МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА»

першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Голова вченої ради

_____ Андрій КРИСОВАТИЙ

(протокол № 9 від "15" вересня 2022 р.)

Освітня програма вводиться в дію з вересня 2022 р.

Ректор _____ Андрій КРИСОВАТИЙ

(наказ № 216 від "20" вересня 2022 р.)

Тернопіль - 2022

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

«КІБЕРБЕЗПЕКА»

першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Перший проректор	*Микола ШИНКАРИК*
Директор навчально-наукового центру моніторингу якості освіти та методичної роботи	*Сергій ШАНДРУК*
Декан факультету	*Микола ДИВАК*
Голова ГЗС	*Василь ЯЦКІВ*
Завідувач кафедри	*Василь ЯЦКІВ*
Гарант ОПП	*Ігор ЯКИМЕНКО*

ПЕРЕДМОВА

Розроблено робочою групою у складі:

1. Яцків В. В. – д.т.н., професор, завідувач кафедри кібербезпеки ЗУНУ;
2. Касянчук М.М. – д.т.н., доцент, доцент кафедри кібербезпеки ЗУНУ;
3. Якименко І. З. – к.т.н., доцент, доцент кафедри кібербезпеки ЗУНУ;
4. Івасьєв С. В. – к.т.н., доцент, доцент кафедри кібербезпеки ЗУНУ
5. Возняк С.І. заступник директора з питань експлуатації та безпеки мереж, ЗУНУ;
6. Бараннік Б.О. – студент групи КБ-41, спеціальності Кібербезпека, ЗУНУ.

Відгуки на освітньо-професійну програму:

1. Стрілецький М.В., директор ТОВ «АПІКО Україна».

2. Волощук О.Б., к.т.н., доцент, координатор освітньої програми в Distributed Lab.

Рецензії на освітньо-професійну програму:

1. Максимович В.М., д.т.н., професор, завідувач кафедри безпеки інформаційних технологій, Національний університет «Львівська політехніка».

2. Загородна Н.В., к.т.н., доцент, завідувач кафедри кібербезпеки, Тернопільський національний технічний університет.

1. Профіль освітньо-професійної програми зі спеціальності 125 "Кібербезпека"

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Західноукраїнський національний університет, Факультет комп'ютерних інформаційних технологій, кафедра кібербезпеки.
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр, бакалавр з кібербезпеки
Офіційна назва освітньої програми	Освітньо-професійна програма "Кібербезпека"
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС (на базі повної загальної середньої освіти), 180 (на базі молодшого бакалавра (молодшого спеціаліста), термін навчання 3 роки 10 місяців
Наявність акредитації	Так, 2021 рік
Цикл/рівень	Перший (бакалаврський) рівень / НРК України– 6 рівень, FQ-EHEA – перший цикл, EQF LLL – 6 рівень.
Передумови	Повна загальна середня освіта, освітні ступені. «молодший бакалавр», «молодший спеціаліст»
Мова(и) викладання	Українська
Термін дії освітньої програми	2021 р.
Інтернет-адреса постійного розміщення опису освітньої програми	https://www.wunu.edu.ua
2 – Мета освітньої програми	
Підготовка висококваліфікованих, конкурентоспроможних фахівців здатних розробляти і використовувати технології інформаційної безпеки та/або кібербезпеки; які мають теоретичні знання та сформоване критичне мислення; володіють сучасними криптографічними методами захисту інформації; методами захисту мережевої інфраструктури та Web ресурсів; вміють безконфліктно та продуктивно працювати в командах щодо розв'язання проблем та прийняття рішень з питань захисту інформації, безперебійного функціонування, оперативного реагування та відновлення роботи після несанкціонованого втручання в інформаційні системи.	
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. Враховуючи різке збільшення кібератак на мережеву інфраструктуру державних та приватних організацій ОПП орієнтується на поглиблене вивчення мережевої безпеки, включаючи тестування на проникнення, а також на захисті web ресурсів, так як більшість зовнішніх атак на корпоративні інформаційні системи націлені саме на вразливості веб-додатків.
Основний фокус освітньої програми	ОП фокусується на формуванні та розвитку у здобувачів професійних компетентностей (застосовувати методи криптографічного захисту інформації; пошук, оцінювання вразливостей та захист Web-додатків; здійснювати тести на проникнення в комп'ютерні системи та мережі шляхом виявлення та експлуатації наявних вразливостей), поєднання яких створює умови для вирішення складних задач щодо захисту програмного забезпечення, мережевої інфраструктури та Web - ресурсів. Ключові слова: кібернетична безпека, криптографія, безпека комп'ютерних мереж, управління інформаційною безпекою, безпека веб-ресурсів, тестування на проникнення.
Особливості програми	Інноваційність, імплементація курсів мережевої академії Cisco в навчальний процес, практична орієнтованість на вирішення актуальних завдань та проблем у інформаційної та/або кібербезпеки. Високий рівень практичної підготовки фахівців забезпечується розвиненою міжнародною співпрацею в науковій і освітній сферах, виконання науково-дослідних проєктів, залученням викладачів практиків, наявністю спеціалізованих лабораторій.

4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець може займати первинні посади (за ДК 003:2010): 2132.2- Розробник систем захисту інформації; 2139.2- Адміністратор мереж і систем; Аналітик з безпеки інформаційно-телекомунікаційних систем; Аналітик загроз безпеки; Аналітик систем захисту інформації та оцінки вразливостей; Аудитор інформаційних технологій Фахівець з криптографічного захисту інформації; Фахівець з питань безпеки (інформаційно-комунікаційні технології); Фахівець з тестування систем захисту інформації; Фахівець з технічного захисту інформації. International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT).
Подальше навчання	Бакалавр може продовжувати навчання на другому (магістерському) рівні вищої освіти
5 – Викладання та оцінювання	
Викладання та навчання	Студентсько-центроване навчання, самонавчання, проблемно-орієнтоване навчання, кредитно-трансферна система організації навчання, навчання з використанням системи дистанційного навчання Moodle, викладання курсів мережевої академії Cisco, навчання на основі досліджень, навчання через лабораторну практику, використання онлайн лабораторій: TryHackMe, RootMe, HackTheBox, використанням елементів дуальної освіти, 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. Атестація здійснюється у формі публічного захисту кваліфікаційної випускної роботи.
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. КФ 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. КФ 13. Здатність виконувати оцінку якості криптографічного захисту інформації в інформаційно-телекомунікаційних системах. КФ 14. Здатність здійснювати пошук, оцінювання вразливостей та захист WEB-додатків. КФ 15. Здатність здійснювати тести на проникнення в комп’ютерні системи та мережі шляхом виявлення та експлуатації наявних вразливостей.
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.
ПРН10. Виконувати аналіз та декомпозицію інформаційно телекомунікаційних систем.
ПРН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
ПРН12. Розробляти моделі загроз та порушника.
ПРН13. Аналізувати проекти інформаційно телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно телекомунікаційних системах програмно апаратними засобами та давати оцінку результативності якості прийнятих рішень.
ПРН15. Використовувати сучасне програмно апаратне забезпечення інформаційно комунікаційних технологій.
ПРН16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно правових документів.
ПРН17. 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.
ПРН18. Використовувати програмні та програмно апаратні комплекси захисту інформаційних ресурсів.
ПРН19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно телекомунікаційних системах;
ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно телекомунікаційних системах.
ПРН21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах.
ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до

інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах.
ПРН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
ПРН25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
ПРН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
ПРН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно телекомунікаційних (автоматизованих) системах.
ПРН28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно телекомунікаційних систем.
ПРН31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно телекомунікаційних систем.
ПРН32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
ПРН33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
ПРН34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
ПРН35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН36. Виявляти небезпечні сигнали технічних засобів.
ПРН37. Вимірювати параметри небезпечних та 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.
ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
ПРН40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на

інциденти інформаційної і/або кібербезпеки. ПРН43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН44. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами. ПРН45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик орієнтованому контролі доступу до інформаційних активів. ПРН46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно телекомунікаційних системах. ПРН47. Вирішувати задачі захисту інформації, що обробляється в інформаційно телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно телекомунікаційних системах. ПРН49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно телекомунікаційних системах. ПРН50. Забезпечувати функціонування програмних та програмно апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично сигнатурних). ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно телекомунікаційних системах. ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно телекомунікаційних системах. ПРН53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. ПРН54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ПРН55. Здійснювати загальну оцінку якості криптографічного захисту інформації в інформаційно-телекомунікаційних системах. ПРН56. Здійснювати пошук, оцінювання вразливостей та захист WEB-додатків. ПРН57. Здійснювати оцінку можливості проникнення в інформаційні системи та мережі шляхом виявлення та експлуатації наявних вразливостей.	
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. Усі науково-педагогічні працівники мають показники академічної та професійної кваліфікації відповідно до дисципліни, викладання якої вони забезпечують.
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 ЗУНУ. 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.; лабораторні стенди на базі одноплатних комп'ютерів Raspberry Pi – 15 шт.; цифровий осцилограф SIGLENT SDS1202X+;

	маршрутизатор VPN Router Cisco SB RV320 Dual Gigabit WAN VPN; детектор електромагнітного випромінювання СС308 +
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. Вільний доступ через сайт ЗУНУ до баз даних періодичних фахових наукових видань (в тому числі, англійською мовою) забезпечується участю бібліотеки університету у консорціуму ElibUkr.
9 – Академічна мобільність	
Національна кредитна мобільність	Відповідно до угод ЗУНУ.
Міжнародна кредитна мобільність	Відповідно до угод ЗУНУ та угод про міжнародну академічну мобільність (Еразмус+ К1)
Навчання іноземних здобувачів вищої освіти	Відповідно до нормативно-правових документів.

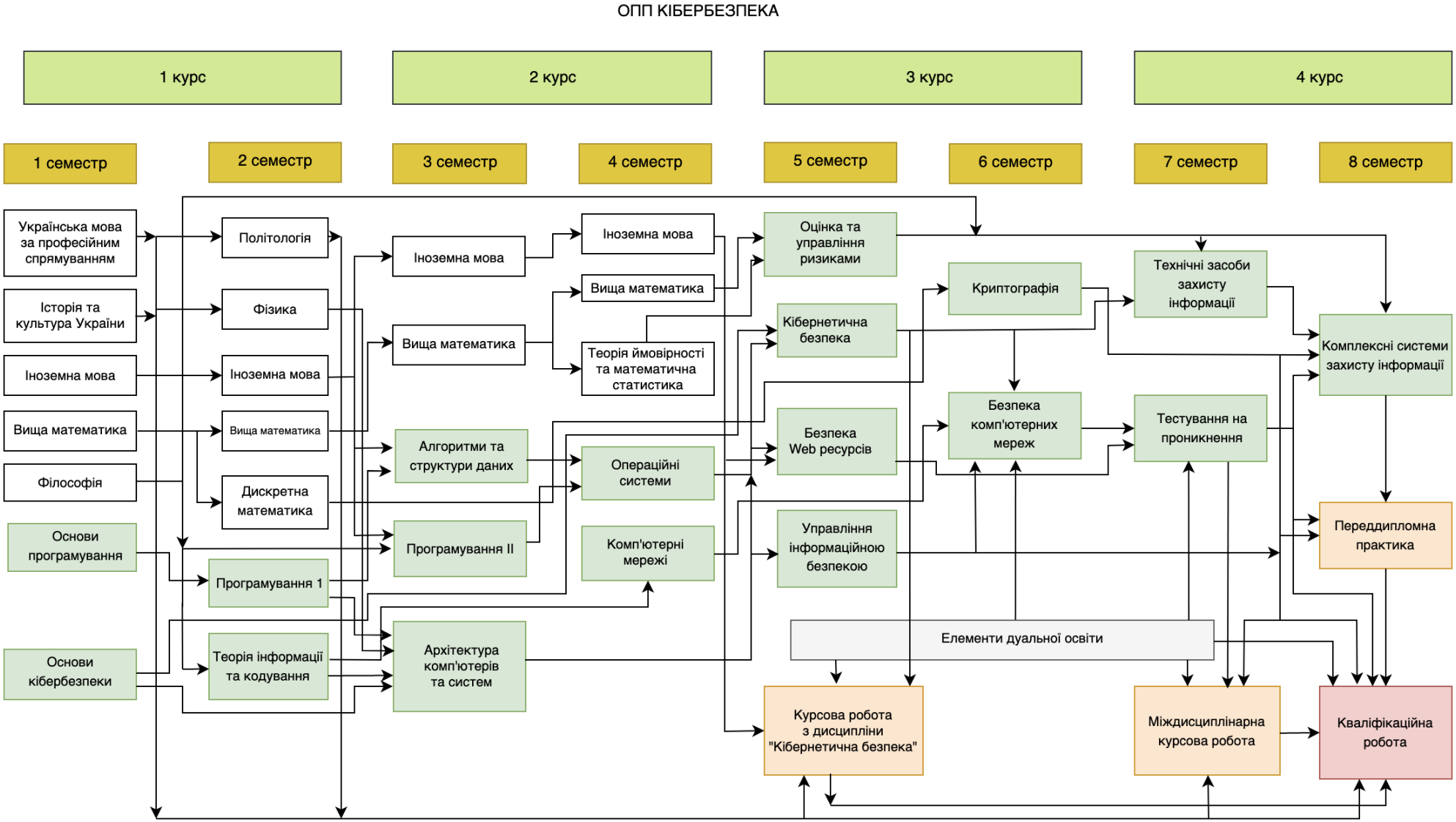
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

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 (ОК)			
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
ОК 1	Українська мова за професійним спрямуванням	4	залік
ОК 2	Історія та культура України	4	екзамен
ОК 3	Англійська мова	9	залік, екзамен
ОК 4	Філософія	4	екзамен
ОК 5	Політологія	4	залік
Разом		29	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОК 6	Вища математика	14	залік, екзамен
ОК 7	Фізика	5	екзамен
ОК 8	Основи програмування	5	екзамен
ОК 9	Основи кібербезпеки	7	екзамен
ОК 10	Дискретна математика	5	екзамен
ОК 11	Програмування I	5	екзамен
ОК 12	Теорія інформації та кодування	5	екзамен
ОК 13	Алгоритми та структури даних	5	екзамен
ОК 14	Програмування II	8	екзамен
ОК 15	Архітектура комп'ютерів та систем	5	екзамен
ОК 16	Теорія ймовірності та математична статистика	4	екзамен
ОК 17	Операційні системи	5	екзамен
ОК 18	Комп'ютерні мережі	5	екзамен
ОК 19	Управління інформаційною безпекою	5	екзамен
ОК 20	Оцінка та управління ризиками	5	екзамен
ОК 21	Кібернетична безпека	6	екзамен
ОК 22	Безпека комп'ютерних мереж	7	екзамен
ОК 23	Технічні засоби захисту інформації	5	екзамен
ОК 24	Комплексні системи захисту інформації	5	екзамен
ОК 25	Криптографія	5	екзамен
ОК 26	Безпека Web ресурсів	7	екзамен
ОК 27	Тестування на проникнення	5	екзамен
ОК 28	Курсова робота з дисципліни "Кібернетична безпека"	3	захист
ОК 29	Міждисциплінарна курсова робота	3	захист
ОК 30	Елементи дуальної освіти	6	залік
ОК 31	Переддипломна практика	9	захист
ОК 32	Кваліфікаційна робота	6	захист
Разом		151	
Разом обсяг обов'язкових компонент		180	

ВИБІРКОВІ КОМПОНЕНТИ	60	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ	240	

2.2. Структурно-логічна схема ОП



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту (демонстрації) кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота передбачає самостійне розв'язання складної задачі у сфері кібербезпеки, що супроводжується проведенням досліджень та/або застосуванням інноваційних підходів та сучасних програмно-апаратних засобів. У кваліфікаційній роботі не повинно бути академічного плагіату, фальсифікації, фабрикації та списування. Кваліфікаційна робота розміщується у репозитарії ЗУНУ.

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
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																	+			+	+						+	+	+			
КФ 13																									+				+			+
КФ 14																										+			+	+		+
КФ 15																											+		+			+

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

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК7	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
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												+			+																	+	+
ПРН 54		+		+	+	+																											
ПРН 55																										+							+
ПРН 56																											+						+
ПРН 57																												+		+			+
	ОК 1	**ОК 2**	**ОК 3**	**ОК 4**	**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**	**ОК33**	**ОК34**