ПРОЄКТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

другого рівня вищої освіти

за спеціальністю 125 “Кібербезпека”

галузі знань 12 “Інформаційні технології”

кваліфікація: Магістр з кібербезпеки

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Голова вченої ради

_____ /_____/

(протокол № __ від "___"_____ 20__ р.)

Освітня програма вводиться в дію з _____20__ р.

Ректор_____ /_____/

(наказ № __ від "___"_____ 20__ р.)

Тернопіль 20__ р.

ПРОЄКТ

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

Рівень вищої освіти	Другий (магістерський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Кваліфікація	Магістр з кібербезпеки

РОЗРОБЛЕНО І СХВАЛЕНО ПОГОДЖЕНО

Науково-методичною радою університету
Протокол № _____від «_____» _____ 2018 р.
Голова НМР університету _____ М. М. Митник

Проректор з науково- педагогічної - роботи Тернопільського національного технічного університету імені Івана Пулюя _____С.Ф. Дячук
«____»_____2018 р.

Начальник навчального відділу І.Г.Ткаченко
«____»_____2018 р.

ПРОЄКТ

ПЕРЕДМОВА

РОЗРОБЛЕНО
Робочою групою спеціальності 125 “Кібербезпека” Тернопільського національного технічного університету імені Івана Пулюя у складі:

Керівник робочої групи, гарант освітньо-професійної програми: Загородна Наталія Володимирівна	к.т.н., доцент кафедри кібербезпеки
Члени:	
Карпінський Микола Петрович	д.т.н, професор кафедри кібербезпеки
Козак Руслан Орестович	к.т.н., доцент кафедри кібербезпеки.

Проект освітньо-професійної програми обговорений та схвалений на засіданні Вченої ради факультету компютерно-інформаційних систем і програмної інженерії

Протокол № _____ від «____» _____ 2018 р.
Голова Вченої ради ФІС _____ І. О. Баран

Проект освітньо-професійної програми обговорений та схвалений на засіданні науково-методичної комісії факультету комп’ютерно-інформаційних систем і програмної інженерії
Протокол № _____від «_____» _____ 2017 р.
Голова НМК ФІС Осухівська Г.М.

ПРОЄКТ

1. Профіль програми магістра зі спеціальності 125 «Кібербезпека»

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Тернопільський національний технічний університет імені Івана Пулюя.
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр з кібербезпеки.
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці
Наявність акредитації	Акредитаційна комісія України (Національне агентство з забезпечення якості вищої освіти). 2016-2021 рр.
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, QF-LLL – 7 рівень
Передумови	Особа має право здобувати ступінь бакалавра за умови наявності в неї повної загальної середньої освіти або ступеня молодшого спеціаліста.
Мова(и) викладання	Українська
Термін дії освітньої програми	2017-2021
Інтернет-адреса постійного розміщення опису освітньої програми	http://cyber.te.ua/wp-content/uploads/2018/06/Osv_progr_mag.pdf
2 – Мета освітньої програми	
Забезпечити студентам фундаментальну підготовку у вигляді поглиблених теоретичних і практичних знань, умінь та навичок за спеціальністю 125 Кібербезпека, достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузях телекомунікацій та інформаційних технологій, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу	
3 - Характеристика освітньої програми	
Предметна область	Галузь знань – 12 «Інформаційні технології». Спеціальність – 125 «Кібербезпека» Об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту.
Орієнтація освітньої програми	Освітньо-професійна програма з прикладною спрямованістю за спеціалізацією безпека інформаційних і комунікаційних систем.
Основний фокус освітньої програми та спеціалізації	Акцент на здатності організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізації, економічної доцільності, можливих

	зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації.
Особливості програми	Інтегрована підготовка фахівців до вирішення завдань у сфері інформаційної безпеки, що передбачає розроблення, впровадження та експлуатацію комплексних (інформаційних, телекомунікаційних, технічних) систем захисту інформації на об'єктах інформаційної діяльності, поглиблене вивчення нормативних документів та стандартів з захисту інформації, принципів побудови систем технічного захисту інформації, підходів до управління ризиками, дій для захисту інформаційних ресурсів організацій і користувачів
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець може займати первинні посади (за ДК 003:2010): 3439 (24771). Фахівець із організації інформаційної безпеки. International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT). Можливість отримати міжнародні сертифікати в галузі інформаційної безпеки.
Подальше навчання	Можливість здобуття освіти на третьому (освітньо-науковому) рівні вищої освіти за спеціальністю 125 «Кібербезпека» або іншими спорідненими (суміжними) спеціальностями галузі знань «Інформаційні технології», що узгоджуються з отриманим дипломом магістра, іншими міждисциплінарними магістерськими програми з IT компонентою. Можливість підвищення кваліфікації та отримання додаткової післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, електронне навчання в системі ATutor, самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді: лекції, мультимедійної лекції, інтерактивної лекції, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, консультації з викладачами, підготовка дипломної роботи магістра .
Оцінювання	Оцінювання навчальних досягнень здійснюється за 100-бальною (рейтинговою) шкалою ЕКТС (ECTS), національною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно») і вербальною («зараховано», «незараховано») системами. Види контролю: поточний, тематичний, періодичний, підсумковий. Форми контролю: усне та письмове опитування, тестові завдання, лабораторні звіти, презентації, захист курсових робіт та проектів, звітів з практик. Атестація – захист дипломної роботи магістра.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

Загальні компетентності (ЗК)	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області та розуміння професії. ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.
Фахові компетентності спеціальності (ФК)	ФК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК 4. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. ФК 5. Здатність забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) ФК 6. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку ФК 7. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. ФК 8. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем. ФК 9. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам.
7 – Програмні результати навчання	
	ПРН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН2. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН3. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності,які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН4. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

	ПРН5. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН6. Виконувати аналіз та декомпозицію ІТС. ПРН7. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. ПРН8. Розробляти моделі загроз та порушника. ПРН9. Вирішувати завдання захисту програм та інформації, що обробляється в ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень. ПРН10. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН11. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС. ПРН12. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в ІТС згідно встановленої політики інформаційної і\або кібербезпеки. ПРН13. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). ПРН14. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. ПРН15. Застосовувати теорії та методи захисту для забезпечення безпеки елементів ІТС. ПРН16. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. ПРН17. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ПРН18. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН19. вирішувати задачі забезпечення неперервності бізнес процесів організації на основі встановленої системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів. ПРН20. Вирішувати задачі захисту інформації, що обробляється в ІТС з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН21. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в ІТС. ПРН22. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в ІТС. ПРН23. Забезпечувати конфігурування та роботоспроможність систем виявлення вторгнень в ІТС.

	ПРН24. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. ПР25. Вирішувати задачі аналізу програмного коду на наявність можливих вразливостей.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Проектна група: 1 доктор наук, професор, 2 кандидати наук, доценти. *Гарант освітньої програми (керівник робочої групи):* Загородна Наталія Володимирівна – вчене звання: доцент за кафедрою комп'ютерних наук (галузь 12 «Інформаційні технології»), 2011 р.; к.т.н., 01.05.02 - Математичне моделювання та обчислювальні методи (галузь: 12 «Інформаційні технології»), з 2007 р.; стаж педагогічної роботи у вищих закладах освіти III-IV рівня акредитації 11 років. Пройшла підвищення кваліфікації в навчальному центрі перепідготовки фахівців в галузі інформаційної безпеки при ФТІ НТУУ «КПІ» за напрямом «Захист інформації. Криптосистеми та засоби криптографічного захисту». Міжнародні стажування: липень 2012 р. – в Національному дослідницькому інституті Франції в галузі інформатики та автоматики. В січні 2017 р. отримала грант за програмою «Erasmus+» для викладання лекцій в тому числі в галузі кібербезпеки в Технічному університеті Ополє (Польща). Виконання міжнародних проектів: «Модернізація магістерських та аспірантських навчальних програм в галузі інформаційної безпеки та стійкості людино-орієнтованих та промислових систем» («Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains» / (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR). *Член робочої групи:* Карпінський М.П. – д.т.н. з 1995 року, вчене звання професора присвоєно у 2001 році за кафедрою безпеки інформаційних технологій. Стаж роботи у вищих закладах освіти III-IV рівнів акредитації 24 роки. Має більше 200 публікацій, з них більше 20 праць стосуються захисту інформації. Опубліковано більше 25 праць, що індексуються в наукометричних базах Scopus; Web of Science. Підготував 7 кандидатів наук та 2 докторів наук. Член редколегій таких фахових наукових журналів: Безпека інформації, ISSN 2225-5036; Захист інформації, ISSN 2221-5212; Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, ISSN 2074-9481. Член спецради Д35.052.18 за спеціальністю 05.13.21 «Системи захисту інформації» у Національному університеті "Львівська політехніка". *Член робочої групи:* Козак Руслан Орестович – вчене звання доцент за кафедрою комп'ютерних наук (галузь 12 «Інформаційні технології»), 2014 р.; к.т.н., 05.13.06 – Автоматизовані системи управління та прогресивні інформаційні технології (галузь: 12 «Інформаційні технології»), з 2007 р. Друга вища освіта: спеціальність "Безпека

	інформаційних та комунікаційних систем" (відповідає спеціальності 125 «Кібербезпека»), Харківський національний університет радіоелектроніки, 2013 р. У 2014 році підвищення кваліфікації в навчальному центрі перепідготовки фахівців в галузі інформаційної безпеки при ФТІ НТУУ «КПІ» за напрямом «Захист інформації на об'єктах інформаційної діяльності. Виявлення закладних пристроїв». Стаж педагогічної роботи у вищих закладах освіти III-IV рівня акредитації 9 років. Виконання міжнародних проектів: «Модернізація магістерських та аспірантських навчальних програм в галузі інформаційної безпеки та стійкості людино-орієнтованих та промислових систем» («Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains» / (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR).
Матеріально-технічне забезпечення	Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає потребі. В університеті діють власні об'єкти соціально-побутової інфраструктури. У тому числі: їдальня, буфети, три гуртожитки, актові зали, студентський палац, спортивні зали, стадіон, спортивні майданчики, медичний пункт, база відпочинку, басейн. Заняття та наукові дослідження проводяться у лабораторіях кафедри кібербезпеки, кафедри комп'ютерних наук, спеціалізованій комп'ютерній лабораторії технічного захисту інформації. Для проведення інформаційного пошуку та обробки результатів є комп'ютерні класи, де наявне спеціалізоване програмне забезпечення та відкритий доступ до Інтернет-мережі.
Інформаційне та навчально-методичне забезпечення	Науково-технічна бібліотека ТНТУ щороку поповнюється спеціалізованою літературою і періодичними виданнями, що відповідають напрямкам роботи кафедри. Бібліотека університету першою серед українських вузівських бібліотек у 2011 році стала членом Міжнародної асоціації науково-техічних бібліотек університетів (IATUL). Також бібліотека є колективним членом Української бібліотечної асоціації. Інституційний репозитарій ELARTU активно продовжує наповнення фо-ндів. На початок 2016 року у репозитарії опубліковано понад 18 855 матеріалів. Згідно рейтингу Webometrics (http://www.webometrics.info/) станом на сі-чень 2017 року інституційний репозитарій ELARTU займає 10 місце серед українських репозитаріїв. Підвищенню рейтингу університету сприяє наявність наповненого та добре структурованого інституційного репозитарію. Навчальний процес базується на 100% навчально-методичному забезпеченні семінарських, практичних, лабораторних занять і самостійної роботи студентів з усіх навчальних дисциплін. Використовуються технології електронного (дистанційного) навчання на базі програмного продукту ATutor (Університет Торонто, Канада). Діє Інститут дистанційного навчання, на який покладено функції розроблення, запровадження та координації

	зусиль із провадження інформаційних технологій в освітній процес.
9 – Академічна мобільність	
Національна кредитна мобільність	Індивідуальна академічна мобільність реалізується у рамках міжуніверситетських договорів про встановлення науково-освітянських відносин для задоволення потреб розвитку освіти і науки з університетами України. До керівництва науковою роботою здобувачів залучаються провідні фахівці університетів України на умовах індивідуальних договорів. Допускається перезарахування кредитів, отриманих у інших університетах України, за умови відповідності їх набутих компетентностей.
Міжнародна кредитна мобільність	Реалізація спільних програм академічної мобільності, зокрема програм подвійних дипломів, є одним з пріоритетних напрямків розвитку міжнародного співробітництва університету. Усі студенти ТНТУ мають можливість брати участь у програмах академічної мобільності, що імплементуються у співпраці з ВНЗ Польщі, Німеччині, Іспанії, Великобританії, Франції та США. Студенти факультету комп'ютерно-інформаційних систем і програмної інженерії мають можливість приймати участь в програмі подвійних дипломів за освітнім рівнем "магістр" з державним університетом «Люблінська Політехніка» (Польща) та з Міжнародною вищою школою комп'ютерних наук та інформаційних технологій (м. Сержі, Франція). Студенти також реалізують своє право на міжнародну кредитну мобільність в рамках програми "Erasmus+". Зокрема студенти факультету скористались перевагами та можливостями програми для навчання в Опольській політехніці (Польща), університеті Валенсії (Іспанія). Заплановано підписання договорів про академічну мобільність з Університетом прикладних наук, Шмалькальден та технічним університетом Кошице (Словаччина) та іншими Європейськими партнерами. В ТНТУ виконується 5 освітніх і 3 наукових міжнародних проекти: «Рівні можливості для здобуття професії молодими матерями-студентками у вищих навчальних закладах»; «Міжуніверситетські стартап центри для розвитку та підтримки студентських інновацій» (SUCSID); «Модернізація післядипломної освіти з безпеки та стійкості до зовнішніх впливів у сферах людської та індустріальної діяльності (SEREIN)»; «Розробка та впровадження міжнародної системи дистанційного навчання» (ініціатива ООН «Сталий розвиток вищої освіти», програма «Академічний вплив ООН»); «Розвиток освітніх, наукових і культурних зв'язків на основі спільного українсько-таджицької факультету» (ініціатива ООН «Сталий розвиток вищої освіти», програма «Академічний вплив ООН»); «Властивості зони термічного впливу зварних з'єднань сучасних сталей стійких до повзучості». У серпні 2015 року університет за результатами другого конкурсу програми Еразмус+ став учасником чотирьох проектів Європейського Союзу, а саме: за напрямом КА1: «Навчальна мобільність» університет увійшов у консорціуми двох Еразмус проектів від Люблінської політехніки та від Опольської політехніки відповідно; за напрямом КА2

	«Розвиток потенціалу вищої освіти» університет увійшов в консорціум проекту «Розвиток інфраструктури мережі для підтримки молодіжного інноваційного підприємництва на базі платформи FABLAB»; за напрямом «Жан Моне» в університеті виграно грант для створення навчального модуля «Екологічно відповідальний бізнес: дослідження та імплементація європейського досвіду».
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти проводиться на загальних умовах (з додатковою мовною підготовкою).

ПРОЄКТ

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

2.1. 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			
ОК 1.	Іноземна мова фахового спрямування 10	4	з
ОК 2.	Інтелектуальна власність 9	4	з
ОК 3.	Педагогіка та етика професійної діяльності 9	4	з
Цикл професійної підготовки			
ОК 4.	Теорія розподілених інформаційних ресурсів, захист баз даних і знань +КП 10	5	е
ОК 5.	Технології створення та застосування систем захисту інформаційно-комунікаційних систем + КП 9	5	е
Практична підготовка			
ОК 6.	Науково-дослідницька 10	9	дз
ОК 7.	Переддипломна 10	7,5	дз
ОК 8.	Науково-педагогічна 11	6	дз
ОК 9.	Дипломна робота 11	19,5	вдр
Загальний обсяг обов'язкових компонент:		**64**	
Вибіркові компоненти			
Цикл загальної підготовки			
ВБ 1.1.	Методи та системи підтримки прийняття рішень 9	3	е
ВБ 1.2.	Методологія та організація наукових досліджень 10	3	з
Цикл професійної підготовки			
ВБ 2.1.	Комп'ютерна криміналістика 9	4	е
ВБ 2.2.	Методи побудови і аналізу криптосистем 10	4	е
ВБ 2.3.	Моніторинг і аудит інформаційно-комунікаційних систем 10	4	е

ВБ 2.4.	Оптимізаційні методи та моделі 9	4	е
ВБ 2.5.	Технології розробки захищеного програмного забезпечення + КР 10	4	е
Загальний обсяг вибіркових компонент:		**26**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**90**	

2.2. Структурно-логічна схема ОП

9 семестр	Інтелектуальна власність	Педагогіка та етика професійної діяльності	Технології створення та застосування систем захисту інформаційно-комунікаційних систем + КП		Методи та системи підтримки прийняття рішень	Комп'ютерна криміналістика		Оптимізаційні методи та моделі
10 семестр	Науково-дослідницька практика	Іноземна мова фахового спрямування	Теорія розподілених інформаційних ресурсів, захист баз даних і знань +КП	Методологія та організація наукових досліджень	Методи побудови і аналізу криптосистем	Моніторинг і аудит інформаційно-комунікаційних	Технології розробки захищеного програмного забезпечення + КР	Переддипломна практика
11 семестр	Науково-педагогічна практика			Дипломна робота				

3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності 125 «Кібербезпека» проводиться у формі захисту кваліфікаційної магістерської роботи та завершується видачею документу встановленого зразка про присудження йому ступеня магістра із присвоєнням кваліфікації: Магістр з кібербезпеки.

До атестації допускаються студенти, які виконали всі вимоги програми підготовки (навчального плану). Термін проведення атестації визначається навчальним планом та графіком освітнього процесу.

Кваліфікаційна робота має передбачати розв’язання складної спеціалізованої задачі або практичні проблеми в галузі інформаційної та кібернетичної безпеки на основі досліджень та/або здійснення інновацій за наявності невизначених умов і вимог. Реферат кваліфікаційної роботи має бути розміщено на сайті вищого навчального закладу. Випускна кваліфікаційна робота має бути перевірена на плагіат

Атестація здійснюється відкрито і публічно.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ВБ1.1	ВБ1.2	ВБ2.1	ВБ2.2	ВБ2.3	ВБ2.4	ВБ2.5
ЗК1		+		+	+	+	+	+	+			+	+			+
ЗК2				+	+	+	+	+	+				+	+	+	+
ЗК3	+		+						+							
ЗК4						+	+	+	+				+			
ЗК5						+	+	+	+							
ФК1		+							+							
ФК2				+	+				+						+	
ФК3				+	+				+			+				+
ФК4									+							+
ФК5									+				+	+		
ФК6									+			+		+		+
ФК7									+			+	+			
ФК8									+					+		
ФК9									+				+	+	+	

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

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ВБ1.1	ВБ1.2	ВБ2.1	ВБ2.2	ВБ2.3	ВБ2.4	ВБ2.5
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						+	+	+	+							+