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: Бакалавр з кібербезпеки

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
ТНТУ імені Івана Пулюя
Голова Вченої ради
_____/Ясній П. В./
(протокол № 8 від 22.06.21)

Освітня програма вводиться в дію з 1 вересня 2021 р.
Ректор _____/Ясній П. В./
(наказ № 4/7-543 від 23.06.21)

Тернопіль, 2021 р.

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

Рівень вищої освіти	Перший (бакалаврський) рівень
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Кваліфікація	Бакалавр з кібербезпеки

ПОГОДЖЕНО

Завідувач кафедри кібербезпеки
к. т. н., доцент _____ Загородна Н. В.

Декан факультету комп'ютерно-інформаційних систем та програмної інженерії
к. т. н., доцент _____ Баран І. О.

Голова експертної ради роботодавців кафедри кібербезпеки та кафедри комп'ютерних систем та мереж Тернопільського національного технічного університету імені Івана Пулюя, виконавчий директор Компанії «Goodahead Ltd»
_____ С. І. Гловак

ПЕРЕДМОВА

РОЗРОБЛЕНО

Проектною групою спеціальності 125 «Кібербезпека» Тернопільського національного технічного університету ім. І. Пулюя у складі:

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

Рецензії-відгуки зовнішніх стейкхолдерів:

1. Рецензія-відгук на освітньо-професійну програму «Кібербезпека», директор ТОВ Хаблейз _____ Шаповалова Т.

2. Рецензія-відгук на освітньо-професійну програму «Кібербезпека», операційний менеджер IT Cyberoo S. p. A. _____ Орланді М.

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

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Тернопільський національний технічний університет імені Івана Пулюя, кафедра кібербезпеки
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
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний. Обсяг освітньої програми бакалавра: - на базі повної загальної середньої освіти– 240 кредитів ЄКТС; - на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста). На основі ступеня «фаховий молодший бакалавр» заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти. 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	-

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 мова
Термін дії освітньої програми	3 роки 10 місяців
Інтернет-адреса постійного розміщення опису освітньої програми	http://tntu.edu.ua/storage/pages/00000120/op125b.pdf

2 – Мета освітньої програми

- Формування та розвиток загальних і професійних компетентностей у 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.
- 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». **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 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. 1. Навчання за програмами подвійних дипломів у ЗВО-партнерах закордоном. 2. Участь у програмах академічної мобільності (зокрема Еразмус+). 3. Читання лекцій іноземними викладачами (штатними та учасниками програм академічної мобільності Еразмус+). 4. Участь у Міжнародних та Всеукраїнських науково-практичних конференціях. 5. Можливість проходження практик закордоном та в міжнародних IT-компаніях. 6. Завдяки тому, що викладачі кафедри є інструкторами Мережевої академії Cisco при ТНТУ ім. І. Пулюя (першій мережевій академії Cisco в Україні – працює 21 рік) студенти здобувають сертифікат Cisco на рівні CCNA за результатами вивчення курсу «Cybersecurity Operations», сертифікати Cisco з курсів «Вступ до кібербезпеки», «Основи кібербезпеки», фахівець з «Інтернет речей», «Безпеки інтернет речей», «Комп'ютерних мереж», «З програмування на мові Python», «З програмування на мові Java», «З програмування на мові C++», «З програмування на мові C#», «Linux», «IT Essentials PC Hardware and Software» та інші.
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» 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 кваліфікаційної 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.

ПРОГРАМНІ РЕЗУЛЬТАТИ РЕКОМЕНДОВАНІ ЗОВНІШНІМИ СТЕЙКХОЛДЕРАМИ (РОБОТОДАВЦЯМИ)

ПР55. Застосування поглиблених знань з англійської мови.

ПР56. Уміння роботи із стеком технологій ELK (Elasticsearch, Logstesh, Kibana, Beats).

ПР57. Використання технології розробки інформаційних систем із застосуванням системи контролю версій (GIT).

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, країн (Польща) та (додатково) фахівців в галузі інформаційних технологій з провідних ІТ-компаній західного регіону. Викладацький склад кафедри регулярно проходить планове стажування в галузі інформаційних технологій у провідних ЗВО та ІТ- компаніях та за кордоном. Троє 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»). Приміщеннями для проведення навчальних занять забезпечені мультимедійним обладнанням, а робочі місця навчальних лабораторій комп’ютерами та необхідним обладнанням, устаткуванням потрібним для проведення занять під час навчального процесу. В процесі реалізації освітньої програми використовується прикладне та спеціалізоване програмне забезпечення таке як: гіпервізори (Oracle VirtualBox, VMware); дистрибутиви Linux (Kali, Security Onion, Mint, Arch, Kodachi); Microsoft Office 365; Python з використанням бібліотек (JupyterLab, TensorFlow та інші); пісочниці (Sandboxie, Cuckoo);

	антивіруси (Eset, Kaspersky, Avast); віртуальне лабораторне середовище Cisco Packet Tracer; SIEM система AlienVault OSSIM; перехоплювач мережевих пакетів Wireshark; сканери вразливостей (Nessus, Greenbone); інструменти криптографії та криптоаналізу (QuickCrypto, Crypto Bench, CrypTool); інструменти стеганографії (QuickStego, Xiao steganography, Steghide); Digital Forensics Framework для комп'ютерної криміналістики; редактори коду Notepad++, Visual Studio Code, C\C++; середовища спільної розробки і тестування програмного забезпечення TestRail, Jira; ELK стек; доступ до демо-середовищ програмного забезпечення для кібербезпеки Cisco (Umbrella, Advanced Malware Protection, Next Generation Firewall, Tetration, Meraki). Здобувачі вищої освіти забезпечені гуртожитком. Наявна соціально-побутова інфраструктура: їдальня, медичний пункт, бібліотека, басейн, спортивний комплекс, актова зала.
Інформаційне та навчально-методичне забезпечення	Відповідає вимогам щодо навчально-методичного та інформаційного 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»). 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 впровадження інформаційних технологій в освітній процес. Наявний інституційний репозитарій ELARTU, де розміщені електронні інформаційно-методичні розробки (збірники статей, збірники конференцій, методичні розробки, кваліфікаційні роботи випускників та інше). Наявний електронний каталог бібліотеки університету, де можна здійснити швидкий пошук книг, методичних розробок та інших матеріалів, що знаходяться в фондах бібліотеки у паперовій формі. Бібліотека університету першою серед українських бібліотек ВНЗ у 2011 році стала членом Міжнародної асоціації науково-техічних бібліотек університетів (IATUL). Також бібліотека є колективним членом Української бібліотечної асоціації. Інституційний репозитарій ELARTU активно продовжує наповнення фондів. На початок 2021 року у репозитарії опубліковано понад 30 000 матеріалів. Згідно рейтингу Webometrics (http://www.webometrics.info/) станом на 2021 р. інституційний репозитарій ELARTU займає 10 місце серед українських репозитаріїв.

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

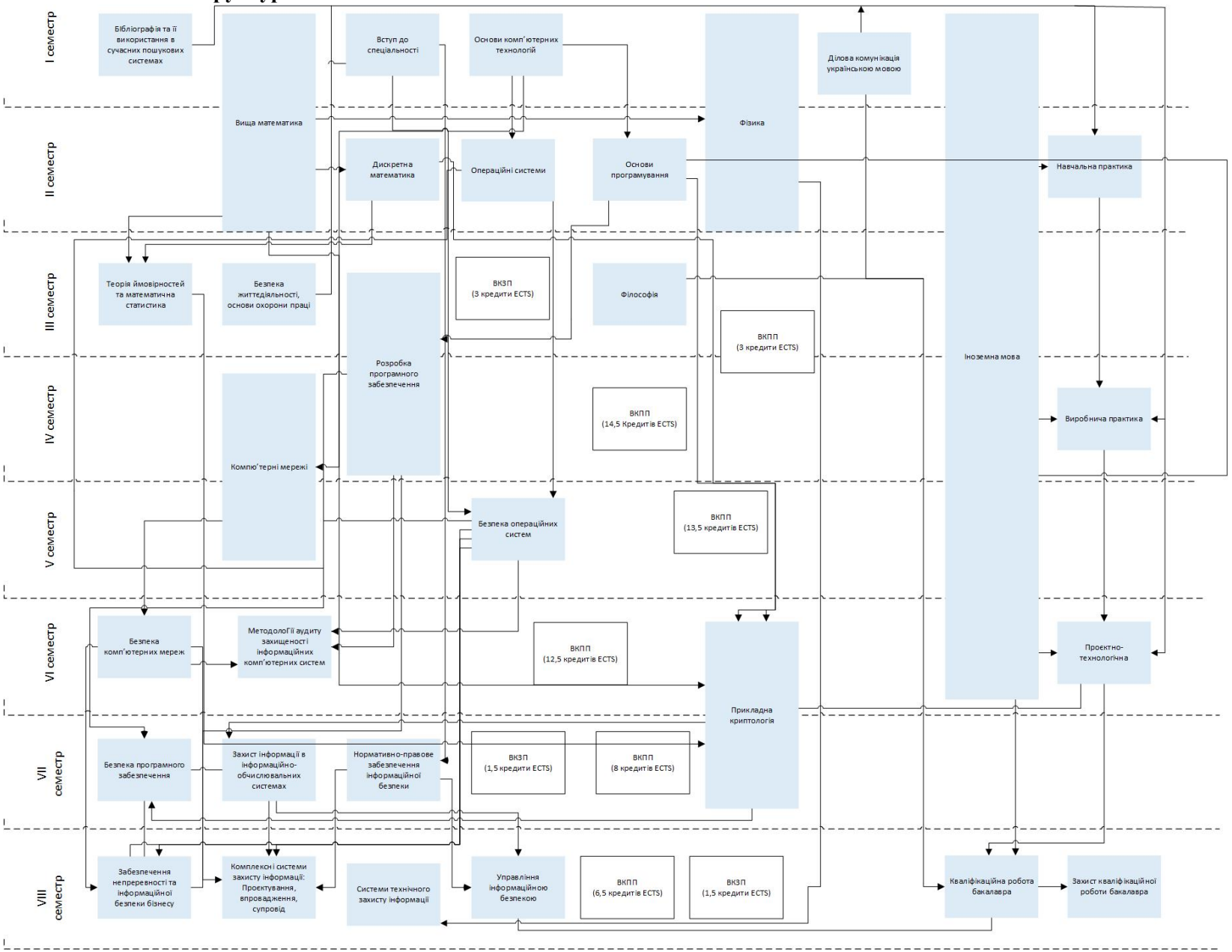
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумк. контролю
Обов'язкові компоненти загальної підготовки (ОКЗП)			
1. Цикл загальної підготовки			
ОКЗП1	Безпека життєдіяльності, основи охорони праці	4	е
ОКЗП2	Бібліографія та її використання в сучасних пошукових системах	4	з
ОКЗП3	Вища математика Передбачені індивідуальні завдання (у двох семестрах)	10	з, е
ОКЗП4	Ділова комунікація українською мовою	4	з
ОКЗП5	Іноземна мова Передбачені індивідуальні завдання (у двох семестрах)	26	з, е
ОКЗП6	Філософія	4	з
ОКЗП7	Теорія ймовірностей та математична статистика Передбачено індивідуальне завдання	4	е
ОКЗП8	Фізика Передбачені індивідуальні завдання (у двох семестрах)	8	е
	Всього за цикл	**64**	
Обов'язкові компоненти професійної підготовки (ОКПП)			
2. Цикл професійної підготовки			
ОКПП1	Вступ до спеціальності	4	е
ОКПП2	Забезпечення неперервності та інформаційної безпеки бізнесу	4	е
ОКПП3	Безпека комп'ютерних мереж. Передбачено курсову роботу	5	е, КР
ОКПП4	Безпека операційних систем Передбачено курсову роботу	5	е, КР
ОКПП5	Безпека програмного забезпечення	5	е
ОКПП6	Дискретна математика Передбачено індивідуальне завдання	5	е
ОКПП7	Захист інформації в інформаційно-комунікаційних системах	4,5	з

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумк. контролю
ОКПП8	Комплексні системи захисту інформації: проєктування, впровадження, супровід Передбачено курсовий проєкт	4	е, КП
ОКПП9	Комп'ютерні мережі Передбачено курсовий проєкт	10	е, КП
ОКПП10	Операційні системи	5	е
ОКПП11	Основи комп’ютерних технологій	4	е
ОКПП12	Основи програмування	4	з
ОКПП13	Прикладна криптологія Передбачено курсовий проєкт	9	е, КП
ОКПП14	Методології аудиту захищеності інформаційних комп’ютерних систем	4	е
ОКПП15	Розробка програмного забезпечення	9,5	е
ОКПП16	Системи технічного захисту інформації	4	е
ОКПП17	Нормативно-правове забезпечення інформаційної безпеки	4	е
ОКПП18	Управління інформаційною безпекою	4	е
	Всього за цикл	**94**	
Практична підготовка			
ОКПП19	Навчальна практика	3	диф.з.
ОКПП20	Виробнича практика	3	диф.з.
ОКПП21	Проєктно-технологічна практика	3	диф.з.
	Всього за практичну підготовку	**9**	
	Всього за професійну та практичну підготовку	**103**	
Загальний обсяг обов'язкових компонентів:		**167**	
Вибіркові компоненти освітньо-професійної програми			
Здобувачі вищої освіти обирають освітні вибіркові компоненти із запропонованого переліку у середовищі електронного навчання ТНТУ Atutor http://dl.tntu.edu.ua/login.php. Доступ до переліку вибіркових навчальних дисциплін мають усі здобувачі вищої освіти, зареєстровані у середовищі електронного навчання ТНТУ Atutor.			
Рекомендовані кафедрою групи вибору вибіркових дисциплін професійної підготовки			
Вибірковий блок 1. Математичне, програмне та апаратне забезпечення для побудови систем виявлення вторгнень			
ВКПП1	Іноземна мова професійно-ділового спрямування	3	з

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумк. контролю
ВКПП2	Навички міжособистісного спілкування, побудова команд і робота в команді	3	з
ВКПП3	Організація баз даних	4,5	е
ВКПП4	Веб-технології	4,5	з
ВКПП5	Електроніка	4	з
ВКПП6	Інтелектуальний аналіз даних	4,5	е
ВКПП7	Комп'ютерна стеганографія	3	з
ВКПП8	Методи та системи штучного інтелекту	4	е
ВКПП9	Обробка сигналів та зображень	3,5	з
ВКПП10	Основи інтернету речей	4,5	з
ВКПП11	Мережеве програмування	3	з
ВКПП12	Основи теорії кіл, сигнали та процеси в електроніці	3	е
ВКПП13	Програмування для мобільних пристроїв	4,5	з
ВКПП14	Теорія інформації та кодування	4,5	з
ВКПП15	Управління ІТ-проєктами	3,5	з
ВКПП16	Чисельні методи	3	з
ВКПП17	Якість і тестування програмного забезпечення	4	з
Вибірковий блок 2. Етичний хакінг			
ВКПП1	Іноземна мова професійного спрямування	3	з
ВКПП2	Психологія тімбілдингу	3	з
ВКПП3	Бази даних та їх захист	4,5	е
ВКПП4	Методи та засоби розробки веб-систем	4,5	з
ВКПП5	Електротехніка та електроніка	4	з
ВКПП6	Тестування на проникнення	4,5	е
ВКПП7	Безпека IoT пристроїв і систем	3	з
ВКПП8	Data Mining і Deep Learning	4	е
ВКПП9	Цифрова обробка сигналів в інформаційних системах	3,5	з
ВКПП10	Архітектура та технології інтернету речей	4,5	з
ВКПП11	Основи хмарних технологій	3	з
ВКПП12	Теорія кіл, сигналів і процесів в інформаційному та кіберпросторах	3	е
ВКПП13	Програмування на мові JAVA	4,5	з
ВКПП14	Безпека хмарних сервісів	4,5	з

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумк. контролю
ВКПП15	Безпека Web-ресурсів	3,5	з
ВКПП16	Комп'ютерна криміналістика	3	з
ВКПП17	Автоматизоване тестування програмного забезпечення	4	з
Загальний обсяг вибіркових компонентів:		**64**	
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 ОП.



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньо-професійної програми «Кібербезпека» спеціальності 125 «Кібербезпека» проводиться у формі публічного захисту кваліфікаційної роботи бакалавра та завершується видачею документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації бакалавра з кібербезпеки за спеціальністю 125 «Кібербезпека».

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.

Кваліфікаційна робота передбачає розв’язання складного спеціалізованого завдання або практичної проблеми в галузі кібербезпеки, що характеризується комплексністю та невизначеністю умов і потребує застосування теорій та методів кібербезпеки. У кваліфікаційній роботі не повинно бути академічного плагіату, фальсифікації та фабрикації. Кваліфікаційна робота повинна бути оприлюднена в інституційному репозитарії ТНТУ, ELARTU: http://elartu.tntu.edu.ua/.

4. Матриця відповідності програмних компетентностей навчальним компонентам освітньо-професійної програми бакалаврів зі спеціальності 125 «Кібербезпека»

	Обов'язкові компоненти																										Атестація	
	ОКЗП1	ОКЗП2	ОКЗП3	ОКЗП4	ОКЗП5	ОКЗП6	ОКЗП7	ОКЗП8	ОКПП1	ОКПП2	ОКПП3	ОКПП4	ОКПП5	ОКПП6	ОКПП7	ОКПП8	ОКПП9	ОКПП10	ОКПП11	ОКПП12	ОКПП13	ОКПП14	ОКПП15	ОКПП16	ОКПП17	ОКПП18	ОКПП19	ОКПП20	ОКПП21	А1	А2
ЗК1	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	
ЗК2		•	•					•	•	•	•	•	•	•	•	•		•	•		•	•	•	•	•	•	•	•	•	•
ЗК3		•		•	•			•										•	•										•	•
ЗК4		•	•		•			•	•	•	•	•	•		•	•		•	•		•	•	•	•	•	•	•	•	•	
ЗК5		•	•		•		•	•						•	•	•	•	•	•		•	•	•		•	•	•	•	•	
ЗК6						•										•									•					
ЗК7	•					•																								
ФК1																•					•			•	•	•	•		•	
ФК2			•						•	•	•	•	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•	
ФК3									•	•	•	•	•		•	•		•	•		•	•	•	•					•	
ФК4									•	•	•	•	•			•										•			•	
ФК5										•					•	•					•			•		•			•	
ФК6										•					•		•												•	
ФК7								•		•				•	•											•			•	
ФК8										•												•				•			•	
ФК9										•									•							•		•	•	
ФК10														•							•			•				•	•	
ФК11										•					•			•	•			•				•	•	•	•	
ФК12		•						•	•	•	•	•	•								•	•		•		•		•	•	

5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньо-професійної програми бакалаврів зі спеціальності 125 «Кібербезпека»

	Обов'язкові компоненти																										Атестація	
	ОКЗП1	ОКЗП2	ОКЗП3	ОКЗП4	ОКЗП5	ОКЗП6	ОКЗП7	ОКЗП8	ОКПП1	ОКПП2	ОКПП3	ОКПП4	ОКПП5	ОКПП6	ОКПП7	ОКПП8	ОКПП9	ОКПП10	ОКПП11	ОКПП12	ОКПП13	ОКПП14	ОКПП15	ОКПП16	ОКПП17	ОКПП18	ОКПП19	ОКПП20	ОКПП21	А1	А2
ПР1		•		•	•				•																		•	•	•		•
ПР2	•	•	•				•		•	•				•												•	•	•	•	•	
ПР3		•	•						•					•							•					•	•	•	•	•	
ПР4			•			•	•	•	•					•							•					•			•	•	
ПР5			•				•		•							•		•	•						•						
ПР6		•	•			•	•		•					•	•						•				•			•	•	•	
ПР7										•											•				•	•	•	•	•		
ПР8																									•	•					
ПР9										•									•										•	•	
ПР10						•									•		•			•						•	•	•	•	•	
ПР11						•				•					•		•		•					•		•				•	
ПР12									•																			•	•	•	
ПР13																	•														
ПР14										•						•		•			•	•	•						•		
ПР15										•				•		•	•	•	•		•		•				•	•	•	•	
ПР16																•														•	
ПР17										•	•																		•	•	
ПР18									•	•	•	•	•						•		•			•					•	•	
ПР19									•	•		•	•	•		•		•			•			•					•	•	
ПР20										•		•	•															•	•	•	

	Обов'язкові компоненти																												Атестація	
	ОКЗП1	ОКЗП2	ОКЗП3	ОКЗП4	ОКЗП5	ОКЗП6	ОКЗП7	ОКЗП8	ОКПП1	ОКПП2	ОКПП3	ОКПП4	ОКПП5	ОКПП6	ОКПП7	ОКПП8	ОКПП9	ОКПП10	ОКПП11	ОКПП12	ОКПП13	ОКПП14	ОКПП15	ОКПП16	ОКПП17	ОКПП18	ОКПП19	ОКПП20	ОКПП21	А1	А2
ПР21										•		•	•											•				•	•	
ПР22										•	•	•	•			•		•	•					•					•	•	
ПР23										•	•	•	•								•	•		•					•	•	
ПР24										•																•				•	
ПР25										•		•	•		•														•	•	
ПР26											•				•															•	
ПР27										•	•	•			•									•					•	•	
ПР28															•							•						•		•	
ПР29															•							•								•	
ПР30															•						•	•				•		•	•	•	
ПР31										•		•	•		•						•			•						•	
ПР32										•		•	•		•														•	•	
ПР33										•																•			•	•	
ПР34										•																•			•	•	
ПР35																•														•	
ПР36								•																•						•	
ПР37								•																•						•	
ПР38								•																•						•	
ПР39																•								•						•	
ПР40								•																•						•	

	Обов'язкові компоненти																											Атестація	
	ОКЗП1	ОКЗП2	ОКЗП3	ОКЗП4	ОКЗП5	ОКЗП6	ОКЗП7	ОКЗП8	ОКППІ1	ОКППІ2	ОКППІ3	ОКППІ4	ОКППІ5	ОКППІ6	ОКППІ7	ОКППІ8	ОКППІ9	ОКППІ10	ОКППІ11	ОКППІ12	ОКППІ13	ОКППІ14	ОКППІ15	ОКППІ16	ОКППІ17	ОКППІ18	ОКППІ19	ОКППІ20	ОКППІ21	А1	А2
ПР41										•																•			•	•	
ПР42										•																•			•	•	
ПР43																									•					•	
ПР44										•																			•	•	
ПР45										•																•				•	
ПР46														•												•			•	•	
ПР47																					•								•	•	
ПР48										•											•					•				•	
ПР49										•																				•	
ПР50										•	•	•	•		•															•	
ПР51										•	•	•	•		•															•	
ПР52										•		•	•						•											•	
ПР53																							•	•						•	
ПР54						•																			•						
ПР55					•																								•	•	
ПР56										•																			•	•	
ПР57																							•							•	