МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ПРОЄКТ

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА»

першого рівня вищої освіти

за спеціальністю 125 «Кібербезпека»

галузі знань 12 «Інформаційні технології»

кваліфікація: бакалавр з кібербезпеки

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Голова вченої ради

_____ А. І. Крисоватий

(протокол № __ від "___"_____ 2020 р.)

Освітня програма вводиться в дію з _____2020 р.

Ректор_____ /_____/

(наказ № __ від "___"_____ 2020 р.)

Тернопіль 2020

1. Профіль освітньої програми зі спеціальності 125 "Кібербезпека"

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Тернопільський національний економічний університет, Факультет комп'ютерних інформаційних технологій, кафедра кібербезпеки.
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	бакалавр, бакалавр з кібербезпеки
Офіційна назва освітньої програми	125 "Кібербезпека"
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	Впровадження в 2017 році
Цикл/рівень	Перший (бакалаврський) рівень / FQ-EHEA – перший цикл, EQF LLL – 6 рівень, НРК – 7 рівень
Передумови	Повна загальна середня освіта
Мова(и) викладання	Українська
Термін дії освітньої програми	2021 р.
Інтернет-адреса постійного розміщення опису освітньої програми	https://www.tneu.edu.ua
2 – Мета освітньої програми	
Підготовка фахівців, здатних розробляти і використовувати технології інформаційної безпеки та кібербезпеки.	
3 - Характеристика освітньої програми	
Опис предметної області	Об'єкти професійної діяльності випускників: – 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 з кібербезпеки.
Основний фокус освітньої програми	Здобуття вищої освіти в галузі 12 «Інформаційні технології», спеціальності «Кібербезпека». Ключові слова: кібернетична безпека, криптографія, інформаційна безпека, комп'ютерні атаки, безпека вуб-ресурсів, тестування безпеки.
Особливості програми	Інтеграція програмно-апаратних засобів виявлення, моніторингу та забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій шифрування даних, виявлення вразливостей в програмному забезпеченні та апаратних засобах. Високий рівень практичної підготовки фахівців забезпечується розвиненою міжнародною співпрацею в науковій і освітній сферах, наявністю спеціалізованих лабораторій.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець може займати первинні посади (за ДК 003:2010): 3439 (24771). Фахівець із організації інформаційної безпеки. International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT).
Подальше навчання	Можливість здобуття освіти на другому (магістерському) рівні
5 – Викладання та оцінювання	
Викладання та навчання	Студентсько-центроване навчання, самонавчання, проблемно-орієнтоване навчання, кредитно-трансферна система організації навчання, електронне навчання в системі Moodle, навчання на основі досліджень. навчання через лабораторну практику, дослідницької роботи з використанням елементів дистанційного

	навчання, розв'язування прикладних задач, виконання проектів, навчальних та виробничих практик, курсових робіт та кваліфікаційної роботи.
Оцінювання	Модульний контроль, заліки, усні екзамени, тести, поточне опитування, комплексні практичні індивідуальні завдання, тренінги, міждисциплінарна курсова робота, звіт про проходження переддипломної практики, кваліфікаційна робота тощо.
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 (КЗ)	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Фахові компетентності спеціальності (КФ)	КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. К 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.

	КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
7 – Програмні результати навчання	
	ПРН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ПРН7. Діяти на основі законодавчої та нормативно правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. ПРН9. впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПРН9. виконувати аналіз та декомпозицію інформаційно телекомунікаційних систем. ПРН10. виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. ПРН11. Розробляти моделі загроз та порушника.

	ПРН12. Аналізувати проекти інформаційно телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. ПРН13. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно телекомунікаційних системах програмно апаратними засобами та давати оцінку результативності якості прийнятих рішень. ПРН14. Використовувати сучасне програмно апаратне забезпечення інформаційно комунікаційних технологій. ПРН15. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно правових документів. ПРН16. Забезпечувати процеси захисту та функціонування інформаційно телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. ПРН17. Використовувати програмні та програмно апаратні комплекси захисту інформаційних ресурсів. ПРН18. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно телекомунікаційних системах; ПРН19. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно телекомунікаційних системах. ПРН20. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах. ПРН21. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН22. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах. ПРН23. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). ПРН24. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту. ПРН25. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно телекомунікаційних

	(автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем. ПРН26. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно телекомунікаційних (автоматизованих) системах. ПРН27. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки. ПРН28. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів. ПРН29. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно телекомунікаційних систем. ПРН30. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно телекомунікаційних систем. ПРН31. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. ПРН32. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. ПРН33. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. ПРН34. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН35. Виявляти небезпечні сигнали технічних засобів. ПРН36. Вимірювати параметри небезпечних 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. ПРН37. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН38. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ПРН39. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

	ПРН40. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. ПРН41. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ПРН42. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН43. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами. ПРН44. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик орієнтованому контролі доступу до інформаційних активів. ПРН45. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно телекомунікаційних системах. ПРН46. Вирішувати задачі захисту інформації, що обробляється в інформаційно телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН47. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно телекомунікаційних системах. ПРН48. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно телекомунікаційних системах. ПРН49. Забезпечувати функціонування програмних та програмно апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично сигнатурних). ПРН50. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно телекомунікаційних системах. ПРН51. Використовувати інструментарій для моніторингу процесів в інформаційно телекомунікаційних системах. ПРН52. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. ПРН53. 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	Всі науково-педагогічні працівники, залучені до реалізації освітньо-професійної програми мають науковий ступінь і/або вчене звання та підтверджений рівень наукової і професійної активності, що відповідає вимогам ліцензійних умов. До освітнього процесу можуть залучатися фахівці з іноземних країн.
Матеріально-технічне забезпечення	Освітній процес здійснюється в спеціально обладнаних аудиторіях і лабораторіях, які відповідають санітарно-технічним нормам і оснащених сучасним навчальним обладнанням,

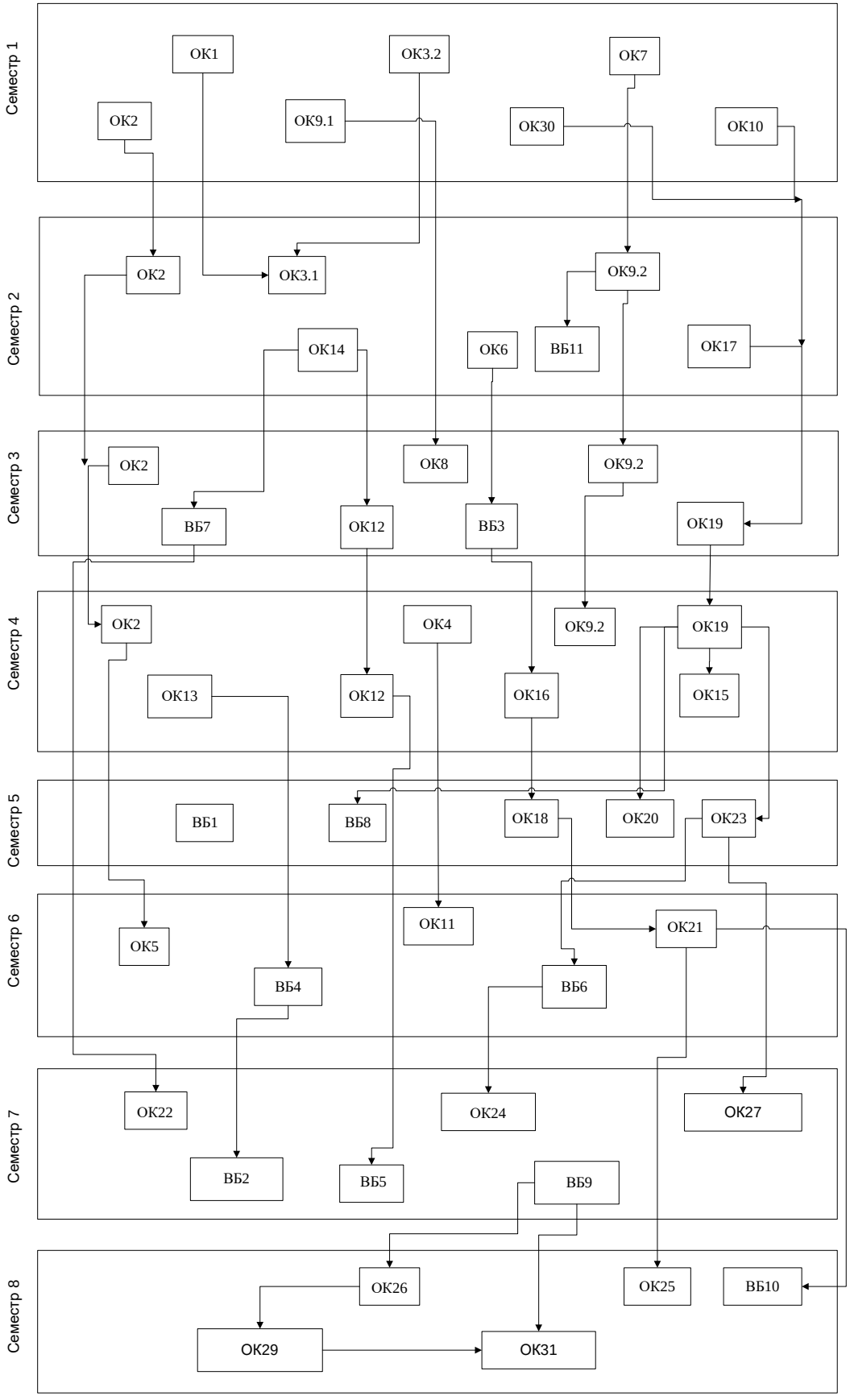
	мультимедійною, комп'ютерною технікою та спеціалізованим програмним забезпеченням, з можливістю постійного доступу до мережі Internet та внутрішньої мережі ТНЕУ. Комп'ютерна лабораторія обладнана наступним устаткуванням: проектор мультимедійний BenQ TH671ST (1 шт.); комп'ютери на базі процесора Intel Xeon W3550, (10 шт): системний блок Precsion T3500 Westmere. N-serie; монітор Dell E2211H 21.5in.
Інформаційне та навчально-методичне забезпечення	Онлайн-бібліотека, електронні навчально-методичні комплекси дисциплін, робочі програми дисциплін, методичні рекомендації та вказівки до вивчення дисциплін, написання міждисциплінарної курсової роботи, проходження практики і написання випускної кваліфікаційної роботи. Офіційний веб-сайт https://www.tneu.edu.ua/ містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти, тощо.
9 – Академічна мобільність	
Національна кредитна мобільність	Відповідно до угод ТНЕУ.
Міжнародна кредитна мобільність	Відповідно до угод ТНЕУ та угод про міжнародну академічну мобільність (Еразмус+ К1)
Навчання іноземних здобувачів вищої освіти	Відповідно до нормативно-правових документів.

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

2.1. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК 1.	Українська мова	2	
ОК 2.	Історія України	4	
ОК 3.	Іноземна мова	7	
ОК 4	Фахова іноземна мова	1	
ОК 5	Охорона праці та навколишнього середовища	4	
ОК 6	Філософія	4	
ОК 7	Політологія	3	
ОК 8	Дискретна математика	5	
ОК 9	Теорія ймовірності та математична статистика	5	
ОК 10	Лінійна алгебра та аналітична геометрія	5	
ОК 11	Математичний аналіз	11	
ОК 12	Фізика	5	
ОК 13	Основи програмування	5	
ОК 14	Алгоритми та структури даних	5	
ОК 15	Операційні системи	5	
ОК 16	Програмування I	5	
ОК 17	Програмування II	7	
ОК 18	Архітектура комп'ютерів та систем	5	
ОК 19	Комп'ютерні мережі	6	
ОК 20	Оцінка та управління ризиками	5	
ОК 21	Кібернетична безпека	8	
ОК 22	Криптографія	8	
ОК 23	Стандарти та нормативно-правове забезпечення кібербезпеки	5	
ОК 24	Мережева безпека	6	
ОК 25	Менеджмент інформаційною безпекою	5	
ОК 26	Безпека Web ресурсів	5	
ОК 27	Тестування безпеки	7	
ОК 28	Технічні засоби захисту інформації	5	
ОК 29	Комплексні системи захисту інформації	6	
ОК 30	Курсова робота з дисципліни "Кібернетична безпека"	3	
ОК 31	Міждисциплінарний курсовий проект	3	
ОК 32	Проектно-технологічна практика	5	
ОК 33	Стажування (виробнича практика)	9	
ОК 34	Випускна кваліфікаційна робота	6	
Загальний обсяг обов'язкових компонент:		**180**	
Вибіркові компоненти ОП *			
ВБ 1-12		60	–
Загальний обсяг вибіркових компонент:		60	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

2.2. **Структурно-логічна схема ОП**



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності 125 "Кібербезпека" проводиться у формі захисту кваліфікаційної бакалаврської роботи та завершується видачею документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації: бакалавр з кібербезпеки.

Атестація здійснюється відкрито і публічно.

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	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34
КЗ 1																														•	•	•	•	•
КЗ 2																					•									•	•	•	•	•
КЗ 3	•		•	•																														
КЗ 4																														•	•	•	•	•
КЗ 5								•	•	•	•																			•	•	•	•	•
КЗ 6						•	•																											
КЗ 7		•			•																													
КФ 1																						•								•	•	•	•	•
КФ 2																			•		•			•						•	•	•	•	•
КФ 3													•	•	•	•	•											•	•	•	•	•	•	•
КФ 4																				•					•					•	•	•	•	•
КФ 5								•														•								•	•	•	•	•
КФ 6															•					•				•	•	•				•	•	•	•	•
КФ 7																												•	•	•	•	•	•	•
КФ 8									•											•			•		•					•	•	•	•	•
КФ 9																								•	•					•	•	•	•	•
КФ 10												•	•			•	•					•								•	•	•	•	•
КФ 11																		•									•		•	•	•	•	•	•
КФ 12															•			•									•		•	•	•	•	•	•

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	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34
ПРН 1	•		•	•																										•	•	•	•	•
ПРН 2																														•	•	•	•	•
ПРН 3																														•	•	•	•	•
ПРН 4									•																				•	•	•	•	•	•
ПРН 5									•												•									•	•	•	•	•
ПРН 6						•			•	•	•																			•	•	•	•	•
ПРН 7																							•							•	•	•	•	•
ПРН 8																							•							•	•	•	•	•
ПРН 9																			•					•						•	•	•	•	•
ПРН 10																		•												•	•	•	•	•
ПРН 11																				•	•									•	•	•	•	•
ПРН 12																			•											•	•	•	•	•
ПРН 13																					•							•		•	•	•	•	•
ПРН 14																			•		•									•	•	•	•	•
ПРН 15																													•	•	•	•	•	•

ПРН 16																								•		•				•	•	•	•	•
ПРН 17																								•					•	•	•	•	•	•
ПРН 18																						•		•						•	•	•	•	•
ПРН 19																	•	•								•				•	•	•	•	•
ПРН 20																											•			•	•	•	•	•
ПРН 21																					•			•						•	•	•	•	•
ПРН 22																					•									•	•	•	•	•
ПРН 23																								•						•	•	•	•	•
ПРН 24																								•						•	•	•	•	•
ПРН 25																			•	•										•	•	•	•	•
ПРН 26																						•		•						•	•	•	•	•
ПРН 27																											•			•	•	•	•	•
ПРН 28																				•							•			•	•	•	•	•
ПРН 29																											•			•	•	•	•	•
ПРН 30																						•								•	•	•	•	•
ПРН 31																									•					•	•	•	•	•
ПРН 32																				•										•	•	•	•	•
ПРН 33																									•				•	•	•	•	•	•
ПРН 34																													•	•	•	•	•	•
ПРН 35																												•		•	•	•	•	•

ПРН 36																												•		•	•	•	•	•
ПРН 37																													•	•	•	•	•	•
ПРН 38																												•	•	•	•	•	•	•
ПРН 39																												•	•	•	•	•	•	•
ПРН 40															•									•						•	•	•	•	•
ПРН 41																										•	•			•	•	•	•	•
ПРН 42																							•							•	•	•	•	•
ПРН 43																			•											•	•	•	•	•
ПРН 44																				•					•					•	•	•	•	•
ПРН 45																				•	•									•	•	•	•	•
ПРН 46																						•								•	•	•	•	•
ПРН 47																					•	•								•	•	•	•	•
ПРН 48																		•						•						•	•	•	•	•
ПРН 49																					•			•				•		•	•	•	•	•
ПРН 50															•									•			•			•	•	•	•	•
ПРН 51																			•					•						•	•	•	•	•
ПРН 52													•	•		•	•									•	•			•	•	•	•	•
ПРН 53		•			•	•	•																											