МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

першого рівня вищої освіти

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

галузі знань **12 "Інформаційні технології"**

кваліфікація: **Бакалавр 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	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Кваліфікація	Бакалавр 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 та захист інформації” Тернопільського національного технічного університету імені Івана Пулюя у складі:

Керівник робочої групи, гарант освітньо-професійної програми:

Козак Руслан Орестович	к.т.н., доцент кафедри кібербезпеки

Члени:

Карпінський Микола Петрович	д.т.н, професор кафедри кібербезпеки
Загородна Наталія Володимирівна	к.т.н., зав. кафедри кібербезпеки
Бабій Віктор Васильович	начальник 1 відділу Управління Держспецзв'язку в Тернопільській області
Шиманська Вікторія Олегівна	студентка групи СБ-32

Рецензії-відгуки зовнішніх стейкхолдерів:

Рецензія-відгук на освітньо-професійну програму «Кібербезпека» першого рівня вищої освіти від консультанта з кібербезпеки компанії ТзОВ «ГлобалЛоджик Україна» Олександра Адамова.

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

1 – Загальна інформація	
Повна назва закладу вищої освіти 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	Бакалавр. Бакалавр з кібербезпеки.
Офіційна назва освітньої програми	Освітньо-професійна програма «Кібербезпека» першого (бакалаврського) рівня вищої освіти галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека та захист інформації»
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний. Обсяг освітньої програми бакалавра: - на базі повної загальної середньої освіти – 240 кредитів ЄКТС; термін навчання 3 роки 10 місяців - на базі ступеня «молодший бакалавр», «фаховий молодший бакалавр» або освітньо-кваліфікаційного рівня «молодший спеціаліст» – 180 кредитів ЄКТС; термін навчання 2 роки 10 місяців. Прийом на основі ступенів «молодший бакалавр», «фаховий молодший бакалавр» або освітньо-кваліфікаційного рівня «молодший спеціаліст» здійснюється за результатами зовнішнього незалежного оцінювання в порядку, визначеному законодавством. Мінімум 75% обсягу освітньої програми має бути спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю визначеною стандартом вищої освіти.
Наявність акредитації	Національне агентство із забезпечення якості вищої освіти, сертифікат про акредитацію освітньої програми Кібербезпека №5410 від 06.07.2023 р., термін дії сертифіката - до 01.07.2027 р.
Цикл/рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл, QF-LLL – 6 рівень.
Передумови	Повна загальна середня освіта, ОКР «Молодший спеціаліст», ОС «Фаховий молодший бакалавр», Молодший бакалавр
Мова(и) викладання	Українська
Термін дії освітньої програми	3 роки 10 місяців
Інтернет-адреса постійного розміщення опису освітньої програми	https://kaf-kb.tntu.edu.ua/educational-profile/

2 – Мета освітньої програми	
– Формування та розвиток загальних і професійних компетентностей у фахівців в галузі інформаційних технологій зі спеціальності 125 «Кібербезпека та захист інформації», 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. – Надання ґрунтовної освіти з кібербезпеки із широким доступом до працевлаштування або продовження навчання за другим (освітньо-професійним або освітньо-науковим) рівнем вищої освіти.	
3 - Характеристика освітньо-професійної програми	
Предметна область (галузь знань, спеціальність)	Галузь знань – 12 «Інформаційні технології». Спеціальність – 125 «Кібербезпека та захист інформації». **Об'єкти вивчення**: об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. **Цілі навчання**: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** *Знання*: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. *Методи, методики та технології*: методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. *Інструменти та обладнання*: – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Освітньо-професійна програма підготовки бакалавра розроблена для студентів, які прагнуть стати фахівцями із захисту інформації для українських чи світових компаній. Програма має прикладний характер, орієнтована на формування широкого науково-технічного світогляду майбутнього фахівця з кібербезпеки.

Основний фокус освітньої програми та спеціалізації	Акцент на здатності організовувати й підтримувати оперативний центр безпеки організації у формі комплексу заходів щодо забезпечення інформаційної безпеки та кібербезпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації. *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	Випускник кваліфікації «Бакалавр з кібербезпеки» може займати первинні посади (за ДК 003:2010): 3439 (24771) - Фахівець із організації інформаційної безпеки, 1495 – Менеджер (управитель) систем з інформаційної безпеки, 1229.7 – керівник (директор, начальник та ін.) підрозділу (служби, управління, департаменту та ін.) з безпеки (фінансово-економічної, інформаційної), 2149.2 – професіонал із організації інформаційної безпеки, 2110.1 – керівник підприємства (установи, організації) (сфера захисту інформації), 1226.2 – керівник структурного підрозділу (сфера захисту інформації), 2149.2 – професіонал із організації захисту інформації з обмеженим доступом, 2149.2 – фахівець (сфера захисту інформації). 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 за спеціальністю 125 «Кібербезпека та захист інформації» або іншими спорідненими (суміжними) спеціальностями галузі знань «Інформаційні технології».

	НРК України – 7, FQ-EHEA – 2 цикл, EQF LLL – 7 рівень.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, навчання з використанням електронних навчальних курсів в системі ATutor, самонавчання, навчання на основі досліджень, формування практичних умінь на базах практики згідно укладених договорів. Основні види занять: лекції (мультимедійні, інтерактивні), семінари, практичні заняття, лабораторні роботи, самостійне навчання на основі електронного навчального курсу, підручників та конспектів, консультації з викладачами, виконання курсових робіт, підготовка кваліфікаційної роботи бакалавра. Самостійна робота студентів забезпечується системою електронного навчання Atutor. Здобуття практичних умінь забезпечується проходженням практик. Обов'язковим елементом навчання є написання та захист дипломної роботи.
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. *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 проектів, звітів з практик. *Атестація:* у формі публічного захисту кваліфікаційної роботи бакалавра.
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)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та розуміння професії. ЗК3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК5. Здатність до пошуку, оброблення та аналізу інформації. ЗК6. 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. ЗК7. 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.
Фахові компетентності спеціальності (ФК)	ФК1. 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. ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ФК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. ФК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). ФК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. ФК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. ФК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. ФК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

7 – Програмні результати навчання (ПР)
ПР1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПР2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПР3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПР4. 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. ПР5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПР6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ПР7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПР8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. ПР9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПР10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. ПР11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. ПР12. Розробляти моделі загроз та порушника. ПР13. Аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних. ПР14. Вирішувати завдання захисту програм та інформації, що обробляється в ІТС програмно-апаратними засобами та давати оцінку результативності, якості прийнятих рішень. ПР15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. ПР16. Реалізовувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативно-правових документів. ПР17. 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. ПР18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПР19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в ІТС. ПР20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС. ПР21. 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. ПР22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в ІТС згідно встановленої політики інформаційної і\або кібербезпеки. ПР23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПР24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в

інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
ПР25. 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.
ПР26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
ПР27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
ПР28. 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;
ПР29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в ІТС та ефективності використання КЗЗ в умовах реалізації загроз різних класів.
ПР30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів ІТС.
ПР31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів ІТС.
ПР32. Вирішувати задачі управління процесами відновлення штатного функціонування ІТС з використанням процедур резервування згідно встановленої політики безпеки.
ПР33. Вирішувати задачі забезпечення неперервності бізнес процесів організації на основі теорії ризиків.
ПР34. Брати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
ПР35. 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.
ПР36. Виявляти небезпечні сигнали технічних засобів.
ПР37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
ПР38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
ПР39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
ПР40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
ПР41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
ПР42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
ПР43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
ПР44. Вирішувати задачі забезпечення неперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів.

ПР45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
ПР46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в ІТС.
ПР47. Вирішувати задачі захисту інформації, що обробляється в ІТС з використанням сучасних методів та засобів криптографічного захисту інформації.
ПР48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в ІТС.
ПР49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в ІТС.
ПР50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
ПР51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в ІТС.
ПР52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
ПР53. Вирішувати задачі аналізу програмного коду на наявність можливих вразливостей.
ПР54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

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 на основі двосторонніх договорів між Тернопільським національним технічним університетом ім. І. Пулюя та закладами вищої освіти України. Допускається перезарахування кредитів, отриманих в інших університетах України за умови відповідності набутих компетентностей даній освітній програмі.

Міжнародна кредитна мобільність	Реалізація програм академічної мобільності, зокрема програм подвійних дипломів, є одним з пріоритетних напрямів розвитку міжнародного співробітництва університету. Студенти мають можливість навчатись за українсько-німецькою програмою подвійних дипломів освітнього рівня "бакалавр" в Університеті прикладних наук Шмалькальдена (Німеччина), Технічному університеті Кошице (Словаччина). Студенти також реалізують своє право на міжнародну кредитну мобільність в рамках програми "Erasmus+". Зокрема студенти кафедри скористались перевагами та можливостями програми для навчання в університеті Ниси (Польща) та університеті прикладних наук Шмалькальдена.
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти проводиться на загальних умовах (з додатковою мовною підготовкою).

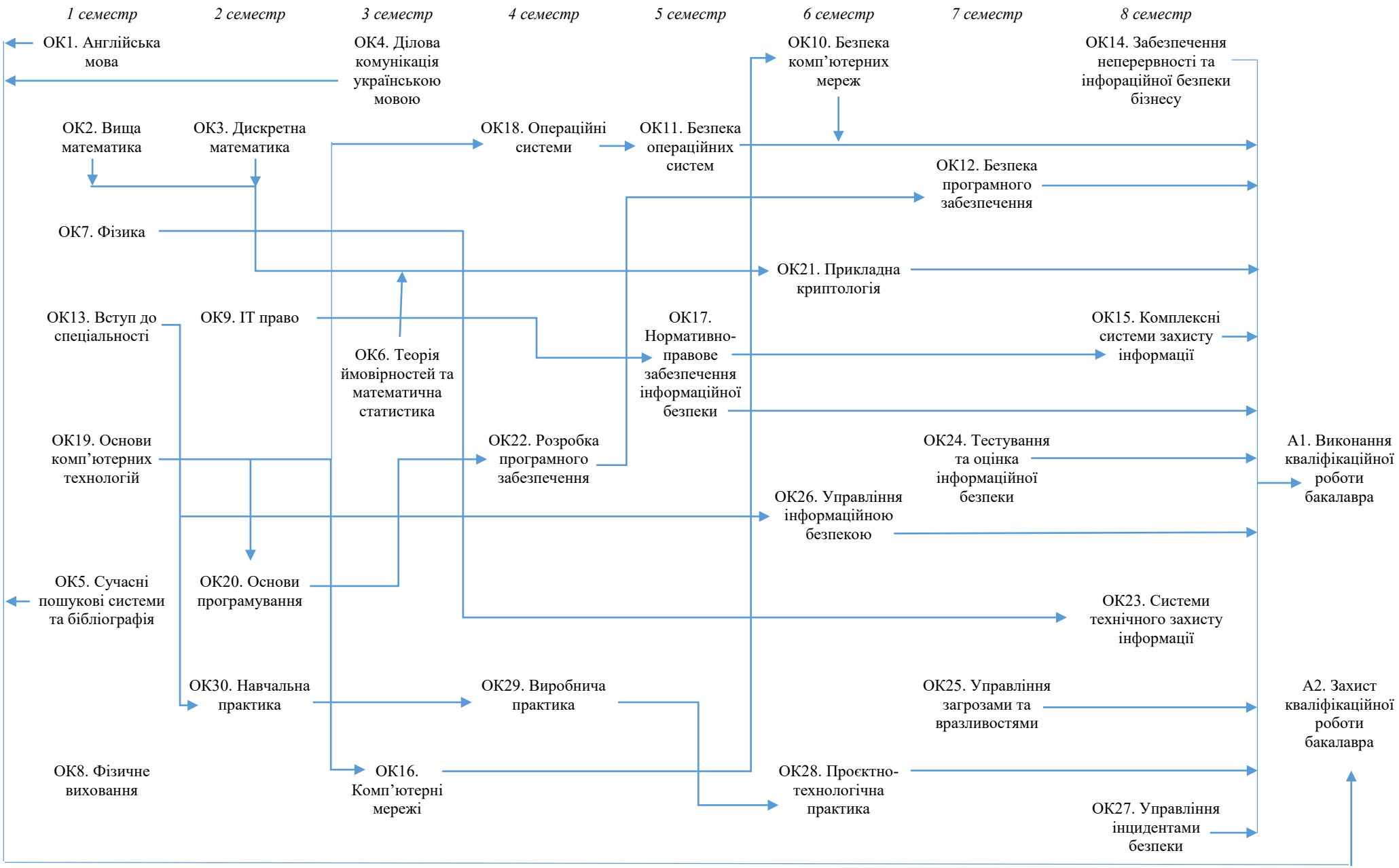
2. Перелік компонентів освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонентів освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумк. контролю
Обов'язкові компоненти ОПП			
Цикл загальної підготовки			
ОК1	Англійська мова	24	екзамен
ОК2	Вища математика	10	екзамен
ОК3	Дискретна математика	5	екзамен
ОК4	Ділова комунікація українською мовою	4	залік
ОК5	Сучасні пошукові системи та бібліографія	4	залік
ОК6	Теорія ймовірностей та математична статистика	4	залік
ОК7	Фізика	8	екзамен
ОК8	Фізичне виховання	4	залік
	Всього за цикл	**63**	
Цикл професійної підготовки			
Професійна підготовка			
ОК9	IT право	4	екзамен
ОК10	Безпека комп'ютерних мереж	5	екзамен, КР
ОК11	Безпека операційних систем	4	екзамен, КР
ОК12	Безпека програмного забезпечення	5	екзамен
ОК13	Вступ до спеціальності	5	екзамен
ОК14	Забезпечення неперервності та інформаційної безпеки бізнесу	4	екзамен
ОК15	Комплексні системи захисту інформації: проєктування, впровадження, супровід	4	екзамен
ОК16	Комп'ютерні мережі	9	екзамен, КР
ОК17	Нормативно-правове забезпечення інформаційної безпеки	4	екзамен
ОК18	Операційні системи	4,5	екзамен
ОК19	Основи комп'ютерних технологій	4,5	екзамен
ОК20	Основи програмування	4	залік
ОК21	Прикладна криптологія	9	екзамен, КП
ОК22	Розробка програмного забезпечення	4	екзамен
ОК23	Системи технічного захисту інформації	4	екзамен
ОК24	Тестування та оцінка інформаційної безпеки	4,5	екзамен

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумк. контролю
ОК25	Управління загрозами та вразливостями	4	екзамен
ОК26	Управління інформаційною безпекою	4,5	екзамен
ОК27	Управління інцидентами безпеки	4	екзамен, КП
	Всього за цикл	**91**	
Практична підготовка			
ОК28	Проєктно-технологічна	3	диф.з.
ОК29	Виробнича	3	диф.з.
ОК30	Навчальна	3	диф.з.
	Всього за практичну підготовку	**9**	
	Всього за професійну та практичну підготовку	**100**	
Загальний обсяг обов'язкових компонент:			
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:		**68**	
Атестація			
А1	Виконання кваліфікаційної роботи бакалавра	7,5	
А2	Захист кваліфікаційної роботи бакалавра	1,5	
Всього за атестацію		**9**	
Загальний обсяг освітньо-професійної програми		**240**	

2.2. Структурно-логічна схема ОПП.



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності 125 «Кібербезпека та захист інформації» проводиться у формі захисту кваліфікаційної роботи бакалавра та завершується видачею документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації "Бакалавр 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 бакалавра.

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 освітнім компонентам

	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ФК1	ФК2	ФК3	ФК4	ФК5	ФК6	ФК7	ФК8	ФК9	ФК10	ФК11	ФК12
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				+							+		+		+	+			

OK27											+		+		+				
OK28	+	+		+								+							
OK29	+	+		+								+							
OK30	+	+		+								+							
A1				+	+							+		+		+			
A2			+																

5. Матриця забезпечення програмних результатів навчання освітніми компонентами

	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	ОК29	ОК30	А1	А2
ПР1	+			+																												+
ПР2													+															+	+	+	+	
ПР3					+																										+	
ПР4															+																+	
ПР5																												+	+	+		
ПР6		+	+			+	+																					+	+	+		
ПР7									+						+		+															
ПР8															+		+									+					+	
ПР9														+	+											+	+					
ПР10																+		+	+	+		+						+			+	
ПР11																+		+	+	+		+						+			+	
ПР12													+		+										+							
ПР13																+		+	+	+		+						+			+	
ПР14										+	+	+			+								+									
ПР15										+	+	+				+		+	+	+		+						+	+	+	+	
ПР16															+		+						+									
ПР17										+	+	+											+					+	+	+	+	
ПР18										+	+	+											+									
ПР19										+	+	+											+					+	+	+	+	
ПР20														+									+									
ПР21										+	+	+														+						
ПР22										+	+	+														+						
ПР23										+	+	+														+						
ПР24										+	+	+														+						
ПР25																											+					
ПР26																								+	+	+	+					

ПР27										+	+	+										+		+									
ПР28																								+	+	+							
ПР29																								+	+	+		+					
ПР30																									+	+							
ПР31										+	+	+			+									+					+	+	+	+	
ПР32														+														+	+				
ПР33														+														+	+				
ПР34																												+		+	+	+	
ПР35															+													+					
ПР36																								+									
ПР37																								+									
ПР38																								+									
ПР39																								+									
ПР40																								+									
ПР41																												+					
ПР42																												+	+				
ПР43																													+				
ПР44														+														+					
ПР45																												+					
ПР46																												+					
ПР47																							+										
ПР48																							+						+				
ПР49																									+	+			+				
ПР50																									+	+			+				
ПР51																									+	+			+				
ПР52										+	+	+													+	+			+				
ПР53												+													+	+							
ПР54								+	+				+				+																

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., доцент кафедри кібербезпеки Козак Р.О.

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