МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

другого (магістерського) рівня вищої освіти
(оновлена)

Спеціальність	**125 Кібербезпека та захист інформації**
Галузь знань	**12 Інформаційні технології**
Кваліфікація:	**Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою**

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Протокол № 10 від 01 квітня 2024 р.
Наказ № 64 від 01 квітня 2024 р.

Ректор _____ Володимир ТОЛУБКО

Освітньо-професійна програма вводиться в дію з 01 вересня 2024 р.

Київ – 2024

ЛИСТ ПОГОДЖЕННЯ

ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

галузь знань	12 «Інформаційні технології»
спеціальність	125 «Кібербезпека та захист інформації»
рівень вищої освіти	другий (магістерський)
кваліфікація	Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою

1. Проректор з навчально-виховної роботи Вадим ВЛАСЕНКО
2. Проректор з навчально-виховної та наукової роботи Любов БЕРКМАН
3. Директор Навчально-методичного центру Ірина СРІБНА
4. Вчена рада Навчально-наукового інституту захисту інформації

Протокол № 8 від «18» квітня 2024 р.

Голова Вченої Ради ННІЗІ _____ Віталій САВЧЕНКО

5. Кафедра управління інформаційною та кібернетичною безпекою

Протокол № 11 від «15» квітня 2024 р.

Завідувач кафедри управління інформаційною та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА

Рецензії від зовнішніх стейкхолдерів (компаній-партнерів):

1. Товариство з обмеженою відповідальністю «ІТ спеціаліст»;
2. ДТ «ЕС ЕНД ТІ Україна»

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Гарант освітньо-професійної програми
Світлана ЛЕГОМІНОВА - доктор економічних наук, професор, завідувач кафедри управління інформаційною та кібернетичною безпекою.

Члени робочої групи:
Дмитро РАБЧУН - кандидат технічних наук, доцент кафедри управління інформаційною та кібернетичною безпекою;
Тетяна МУЖАНОВА - кандидат наук з державного управління, доцент, доцент кафедри управління інформаційною та кібернетичною безпекою;
Юрій ЯКИМЕНКО - кандидат військових наук, доцент, доцент кафедри управління інформаційною та кібернетичною безпекою;
Михайло ЗАПОРОЖЧЕНКО – асистент кафедри управління інформаційною та кібернетичною безпекою;
Юрій СЄМЄЙКІН – директор ТОВ «ІТ Спеціаліст»;
Юрій ЛИСЕЦЬКИЙ – директор ДП «ЕС ЕНД ТІ Україна»;
Діана ПРИМАЧЕНКО – студентка спеціальності 125 «Кібербезпека та захист інформації».

ВІДОМОСТІ ПРО ПЕРЕГЛЯД ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Освітньо-професійна програма розроблена відповідно до:

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;

Наказом Міністерства економіки України «Про затвердження зміни № 13 до національного класифікатора ДК 003:2010» «Класифікатор професій» від 16.01.2024 № 1410;

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

1. Профіль освітньо-професійної 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 Управління інформаційною та кібернетичною безпекою
Офіційна назва освітньої програми	Освітньо-професійна програма «Управління інформаційною та кібернетичною безпекою»
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний Обсяг освітньої програми - 90 кредитів ЄКТС; термін навчання 1рік та 5 місяців
Наявність акредитації	
Цикл/рівень	НРК України – 7 рівень/ Магістр, QF-EHEA- другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність освітнього рівня бакалавра, освітнього рівня магістра 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	http://www.dut.edu.ua/ua/1826-osvitno-profesiyni-programi-kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu

2 – Мета освітньо-професійної програми
Метою програми є підготовка висококваліфікованих фахівців магістрів з кібербезпеки та захисту інформації за освітньо-професійною програмою «Управління інформаційною та кібернетичною безпекою», які здатні проводити наукові дослідження, описувати й роз'яснювати процеси, що відбуваються у сфері інформаційної безпеки та/або кібербезпеки, формувати розуміння закономірностей процесів управління інформаційною безпекою та/або кібербезпекою, здійснювати апробацію та практичне впровадження наукових результатів, володіють інноваційним способом мислення та компетентностями, необхідними для ефективного управління інформаційною безпекою та/або кібербезпекою, і здатні вирішувати управлінські та науково-дослідні завдання щодо управління ризиками, розслідування інцидентів та проведення аудиту систем інформаційної безпеки та/або кібербезпеки, володіють навичками аналітичної роботи з інформацією.

Набуті компетентності можуть бути застосовані в дослідницькій, управлінській, освітній, бізнесовій та інших дисциплінарно-професійних сферах.	
3 – Характеристика освітньо-професійної 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, критичної інфраструктури, сфери інформаційної безпеки та/або кібербезпеки; – інформаційні, комунікаційні та інформаційно-комунікаційні, автоматизовані системи та технології; – інфраструктура об'єктів інформаційної діяльності та критичної інфраструктури; – 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 завдання дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** Теоретичні засади наукоємних технологій, фундаментальні фізико-математичні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання й 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 й використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних завдань у 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, мережеве устаткування й середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проєктування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні й супроводженні об'єктів інформаційної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньо-професійної програми	Освітньо-професійна. Програма має прикладний характер, спрямована на забезпечення потреб ринку праці, зокрема в галузі ІТ.
Основний фокус освітньо-професійної програми та спеціалізації	Дослідження в галузі інформаційної та кібербезпеки. Акцент на впровадженні інноваційних методів і технологій в процесі управління інформаційною та/або кібербезпекою на підприємствах, в установах і організаціях. Ключові слова: РИЗИКИ, ЗАГРОЗИ І ВРАЗЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКИ, ЗАХИСТ ІНФОРМАЦІЇ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА КІБЕРБЕЗПЕКОЮ
Особливості програми	Програма реалізується науковими групами, передбачає застосування широкого кола загальнонаукових і спеціальних аналітичних методів, принципів і прийомів наукових досліджень, з урахуванням сучасного світового досвіду в сфері інформаційної безпеки та/або кібербезпеки. Передбачено проведення лекційних курсів, лабораторних, семінарських та практичних занять, тренінгів, із залученням фахівців з інформаційної безпеки та/або кібербезпеки, самостійної науково-дослідної роботи. ***У програму впроваджені результати проєкту 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	Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою (випускник) здатний виконувати професійні роботи за Державним класифікатором професій ДК 003: 2010 **Основна**: **2139.2 –** Фахівець з планування політики та стратегії кібербезпеки; **2132.2** – Розробник систем захисту інформації; **2139.2** – Аудитор інформаційних технологій (з кібербезпеки); **Додаткова:** **2139.2** – Фахівець з оцінки заходів захисту інформації (кібербезпеки) **2139.2** – Фахівець з питань безпеки
Подальше навчання	Продовжити освіту за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
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 спрямоване на засвоєння знань, умінь і навичок для подальшого застосування на практиці. Основними способами передачі змісту освітньої програми є проведення лекцій, практичних, лабораторних та індивідуальних занять, консультацій, розв'язання ситуативних завдань, тестування, презентацій, практичні 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 освітньо-професійною програмою та зазначені у навчальному

	плані. Критерії оцінювання знань, умінь та навичок здобувачів вищої освіти розроблені відповідно до чинного законодавства й затверджені у «Положенні про організацію освітнього процесу у Державному університеті інформаційно-комунікаційних технологій». 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 завдання 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. КЗ-3. 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 проєктів 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 (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 завдань 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 відповідно 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 запобігання 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	
	ПРН1. 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. ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних завдань інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. ПРН5. 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. ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних завдань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або

	кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН12. 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. ПРН13. 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. ПРН14. 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. ПРН15. 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. ПРН16. 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. ПРН17. 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. ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. ПРН19. 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. ПРН20. Ставити та вирішувати складні інженеПРНо-прикладні та наукові завдання інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. ПРН22. 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. ПРН23. 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. ПРН24. Уміти розробляти проекти досліджень та моделювати їх структуру, застосовуючи різні способи подання статистичної інформації та результатів. ПРН25. Уміти використовувати знання й уміння для прогнозування, виявлення та оцінювання можливих загроз інформаційному простору держави, дестабілізуючих чинників. ПРН26. 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. ПРН27. 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. ПРН28. Здатність використовувати професійно профільні знання, готувати та приймати управлінські рішення у сфері інформаційної безпеки. ПРН29. 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. ПРН30. Уміти застосовувати сучасні способи, методи та засоби управління наступними аспектами захисту: політикою безпеки, архітектурою захисту, механізмами захисту та засобами захисту. ПРН31. 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 інформаційно-комунікаційних технологій, мають підтверджений рівень наукової і професійної активності. Група забезпечення спеціальності 125 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 125 Кібербезпека та захист інформації спеціалізації Управління інформаційною та кібернетичною 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: USM/SIEM від компанії-вендора AlienVault, IBM QRadar SIEM, IBM i2 Analyze Notebook Premium, Tenable Nessus Professional. Лабораторія 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 із 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 відповідно до вимог міжнародних стандартів з інформаційної безпеки та/або кібербезпеки. Програмні засоби підтримки прийняття рішень у сфері інформаційної безпеки («Вибір», Mpriority1.0). Використання програмного забезпечення: • Microsoft Project, Spider Project Lite, OpenProj, GanttProject, Microsoft Excel, Project Expert – управління проєктами та інвестиційна оцінка; • MindMap, Mindomo – інструменти для створення карт проєктів та генерування інноваційних ідей

	• Microsoft Power BI, Microsoft Visio – аналітика й візуалізації даних. • НАВЧАЛЬНА ЛАБОРАТОРІЯ ЗАСОБІВ КОНТРОЛЮ ДОСТУПУ «HIKVISION» – забезпечує проведення практичних занять та досліджень з питань контролю та управління доступом, використання автономних біометричних терміналів, мережевих контролерів, програмно-апаратного комплексу системи відеоспостереження HikVision. Обладнана автоматизованим комплексом відеоспо-стереження та охорони об'єктів інформаційної діяльності (Harbor), програмно-апаратними комплексами контролю доступу (HikVision), сповіщувачами інфрачервоними (SRP 600) та магніто-контактними (СОМК-10). Дозволяє вивчати питання застосування програмних комплексів захисту інформації («Лоза», «Гриф», «Рубіж»). НАВЧАЛЬНА ЛАБОРАТОРІЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ «PIAC» – забезпечує проведення практичних занять з питань технічного захисту конфіденційної інформації на об'єктах інформаційної діяльності від витоку акустичним, віброакустичним та електромагнітним каналами з використанням широкосмугових генераторів акустичного та електромагнітного шуму (Piac-2ГС, ГШ 1000, «Беркут»). Крім того, у лабораторії досліджуються питання застосування пошукового програмно-апаратного комплексу DigiSkan EX; методів виявлення випромінювань за допомогою індикаторів поля типу PROTEKT; порядку застосування скануючих приймачів AR 8200, IC-R5, IC-R2500 та локатора нелінійностей NR-900 EM.
Інформаційне та навчально-методичне забезпечення	Інформація про освітньо-професійну 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 освітньо-професійної програми забезпечені навчально-методичними матеріалами, є у вільному доступі в якості ресурсів бібліотеки, електронної бібліотеки університету й системи управління навчанням Moodle.

9 – Академічна мобільність	
Національна кредитна мобільність	Наявність двосторонніх договорів між ДУІКТ та закладами вищої освіти України забезпечує національну кредитну мобільність.
Міжнародна кредитна мобільність	Зміст навчання відповідає світовим освітнім стандартам, що дозволяє здобувачам брати участь у програмах подвійних дипломів і бути конкурентоспроможними на світовому ринку праці.
Навчання іноземних здобувачів вищої освіти	Надається можливість навчання іноземним громадянам.

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

2.1. Зміст підготовки за освітньо-професійною програмою компетентності та результатами навчання

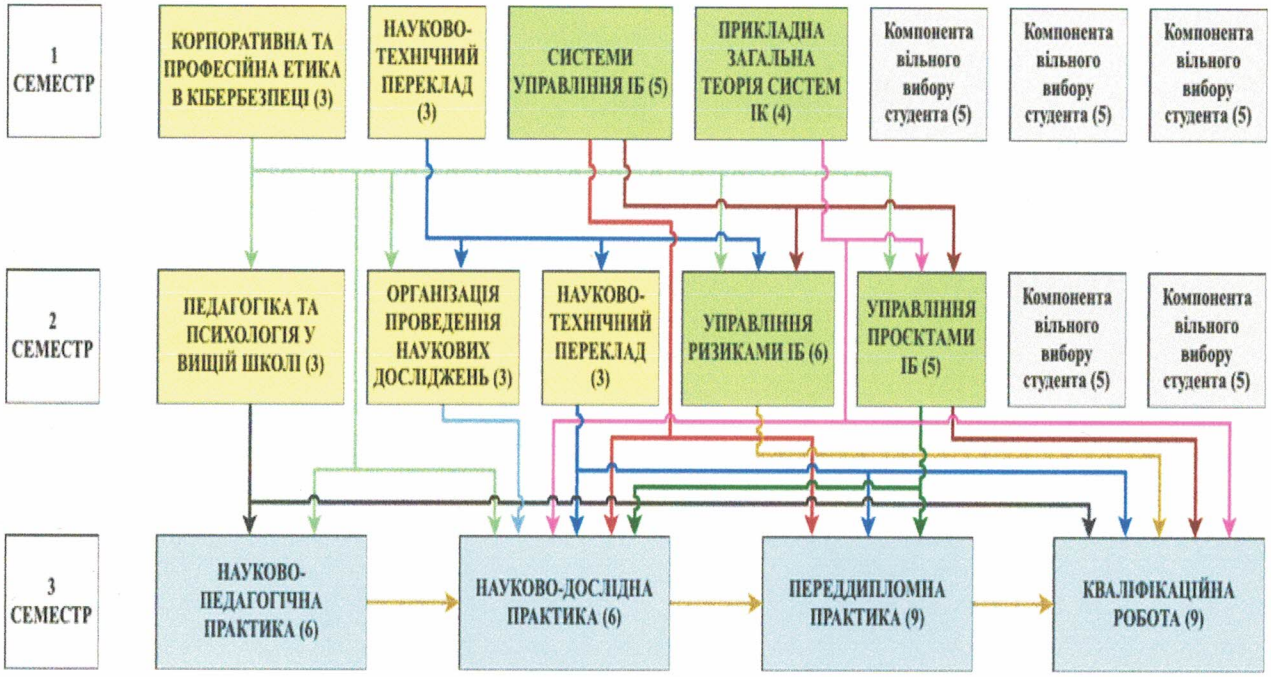
№ п.п.	Компонента	Шифр	Компетентність	Результат навчання
Цикл компонент загальної підготовки				
1.	Корпоративна та професійна етика в кібербезпеці	ЗК.13.1.01	КЗ-1, КЗ-3, КЗ-4, КЗ-5, КЗ-7, КЗ-8, КЗ-9, КФ2, КФ4, КФ10	РН1, РН7, РН15, РН16, РН18, РН27
2.	Педагогіка та психологія у вищій школі	ЗК.13.1.02	КЗ-1, КЗ-3, КЗ-4, КЗ-5, КЗ-9, КФ10	РН1, РН2, РН17, РН18
3.	Організація проведення наукових досліджень	ЗК.13.1.03	КЗ-2, КЗ-3, КФ2, КФ10	РН3, РН17, РН20, РН22
4.	Науково-технічний переклад	ЗК.13.1.04	КЗ-2, КЗ-5, КЗ-9, КФ2, КФ4	РН1, РН3, РН26
Цикл компонент професійної підготовки				
1.	Управління ризиками інформаційної безпеки	ПП.13.2.01	КЗ-2, КЗ-3, КЗ-4, КЗ-5, КФ2, КФ5	РН10, РН31
2.	Системи управління інформаційною безпекою	ПП.13.2.02	КЗ-1, КЗ-6, КФ1, КФ2, КФ4, КФ6	РН6, РН8, РН9, РН11, РН14, РН23, РН26, РН29, РН30, РН31
3.	Управління проєктами інформаційної безпеки	ПП.13.2.03	КЗ-1, КЗ-2, КЗ-4, КЗ-5, КФ1, КФ2, КФ3, КФ4, КФ9	РН4, РН8, РН9, РН14, РН17, РН20
4.	Прикладна загальна теорія систем інформаційної та кібербезпеки	ПП.13.2.04	КЗ-1, КЗ-4, КФ2, КФ3, КФ4, КФ6, КФ8	РН5, РН6, РН7, РН11, РН16, РН17, РН23
5.	Науково-педагогічна практика	ПП.13.2.05	КЗ-1, КЗ-6, КЗ-8, КЗ-9, КФ10	РН1, РН15, РН17, РН18
6.	Науково-дослідна практика	ПП.13.2.06	ІК, КЗ-1, КЗ-2, КЗ-3, КЗ-4, КЗ-8, КЗ-9, КФ1, КФ2, КФ3, КФ5, КФ7, КФ8	РН2, РН3, РН4, РН5, РН8, РН11, РН12, РН13, РН17, РН19, РН20, РН21, РН22, РН23, РН24, РН25, РН31
7.	Переддипломна практика	ПП.13.2.07	ІК, КЗ-1, КЗ-2, КЗ-3, КЗ-4, КЗ-9, КФ1, КФ2, КФ5, КФ6, КФ7, КФ8	РН2, РН3, РН4, РН5, РН7, РН8, РН10, РН11, РН12, РН13, РН17, РН19, РН20, РН21, РН22,РН23, РН24, РН25, РН26, РН28, РН29, РН30, РН31
8.	Підготовка кваліфікаційної роботи, підсумкова атестація	ПП.13.2.08	ІК, КЗ-1, КЗ-2, КЗ-3, КЗ-4, КФ1, КФ2, КФ3, КФ6, КФ7,	РН2, РН4, РН5, РН8, РН12, РН13, РН17, РН19, РН20,

			КФ9	РН22,РН23, РН24, РН25, РН26, РН29, РН31
Компоненти вільного вибору студента				
1.	Компонента вільного вибору студента			
2.	Компонента вільного вибору студента			
3.	Компонента вільного вибору студента			
4.	Компонента вільного вибору студента			
5.	Компонента вільного вибору студента			

2.2. Перелік компонент ОПП

Код н/д	Компоненти освітньо-професійної програми (навчальні компоненти, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОПП			
Цикл загальної підготовки			
ЗК.13.1.01	Корпоративна та професійна етика в кібербезпеці	3	Іспит
ЗК.13.1.02	Педагогіка та психологія у вищій школі	3	Залік
ЗК.13.1.03	Організація проведення наукових досліджень	3	Залік
ЗК.13.1.04	Науково-технічний переклад	6	Залік, Іспит
Цикл професійної підготовки			
ПП.13.2.01	Управління ризиками інформаційної безпеки	6	Іспит
ПП.13.2.02	Системи управління інформаційною безпекою	5	Іспит
ПП.13.2.03	Управління проєктами 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	Підготовка кваліфікаційної роботи, підсумкова атестація	9	Залік
Загальний обсяг обов'язкових компонент:		**65**	
Вибіркові компоненти ОПП			
ВК1	Компонента вільного вибору студента	5	Залік
ВК2	Компонента вільного вибору студента	5	Залік
ВК3	Компонента вільного вибору студента	5	Залік
ВК4	Компонента вільного вибору студента	5	Залік
ВК5	Компонента вільного вибору студента	5	Залік
Загальний обсяг вибіркових компонент:		**25**	Залік
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ		**90**	

2.3. Структурно-логічна схема ОПП



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

3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація магістрів з кібербезпеки за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складні завдання 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 з «Положенням про запобігання академічному плагіату у Державному університеті інформаційно-комунікаційних технологій». 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 освітньо-професійної 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
КЗ1	•	•				•	•	•	•	•	•	•
КЗ2			•	•	•		•			•	•	•
КЗ3	•	•	•		•					•	•	•
КЗ4	•	•			•		•	•		•	•	•
КЗ5	•	•		•	•		•					
КЗ6						•			•			
КЗ7	•											
КЗ8	•								•	•		
КЗ9	•	•		•					•	•	•	
КФ1						•	•			•	•	•
КФ2	•		•	•	•	•	•	•		•	•	•
КФ3							•	•		•		•
КФ4	•			•		•	•	•				
КФ5					•					•	•	
КФ6						•		•			•	•
КФ7										•	•	•
КФ8								•		•	•	
КФ9		•					•					•
КФ10	•	•	•						•			

5. Матриця забезпечення програмних результатів навчання (РН) відповідними компонентами освітньо-професійної 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 освітньо-професійної програми
Завідувач кафедри управління інформаційною та кібернетичною безпекою
Навчально-наукового інституту захисту інформації
Державного університету
інформаційно-комунікаційних технологій
доктор економічних наук, професор **Світлана ЛЕГОМІНОВА**