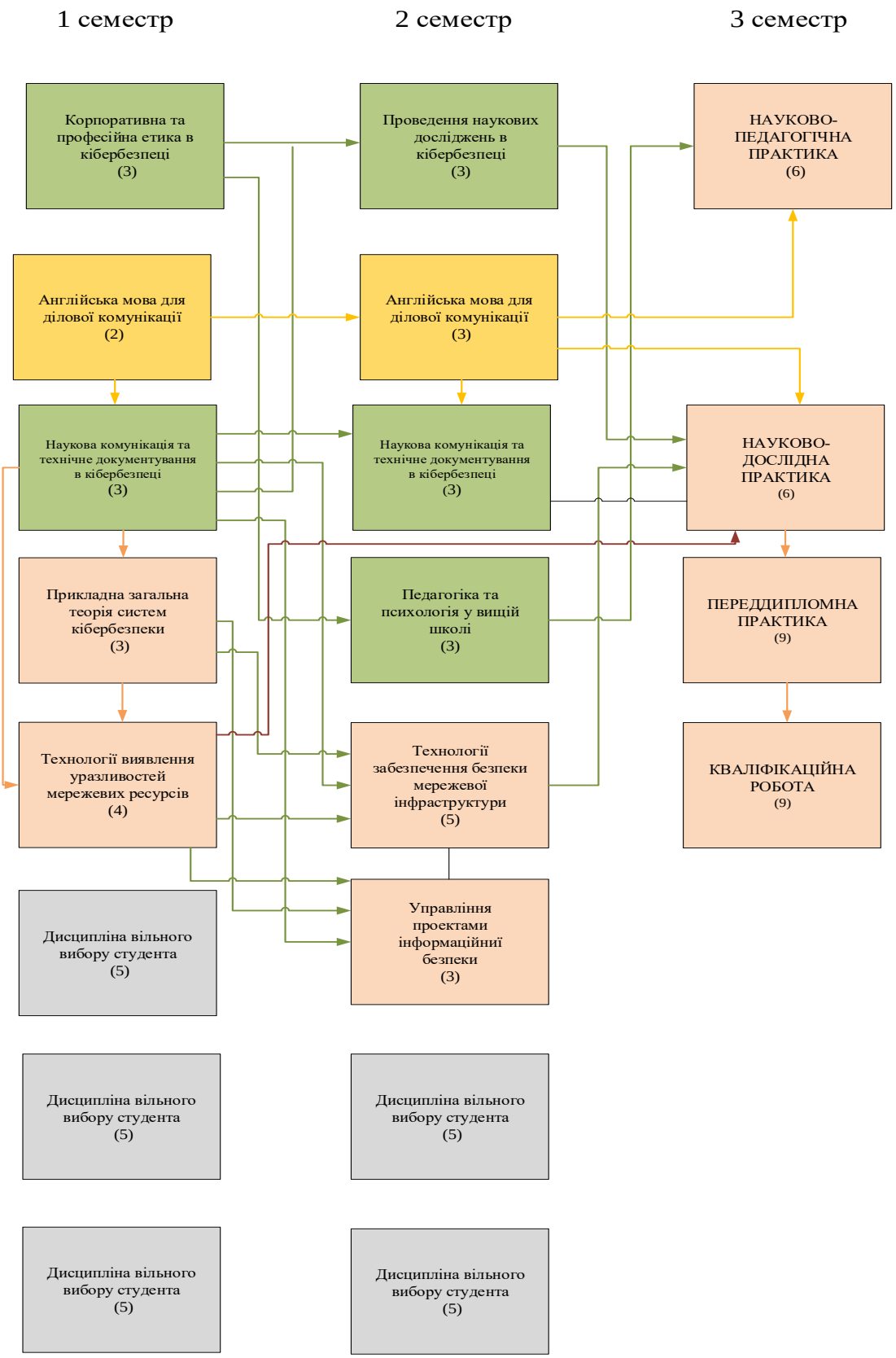
2.2. Перелік компонент ОП

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 ОПП			
Цикл загальної підготовки			
ОК1	Корпоративна та професійна етика в кібербезпеці	3	Іспит
ОК2	Педагогіка та психологія у вищій школі	3	Залік

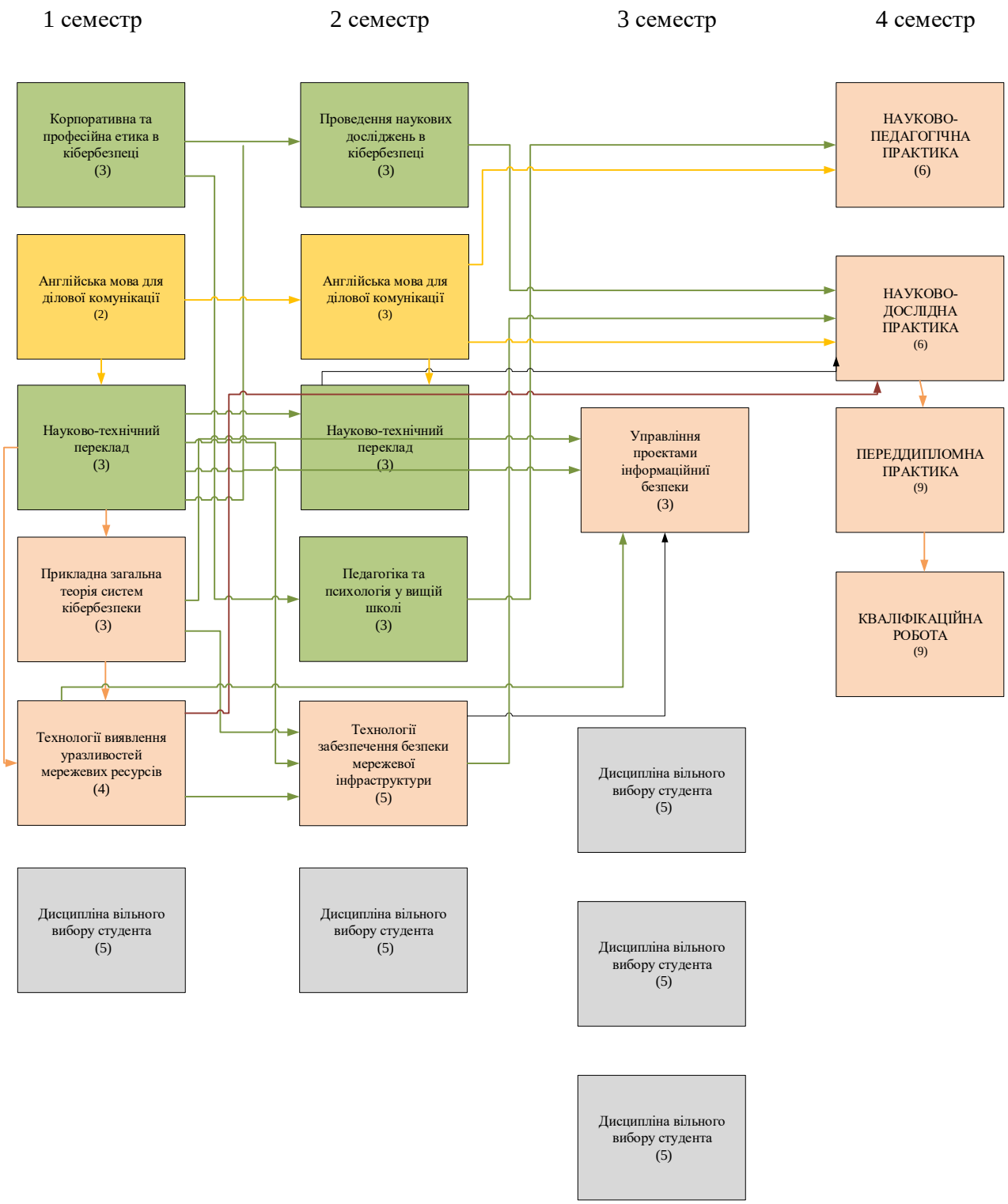
ОК3	Проведення наукових досліджень в кібербезпеці	3	Залік
ОК4	Наукова комунікація та технічне документування в кібербезпеці	6	Залік, Іспит
ОК5	Англійська мова для ділової комунікації	5	Залік, Іспит
Цикл професійної та практичної підготовки			
ОК6	Прикладна загальна теорія систем кібербезпеки	3	Іспит
ОК7	Управління проектами інформаційної безпеки	3	Іспит
ОК8	Технології забезпечення безпеки мережевої інфраструктури	5	Іспит
ОК9	Технології виявлення уразливостей мережевих ресурсів	4	Іспит
ОК10	Науково-педагогічна практика	6	Залік
ОК11	Науково-дослідна практика	6	Залік
ОК12	Переддипломна практика	9	Залік
ОК13	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 вибіркових компонент:		**25**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**90**	

2.3. Структурно-логічна схема ОПП

Денна



Заочна


1 семестр
2 семестр
3 семестр
4 семестр
Корпоративна та професійна етика в кібербезпеці (3)
Проведення наукових досліджень в кібербезпеці (3)
НАУКОВО-ПЕДАГОГІЧНА ПРАКТИКА (6)
Англійська мова для ділової комунікації (2)
Англійська мова для ділової комунікації (3)
НАУКОВО-ДОСЛІДНА ПРАКТИКА (6)
Науково-технічний переклад (3)
Науково-технічний переклад (3)
Управління проектами інформаційної безпеки (3)
ПЕРЕДДИПЛОМНА ПРАКТИКА (9)
Прикладна загальна теорія систем кібербезпеки (3)
Педагогіка та психологія у вищій школі (3)
КВАЛІФІКАЦІЙНА РОБОТА (9)
Технології виявлення уразливостей мережевих ресурсів (4)
Технології забезпечення безпеки мережевої інфраструктури (5)
Дисципліна вільного вибору студента (5)
Дисципліна вільного вибору студента (5)
Дисципліна вільного вибору студента (5)
Дисципліна вільного вибору студента (5)
Дисципліна вільного вибору студента (5)

3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	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.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1	ОК 2	ОК 3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13
ІК	•	•	•	•	•	•	•	•	•	•	•	•	•
КЗ 1	•	•	•	•		•	•	•	•	•	•	•	•
КЗ 2	•	•	•	•		•	•	•	•	•	•	•	•
КЗ 3	•	•	•	•		•	•	•	•	•	•	•	•
КЗ 4	•	•	•	•		•	•	•	•	•	•	•	•
КЗ 5	•	•	•	•	•	•	•	•	•	•	•	•	•
КЗ 6	•	•								•			
КЗ 7		•	•							•			
КЗ 8		•	•							•			
КЗ 9		•	•							•			
КЗ 10		•	•							•			
КЗ 11		•								•			
КФ 1	•	•	•	•		•	•	•	•	•	•	•	•
КФ 2		•	•	•		•	•	•	•	•	•	•	•
КФ 3	•	•	•	•		•	•	•	•	•	•	•	•
КФ 4	•		•			•	•				•	•	•
КФ 5	•					•		•	•		•	•	•
КФ 6	•		•	•		•		•	•		•	•	•
КФ 7	•		•	•		•		•	•		•	•	•
КФ 8			•	•		•		•	•		•	•	•
КФ 9	•		•	•		•	•	•	•		•	•	•
КФ 10	•	•	•	•		•	•	•	•	•	•	•	•

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

	ОК 1	ОК 2	ОК 3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13
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 систем та технологій кібербезпеки
Навчально-наукового інституту кібербезпеки та захисту інформації
Державного університету інформаційно-комунікаційних технологій

доктор технічних наук, професор **Галина ГАЙДУР**

РЕЦЕНЗІЯ
на освітньо-професійну програм
другого (магістерського) рівня вищої освіти
«ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА»
за спеціальністю F5 «Кібербезпека та захист інформації»

Освітньо-професійна програма «Інформаційна та кібернетична безпека» другого (магістерського) рівня спрямована на підготовку фахівців, здатних розв'язувати складні задачі та проблеми у сфері кібербезпеки, що передбачають проведення досліджень, аналізу та впровадження сучасних методів і технологій захисту інформації в умовах невизначеності та динамічного розвитку інформаційних технологій.

Мета, інтегральна компетентність, загальні та фахові компетентності освітньої програми узгоджені між собою та відповідають вимогам стандарту вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації». Програмні результати навчання логічно пов'язані з освітніми компонентами, що свідчить про системність і методичну обґрунтованість проєктування освітнього процесу.

Зміст програми передбачає поглиблене вивчення сучасних підходів до побудови систем управління інформаційною безпекою, управління ризиками, криптографічного захисту, аналізу та протидії складним кіберзагрозам, а також дослідження інцидентів інформаційної безпеки. Особлива увага приділяється формуванню здатності приймати обґрунтовані рішення щодо архітектури захищених інформаційних систем та розроблення політик безпеки організації.

Позитивною характеристикою освітньої програми є орієнтація на дослідницьку діяльність здобувачів вищої освіти, використання сучасних інструментів аналізу кіберзагроз, виконання індивідуальних проєктів та підготовка кваліфікаційної роботи, що відповідає вимогам другого рівня вищої освіти.

Структура програми є логічною та послідовною, забезпечує поєднання теоретичної підготовки з практичною складовою та створює передумови для професійної діяльності у сфері управління кібербезпекою, аудиту безпеки та проєктування комплексних систем захисту інформації, а також для подальшого навчання на третьому (освітньо-науковому) рівні.

Форми контролю та атестації забезпечують об'єктивну перевірку досягнення програмних результатів навчання та відповідають вимогам академічної доброчесності.

Освітньо-професійна програма «Інформаційна та кібернетична безпека» другого (магістерського) рівня є актуальною, методично обґрунтованою та відповідає вимогам підготовки фахівців у сфері кібербезпеки. Програма може бути рекомендована до впровадження в освітній процес.

РЕЦЕНЗЕНТ
Професор кафедри кібербезпеки та захисту інформації
факультету інформаційних технологій Київського національного
університету імені Тараса Шевченка
доктор технічних наук, професор Володимир НАКОНЕЧНИЙ

Підпис професора Володимира НАКОНЕЧНОГО засвідчую.
Заступник декана з навчально-виховної роботи
кандидат фізико - математичних наук, доцент Наталія ТМЄНОВА

Рецензія
на освітньо-професійну програму
другого (магістерського) рівня вищої освіти
«Інформаційна та кібернетична безпека»
за спеціальністю F5 «Кібербезпека та захист інформації»

У сучасних умовах зростання кількості складних та цілеспрямованих кіберзагроз організації потребують фахівців, здатних не лише експлуатувати засоби захисту, а й аналізувати інциденти, оцінювати ризики та проєктувати комплексні системи інформаційної безпеки. Тому підготовка магістрів у сфері кібербезпеки є важливою складовою забезпечення кіберстійкості підприємств та установ.

Освітньо-професійна програма «Інформаційна та кібернетична безпека» орієнтована на формування у здобувачів здатності вирішувати практичні та управлінські завдання у сфері кіберзахисту. Зміст програми охоплює управління інформаційною безпекою, аналіз та оброблення кіберінцидентів, оцінювання ризиків, аудит безпеки та розроблення політик безпеки організації.

Позитивно оцінюється спрямованість програми на практичну діяльність фахівця, зокрема:

- моделювання та аналіз кіберзагроз;
- організацію процесів реагування на інциденти;
- управління системами захисту інформації;
- проведення аудиту та оцінювання рівня захищеності;
- підготовку управлінської та технічної документації з безпеки.

Отримані компетентності відповідають завданням, які виконують фахівці підрозділів інформаційної безпеки, SOC-центрів, служб управління ризиками та аудиту безпеки. Випускники програми можуть бути залучені до виконання професійних функцій на посадах аналітика кібербезпеки, інженера з інформаційної безпеки, спеціаліста з реагування на інциденти, аудитора безпеки та адміністратора систем захисту інформації.

Окремо слід відзначити формування навичок прийняття рішень в умовах невизначеності та відповідальності за функціонування захищених інформаційних систем, що є характерною ознакою підготовки фахівців магістерського рівня.

Освітньо-професійна програма «Інформаційна та кібернетична безпека» другого (магістерського) рівня відповідає сучасним вимогам ринку праці та забезпечує підготовку фахівців, готових до виконання складних професійних завдань у сфері кібербезпеки. Програма підтримується роботодавцями та рекомендується до впровадження в освітній процес.

Технічний директор ТОВ «Світ ІТ» _____ Порошин М.Г.