ПРОЄКТ

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

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 «Кібербезпека»

галузі знань 12 «Інформаційні технології»

кваліфікація: бакалавр 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

ПЕРЕДМОВА

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

Керівник робочої групи, гарант освітньо-професійної програми:	
Кареліна Олена Володимирівна	к.пед.н., доцент кафедри кібербезпеки
Члени:	
Загородна Наталія Володимирівна	к.т.н, завідувачка кафедри кібербезпеки
Томашевський Богдан Паїсійович	к.т.н., доцент кафедри кібербезпеки.
Бабій Віктор Васильович	Член Експертної ради роботодавців кафедри кібербезпеки та кафедри комп’ютерних систем та мереж, начальник 1 відділу Управління Держспецзв'язку в Тернопільській області
Сміх Олена	Студентка групи СБ-31

Рецензії-відгуки зовнішніх стейкхолдерів:

1. Профіль освітньої програми 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	Бакалавр з кібербезпеки. Фахівець з організації інформаційної безпеки.
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний. Обсяг: - на базі повної загальної середньої освіти з терміном навчання 11 років становить 240 кредитів ЄКТС, - на базі молодшого бакалавра становить 120 кредитів ЄКТС.
Наявність акредитації	Акредитаційна комісія України (Національне агентство з забезпечення якості вищої освіти). 2016-2021 р р.
Цикл/рівень	НРК України – 6, FQ-EHEA – перший цикл, EQF LLL – 6 рівень, 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	
Інтернет-адреса постійного розміщення опису освітньої програми	http://cyber.te.ua/wp-content/uploads/2018/06/Osv_progr.pdf
2 – Мета освітньої програми	
Забезпечити підготовку висококваліфікованих фахівців в галузі інформаційних технологій зі спеціальності 125 «Кібербезпека», здатних вирішувати складні спеціалізовані задачі та практичні проблеми інформаційної безпеки, 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».
Орієнтація освітньої програми	Освітньо-професійна, прикладна орієнтація.
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.
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 продовжити навчання на другому (магістерському) рівні вищої освіти. НРК України – 7, FQ-EHEA – 2 цикл, EQF LLL – 7 рівень, рівень.
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 кваліфікаційної роботи бакалавра (проекту).
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 – кваліфікаційний іспит (екзамен з фаху).
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 неперервність бізнесу згідно встановленої політики безпеки. ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. ФК 7. Здатність забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою. ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем. ФК 12. 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. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблему професійній діяльності, оцінювати їхню ефективність. ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН4. 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.

	ПРН5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ПРН7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. ПРН9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПРН10. Виконувати аналіз та декомпозицію ІТС. ПРН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. ПРН12. Розробляти моделі загроз та порушника. ПРН13. Аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних. ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень. ПРН15. Реалізовувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативно-правових документів. ПРН16. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. ПРН17. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН18. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в ІТС. ПРН19. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС. ПРН20. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН21. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в ІТС згідно встановленої політики інформаційної і\або кібербезпеки. ПРН22. Здійснювати протидію отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН23. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). ПРН24. Забезпечувати введення підзвітності системи управління

	доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту. ПРН25. Забезпечувати процеси захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем. ПРН26. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. ПРН27. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; ПРН28. Виконувати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в ІТС та ефективності використання КЗЗ в умовах реалізації загроз різних класів. ПРН29. Здійснювати оцінювання можливості несанкціонованого доступу до елементів ІТС. ПРН30. Застосовувати теорії та методи захисту для забезпечення безпеки елементів ІТС. ПРН31. Вирішувати задачі управління процесами відновлення штатного функціонування ІТС з використанням процедур резервування згідно встановленої політики безпеки. ПРН32. Вирішувати задачі забезпечення неперервності бізнес процесів організації. ПРН33. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. ПРН34. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН35. Виявляти небезпечні сигнали технічних засобів. ПРН36. Вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН37. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН38. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ПРН39. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. ПРН40. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

	ПРН41. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН42. вирішувати задачі забезпечення неперервності бізнес процесів організації на основі встановленої системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів. ПРН43. Застосовувати політики, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. ПРН44. Здійснювати аналіз ризиків обробки інформації в ІТС. ПРН45. Вирішувати задачі захисту інформації, що обробляється в ІТС з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН46. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в ІТС. ПРН47. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в ІТС. ПРН48. Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). ПРН49. Забезпечувати конфігурування та роботоспроможність систем виявлення вторгнень в ІТС. ПРН50. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. ПРН51. 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):* 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:* 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:* 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/) ста-

	ном 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), навчатись за українсько-німецькою програмою подвійних дипломів освітнього рівня "бакалавр" в Університеті прикладних наук Шмалькальдену (Німеччина). Студенти також реалізують своє право на міжнародну кредитну мобільність в рамках програми "Erasmus+". Зокрема студенти факультету скористались перевагами та можливостями програи 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).

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

2.1. Перелік компонент ОП

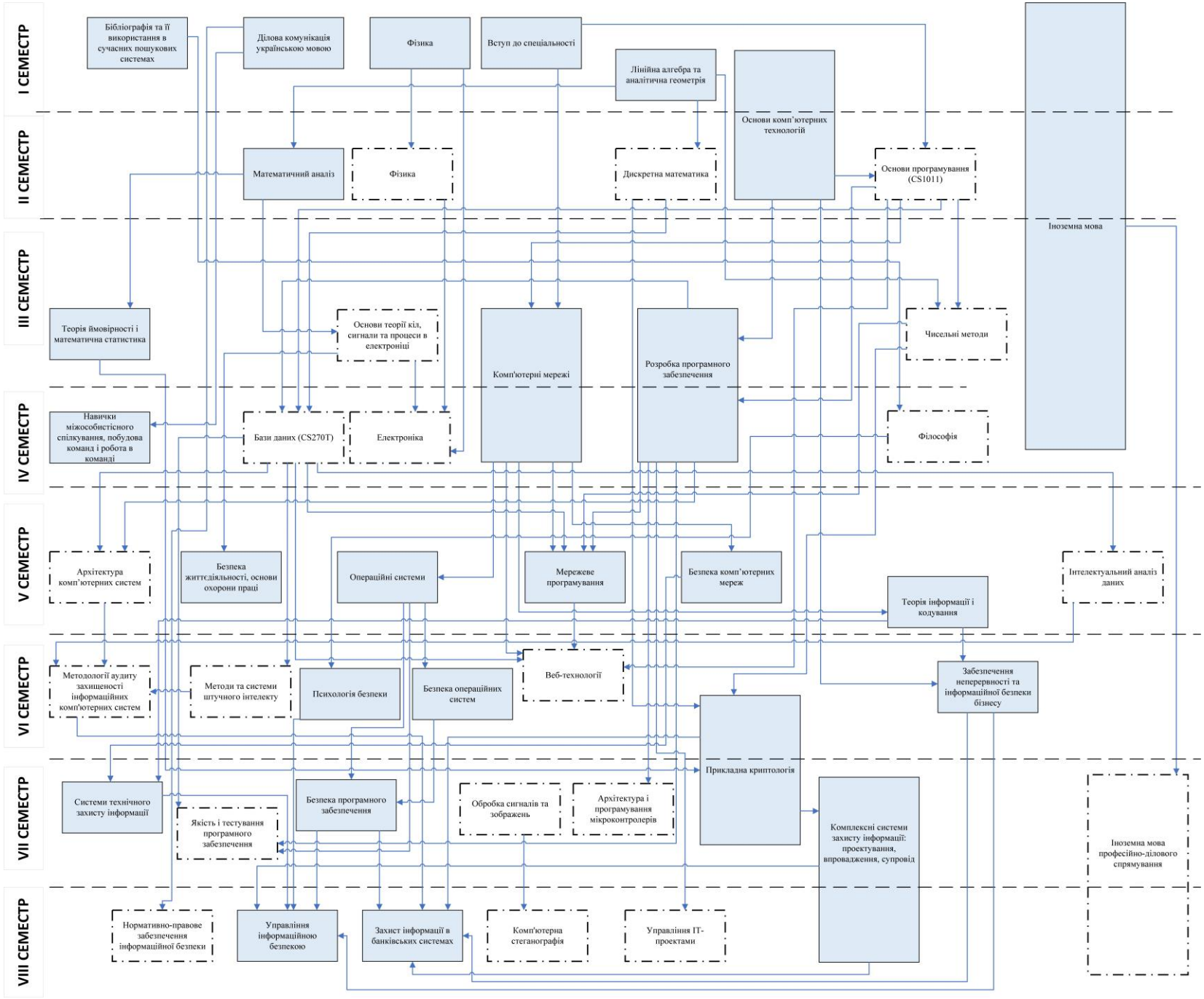
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК 1.	Безпека життєдіяльності, основи охорони праці	4	е
ОК 2.	Бібліографія та її використання в сучасних пошукових системах	3	з
ОК 3.	Вступ до спеціальності	3	е
ОК 4.	Ділова комунікація українською мовою	3	з
ОК 5.	Іноземна мова	29	е
ОК 6.	Лінійна алгебра та аналітична геометрія	4	з
ОК 7.	Математичний аналіз	6	з
ОК 8.	Навички міжособистісного спілкування, побудова команд і робота в команді	3	з
ОК 9.	Теорія ймовірності і математична статистика	4	е
ОК 10.	Фізика	4	е
ОК 11.	Забезпечення неперервності та інформаційної безпеки бізнесу	4	е
ОК 12.	Безпека комп'ютерних мереж	4	е
ОК 13.	Безпека операційних систем	5	е
ОК 14.	Безпека програмного забезпечення	4	е

ОК 15.	Захист інформації в банківських системах	4,0	е
ОК 16.	Комплексні системи захисту інформації: проектування, впровадження, супровід	7,5	е
ОК 17.	Комп'ютерні мережі	10	е
ОК 18.	Операційні системи	4,0	з
ОК 19.	Основи комп’ютерних технологій	9,0	е
ОК 20.	Мережеве програмування	4,0	е
ОК 21.	Прикладна криптологія	8,5	е
ОК 22.	Психологія безпеки	4,0	з
ОК 23.	Розробка програмного забезпечення	10,0	е
ОК 24.	Системи технічного захисту інформації	4,0	е
ОК 25.	Теорія інформації та кодування	4,0	е
ОК 26.	Управління інформаційною безпекою	4,0	е
ОК 27.	Проектно-технологічна практика	3,0	диф.з.
ОК 28.	Стажування з фаху	7,5	диф.з.
Загальний обсяг обов'язкових компонент:		163,5	
Вибіркові компоненти ОП			
Вибірковий блок 1			
ВБ 1.1.	Фізика	5,0	е
ВБ 1.2.	Філософія	3,0	з
ВБ 1.3.	Архітектура і програмування мікроконтролерів	3,0	з
ВБ 1.4.	Архітектура комп'ютерних систем	3,0	з
ВБ 1.5.	Бази даних (CS270T)	4,0	е
ВБ 1.6.	Веб-технології	5,0	з
ВБ 1.7.	Дискретна математика	5,0	е
ВБ 1.8.	Електроніка	4,0	з
ВБ 1.9.	Іноземна мова професійно-ділового спрямування	3,5	е
ВБ 1.10.	Інтелектуальний аналіз даних	4,0	з
ВБ 1.11.	Комп'ютерна стеганографія	3,0	з
ВБ 1.12.	Методи та системи штучного інтелекту	4,0	е
ВБ 1.13.	Методології аудиту захищеності інформаційних комп'-ютерних систем	3,0	з
ВБ 1.14.	Нормативно-правове забезпечення інформаційної безпе-ки	3,5	з

ВБ 1.15.	Обробка сигналів та зображень	3,0	з
ВБ 1.16.	Основи програмування (CS1011)	4,0	з
ВБ 1.17.	Основи теорії кіл, сигнали та процеси в електроніці	4,0	з
ВБ 1.18.	Управління ІТ-проектами	4,0	з
ВБ 1.19.	Чисельні методи	3,0	з
ВБ 1.20.	Якість і тестування програмного забезпечення	4,0	з
Вибірковий блок 2			
ВБ 2.1.	Вибрані розділи фізики	5,0	е
ВБ 2.2.	Соціологія	3,0	з
ВБ 2.3.	Цифрова схемотехніка та мікропроцесорні системи	3,0	з
ВБ 2.4.	Архітектура комп'ютера	3,0	з
ВБ 2.5.	Основи теорії реляційних та інших баз даних	4,0	е
ВБ 2.6.	Методи та засоби розробки веб-систем	5,0	з
ВБ 2.7.	Комп’ютерна дискретна математика	5,0	е
ВБ 2.8.	Електротехніка та електроніка	4,0	з
ВБ 2.9.	Іноземна мова професійно-ділового спрямування	3,5	е
ВБ 2.10.	Машинне навчання	4,0	з
ВБ 2.11.	Стеганографічні методи приховування інформації	3,0	з
ВБ 2.12.	Основи штучного інтелекту	4,0	е
ВБ 2.13.	Оцінка та аналіз захищеності комп'ютерних систем	3,0	з
ВБ 2.14.	Нормативно-правові акти в сфері кібербезпеки	3,5	з
ВБ 2.15.	Цифрова обробка сигналів в інформаційних системах	3,0	з
ВБ 2.16.	Алгоритмізація і програмування	4,0	з
ВБ 2.17.	Теорія кіл, сигналів і процесів в інформаційному та кіберпросторах	4,0	з
ВБ 2.18.	Методи управління проектами в ІТ-галузі	4,0	з
ВБ 2.19.	Чисельні методи та моделювання ЕОМ	3,0	з
ВБ 2.20.	Забезпечення та контроль якості програмних продуктів	4,0	з
Загальний обсяг вибіркових компонент:		75	
Екзамен з фаху		1,5	
Загальний обсяг освітньої програми		240	

2.2. Структурно-логічна схема ОП

ПРОЄКТ


I СЕМЕСТР
II СЕМЕСТР
III СЕМЕСТР
IV СЕМЕСТР
V СЕМЕСТР
VI СЕМЕСТР
VII СЕМЕСТР
VIII СЕМЕСТР
Бібліографія та її використання в сучасних пошукових системах
Ділова комунікація українською мовою
Фізика
Вступ до спеціальності
Лінійна алгебра та аналітична геометрія
Основи комп'ютерних технологій
Іноземна мова
Математичний аналіз
Фізика
Дискретна математика
Основи програмування (CS1011)
Теорія ймовірності і математична статистика
Основи теорії кіл, сигнали та процеси в електроніці
Комп'ютерні мережі
Розробка програмного забезпечення
Чисельні методи
Навички міжособистісного спілкування, побудова команд і робота в команді
Бази даних (CS270T)
Електроніка
Філософія
Архітектура комп'ютерних систем
Безпека життєдіяльності, основи охорони праці
Операційні системи
Мережеве програмування
Безпека комп'ютерних мереж
Інтелектуальний аналіз даних
Теорія інформації і кодування
Методології аудиту захищеності інформаційних комп'ютерних систем
Методи та системи штучного інтелекту
Психологія безпеки
Безпека операційних систем
Веб-технології
Забезпечення неперервності та інформаційної безпеки бізнесу
Системи технічного захисту інформації
Якість і тестування програмного забезпечення
Безпека програмного забезпечення
Обробка сигналів та зображень
Архітектура і програмування мікроконтролерів
Прикладна криптологія
Комплексні системи захисту інформації: проектування, впровадження, супровід
Іноземна мова професійно-ділового спрямування
Нормативно-правове забезпечення інформаційної безпеки
Управління інформаційною безпекою
Захист інформації в банківських системах
Комп'ютерна стеганографія
Управління IT-проектами

ПРОЄКТ

3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності 125 «Кібербезпека» проводиться у формі кваліфікаційного іспиту (екзамену з фаху) та завершується видачею документу встановленого зразка про присудження йому ступеня бакалавра з кібербезпеки із присвоєнням кваліфікації: 3439 – фахівець з організації інформаційної безпеки.

Кваліфікаційний іспит передбачає оцінювання обов'язкових результатів навчання, визначених стандартом вищої освіти за спеціальністю 125 «Кібербезпека» та цією освітньою програмою.

Атестація здійснюється відкрито і публічно.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

4.1. Обов'язкові компоненти освітньої програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28
ЗК1	+	+						+			+					+										+	+	+
ЗК2			+								+																	
ЗК3				+	+			+																				
ЗК4						+	+		+	+												+						
ЗК5		+																										
ФК1																+												
ФК2																	+	+	+	+			+		+			
ФК3																												
ФК4											+															+		
ФК5			+									+	+	+	+									+				
ФК6																												
ФК7																+								+				
ФК8											+				+	+								+		+		
ФК9																+										+	+	+
ФК10																					+							
ФК11																	+								+			
ФК12												+	+	+	+	+								+		+		

4.2. Вибіркові компоненти освітньої програми

	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6	ВК7	ВК8	ВК9	ВК10	ВК11	ВК12	ВК13	ВК14	ВК15	ВК16	ВК17	ВК18	ВК19	ВК20
ЗК1																				
ЗК2																				
ЗК3									+											
ЗК4	+	+																		
ЗК5																				
ФК1														+						
ФК2			+	+	+	+														
ФК3										+		+				+			+	+
ФК4																				
ФК5																				
ФК6			+					+							+		+	+		
ФК7																				
ФК8																		+		
ФК9																				
ФК10							+				+									
ФК11													+							
ФК12																				

ПРОЄКТ

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

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6	ВК7	ВК8	ВК9	ВК10	ВК11	ВК12	ВК13	ВК14	ВК15	ВК16	ВК17	ВК18	ВК19	ВК20
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																								+			+	+																				

ПРОЄКТ

ПРН31												+	+	+										+		+															+					+		
ПРН32											+																																					
ПРН33																+																																
ПРН34																+																																
ПРН35																								+	+				+			+				+							+		+			
ПРН36																								+	+				+			+				+							+		+			
ПРН37																+								+		+																+						
ПРН38																+								+		+																+						
ПРН39											+					+																																
ПРН40											+																+	+														+						
ПРН41																+											+	+														+						
ПРН42											+																																					
ПРН43											+															+																						
ПРН44											+															+																						
ПРН45																					+														+				+								+	
ПРН46												+									+																		+									
ПРН47												+					+																								+							
ПРН48												+	+	+	+	+	+							+		+																						
ПРН49												+	+													+															+							
ПРН50																	+														+																	
ПРН51														+						+			+										+	+				+		+				+		+		+