ВІДОМОСТІ ПРО ПЕРЕГЛЯД ОСВІТНЬОЇ ПРОГРАМИ

Оновлення (змісту освітніх компонентів та освітньої програми) відповідно до: 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 Мінекономіки від 23.03.2021 № 610); рекомендацій акредитаційних комісій Університету; пропозицій роботодавців; побажань здобувачів вищої освіти.

Затверджено рішенням випускової кафедри Управління інформаційною та кібернетичною безпекою протокол № 10 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.

1. Профіль освітньої програми

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Державний університет телекомунікацій, Навчально-науковий інститут захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Освітня кваліфікація – Магістр з кібернетичної безпеки
Офіційна назва освітньої програми	Освітньо-професійна програма «Управління інформаційною безпекою»
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний Обсяг освітньої програми-90 кредитів ЄКТС; термін навчання 1,5 роки
Наявність акредитації	До 01.07.2023
Цикл/рівень	НРК України – 7 рівень/ Магістр, QF-EHEA- другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра
Мова(и) викладання	Українська, англійська
Термін дії освітньої програми	Введена в дію з 01.09.2016 року
Інтернет - адреса постійного розміщення опису освітньої програми	http://www.dut.edu.ua/ua/1826-osvitno-profesiyni-programi-kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu

2 – Мета освітньої програми
Метою магістерської програми є підготовка висококваліфікованих фахівців магістрів з управління інформаційною безпекою, які здатні проводити наукові дослідження, описувати та роз'яснити процеси, що відбуваються у сфері інформаційної безпеки, формувати розуміння закономірностей процесів управління інформаційною безпекою, здійснювати апробацію та практичне впровадження наукових результатів, які володіють інноваційним способом мислення та компетентностями, необхідними для ефективного управління інформаційною безпекою, і здатні вирішувати управлінські та науково-дослідні завдання щодо розслідування інцидентів, управління ризиками та аудиту систем інформаційної та кібербезпеки, володіють 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	Освітня-професійна. Програма носить прикладний характер, спрямована на забезпечення потреб ринку праці, зокрема в IT галузі
Основний фокус освітньої програми та спеціалізації	Дослідження в галузі інформаційної безпеки. Акцент на впровадженні інноваційних методів та технологій в процесі управління інформаційною безпекою на підприємствах в установах і організаціях. Ключові слова: ІНФОРМАЦІЯ, ЗАГРОЗИ, ВРАЗЛИВОСТІ, РИЗИК, АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, 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 сфері інформаційної безпеки. 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».***

4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Професіонал з управління інформаційною безпекою (випускник) здатний виконувати професійні роботи за Державним класифікатором професій ДК 003: 2010: **1210** – Керівники підприємств, установ та організацій **1229 –** Керівники інших основних підрозділів **1495** – Менеджери (управителі) систем з інформаційної безпеки **2149.2** – професіонал із організації інформаційної безпеки **2310** – Викладачі університетів та закладів вищої освіти **2433 –** Професіонали в галузі інформації та інформаційного аналізу **2433.1 -** Науковий співробітник (інформаційна аналітика) **3436.1** – Помічник керівника підприємства (установи, організації)
Подальше навчання	Продовжити освіту за третім (освітньо-науковим) рівнем вищої 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	Види контролю: вхідний, поточний, рубіжний (модульний, тематичний) та підсумковий контроль. Оцінювання сформованих компетенцій проводиться під час контрольних заходів, які передбачені цією освітньою програмою та зазначені у навчальному плані. Критерії оцінювання знань, умінь та навичок здобувачів

	вищої освіти розроблені у відповідності до чинного законодавства та затверджені у «Положенні про організацію освітнього процесу у Державному університеті телекомунікацій». 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 (КЗ)	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. Здатність використовувати інформаційні і комунікаційні технології для впровадження проектів в інформаційній та безпековій сферах. КЗ7. Здатність визначати підприємницькі можливості чи вид діяльності або громадського впливу, здатність приймати обґрунтовані рішення, здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ8. Знання про стимули та бар'єри в ефективній командній роботі, вміння виявляти, ставити та вирішувати проблеми. КЗ9. Володіння навичками критичного мислення.
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. РН24. Уміти розробляти проекти досліджень та моделювати їх структуру, застосовуючи різні способи подання статистичної інформації та результатів. РН25. Уміти використовувати знання й уміння для прогнозування, виявлення та оцінювання можливих загроз інформаційному простору держави, дестабілізуючих чинників. РН26. Здатність використовувати професійно профільовані знання й практичні навички для розроблення та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із

	відповідними європейськими стандартами. РН27. Здатність використовувати професійно профільовані знання й практичні навички для забезпечення результативної та ефективної взаємодії державних установ і організацій зі спеціальними та правоохоронними органами у сфері управління й забезпечення інформаційної безпеки. РН28. Здатність використовувати професійно профільні знання, готувати та приймати управлінські рішення у сфері інформаційної безпеки. РН29. Уміти застосовувати системний підхід для побудови системи управління (менеджменту) інформаційною безпекою організації (підприємства), яка визначає загальну організацію і класифікацію системи даних, систему доступу, напрямки планування, відповідальність співробітників, використання оцінки ризиків, тощо в контексті інформаційної безпеки. РН30. Уміти застосовувати сучасні способи, методи та засоби управління наступними аспектами захисту: політикою безпеки, архітектурою захисту, механізмами захисту та засобами захисту. РН31. На основі інформації, одержаної у ході дослідження об'єкта інформаційної діяльності замовника та результатів аналізу ризиків, розробляти рекомендації щодо удосконалення системи управління інформаційною безпекою, застосування яких дозволить мінімізувати ризики та формулювати перелік уразливостей.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Всі науково-педагогічні працівники, залучені до реалізації освітньої складової освітньо-професійної програми є штатними співробітниками Державного університету телекомунікацій, мають підтверджений рівень наукової і професійної активності. Група забезпечення спеціальності 125 Кібербезпека, сформована з числа науково-педагогічних працівників Державного університету телекомунікацій. Кількісний та якісний склад групи відповідають Ліцензійним вимогам

Матеріально-технічне забезпечення	Для проведення практичних та лабораторних занять з метою формування спеціальних компетентностей зі спеціальності 125 Кібербезпека спеціалізації Управління інформаційною безпекою використовуються спеціалізовані лабораторії університету, які оснащені сучасними комп'ютерами та програмно-апаратними комплексами. НАВЧАЛЬНА ЛАБОРАТОРІЯ АКАДЕМІЧНИЙ ЦЕНТР КОМПЕТЕНЦІЙ IBM «КІБЕРПОЛІГОН» 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. НАВЧАЛЬНА ЛАБОРАТОРІЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ CISCO Лабораторія призначена для вивчення технологій мережевої безпеки CISCO, проведення тренінгів з впровадження технології HoneyPot щодо протидії кібератакам зловмисників на корпоративні інформаційні системи та сертифікаційних курсів від партнера кафедри Інформаційної та кібернетичної безпеки – компанії CISCO: Introduction to Cybersecurity, CCNA Security, CCNA Cybersecurity Operations. Лабораторія створена за сприяння компанії CISCO. 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, OCTAVE та RiskWatch у відповідності до вимог міжнародних стандартів з інформаційної та кібербезпеки.

	Використання програмного забезпечення: • «ГРИФ» – аналіз та контроль ризиків інформаційних систем компаній • «КОНДОР+» - розробка і управління політикою інформаційної безпеки компанії • Microsoft Project, Spider Project Lite, OpenProj, GanttProject, Microsoft Excel, Project Expert – управління проектами та інвестиційна оцінка; • MindMap, Mindomo – інструменти для створення карт проєктів та генерування інноваційних ідей • Microsoft Power BI, Microsoft Visio – аналітика та візуалізація даних
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 телекомунікацій. Усі освітні компоненти освітньої програми забезпечені навчально-методичними матеріалами, є у вільному доступі у якості ресурсів бібліотеки, електронної бібліотеки університету та системи дистанційного навчання Moodle
9 – Академічна мобільність	
Національна кредитна мобільність	Наявність двосторонніх договорів між ДУТ 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 / наукової програми та їх логічна послідовність

2.1. Зміст підготовки за освітньою програмою компетентності та результатами навчання

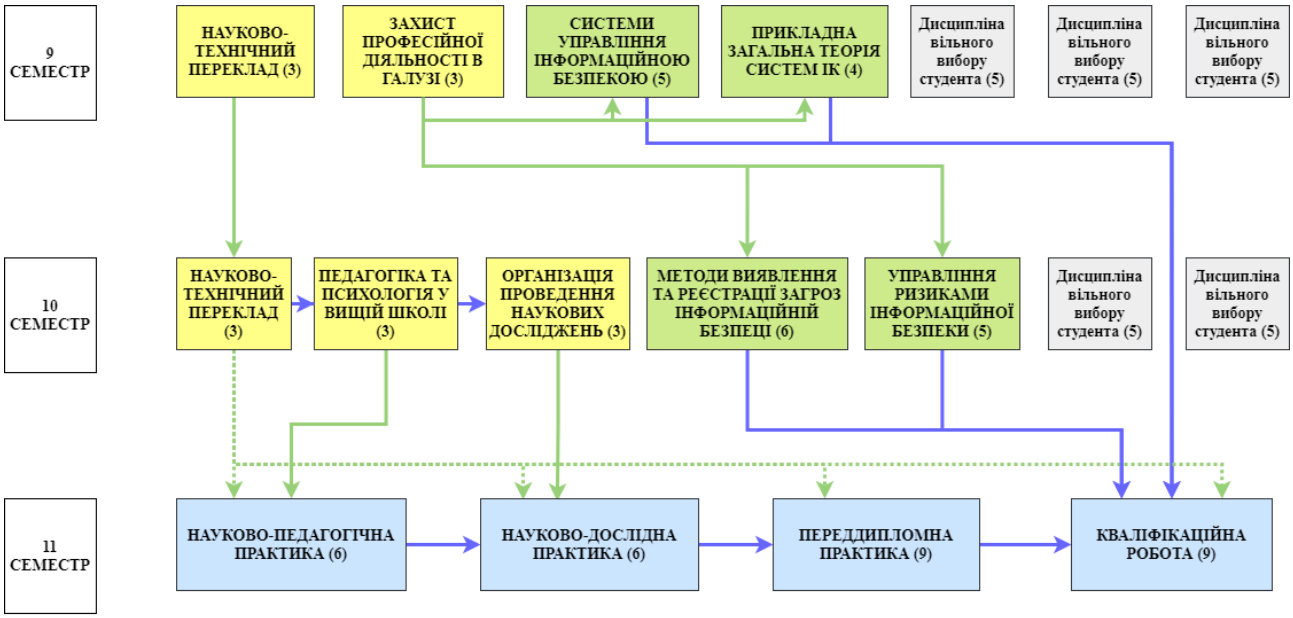
№ п.п.	Дисципліна	Шифр	Компетентність	Результат навчання
Цикл дисциплін загальної підготовки				
1.	Захист професійної діяльності в галузі	ЗК.13.1.01	К31, К34, К35, К36	РН2, РН17
2.	Педагогіка та психологія у вищій школі	ЗК.13.1.02	К33, К34, К35, К36, К38, К39, КФ10	РН2, РН17, РН18
3.	Організація проведення наукових досліджень	ЗК.13.1.03	К31, К32, К34, К35, К36, К38, К39, КФ3	РН3, РН17, РН19, РН20, РН23
4.	Науково-технічний переклад	ЗК.13.1.04	К31, К32, К33, К34, К35, К38, К39, КФ2, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	РН1, РН2, РН3, РН5, РН7, РН9, РН10, РН11, РН12, РН13, РН14, РН15, РН16, РН17, РН18, РН19, РН20, РН22, РН28
Цикл дисциплін професійної підготовки				
1.	Методи виявлення та регістрації загроз інформаційній безпеці	ПП.13.2.01	К31, К32, КФ1, КФ2, КФ5	РН1, РН4, РН6, РН7, РН10, РН16, РН28
2.	Системи управління інформаційною безпекою	ПП.13.2.02	К31, К32, К35, К38, КФ1, КФ2, КФ4, КФ6	РН1, РН2, РН5, РН6, РН8, РН9, РН11, РН14, РН15, РН17, РН20, РН23, РН26, РН28, РН29, РН30, РН31
3.	Управління ризиками інформаційної безпеки	ПП.13.2.03	К33, К38, К39, КФ1, КФ2, КФ5	РН6, РН24, РН25, РН26, РН27, РН28, РН29, РН30
4.	Прикладна загальна теорія систем інформаційної та кібербезпеки	ПП.13.2.04	К31, К34, КФ2, КФ3, КФ4, КФ8	РН5, РН6, РН7, РН11, РН16, РН17
5.	Науково-педагогічна практика	ПП.13.2.05	К31, К34, К36, К38, К39, КФ10	РН1, РН2, РН15, РН17, РН18
6.	Науково-дослідна практика	ПП.13.2.06	К31, К32, К33, К34, К38, К39, КФ1, КФ2, КФ3, КФ6, КФ8	РН3, РН4, РН5, РН8, РН11, РН12, РН13, РН17, РН19, РН20, РН21, РН22, РН23, РН24, РН25, РН31
7.	Переддипломна практика	ПП.13.2.07	К31, К32, К33, К34, К39, КФ1, КФ2, КФ6, К37, КФ8	РН3, РН4, РН5, РН8, РН10, РН11, РН12, РН13, РН17, РН19, РН20, РН22,РН23, РН24, РН25, РН26, РН29, РН31
8.	Дипломне проектування, Захист магістерської	ПП.13.2.08	К31, К32, К33, К34, КФ1, КФ2,	РН3, РН4, РН5, РН8, РН10, РН11, РН12,

	роботи		КФ3, КФ6, КЗ7, КФ9	РН13, РН17, РН19, РН20, РН22,РН23, РН24, РН25, РН26, РН29, РН31
Дисципліни вільного вибору студента				
1.	Дисципліни вільного вибору студента			
2.	Дисципліни вільного вибору студента			
3.	Дисципліни вільного вибору студента			
4.	Дисципліни вільного вибору студента			
5.	Дисципліни вільного вибору студента			

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 ОП			
Цикл загальної підготовки			
ЗК13.1.01	Захист професійної діяльності в галузі	3	Іспит
ЗК13.1.02	Педагогіка та психологія у вищій школі	3	Залік
ЗК13.1.03	Організація проведення наукових досліджень	3	Залік
ЗК13.1.04	Науково-технічний переклад	6	Залік, Іспит
Цикл професійної підготовки			
ПП.13.2.01	Методи виявлення та реєстрації загроз інформаційній безпеці	6	Іспит
ПП.13.2.02	Системи управління інформаційною безпекою	5	Іспит
ПП.13.2.03	Управління ризиками інформаційної безпеки	5	Іспит
ПП.13.2.04	Прикладна загальна теорія систем інформаційної та кібербезпеки	4	Іспит
ПП.13.2.05	Науково-педагогічна практика	6	Залік
ПП.13.2.06	Науково-дослідна практика	6	Залік
ПП.13.2.07	Переддипломна практика	9	Залік
ПП.13.2.08	Дипломне проектування, Державна атестація	9	Іспит
Загальний обсяг обов'язкових компонент:		**65**	
Вибіркові компоненти ОП			
	Дисципліни вільного вибору студента	5	
	Дисципліни вільного вибору студента	5	
	Дисципліни вільного вибору студента	5	
	Дисципліни вільного вибору студента	5	
	Дисципліни вільного вибору студента	5	
Загальний обсяг вибіркових компонент:		**25**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**90**	

2.3. Структурно-логічна схема ОП



Дисципліни циклу загальної підготовки	Дисципліни вільного вибору студента
Дисципліни циклу професійної підготовки	ПРАКТИКА

3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація магістрів з управління інформаційною безпекою 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. Перевірка на плагіат проводиться згідно «Положення про запобігання академічному плагіату у Державному університеті телекомунікацій». Кваліфікаційна робота має бути розміщена на офіційному сайті (або депозитарії) закладу вищої освіти або його підрозділу. Атестація здійснюється відкрито і гласно.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ЗК13.1.01	ЗК13.1.02	ЗК13.1.03	ЗК13.1.04	ПП13.2.01	ПП13.2.02	ПП.13.2.03	ПП.13.2.04	ПП.13.2.05	ПП.13.2.06	ПП.13.2.07	ПП.13.2.08
КЗ 1	•		•	•	•	•		•	•	•	•	•
КЗ 2			•	•	•	•				•	•	•
КЗ 3		•		•			•			•	•	•
КЗ 4	•	•	•	•				•	•	•	•	•
КЗ 5	•	•	•	•		•						
КЗ 6	•	•	•						•			
КЗ 7											•	
КЗ 8		•	•	•			•		•	•		
КЗ 9		•	•	•			•		•	•	•	
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

	ЗК13.1.01	ЗК13.1.02	ЗК13.1.03	ЗК13.1.04	ПП13.2.01	ПП13.2.02	ПП.13.2.03	ПП.13.2.04	ПП.13.2.05	ПП.13.2.06	ПП.13.2.07	ПП.13.2.08
РН1				•	•	•			•			
РН2	•	•		•		•			•			
РН3			•	•						•	•	•
РН4					•					•	•	•
РН5				•		•		•		•	•	•
РН6					•	•	•	•				
РН7				•	•			•				
РН8						•				•	•	•
РН9				•		•						
РН10				•	•					•	•	•
РН11				•		•		•		•	•	•
РН12				•						•	•	•
РН13				•						•	•	•
РН14				•		•						
РН15				•		•			•			
РН16				•	•			•				
РН17	•	•	•	•		•		•	•	•	•	•
РН18		•		•					•			
РН19			•	•						•	•	•
РН20			•	•		•				•	•	•
РН21										•		
РН22				•						•	•	•
РН23			•			•				•	•	•
РН24							•			•	•	•
РН25							•			•	•	•
РН26						•	•				•	•
РН27							•					
РН28				•	•	•	•					
РН29						•	•				•	•
РН30						•	•					
РН31						•				•	•	•

Гарант освітньої програми
Завідувач кафедри управління інформаційною та кібернетичною безпекою
Навчально-наукового інституту захисту інформації
Державного університету телекомунікацій,
доктор економічних наук, професор **С.В. Легомінова**