МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Державний університет інтелектуальних технологій і зв'язку

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека та захист інформації»

«Cybersecurity and information protection»

Рівень вищої освіти	Другий (магістерський)
Ступінь вищої освіти	Магістр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Освітня кваліфікація	Магістр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО
Вченою радою Державного університету інтелектуальних технологій і зв'язку
(протокол від 08 07 2024 р. № 3)

Освітньо-професійна програма (*оновлена*) вводиться в дію з 01 09 2024 р.
Ректор
_____ Олександр НАЗАРЕНКО
(наказ від 08 07 2024 р. № 01-02-114)

Одеса 2024

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми
«Кібербезпека та захист інформації»
зі спеціальності 125 Кібербезпека та захист інформації
за другим (магістерським) рівнем вищої освіти

ВНЕСЕНО
Кафедрою Кібербезпеки та технічного захисту інформації
Протокол № 10 від «14» 06 2024 р.

Зав. кафедри Володимир КОРЧИНСЬКИЙ

ПОГОДЖЕНО
Декан факультету Інформаційних технологій та кібербезпеки
14 06 2024 р. Євгеній ВАСИЛІУ

ПОГОДЖЕНО
Начальник відділу ліцензування та акредитації
24 06 2024 р. Юлія ШТОВБА

ПОГОДЖЕНО
Навчально-методичною радою Державного університету інтелектуальних технологій і зв'язку
Протокол від 28 06 2024 р. № 8

Голова Світлана ХАДЖИРАДЄВА

ПЕРЕДМОВА

Освітньо-професійна програма «Кібербезпека та захист інформації» підготовки здобувачів вищої освіти другого (магістерського) рівня за спеціальністю 125 Кібербезпека та захист інформації, галузі знань 12 Інформаційні технології розроблена відповідно до закону України «Про вищу освіту» №1556-VII від 01.07.2014 р., Стандарту вищої освіти за спеціальністю 125 Кібербезпека для другого (магістерського) рівня вищої освіти, затвердженого Наказом МОН України № 332 від 18.03.2021, враховує вимоги Професійного стандарту «Фахівець сфери захисту інформації», затвердженого наказом Адміністрації Держспецзв'язку № 715 від 25.11.2022.

1. **Внесено:** кафедрою Кібербезпеки та технічного захисту інформації.
2. **Затверджено та надано чинності** рішенням Вченої ради Державного університету інтелектуальних технологій і зв'язку, протокол від 08.07 2024р. № 3.
3. **Розроблено робочою групою у складі:**
   Керівник робочої групи (гарант освітньої програми):
   Кільдішев Віталій Йосипович, к.т.н., доц., доцент каф. Кібербезпеки та технічного захисту інформації
   Члени робочої групи:
   - Василіу Євген Вікторович, д.т.н., проф., проф. каф. Кібербезпеки та технічного захисту інформації
   - Рябуха О.М., к.т.н., ст.викл. каф. Кібербезпеки та технічного захисту інформації

4 . Ріцензії – відгуки зовнішніх стейкхолдерів:

Корченко О.Г. – президент ГО Асоціація спеціалістів кібербезпеки;

Ткаченко О.В. – заступник Генерального директора ТОВ «Консалтингова компанія СІДКОН»;

Барановський С.В. – директор департаменту інформаційних систем та систем безпеки ТОВ «Роберт Бош ЛТД».

1. Профіль освітньої-професійної програми «Кібербезпека та захист інформації» зі спеціальності 125 «Кібербезпека та захист інформації»

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Державний університет інтелектуальних технологій і зв'язку Факультет Інформаційних технологій та кібербезпеки Кафедра Кібербезпеки та технічного захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр (другий) Кваліфікація - Магістр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Кібербезпека та захист інформації
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний Обсяг кредитів ЄКТС, необхідний для здобуття другого (магістерського) ступеня вищої освіти: на базі ступеня «бакалавр» становить 90 кредитів ЄКТС. Термін навчання 1 рік 4 місяці
Наявність акредитації	Остання акредитація: Сертифікат про акредитацію УД № 16014202 від 19.05.2021р., виданий АК
Цикл/рівень	НРК України – 7 рівень, QF-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Особа має право здобувати ступінь магістра за умови наявності в неї ступеня бакалавра
Мова(и) викладання	Українська
Термін дії освітньої програми	До повного завершення періоду навчання або наступного оновлення програми
Інтернет-адреса постійного розміщення опису освітньої програми	https://suitt.edu.ua

2 – Мета освітньої програми	
Забезпечення фундаментальної та професійної підготовки; інтеграція науково-дослідної, інноваційної діяльності і навчального процесу; орієнтація на міжнародні вимоги та стандарти в сфері кібербезпеки та захисту інформації, світові наукові досягнення; дуальна освіта, орієнтація на вимоги ринку праці. Підготовка професіоналів, здатних забезпечувати захищеність інформації, що обробляється та передається в інформаційно-комунікаційних системах, від несанкціонованих дій з інформацією, витоку технічними каналами та спеціальних впливів на засоби обробки інформації. Інтеграція в освітню програму професійних компетентностей, знань, умінь та навичок професійного стандарту «Фахівець сфери захисту інформації».	
3 - Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності)	*Галузь знань:* 12 Інформаційні технології *Спеціальність:* 125 Кібербезпека та захист інформації *Об'єкт вивчення та професійної діяльності:* – 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; – комплексні системи захисту інформації

	– інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем. *Цілі навчання*: Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері захисту інформації, 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
Основний фокус освітньої програми	Підготовка професіоналів, здатних до інноваційної та науково-дослідницької діяльності при дослідженні, проектуванні, модернізації, впровадженні та експлуатації сучасних систем та технологій інформаційної та/або кібербезпеки; підготовка до виконання основних трудових функцій за професією «Фахівець сфери захисту інформації», код 2139.2. *Ключові слова*: кібернетична безпека, інформаційна безпека, системи і технології інформаційної та кібербезпеки, комплексні системи безпеки; безпека об'єктів критичної інфраструктури; криптологія; управління інформаційною безпекою.
Особливості програми	Розроблена з урахуванням міжнародних стандартів, рекомендацій та практик щодо студентоцентрованого навчання. Розроблена з врахуванням основних трудових функцій та професійних компетентностей професійного стандарту «Фахівець сфери захисту інформації», затвердженого наказом Адміністрації Держспецзв'язку № 715 від 25.11.2022. Передбачає ґрунтовну фундаментальну підготовку у поєднанні із сучасною професійною підготовкою, яка дозволяє проводити науково-дослідну та інноваційну діяльність і працювати з наукоємними технологіями кібербезпеки. Враховує особливості розвитку спеціальності та ринку праці шляхом залучення роботодавців, як зовнішніх аудиторів навчальних програм з метою підтвердження їхньої релевантності. Орієнтована на партнерство із вітчизняними та закордонними закладами освіти та науки, приватним сектором, науковцями та практиками, передбачає участь у міжнародних програмах з метою підвищення якості освіти. Передбачає дуальну освіту.

4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Види економічної діяльності згідно з Національним класифікатором України ДК 009:2010 «Класифікація видів економічної діяльності»: Секція J, розділ 62, група 62.0 – Комп'ютерне програмування, консультування та пов'язана з ними діяльність; розділ 63, група 63.9 – Надання інших інформаційних послуг. Секція M, розділ 71, група 71.2 – Технічні випробування та дослідження; розділ 74, група 74.9 – Інша професійна, наукова та технічна діяльність. Види професійної діяльності згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»: Розділ 2 – Професіонали, Клас 213 – Професіонали в галузі обчислень (комп'ютеризації), підклас 2139 – Професіонали в інших галузях обчислень (комп'ютеризації).
Подальше навчання	Можливість навчання на третьому (освітньо-науковому) рівні вищої освіти (НРК України – 8, рівень QF-EHEA – третій цикл, EQF-LLL – 8 рівень).
5 – Викладання та оцінювання	
Викладання та навчання	Проблемно-орієнтоване та студентоцентроване навчання із запровадженням в освітній процес індивідуальної траєкторії навчання та забезпеченням принципів академічної свободи. Комбінація лекцій, мультимедійних лекцій, семінарів, дослідницьких практичних занять, виконання проектів (в тому числі командних) самостійно та за участю менторів від компаній-стейкхолдерів, участь у конкурсах та хакатонах, самонавчання. На захист кваліфікаційних робіт (проектів) запрошуються представники компаній-стейкхолдерів. Методи навчання і викладання базуються на принципах свободи слова і творчості, застосування проектних методів роботи, поширення знань та інформації, поєднанні навчання, досліджень та виконання навчальних проектів під час освітнього процесу.

Оцінювання	Оцінювання знань студентів здійснюється у відповідності до Положення про оцінювання знань студентів ДУІТЗ. Екзамени, заліки, захист звіту з практики, захист курсових робіт (проектів), публічний захист кваліфікаційної роботи. Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано); 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F)
6 – Програмні компетентності (ПК)	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Здатність проводити дослідження на відповідному рівні. ЗК3. Здатність до абстрактного мислення, аналізу та синтезу. ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Спеціальні (фахові, предметні) компетентності (СК)	СК1. 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. СК2. 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. СК3. Здатність досліджувати, розробляти і

	супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. СК4. 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. СК5. 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. СК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. СК7. 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. СК8. 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. СК9. 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.

	СК10. 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. СК11. Здатність розробляти та впроваджувати комплексну систему захисту інформації, що протидіє багатьом різним за природою загрозам (кібератаки з боку інсайдерів та хакерів, злам програм, віруси, перехоплення трафіку, помилки тощо). СК12. Здатність ефективно використовувати на практиці різні теорії в області навчання технологіям, засобам та організаційним аспектам безпеки інформаційних і комунікаційних систем та мереж. СК13. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності. СК14. Здатність здійснювати постійний моніторинг та аудит загроз для інформації та відповідну модернізацію (доробку) систем і комплексів захисту інформації. СК15. Здатність проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки. СК16. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації. СК17. Здатність проводити оцінку відповідності (атестацію) комплексів технічного захисту інформації.

7 – Програмні результати навчання (ПРН)	
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 задач 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 задач 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 інженерно-прикладні та наукові задачі 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	Розроблювати плани аварійного відновлення та безперервності операцій в інформаційних, електронних, комунікаційних та інформаційно-комунікаційних системах.
ПРН25	Застосовувати сервіс-орієнтовані принципи архітектури безпеки, щоб задовольнити вимоги конфіденційності, цілісності та доступності організації.

ПРН26	Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі або на об'єкті інформаційної діяльності.
ПРН27	Здійснювати моніторинг та аудит загроз для інформації в інформаційних системах та мережах та оцінку ризиків безпеки інформації.
ПРН28	Здійснювати моніторинг та аудит загроз для інформації, що озвучується.
ПРН29	Використовувати інструменти та технології безперервного моніторингу з метою оцінки ризиків, користуватися прикладними програмами моніторингу та аудиту загроз для інформації в інформаційних системах та мережах
ПРН30	Проводити сканування вразливостей і розпізнання вразливостей в ІКС і системах безпеки.
ПРН31	Використовувати моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації.
ПРН32	Складати програму та методику атестації комплексу технічного захисту інформації (ТЗІ).
ПРН33	Здійснювати перевірку повноти і відповідності реалізованих заходів із захисту інформації вимогам технічного завдання на створення комплексу ТЗІ (або на створення КСЗІ в інформаційно-комунікаційних системах в частині вимог до захисту інформації від витоку технічними каналами), нормативно-правових актів та нормативних документів системи ТЗІ.
ПРН34	Приймати участь в організації та навчанні (підвищенні кваліфікації) працівників структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки, з відповідних питань.

8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Кадрове забезпечення відповідає кадровим вимогам щодо провадження освітньої діяльності для другого (магістерського) рівня вищої освіти відповідно до Ліцензійних умов провадження освітньої діяльності. Реалізація програми забезпечується кадрами високої кваліфікації, які мають значний досвід навчально-методичної, науково-дослідної та практичної роботи, є визнаними професіоналами за фахом. До реалізації програми злучається не менше 50% науково-педагогічних працівників, які мають науковий ступінь та/або вчене звання, не менше 25% мають науковий ступінь доктора наук або вчене звання професора. Система професійного розвитку викладачів реалізується через співпрацю з декількома провідними компаніями у сфері кібербезпеки/інформаційної безпеки. З 2021 року університет бере участь у проекті USAID «Кібербезпека критично важливої інфраструктури України», в рамках якого 10 викладачів кафедри Кібербезпеки та технічного захисту інформації підвищили кваліфікацію на курсах Cybersecurity Summer Training Program (від 90 до 180 годин). До освітнього процесу залучаються роботодавці сфери захисту інформації та професіонали-практики в цій сфері.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення відповідає технологічним вимогам щодо провадження освітньої діяльності для другого (магістерського) рівня вищої освіти відповідно до Ліцензійних умов провадження освітньої діяльності. Реалізація програми забезпечується: - приміщеннями для проведення навчальних занять та контрольних заходів; - мультимедійним обладнанням для одночасного використання в навчальних аудиторіях; - наявністю соціально-побутової інфраструктури, в тому числі бібліотеки з читальним залом та гуртожитків; - комп'ютерними робочими місцями, лабораторіями, обладнанням, устаткуванням, доступом до

	кіберполігонів, доступом до Інтернету та інформаційних ресурсів, , необхідних для навчання, викладацької та наукової діяльності.
Інформаційне та навчально-методичне забезпечення	Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого освітній програмі профілю, в тому числі в електронному вигляді. Наявність безоплатного доступу викладачів і здобувачів вищої освіти до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. Наявність офіційного веб-сайту закладу освіти, на якому розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня / освітньо-наукова / видавнича / атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація). Наявність електронного ресурсу закладу освіти, який містить матеріали, необхідні для навчання, викладацької та наукової діяльності.

9 – Академічна мобільність	
Національна кредитна мобільність	На загальних підставах в межах України. На основі двосторонніх договорів між Державним університетом інтелектуальних технологій і зв'язку та закладами вищої освіти України. Можливість подвійного дипломування.
Міжнародна кредитна мобільність	В рамках програми ЄС Еразмус+ на основі двосторонніх договорів між Державним університетом інтелектуальних технологій і зв'язку та навчальними закладами зарубіжних країн-партнерів. Можливість подвійного дипломування.
Навчання іноземних здобувачів вищої освіти	В окремих академічних групах, при цьому українська мова вивчається як іноземна, або українською мовою при навчанні у спільних академічних групах з україномовними здобувачами ВО українською мовою при навчанні у спільних академічних групах з україномовними здобувачами ВО

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

2.1 Перелік освітніх компонентів освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ECTS	Форма підсумкового контролю
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ (ОК)			
ОК1	Методологія та організація наукових досліджень	4	Залік
ОК2	Педагогіка та психологія	4	Іспит
ОК3	Спеціальні вимірювання в галузі технічного захисту інформації	4	Іспит
ОК4	Управління доступом до інформаційних ресурсів	4	Іспит
ОК5	Менеджмент інформаційної безпеки	4	Іспит
ОК6	Комплексні системи безпеки	5	Залік, КП
ОК7	Кіберфізична безпека об'єктів критичної інфраструктури	4	Іспит
ОК8	Криптологія	4	Іспит
ОК9	Процесний менеджмент в системі корпоративної безпеки	4	Іспит
ОК10	Моніторинг та аудит інформаційно-комунікаційних систем	5	Іспит, КР
ОК 11	Ділова іноземна мова	6	Іспит
ОК12	Практика (виробнича)	10	Залік
ОК13	Кваліфікаційна (магістерська) робота. Атестація	8	Публічний захист
Загальний обсяг обов'язкових компонентів		**66 кредитів 1980 акад.годин**	9 іспитів, 4 заліка
Загальний обсяг вибіркових компонентів *(4 дисципліни по 6 кредитів ЄКТС)*		**24 кредитів 720 акад. год**	4 заліки
Усього		**90 кредитів ЄКТС 2700 акад. годин**	

2.2. Структурно-логічна схема освітньо-професійної програми

Складові програми	Таймінг навчання протягом 1 року 4 місяців (за семестрами)		
	1	2	3
Обов'язкові та вибіркові компоненти теоретичної підготовки	ОК3/4 ОК4/4 ОК6/5 ОК7/4 ОК8/4 ОК9/4 ОК10/5	ОК11/6	ОК1/4 ОК2/4 ОК5/4
		ВК1/6 ВК2/6 ВК3/6 ВК4/6	
Практична підготовка			ОК12/10
Кваліфікаційна (магістерська) робота. Атестація			ОК13/8
Кількість кредитів ЄКТС	**30**	**30**	**30**

3. Форми атестації здобувачів вищої освіти

Атестація здобувачів вищої освіти за освітньо-професійною програмою «Кібербезпека та захист інформації» здійснюється у формі публічного захисту (демонстрації) випускної кваліфікаційної роботи та завершується видачою документу встановленого зразка про присудження ступеня магістр із присвоєнням кваліфікації: магістр з кібербезпеки та захисту інформації.

Виконання кваліфікаційної роботи має за мету систематизувати, закріпити та розширити теоретичні знання та практичні навички зі спеціальності, розвинути творчі здібності та вміння здобувача повною мірою застосувати свої знання для вирішення технічних, проектних і організаційних задач у галузі кібербезпеки та захисту інформації.

Випускна кваліфікаційна робота має продемонструвати здатність випускника виконувати актуальні завдання спеціальності та вміння використовувати надбані компетентності та результати навчання, логічно, на підставі проведених досліджень обґрунтувати проєктні рішення, робити аргументовані висновки та формулювати конкретні пропозиції та рекомендації щодо виконаного завдання.

Кваліфікаційна робота має бути перевірена на академічний плагіат.

Вимоги до змісту, обсягу й структури кваліфікаційної роботи визначаються закладом вищої освіти.

Кваліфікаційна робота має бути оприлюднена на офіційному сайті закладу вищої освіти або його підрозділу, або у репозитарії закладу вищої освіти.

У процесі публічного захисту кандидат на присвоєння магістерського ступеня повинен показати уміння чітко і упевнено викладати зміст проведених досліджень, аргументовано відповідати на запитання та вести дискусію.

Доповідь здобувача вищої освіти повинна супроводжуватися презентаційними матеріалами та пояснювальною запискою, призначеними для загального перегляду.

4. Матриця відповідності компетентностей обов'язковим компонентам освітньої програми

	Загальні компетентності (ЗК)						Спеціальні (фахові) компетентності (СК)															
	1	2	3	4	5		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
ОК1	+	+	+				+																
ОК2	+	+	+		+											+							
ОК3	+	+		+				+	+					+	+				+			+	+
ОК4	+	+		+						+		+							+				
ОК5	+	+		+	+			+		+								+				+	
ОК6	+	+	+				+	+	+								+					+	+
ОК7	+	+	+		+			+	+	+	+			+								+	
ОК8	+	+	+						+					+							+		
ОК9	+		+	+	+						+		+								+		
ОК10	+	+	+	+											+					+			
ОК11	+				+																		
ОК12	+			+	+											+							
ОК13	+	+	+	+	+		+	+	+							+		+	+				

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньо-професійної програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13
ПРН1	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН2	+		+	+	+	+	+	+	+	+		+	+
ПРН3	+		+	+	+	+	+	+	+	+	+		+
ПРН4			+	+	+	+	+	+	+	+			+
ПРН5			+	+	+	+	+	+	+	+			+
ПРН6			+	+		+	+	+	+	+			
ПРН7			+	+	+	+	+	+	+	+			+
ПРН8			+	+		+	+		+	+			+
ПРН9					+		+						
ПРН10				+	+				+				
ПРН11				+	+								
ПРН12				+						+			
ПРН13			+			+	+	+					
ПРН14										+			
ПРН15												+	
ПРН16					+	+			+	+			
ПРН17		+										+	+
ПРН18		+	+										
ПРН19	+				+	+			+				+
ПРН20	+												+
ПРН21			+					+		+			
ПРН22	+					+							+
ПРН23			+	+	+	+	+	+				+	+
ПРН24							+		+				
ПРН25							+						
ПРН26							+						
ПРН27										+			
ПРН28										+			
ПРН29										+			
ПРН30							+			+			
ПРН31			+				+						
ПРН32			+										
ПРН33			+										
ПРН34			+										

6. Характеристика системи внутрішнього забезпечення якості підготовки здобувачів другого (магістерського) рівня вищої освіти

Система внутрішнього забезпечення ЗВО якості вищої освіти складається з таких процедур і заходів, передбачених Законом України «Про вищу освіту»:

1) визначення принципів та процедур забезпечення якості вищої освіти;

2) здійснення моніторингу та періодичного перегляду освітніх програм;

3) щорічне оцінювання здобувачів другого рівня вищої світи, науково-педагогічних працівників ЗВО та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті ЗВО або на інформаційних стендах;

4) забезпечення підвищення кваліфікації науково-педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи здобувачів другого рівня вищої освіти, за освітньою програмою;

6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітні програми, ступені освіти та кваліфікації;

8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників ЗВО і здобувачів другого рівня вищої освіти.

7. Перелік нормативних документів, на яких базується освітня програма

1. Закон України «Про вищу освіту» від 01.07.2014 № 1556-VII.
2. Постанова КМУ від 23.11.2011 р. № 1341 «Про затвердження національної рамки кваліфікацій».
3. Постанова КМУ від 29.04.2015 р. № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти».
4. Класифікація видів економічної діяльності: ДК 009:2010. – На зміну ДК 009:2005; Чинний від 2012-01-01 – (Національний класифікатор України).
5. Класифікатор професій ДК 003:2010. На зміну ДК 003:2005; Чинний від 2010-11-01 – (Національний класифікатор України).
6. Постанова Кабінету Міністрів України від 30 грудня 2015 р. № 1187 «Ліцензійні умови провадження освітньої діяльності закладів освіти».
7. Стандарт вищої освіти України за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, затверджений Наказом МОН України від 18.03.2021 № 332.
8. Професійний стандарт «Фахівець сфери захисту інформації», затверджений наказом Адміністрації Держспецзв'язку № 715 від 25.11.2022.
9. Положення про акредитацію освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти, затверджене Наказом Міністерства освіти і науки України від 11 липня 2019 р. № 977.
10. Положення про організацію освітнього процесу в ДУІТЗ від 13.07.2022.
11. Положення про розроблення та затвердження, моніторинг та перегляд освітніх програм в ДУІТЗ від 13.07.2022.

Гарант освітньої програми Віталій КІЛЬДІШЕВ