МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА

другого (магістерського) рівня вищої освіти

(оновлена)

Спеціальність 125 Кібербезпека та захист інформації

Галузь знань 12 Інформаційні технології

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

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Протокол № 10 від 01 квітня 2024 р.
Наказ № 64 від 1 квітня 2024 р.

Ректор _____ Володимир ТОЛУБКО

Освітня програма вводиться в дію з 01 вересня 2024 р.

Київ 2024

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

спеціальність	*125 Кібербезпека та захист інформації*
галузь знань	*12 Інформаційні технології*
рівень вищої освіти	*другий (магістерський)*
освітня кваліфікація	*Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою інформаційна та кібернетична безпека*

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» березня 2024 р.

Голова Вченої Ради ННІЗІ _____ Віталій САВЧЕНКО

5. Кафедра інформаційної та кібернетичної безпеки

Протокол № 8 від «05» березня 2024 р.

Завідувач кафедри інформаційної та кібернетичної безпеки _____ Галина ГАЙДУР

Рецензії від зовнішніх стейкхолдерів:

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

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Гарант освітньої програми (голова робочої групи)

Галина ГАЙДУР – доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки;

Члени робочої групи:

Андрій КОЖУХІВСЬКИЙ – доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки;

Сергій ГАХОВ – кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки

Юрій БОРСУКОВСЬКИЙ – кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки;

Павло БУЛАВІН –директор ТОВ "ЄВРОТЕЛЕКОМ;

Тетяна ПАРФЕНЮК – студентка спеціальності 125 Кібербезпека та захист інформації, ОПП «Інформаційна та кібернетична безпека».

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 Міністерства освіти та науки України від 18.03.2021 № 332);

Внесення до Реєстру кваліфікацій відомості про професійний стандарт «Викладачі закладів вищої освіти» (Наказ Мінекономіки від 23.03.2021 № 610);

Внесення до Реєстру кваліфікацій відомості щодо професійних стандартів у галузі кібербезпеки: «Аналітик з безпеки інформаційно-телекомунікаційних систем», «Адміністратор мереж та систем» (Наказ Адміністрації Держспецзв'язку від 25 листопада 2022 № 715);

Постанови Кабінету Міністрів України «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 16 грудня 2022 року №1392;

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

Внесення до Реєстру кваліфікацій відомості про професійні стандарти у сфері кібербезпеки та захисту інформації від 23 січня 2024 року, рекомендацій стейкхолдерів та побажань здобувачів вищої освіти.

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
Наявність акредитації	
Цикл/рівень	НРК України – 7 рівень/ Магістр, QF-EHEA- другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра, освітнього ступеня магістра (освітньо-кваліфікаційного рівня спеціаліста) іншої спеціальності.
Мова(и) викладання	Українська, англійська
Термін дії освітньої програми	Введена в дію з 01.09.2017 року
Інтернет - адреса постійного розміщення опису освітньої програми	https://www.dut.edu.ua/ua/1822-osvitno-profesiyni-programi-kafedra-informaciynoi-ta-kibernetichnoi-bezpeki
2 – Мета освітньої програми	
Метою магістерської програми є підготовка висококваліфікованих фахівців магістрів з захисту інформації в інформаційних і комунікаційних системах, які здатні розв'язувати задачі дослідницького та інноваційного характеру, описувати та роз'яснити процеси, що відбуваються у сфері інформаційної та/або кібернетичної безпеки, формувати розуміння закономірностей процесів при захисті інформації в інформаційних і кібернетичних системах, здійснювати апробацію та практичне впровадження наукових результатів, які володіють інноваційним способом мислення та мають компетентності, необхідні для проведення дослідження сучасних процесів, аналізу, створення та забезпечення захисту інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки щодо розслідування інцидентів,	

підтримки інфраструктури кіберзахисту, 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	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 зі врахуванням сьогоднішнього стану сфери кібербезпеки, має прикладний характер, спрямована на забезпечення потреб ринку праці при вирішенні професійних задач в галузі інформаційної безпеки та кібербезпеки.
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.

	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 співпраці з компанією IBM на основі підписаного меморандуму щодо створення «Центру компетенцій IBM».***
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 **Додаткова:** 2139.2 Аналітик з безпеки інформаційно-телекомунікаційних систем Фахівець з питань безпеки Аналітик загроз безпеки Фахівець з криптографічного захисту інформації Аналітик з оцінки вразливостей Фахівець з тестування систем захисту інформації Аудитор інформаційних технологій (з кібербезпеки) Фахівець з оцінки заходів захисту інформації (кібербезпеки) Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту
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. *К310. Здатність застосовувати кращі практики у професійній діяльності.* *К311. 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 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 освітньої програми Інформаційна та кібернетична безпека 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, 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 КРИПТОГРАФІЧНОГО ЗАХИСТУ НА БАЗІ ТЕХНОЛОГІЙ «АВТОР» 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. 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.
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 / 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.	Корпоративна та професійна етика в кібербезпеці	ЗК.11.1.01	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	ЗК.11.1.02	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	ЗК.11.1.03	К31, К32, К33, К34, К35, К37 К38, К39, К310, КФ1, КФ2, КФ3, КФ4, КФ6, КФ7, КФ8, КФ9, КФ10	РН3, РН17, РН19, РН20, РН23
4.	Науково-технічний переклад	ЗК.11.1.04	К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ6, КФ7, КФ8, КФ9, КФ10	РН1, РН2, РН17, РН20, РН23
Цикл дисциплін професійної підготовки				
1.	Прикладна загальна теорія систем інформаційної та кібербезпеки	ПП.11.2.01	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	ПП.11.2.02	К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ4, КФ9, КФ10	РН4, РН8, РН9, РН14, РН17, РН20
3.	Технології забезпечення безпеки мережевої інфраструктури	ПП.11.2.03	К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21
5.	Технології виявлення уразливостей мережевих ресурсів	ПП.11.2.04	К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21
6.	Науково-педагогічна практика	ПП.11.2.05	К31, К32, К33,	РН1, РН2, РН15,

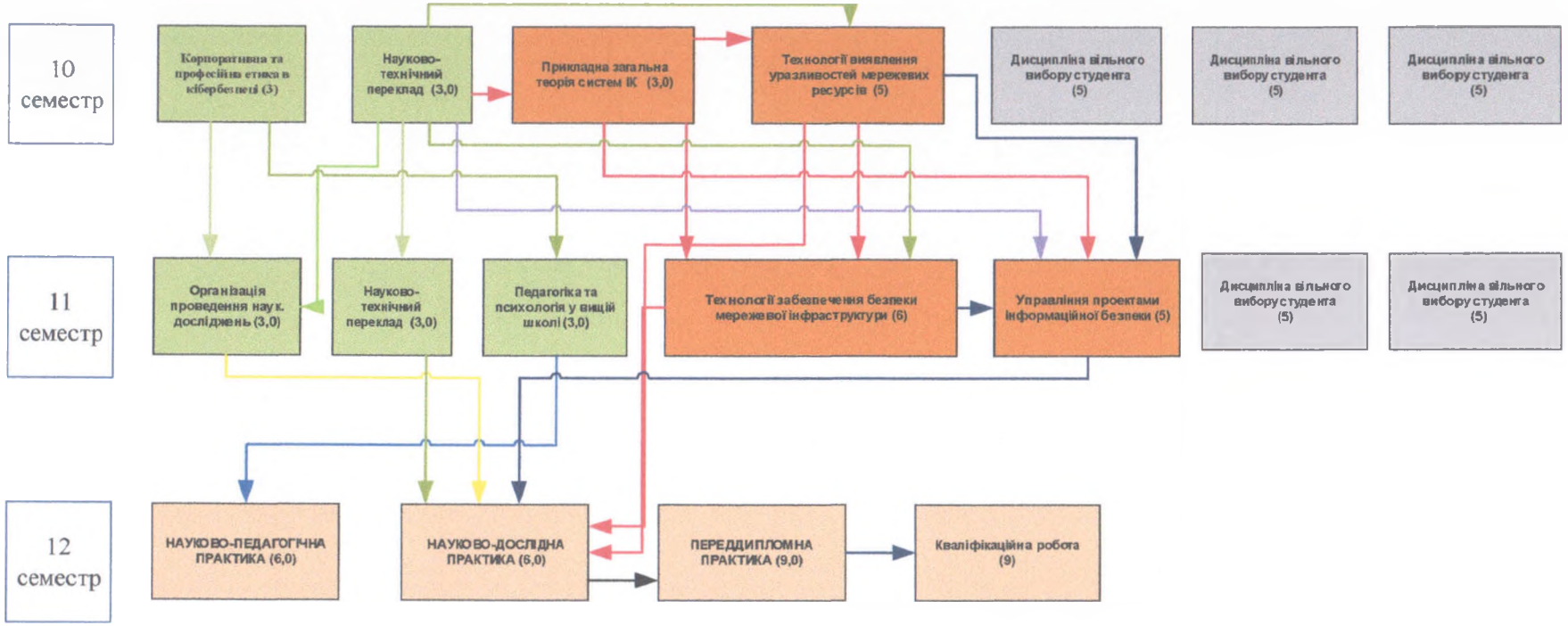
			К34, К35, К36, К36, К37, К38, К39, К310, К311, КФ1, КФ2, КФ3, КФ10	РН17, РН18
5.	Науково-дослідна практика	ПП.11.2.06	К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	РН3, РН4, РН5, РН8, РН11, РН12, РН13, РН17, РН19, РН20, РН21, РН22, РН23
6.	Переддипломна практика	ПП.11.2.07	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
7.	Кваліфікаційна робота	ПП.11.2.08	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
Дисципліни вільного вибору студента				
1.	Дисципліни вільного вибору здобувача			
2.	Дисципліни вільного вибору здобувача			
3.	Дисципліни вільного вибору здобувача			
4.	Дисципліни вільного вибору студента			
5.	Дисципліни вільного вибору здобувача			

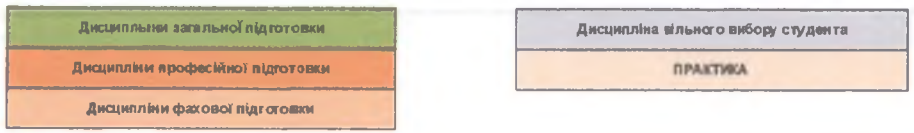
2.2. Перелік компонент ОП

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 ОП			
Цикл загальної підготовки			
ЗК.11.1.01	Корпоративна та професійна етика в кібербезпеці	3	Іспит
ЗК.11.1.02	Педагогіка та психологія у вищій школі	3	Залік
ЗК.11.1.03	Проведення наукових досліджень в кібербезпеці	3	Залік
ЗК.11.1.04	Науково-технічний переклад	6	Залік, Іспит
Цикл професійної та практичної підготовки			
ПП.11.2.01	Прикладна загальна теорія систем інформаційної та	4	Іспит

	кібербезпеки		
ПП.11.2.02	Управління проектами інформаційної безпеки	5	Іспит
ПП.11.2.03	Технології забезпечення безпеки мережевої інфраструктури	6	Іспит
ПП.11.2.04	Технології виявлення уразливостей мережевих ресурсів	5	Іспит
ПП.11.2.05	Науково-педагогічна практика	6	Залік
ПП.11.2.06	Науково-дослідна практика	6	Залік
ПП.11.2.07	Переддипломна практика	9	Залік
ПП.11.2.08	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 ОП





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

	ЗК11.1.01	ЗК11.1.02	ЗК11.1.03	ЗК11.1.04	ПП11.2.01	ПП11.2.02	ПП.11.2.03	ПП.11.2.04	ПП.11.2.05	ПП.11.2.06	ПП.11.2.07	ПП.11.2.08
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

	ЗК11.1.01	ЗК11.1.02	ЗК11.1.03	ЗК11.1.04	ПП11.2.01	ПП11.2.02	ПП.11.2.03	ПП.11.2.04	ПП.11.2.05	ПП.11.2.06	ПП.11.2.07	ПП.11.2.08
РН1	•			•					•			
РН2		•		•					•			
РН3			•		•					•	•	•
РН4						•	•	•		•	•	•
РН5					•		•	•		•	•	•
РН6					•		•	•				
РН7					•							
РН8						•	•	•		•	•	•
РН9						•						
РН10											•	•
РН11					•		•	•		•	•	•
РН12										•	•	•
РН13							•	•		•	•	•
РН14						•						
РН15	•								•			
РН16	•				•							
РН17	•	•	•	•	•	•	•	•	•	•	•	•
РН18	•	•							•			
РН19			•							•	•	•
РН20			•	•		•				•	•	•
РН21							•	•		•		•
РН22										•	•	
РН23			•	•	•					•	•	

Гарант освітньої програми
Завідувач кафедри інформаційної та кібернетичної безпеки
Навчально-наукового інституту захисту інформації
Державного університету інформаційно-комунікаційних технологій

доктор технічних наук, професор **Галина ГАЙДУР**

РЕЦЕНЗІЯ

на освітню програму «Інформаційна та кібернетична безпека»
за спеціальністю 125 «Кібербезпека та захист інформації»
другого (магістерського) рівня вищої освіти

Державний університет інформаційно-комунікаційних технологій, зокрема навчально-науковий інститут захисту інформації, провів оновлення освітньої програми (ОП) «Інформаційна та кібернетична безпека» за спеціальністю 125 «Кібербезпека та захист інформації». Оновлена програма узгоджена з освітнім та професійними стандартами, потребами стейкхолдерів, а також здобувачами вищої освіти.

Освітня програма включає у себе комплекс загальних та спеціалізованих (фахових) компетенцій, які становлять основу для навчального процесу, організованого за структурно-логічною схемою, що забезпечує чітку послідовність та логічну взаємопов'язаність між навчальними дисциплінами. Додатково, програма пропонує 25 кредитів на вибіркові дисципліни, що дає здобувачам можливість формувати власну індивідуальну освітню траєкторію відповідно до професійних інтересів та кар'єрних амбіцій.

Значну роль у досягненні поставлених навчальних цілей освітньої програми відіграє оснащеність спеціалізованих лабораторій інституту, зокрема, «Академічний центр компетенцій ІВМ «Кіберполігон», що забезпечує можливість відпрацювання практичних навичок в контексті реальних умов роботи у центрі забезпечення кібербезпеки, використовуючи сучасні технології для моніторингу, виявлення, аналізу та реагування на кіберінциденти в корпоративних інформаційних системах.

Розглянута освітня програма сприяє отриманню здобувачами професійної кваліфікації за двома професійними стандартами: «Фахівець з реагування на інциденти кібербезпеки» та «Фахівець з підтримки інфраструктури кіберзахисту». Впровадження цих стандартів в освітній процес підкреслює унікальність програми, акцентуючи увагу на компетенціях, які отримують здобувачі.

У підсумку, розглянута освітня програма «Інформаційна та кібернетична безпека» для підготовки здобувачів другого (магістерського) рівня вищої освіти демонструє високу відповідність Стандарту вищої освіти України та профільним професійним стандартам. Вона є актуальним інструментом для підготовки висококваліфікованих фахівців у сфері кібербезпеки, здатних ефективно використовувати сучасні технології та методики для захисту інформаційних ресурсів організацій в умовах зростаючих кіберзагроз.

Таким чином, на основі проведеного аналізу, можна зробити висновок, що дана освітня програма є вагомим внеском у розвиток освітніх практик у галузі кібербезпеки, сприяє підвищенню професійного рівня випускників та забезпечує їх готовність до вирішення комплексних завдань у цій динамічно змінюваній сфері.

РЕЦЕНЗЕНТ:

Доктор технічних наук, професор, професор кафедри
кібербезпеки та захисту інформації, факультету інформаційних
технологій Київського національного університету
імені Тараса Шевченка Сергій ТОЛЮПА

Підпис професора Толюпи С.В. засвідчую.
Заступник декана з навчально-виховної роботи
кандидат фіз. - матем. наук., доцент Наталія ГМЄНОВА

eurotelecom

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ЄВРОТЕЛЕКОМ» 34637389 | +38 099 915-915 9 office@etele.com.ua | 03191, Україна, м. Київ, вул.Волинська, буд.10

№ 27032024-72 від 27 березня 2024 р.

РЕЦЕНЗІЯ–ВІДГУК

на освітньо-професійну програму
«ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА»
за спеціальністю 125 «Кібербезпека та захист інформації»
другого (магістерського) рівня вищої освіти

Відповідно до стандарту вищої освіти другого (магістерського) рівня вищої освіти рівня вищої освіти в Державному університеті інформаційно-комунікаційних технологій навчально-наукового інституту захисту інформації оновлено освітню програму (ОП) «Інформаційна та кібернетична безпека» за спеціальністю 125 Кібербезпека та захист інформації.

Розроблена освітня програма враховує вимоги освітнього та професійних стандартів, стейкхолдерів, та здобувачів вищої освіти. Досягнення результатів навчання в ОП «Інформаційна та кібернетична безпека» відбувається шляхом вивчення циклу дисциплін загальної та професійної підготовки, які дозволять набути компетентностей щодо отримання ступеня магістра за зазначеною спеціальністю.

Розглянута освітня програма надає можливість здобувачам отримати професійну кваліфікацію за двома професійними стандартами «Фахівець з реагування на інциденти кібербезпеки» та «Фахівець з підтримки інфраструктури кіберзахисту». Набуття компетентностей даних стандартів прослідковується в структурно-логічній схемі підготовки фахівця. Саме це робить ОП «Інформаційна та кібернетична безпека» унікальною між іншими освітніми програмами, яка акцентує увагу на вивчення питань щодо впровадження та адміністрування систем кіберзахистуй; реагування фахівців на кіберінциденти.

Відмічено, що ціль освітньої програми корелюється з сучасними вимогами до фахівців за даною спеціальністю, а саме, підготовка фахівців, здатних застосовувати і впроваджувати системи кіберзахисту на основі сучасних технологій кібербезпеки. Досягти таких результатів здобувачам дозволяє оснащення лабораторій «Інформаційної та кібернетичної безпеки». Наприклад «Академічний центр компетенцій IBM «Кіберполігон» дозволяє відпрацьовувати навички роботи у центрі забезпечення кібербезпеки (security operation center) з використанням технологій моніторингу, виявлення, аналізу та реагування на кіберінцидентів в корпоративних інформаційних системах.

ОП містить загальні та професійні компетентності, на які орієнтовано навчання в рамках даної програми; структурно-логічну схему взаємозв'язків та логіки й послідовності викладання навчальних дисциплін. В освітній програмі передбачено 25 кредитів на вибіркові дисципліни, які обираються здобувачами для формування їхньої індивідуальної освітньої траєкторії.

Враховуючи викладене зазначаю, що освітня програма «Інформаційна та кібернетична безпека» підготовки здобувачів другого (магістерського) рівня вищої освіти відповідає Стандарту вищої освіти України і зазначеним професійним стандартам і може використовуватися для підготовки фахівців спеціальності 125 «Кібербезпека».

Директор ТОВ «ЄВРОТЕЛЕКОМ» **Павло БУЛАВІН**