

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

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

першого рівня вищої освіти

за спеціальністю 125 «Кібербезпека»

галузі знань 12 «Інформаційні технології»

кваліфікація: 3439- фахівець з організації інформаційної безпеки



ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Голова вченої ради

Геній Т.В.

(протокол № 4 від "16" квітня 2019р.)

Освітня програма вводиться в дію з "01" вересня 2019р.

Ректор Геній Т.В.

(наказ № 4/7-381 від "23" квітня 2019 р.)

Тернопіль 2019 р.

ЛИСТ ПОГОДЖЕННЯ
Освітньо-професійної програми
«Кібербезпека»

Рівень вищої освіти: Перший
Спеціальність: 125 «Кібербезпека»
Галузь знань: 12 «Інформаційні технології»

СХВАЛЕНО:

Науково-методичною радою Тернопільського національного технічного
університету імені Івана Пулюя

Протокол № ____ від « ____ » _____ 201_ р.

Голова НМР університету



М.М. Митник

ПОГОДЖЕНО:

Проректор з науково-педагогічної роботи ТНТУ:

« 04 » квітня 2019 р.



С.Ф. Дячук

Начальник навчального відділу ТНТУ:

« 04 » квітня 2019 р.



І.Г. Ткаченко

ПЕРЕДМОВА

Розроблено робочою групою у складі:

1. Карпінський Микола Петрович – гарант освітньої програми, керівник робочої групи, д.т.н, професор кафедри кібербезпеки;
2. Загородна Наталія Володимирівна – член робочої групи, к.т.н., доцент кафедри кібербезпеки.
3. Козак Руслан Орестович – член робочої групи, к.т.н., доцент кафедри кібербезпеки.
4. Кареліна Олена Володимирівна - член робочої групи, к.пед.н., доцент кафедри кібербезпеки.

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.
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	2019-2021
Інтернет-адреса постійного розміщення опису освітньої програми	http://tntu.edu.ua/storage/pages/00000120/op125b.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 організувати 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.
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.

<p>Загальні компетентності (ЗК)</p>	<p>ЗК 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>ЗК 2. Знання та розуміння предметної області та розуміння професії.</p> <p>ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.</p> <p>ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.</p> <p>ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p> <p>ЗК 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.</p>
<p>Фахові компетентності спеціальності (ФК)</p>	<p>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.</p> <p>ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.</p> <p>ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.</p> <p>ФК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).</p> <p>ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p> <p>ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>ФК 11. Здатність виконувати моніторинг процесів</p>

	<p>функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.</p>
7 – Програмні результати навчання	
	<p>ПРН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.</p> <p>ПРН2. Організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.</p> <p>ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.</p> <p>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.</p> <p>ПРН5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.</p> <p>ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.</p> <p>ПРН7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.</p> <p>ПРН8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.</p> <p>ПРН9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.</p> <p>ПРН10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.</p> <p>ПРН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.</p> <p>ПРН12. Розробляти моделі загроз та порушника.</p> <p>ПРН13. Аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних.</p> <p>ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в ІТС програмно-апаратними засобами та давати оцінку резильтативності, якості прийнятих рішень.</p> <p>ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.</p> <p>ПРН16. Реалізовувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативно-правових документів.</p> <p>ПРН17. Забезпечувати процеси захисту та функціонування</p>

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.

ПРН18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в ІТС.

ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС.

ПРН21. 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.

ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в ІТС згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

ПРН25. 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.

ПРН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

ПРН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;

ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в ІТС та ефективності використання КЗЗ в умовах реалізації загроз різних класів.

ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів ІТС.

ПРН31. Застосовувати теорії та методи захисту для забезпечення

безпеки елементів ІТС.

ПРН32. Вирішувати задачі управління процесами відновлення штатного функціонування ІТС з використанням процедур резервування згідно встановленої політики безпеки.

ПРН33. Вирішувати задачі забезпечення неперервності бізнес процесів організації на основі теорії ризиків.

ПРН34. Брати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

ПРН35. 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.

ПРН36. Виявляти небезпечні сигнали технічних засобів.

ПРН37. Вимірювати параметри небезпечних та заводових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витoku технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

ПРН40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

ПРН43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів.

ПРН44. Вирішувати задачі забезпечення неперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів.

ПРН45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

ПРН46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в ІТС.

ПРН47. Вирішувати задачі захисту інформації, що обробляється в ІТС з використанням сучасних методів та засобів криптографічного захисту інформації.

	<p>ПРН48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в ІТС.</p> <p>ПРН49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в ІТС.</p> <p>ПРН50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).</p> <p>ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в ІТС.</p> <p>ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.</p> <p>ПРН53. Вирішувати задачі аналізу програмного коду на наявність можливих вразливостей.</p> <p>ПРН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p>
--	--

8 – Ресурсне забезпечення реалізації програми

<p>Кадрове забезпечення</p>	<p>Проектна група: 1 доктор наук, професор, 3 кандидати наук, доценти.</p> <p><i>Гарант освітньої програми (керівник робочої групи):</i> 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».</p> <p><i>Член робочої групи:</i> 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</p>
------------------------------------	---

	<p>автоматики. В січні 2017 р. отримала грант за програмою «Erasmus+» для викладання лекцій в тому числі в галузі кібербезпеки в Технічному університеті Ополь (Польща).</p> <p>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-12013-1-EE-TEMPUS-JPCR).</p> <p><i>Член робочої групи:</i> 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.</p> <p>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-12013-1-EE-TEMPUS-JPCR).</p> <p><i>Член робочої групи:</i> Кареліна Олена Володимирівна – вчене звання доцент за кафедрою загальноекономічних дисциплін (галузь: 05 «Соціальні та поведінкові науки»), 2008 р., к. пед. н., 13.00.04 – Теорія та методика професійної освіти (галузь: 01 «Освіта»), 2005 р., із 2018 р. друга вища освіта: спеціальність 125 «Кібербезпека», Національний університет «Львівська політехніка». 2017-2018 р. – підвищення кваліфікації на кафедрі економічної кібернетики Львівського національного університету ім. І. Франка. Стаж педагогічної роботи у вищих закладах освіти III-IV рівня акредитації 19 років.</p>
<p>Матеріально-технічне забезпечення</p>	<p>Забезпеченість навчальними приміщеннями, комп’ютерними робочими місцями, мультимедійним обладнанням відповідає вимогам.</p> <p>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.</p> <p>Заняття та наукові дослідження проводяться у лабораторіях кафедри кібербезпеки, кафедри комп’ютерних наук, спеціалізованій комп’ютерній лабораторії технічного захисту інформації, лабораторії кіберфізичних систем.</p> <p>Для проведення інформаційного пошуку та обробки результатів є комп’ютерні класи, де наявне спеціалізоване програмне забезпечення та відкритий доступ до Інтернет-мережі.</p>

<p>Інформаційне та навчально-методичне забезпечення</p>	<p>Науково-технічна бібліотека ТНТУ щороку поповнюється спеціалізованою літературою і періодичними виданнями, що відповідають напрямкам роботи кафедри.</p> <p>Бібліотека університету першою серед українських вузівських бібліотек у 2011 році стала членом Міжнародної асоціації науково-технічних бібліотек університетів (IATUL). Також бібліотека є колективним членом Української бібліотечної асоціації.</p> <p>Інституційний репозитарій ELARTU активно продовжує наповнення фо-ндів. На початок 2016 року у репозитарії опубліковано понад 18 855 матеріалів.</p> <p>Згідно рейтингу Webometrics (http://www.webometrics.info/) станом на 2017 р. інституційний репозитарій ELARTU займає 10 місце серед українських репозитаріїв. Підвищенню рейтингу університету сприяє наявність наповненого та добре структурованого інституційного репозитарію.</p> <p>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 впровадження інформаційних технологій в освітній процес.</p>
<p>9 – Академічна мобільність</p>	
<p>Національна кредитна мобільність</p>	<p>Індивідуальна академічна мобільність реалізується у рамках міжуніверситетських договорів про встановлення науково-освітніх відносин для задоволення потреб розвитку освіти і науки з університетами України.</p> <p>До керівництва науковою роботою здобувачів залучаються провідні фахівці університетів України на умовах індивідуальних договорів.</p> <p>Допускається перезарахування кредитів, отриманих у інших університетах України, за умови відповідності їх набутих компетентностей.</p>
<p>Міжнародна кредитна мобільність</p>	<p>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, Німеччини, Іспанії, Великобританії, Франції та США.</p> <p>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).</p> <p>Студенти також реалізують своє право на міжнародну кредитну мобільність в рамках програми "Erasmus+". Зокрема студенти</p>

	<p>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.</p> <p>В ТНТУ виконується 5 освітніх і 3 наукових міжнародних проекти: «Рівні можливості для здобуття професії молодими матерямистудентками 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 KA1: «Навчальна мобільність» університет увійшов у консорціуми двох Еразмус проектів від Люблінської політехніки та від Опольської політехніки відповідно; за напрямом KA2 «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».</p>
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

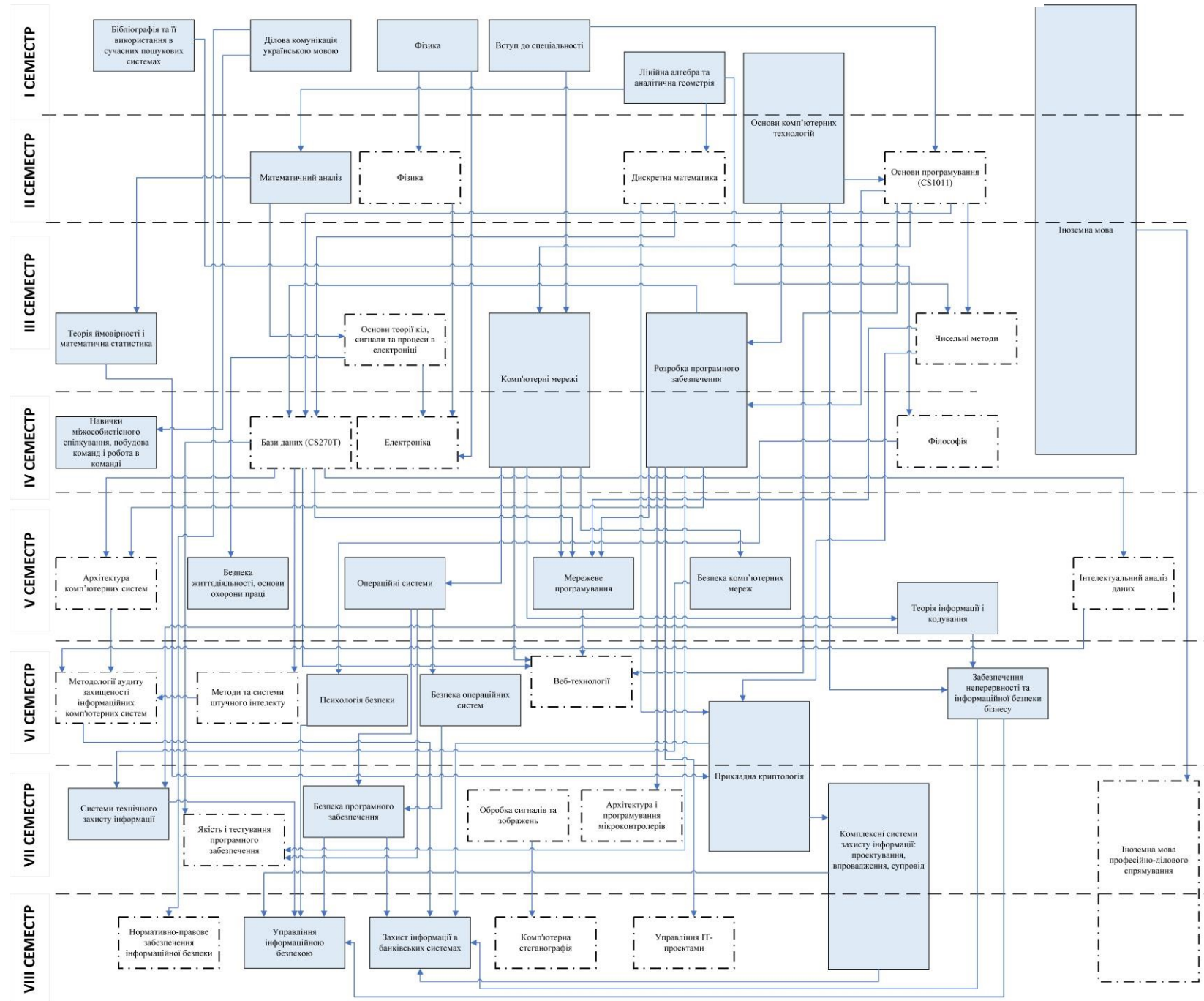
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
Обов'язкові компоненти ОП			
ОК 1.	Безпека життєдіяльності, основи охорони праці	3	е
ОК 2.	Бібліографія та її використання в сучасних пошукових системах	3	з
ОК 3.	Вища математика	10	е
ОК 4.	Вступ до спеціальності	3	е
ОК 5.	Ділова комунікація українською мовою	3	з

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
ОК 6.	Іноземна мова	29	е
ОК 7.	Навички міжособистісного спілкування, побудова команд і робота в команді	3	з
ОК 8.	Теорія ймовірності і математична статистика	4	е
ОК 9.	Фізика	4	е
ОК 10.	Забезпечення неперервності та інформаційної безпеки бізнесу	4	е
ОК 11.	Безпека комп'ютерних мереж	4	е
ОК 12.	Безпека операційних систем	5	е
ОК 13.	Безпека програмного забезпечення	4	е
ОК 14.	Захист інформації в банківських системах	4	е
ОК 15.	Комплексні системи захисту інформації: проектування, впровадження, супровід	7	е
ОК 16.	Комп'ютерні мережі	10	е
ОК 17.	Операційні системи	4	з
ОК 18.	Основи комп'ютерних технологій	9	е
ОК 19.	Мережеве програмування	4	е
ОК 20.	Прикладна криптологія	8,5	е
ОК 21.	Психологія безпеки	4	з
ОК 22.	Розробка програмного забезпечення	9,5	е
ОК 23.	Системи технічного захисту інформації	4	е
ОК 24.	Теорія інформації та кодування	4	е
ОК 25.	Управління інформаційною безпекою	4	е
ОК 26.	Проектно-технологічна практика	3	диф.з.
Загальний обсяг обов'язкових компонент:		154	
Вибіркові компоненти ОП			
<i>Вибірковий блок 1</i>			
ВБ 1.1.	Фізика	5	е
ВБ 1.2.	Філософія	3	з
ВБ 1.3.	Організація баз даних	4	е
ВБ 1.4.	Веб-технології	4,5	з
ВБ 1.5.	Дискретна математика	5	е
ВБ 1.6.	Електроніка	4	з

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
ВБ 1.7.	Іноземна мова професійно-ділового спрямування	3	е
ВБ 1.8.	Інтелектуальний аналіз даних	4	з
ВБ 1.9.	Комп'ютерна стеганографія	3	з
ВБ 1.10.	Методи та системи штучного інтелекту	4	е
ВБ 1.11.	Методології аудиту захищеності інформаційних комп'ютерних систем	3,5	з
ВБ 1.12.	Нормативно-правове забезпечення інформаційної безпеки	3,5	з
ВБ 1.13.	Обробка сигналів та зображень	3	з
ВБ 1.14.	Основи інтернету речей	4,5	з
ВБ 1.15.	Основи програмування	4	з
ВБ 1.16.	Основи теорії кіл, сигнали та процеси в електроніці	4	з
ВБ 1.17.	Програмування для мобільних пристроїв	4,5	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
<i>Вибірковий блок 2</i>			
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

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
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 вибіркового компонента:		77	
Дипломна робота		9	
Загальний обсяг освітньої програми		240	

2.2. Структурно-логічна схема ОП.



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності 125 «Кібербезпека» проводиться у формі публічного захисту кваліфікаційного проекту/роботи та завершується видачею документу встановленого зразка про присудження йому ступеня бакалавра з кібербезпеки із присвоєнням кваліфікації: 3439 – фахівець з організації інформаційної безпеки.

На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання згідно із стандартом вищої освіти за спеціальністю 125 «Кібербезпека» та цією освітньою програмою. До атестації допускаються студенти, які виконали всі вимоги програми підготовки. Атестація здійснюється відкрито і публічно.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

4.1. Обов'язкові компоненти освітньої програми

	О К1	О К2	О К3	О К4	О К5	О К6	О К7	О К8	О К9	О К1 0	О К1 1	О К1 2	О К1 3	О К1 4	О К1 5	О К1 6	О К1 7	18 О 17	О К1 8	О К2 0	О К2 1	О К2 2	О К2 3	О К2 4	О К2 5	О К2 6	
ЗК1	+	+						+			+																+
ЗК2			+								+																
ЗК3				+	+			+																			
ЗК4						+	+		+	+														+			
ЗК5		+																									
ФК1																	+										
ФК2																	+	+	+	+				+		+	
ФК3																											
ФК4											+																+
ФК5			+									+	+	+	+										+		
ФК6																											
ФК7																	+								+		
ФК8											+				+	+									+		+
ФК9																+											+
ФК1 0																					+						
ФК1 1																	+									+	
ФК1 2												+	+	+	+	+									+		+

