МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРБЕЗПЕКА»

другого рівня вищої освіти

за спеціальністю **125 "Кібербезпека та захист інформації"**

галузі знань **12 "Інформаційні технології"**

кваліфікація: **Магістр з кібербезпеки**

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Голова вченої ради

_____ /Микола МИТНИК/

(протокол № 3 від "19" березня 2024 р.)

Освітня програма вводиться в дію з 1 вересня 2024р.

Ректор _____ / Микола МИТНИК /

(наказ № 4/7-242 від "22" березня 2024 р.)

Тернопіль 2024 р.

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

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

ПОГОДЖЕНО:

Завідувач кафедри кібербезпеки — Наталія Загородна

Декан факультету комп'ютерно-інформаційних систем і програмної інженерії — Ігор Баран

Голова Експертної ради роботодавців кафедри кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя, заступник начальника відділу здійснення державного контролю Управління Держспецзв'язку в Тернопільській області — Олександр МАКСИМЧУК

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., зав. кафедри кібербезпеки
Члени:	
Карпінський Микола Петрович	д.т.н, професор кафедри кібербезпеки
Козак Руслан Орестович	к.т.н., доцент кафедри кібербезпеки.
Бабій Віктор Васильович	начальник 1 відділу Управління Держспецзв'язку в Тернопільській області
Пилипів Павло Володимирович	Студент групи СБм-52

Рецензії-відгуки зовнішніх стейкхолдерів:

Рецензія-відгук на освітньо-професійну програму «Кібербезпека» другого рівня вищої освіти від начальника Управління Дежавної служби спеціального зв’язку та захисту інформації в Тернопільській області Ігоря Вуїва.

1. Профіль програми магістра зі спеціальності 125 «Кібербезпека та захист інформації»

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Тернопільський національний технічний університет імені Івана Пулюя http://tntu.edu.ua/?p=uk/main Кафедра кібербезпеки http://kaf-kb.tntu.edu.ua/
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Магістр з кібербезпеки.
Офіційна назва освітньої програми	Освітньо-професійна програма «Кібербезпека» другого (магістерського) рівня вищої освіти галузі знань 12 «Інформаційні технології», спеціальності 125 Кібербезпека та захист інформації
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці
Наявність акредитації	Національне агентство із забезпечення якості вищої освіти, сертифікат про акредитацію освітньої програми Кібербезпека №5411 від 06.07.2023 р., термін дії сертифіката - до 01.07.2033 р.
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 освітньо-кваліфікаційного рівня бакалавра або магістра (спеціаліста)
Мова(и) викладання	Українська
Термін дії освітньої програми	До наступного перегляду ОП
Інтернет-адреса постійного розміщення опису освітньої програми	https://kaf-kb.tntu.edu.ua/educational-profile/
2 – Мета освітньої програми	
Фундаментальна підготовка висококваліфікованих фахівців, здатних використовувати набуті теоретичні та практичні знання, уміння та навички для розв’язання задачі дослідницького та/або інноваційного характеру та викликів професійної діяльності у сфері інформаційної та/або кібербезпеки	
3 - Характеристика освітньої програми	
Предметна область	*Галузь знань* – 12 «Інформаційні технології». *Спеціальність* – 125 «Кібербезпека та захист інформації» *Об’єкти вивчення*: – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об’єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології;

	– інфраструктура об’єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки *Цілі навчання:* Фундаментальна підготовка висококваліфікованих фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. *Теоретичний зміст предметної області*: Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. *Методи, методики та технології*: Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. *Інструменти та обладнання*: інформаційно-комунікаційні системи, прилади та обладнання (комп’ютерна техніка, контрольно-вимірювальні прилади, програмно-технічні комплекси та засоби, мережеве обладнання, спеціалізоване програмне забезпечення, пакети прикладних програм, комплекси проєктування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних тощо), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об’єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньої програми	Освітньо-професійна програма підготовки магістра розроблена для інтегрованої підготовки фахівців до вирішення прикладних завдань у сфері інформаційної безпеки, що передбачає вміння організовувати й підтримувати комплекс заходів та рішень 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.
Основний фокус освітньої програми та спеціалізації	Освітня програма робить акцент на розроблення, впровадження та експлуатацію систем захисту інформації (інформаційних, телекомунікаційних, технічних) та систем управління інформаційною безпекою на об'єктах інформаційної діяльності, проведення незалежної оцінки інструментів, практик і політик кібербезпеки організації, в тому числі на відповідність нормативним документам та стандартам з захисту інформації, принципах побудови кібер-фізичних систем захисту інформації, розробці комплексного підходу та впровадженні системи менеджменту для захисту інформаційних ресурсів організацій і користувачів *Ключові слова*: кібербезпека, системи управління інформаційною безпекою, аудит, відповідність стандартам, кіберфізичні системи, розслідування інцидентів.
Особливості програми	1. Формування у здобувачів комплексного підходу щодо розроблення, впровадження, управління, моніторингу та аудиту систем захисту інформації. 2. Отримання знань через відвідування лекцій викладачів-іноземців або викладачів ЗВО, які беруть участь у програмах академічної мобільності (зокрема, Еразмус+), проходять науково-педагогічне стажування у ЗВО-партнерах за кордоном, працюють в Європейських закладах вищої освіти тощо. 3. Отримання знань англійською мовою (додатково) при вивченні компонент ОПП від викладачів, які отримали сертифікати про рівень володіння нею не нижче В2. 4. Отримання фахових консультацій від залучених представників зовнішніх стейкхолдерів, зокрема консультантів та інженерів інформаційної безпеки великих компаній, представників державних органів влади за профілем спеціальності (Департамент кіберполіції, Управління Держспецзв'язку, тощо). 5. Можливість отримання міжнародних сертифікатів та сертифікатів відомих вендорів в сфері кібербезпеки.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Згідно з чинною редакцією Класифікатора професій (ДК 003:2010) випускник кваліфікації «Магістр кібербезпеки» може працевлаштуватися на посади з наступною назвою професійної роботи: 1210.1 - Керівник підприємства (установи, організації) (сфера захисту інформації); 1226.2 - Начальник відділення (сфера захисту інформації); 2149.2 - Професіонал із організації інформаційної безпеки; 1495 - Менеджери (управителі) систем з інформаційної безпеки; Та згідно з Міжнародним стандартом класифікації професій (International Standard Classification of Occupations 2008 – ISCO-08): 2529 – Спеціаліст з інформаційної безпеки (Security specialist – ICT).

	Випускники можуть працювати підприємцями; на підприємствах будь-яких форм власності та організаційно-правових форм господарювання, в ІТ-компаніях, науково-дослідних та проектно-конструкторських установах, місцевих органах державної влади; службі безпеки України, Державній службі спеціального зв'язку та захисту інформації, кіберполіції, керівниками підрозділів комп'ютерних послуг та інформаційної безпеки; викладачами університетів та вищих навчальних закладів; науковими співробітниками. Випускник має 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 ІТ компонентою. Можливість підвищення кваліфікації та отримання додаткової післядипломної освіти, підвищення кваліфікації.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, проблемно-орієнтоване навчання, електронне навчання в системі ATutor, самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді лекцій, семінарів, практичних і лабораторних занять, самостійної роботи з можливістю консультацій з викладачем, передбачає самонавчання, електронне навчання, проектну роботу в командах, навчання через проходження практик в установах та на підприємствах
Оцінювання	Оцінювання навчальних досягнень за: 100-бальною (рейтинговою) шкалою ECTS (A,B,C,D,E,F,FX), національною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно») і вербальною («зараховано», «незараховано») системами. Методи оцінювання: письмові та усні екзамени, тестування засобами електронних навчальних курсів в системі ATutor, звіти лабораторних робіт, реферати, презентації, індивідуальні завдання, захисти курсових робіт та проектів, публічний захист кваліфікаційної роботи бакалавра Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль. Можливий ректорський контроль. Форми контролю: усне та письмове опитування, тестові завдання, лабораторні звіти, презентації, захист курсових робіт та проєктів, звітів з практик. Атестація у формі публічного захисту кваліфікаційної роботи магістра.
6 – Програмні компетентності	

Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (КЗ)	КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові компетентності (КФ)	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

	КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
7 –Результати навчання	
	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

	РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

	РН24. Впроваджувати та використовувати системи, методи та засоби виявлення кібератак на ІТ інфраструктуру організації, аналізувати тренди появи вразливостей та загроз кібербезпеці з метою превентивного розгортання засобів захисту інформаційних ресурсів. РН25. Розробляти та впроваджувати системи та заходи інформаційної безпеки та кібербезпеки в процесах розробки програмного забезпечення та його інтеграції з комп'ютерними системами та мережами. РН26. Моделювати, проєктувати та впроваджувати елементи кіберфізичних систем при реалізації проєктів, в смарт-екосистемах, на об'єктах критичної інфраструктури з врахуванням характерних вразливостей, щодо яких розробляти та впроваджувати відповідні заходи захисту РН27. Аналізувати вимоги чинного законодавства в сфері захисту інформації та впроваджувати метод, способи та засоби для забезпечення їх ефективної реалізації по відношенню до інформаційно-комунікаційних систем, що використовуються органами державної влади, а також об'єктами критичної інфраструктури для обробки державних інформаційних ресурсів та інформації, вимога щодо захисту яких встановлена законом.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Реалізація освітньої програми забезпечується кадрами високої кваліфікації з науковими ступенями та вченими званнями, які мають значний досвід навчально-методичної, науково-дослідної роботи та відповідають кадровим вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (підтверджений рівень наукової та професійної активності). Освітній процес здійснюється науково-педагогічними працівниками кафедри кібербезпеки із залученням науково-педагогічних працівників з інших кафедр та викладачів з провідних закладів вищої освіти Європи. Додатково залучаються фахівці в галузі кібербезпеки з провідних ІТ-компаній західного регіону та спеціалізованих органів державної влади. Викладацький склад кафедри регулярно проходить планове стажування в галузі інформаційних технологій у провідних ЗВО та ІТ- компаніях та за кордоном. Четверо НПП отримали сертифікати про рівень володіння англійською мовою (B2, C1 – Aptis) та два викладачі підтвердили володіння польською мовою. Двоє викладачів були учасниками тренінгів, проведених іноземними організаторами з Великобританії ("Academic Teacher Excellence" (English as the Medium of Instruction) отримали відповідні сертифікати. Троє викладачів брали участь у виконанні міжнародних наукових та освітніх проєктів, академічній мобільності за програмами Tempus та Еразмус+.
Матеріально-технічне забезпечення	Реалізація освітньої програми забезпечується матеріально-технічними ресурсами університету і відповідає вимогам щодо матеріально-технічного забезпечення освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова кабінету міністрів України «Про затвердження

	Ліцензійних умов провадження освітньої діяльності закладів освіти») 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, лабораторіях академії Cisco. 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. Наявний електронний каталог бібліотеки університету, де можна здійснити швидкий пошук книг, методичних розробок та інших матеріалів, що знаходяться в фондах бібліотеки у паперовій формі. Наявний інституційний репозитарій ELARTU, де розміщені електронні інформаційно-методичні розробки (збірники статей, збірники конференцій, методичні розробки, кваліфікаційні роботи випускників та інше). Інституційний репозитарій ELARTU активно продовжує наповнення фондів. Наявність наповненого та добре структурованого інституційного репозитарію сприяє підвищенню рейтингу університету. Навчальний процес базується на 100% навчально-методичному забезпеченні семінарських, практичних, лабораторних занять і самостійної роботи студентів з усіх навчальних дисциплін. Дисципліни забезпечені електронними навчальними курсами, розміщеними в системі ATutor, що включають необхідні методичні матеріали (лекції, лабораторні роботи, практичні роботи тощо), а також підсистему тестування рівня засвоєння знань. 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 їх відповідності набутим компетентностям.
Міжнародна кредитна мобільність	Міжнародна кредитна мобільність є одним з пріоритетних напрямків розвитку міжнародного співробітництва університету та відбувається на основі двосторонніх договорів між

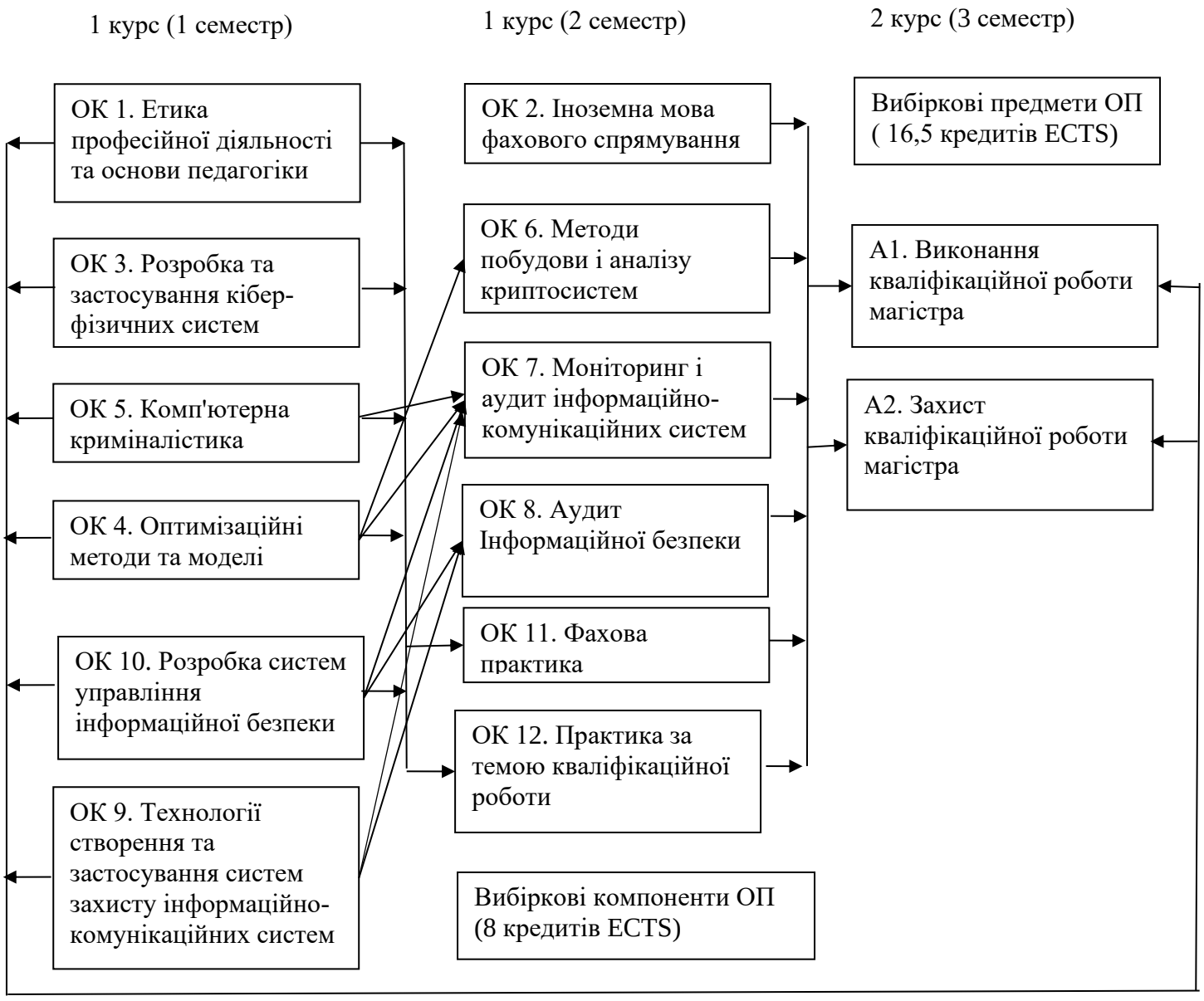
	Тернопільським національним технічним університетом імені Івана Пулюя та закладами вищої освіти інших країн. Студенти – здобувачі освітнього рівня "магістр" спеціальності 125 Кібербезпека за даною ОПП мають можливість брати участь у програмах академічної мобільності, у межах яких вони можуть навчатися за програмами подвійних дипломів у ЗВО-партнерах за кордоном, брати участь у програмі академічної мобільності Еразмус+ або проходити практики за кордоном. Студенти мають можливість приймати участь в програмі подвійних дипломів за освітнім рівнем "магістр" з державним університетом «Люблінська Політехніка» (Польща). Студенти також реалізують своє право на міжнародну кредитну мобільність в рамках програми "Erasmus+". Зокрема студенти кафедри скористались перевагами та можливостями програми для навчання в Вищому професійному державному університеті, Ниси (Польща), університеті Валенсії (Іспанія), університеті прикладних наук Шмалькальден (Німеччина), університеті прикладих наук Санкт-Пельтен (Австрія), Каунаському технологічному університеті (Литва).
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти проводиться на загальних умовах (з додатковою мовною підготовкою).

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

2.1. Перелік компонент ОП

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОПП			
Цикл Загальної підготовки			
ОК 1	Етика професійної діяльності та основи педагогіки	4,0	залік
ОК 2	Іноземна мова фахового спрямування	4,0	залік
Разом за циклом:		**8,0**	
Цикл Професійної підготовки			
Професійна підготовка			
ОК 3	Розробка та застосування кіберфізичних систем	4,0	залік
ОК 4	Оптимізаційні методи та моделі	4,0	екзамен
ОК 5	Комп'ютерна криміналістика	4,0	екзамен
ОК 6	Методи побудови і аналізу криптосистем, передбачено курсовий проєкт	4,0	екзамен, КП
ОК 7	Моніторинг і аудит інформаційно-комунікаційних систем	4,0	екзамен
ОК 8	Аудит інформаційної безпеки	4,0	залік
ОК 9	Технології створення та застосування систем захисту інформаційно-комунікаційних систем, передбачено курсовий проєкт	4,0	Екзамен, КП
ОК 10	Розробка систем управління інформаційної безпеки	4,0	екзамен
Разом за професійною підготовкою:		**32,0**	
Практична підготовка			
ОК 11	Фахова	9,0	залік диф.
ОК 12	Практика за темою кваліфікаційної роботи	7,5	залік диф.
Разом за практичною підготовкою:		**16,5**	
Разом за циклом:		**48,5**	
Загальний обсяг обов'язкових компонент:		**56,5**	
Вибіркові компоненти ОПП *здобувачі вищої освіти обирають освітні компоненти із запропонованого переліку у середовищі електронного навчання ТНТУ ATutor* *(Вкладка – Навчальні дисципліни для вибору студентами)* https://dl.tntu.edu.ua/login.php *(доступ до переліку вибіркових дисциплін мають усі здобувачі вищої освіти, зареєстровані у середовищі ЕН ТНТУ ATutor)*			
Загальний обсяг вибіркових компонент:		**24,5**	
Атестація			
А1	Виконання кваліфікаційної роботи магістра	7,5	
А2	Захист кваліфікаційної роботи магістра	1,5	
Разом за атестацію:		**9,0**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ		**90,0**	

2.2. Структурно-логічна схема ОП



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності 125 «Кібербезпека та захист інформації» проводиться у формі захисту кваліфікаційної роботи магістра 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.

Атестація здійснюється у формі публічного захисту кваліфікаційної роботи магістра.

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

У кваліфікаційній роботі не повинно бути академічного плагіату, фальсифікації та фабрикації. Згідно Положення про кваліфікаційні роботи студентів Тернопільського національного технічного університету імені Івана Пулюя – наказ №4/7-241 від 15.04.2020, кваліфікаційна робота підлягає перевірці на академічний плагіат та оприлюдненню шляхом розміщення в інституційному репозитарії університету ELARTU(http://elartu.tntu.edu.ua/).

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	А1	А2
КЗ 1	+	+	+	+	+	+	+	+	+	+	+	+	+	
КЗ 2			+	+		+						+	+	
КЗ 3				+		+						+	+	
КЗ 4							+	+	+	+	+	+	+	+
КЗ 5		+	+	+			+	+	+	+	+	+	+	+
КФ 1			+	+		+			+		+	+	+	
КФ 2						+		+	+	+	+	+	+	
КФ 3			+		+		+		+		+	+	+	
КФ 4										+	+	+	+	
КФ 5							+	+		+	+		+	
КФ 6									+		+		+	
КФ 7					+		+			+		+	+	
КФ 8			+			+					+	+	+	
КФ 9			+				+	+			+	+	+	
КФ 10	+						+	+						

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

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	А1	А2
РН 1	+	+						+					+	+
РН 2				+	+	+		+	+	+	+	+	+	
РН 3						+					+	+	+	
РН 4			+	+		+			+			+	+	
РН 5			+	+	+	+	+	+			+	+	+	
РН 6			+			+	+	+	+	+	+	+	+	
РН 7					+	+		+		+	+	+	+	+
РН 8			+					+	+		+	+	+	
РН 9									+	+	+	+	+	
РН 10							+			+	+		+	
РН 11			+				+		+	+	+	+	+	
РН 12					+		+				+	+	+	
РН 13			+			+					+	+	+	
РН 14							+	+		+	+	+	+	
РН 15					+		+	+	+	+	+	+	+	+
РН 16				+			+		+	+		+	+	
РН 17	+	+					+						+	
РН 18	+							+		+	+			
РН 19				+					+	+	+	+	+	
РН 20						+		+	+		+	+	+	
РН 21			+	+					+			+	+	
РН 22				+		+						+	+	
РН 23			+		+	+	+		+	+	+	+	+	
РН 24							+		+	+		+	+	
РН 25									+			+	+	
РН 26			+									+	+	
РН27							+	+		+			+	

Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

Вимоги щодо внутрішнього забезпечення якості вищої освіти регламентуються окремим положенням ТНТУ – Система управління якістю (СУЯ). Стратегічне управління університетом (наказ №4/7-568 від 25.07.2016, https://docs.tntu.edu.ua/base/document?id=24).

Відповідно до рішення Органу сертифікації 31 серпня 2017 року Тернопільський національний технічний університет імені Івана Пулюя отримав сертифікати, які підтверджують відповідність системи управління якістю вимогам міжнародного стандарту ISO 9001:2015. Перші два сертифікати українською та німецькою мовами видані німецьким сертифікаційним органом “DQS GmbH”, який входить в трійку лідерів серед сертифікаційних органів у світі, що свідчить про міжнародне визнання якості освітньої діяльності (сертифікат видано 31.08.2018, дійсний – до 30.08.2021, http://tntu.edu.ua/storage/pages/00000287/QM15_31400225_QM15_UK.pdf).

Ще один сертифікат єдиного міжнародного зразка IQNet (видано 31.08.2018, дійсний – до 30.08.2021, реєстраційний номер DE-31400225 QM15, http://tntu.edu.ua/storage/pages/00000287/IQNet_31400225_QM15_EN.pdf) виданий міжнародною сертифікаційною мережею (зі штаб квартирою у м. Берн, Швейцарія), що об’єднує 37 провідних органів з сертифікації в 34 країнах світу.

У Тернопільському національному технічному університеті імені Івана Пулюя функціонує система забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

1) визначення принципів та процедур забезпечення якості вищої освіти;

2) здійснення моніторингу та періодичного перегляду освітніх програм;

3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників вищого навчального закладу та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті вищого навчального закладу, на інформаційних стендах та в будь-який інший спосіб;

4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою;

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

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

8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників вищих навчальних закладів і здобувачів вищої освіти;

9) інших процедур і заходів.

Система забезпечення Тернопільським національним технічним університетом імені Івана Пулюя якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) за поданням Тернопільського національного технічного університету імені Івана Пулюя оцінюється Національним агентством із забезпечення якості вищої освіти або акредитованими ним незалежними установами оцінювання та забезпечення якості вищої освіти на предмет її відповідності вимогам до системи забезпечення якості вищої освіти, що затверджуються Національним агентством із забезпечення якості вищої освіти, та міжнародним стандартам і рекомендаціям щодо забезпечення якості вищої освіти.

Гарант освітньої програми,
к.т.н., зав. кафедри кібербезпеки Загородна Н.В.

Перелік нормативних документів, на яких базується ОПП

1. Standards and guidelines for quality assurance in the European higher education area (ESG). URL: https://enqa.eu/index.php/home/esg/. Україномовна версія: Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти. URL: https://enqa.eu/indirme/esg/ESG%20in%20Ukrainian_by%20the%20British%20Council.pdf.
2. Tuning Educational Structures in Europe, TUNING project. URL: http://www.unideusto.org/tuningeu/. Україномовна версія: Проект Європейської Комісії «Гармонізація освітніх структур в Європі». URL: https://www.unideusto.org/tuningeu/images/stories/documents/General_Brochure_Ukrainian_version.pdf.
3. Про вищу освіту : Закон України від 01.07.2014 р. № 1556-VII. Відомості Верховної Ради України. URL: http://zakon4.rada.gov.ua/laws/show/1556-18.
4. Про освіту : Закон України від 05.09.2017 р. № 2145-VIII. Відомості Верховної Ради України. URL: http://zakon5.rada.gov.ua/laws/show/2145-19
5. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти : Постанова Кабінету Міністрів України від 29.04.2015 р. № 266. URL: http://zakon4.rada.gov.ua/laws/show/266-2015-п
6. Про затвердження Національної рамки кваліфікацій : Постанова Кабінету Міністрів України від 23 листопада 2011 р. № 1341. URL: http://zakon4.rada.gov.ua/laws/show/1341-2011-п (в редакції постанови Кабінету Міністрів України від 25 червня 2020 р. №519)
7. Класифікатор професій ДК 003:2010 : Національний класифікатор України. Держспоживстандарт України ; Наказ від 28.07.2010 № 327. URL: https://zakon.rada.gov.ua/rada/show/va327609-10#Text.
8. Рашкевич Ю.М. Болонський процес та нова парадигма вищої освіти :монографія. Львів : Видавництво Львівської Політехніки, 2014. 168 с.
9. Стандарт вищої освіти другого (магістерського) рівня галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека», затверджений та введений у дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.
10. Положення про порядок розроблення, затвердження, моніторингу та припинення освітніх програм Тернопільського національного технічного університету імені Івана Пулюя – наказ №4/7-965 від 01.11.2019 зі змінами від 18.09.2020 – наказ №4/7-668 від 25.09.2020. URL: https://docs.tntu.edu.ua/base/document?id=466
11. Методичні рекомендації щодо розроблення стандартів вищої освіти. Затверджено Наказом Міністерства освіти і науки України від 01.06.2017 р. № 600 (у редакції наказу Міністерства освіти і науки України від 30.04.2020 р. № 584 – https://mon.gov.ua/storage/app/media/vyshcha/naukovo-metodychna_rada/2020metod-rekomendacziyi.docx