МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА»

другого (магістерського) рівня вищої освіти
за спеціальністю 125 Кібербезпека та захист інформації
галузі знань 12 Інформаційні технології

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Голова вченої ради
_____ Андрій КРИСОВАТИЙ
(протокол № 11 від "26" червня 2024 р.)

Освітня програма вводиться в дію з вересня 2024 р.

Ректор _____ Оксана ДЕСЯТНЮК
(наказ № 496 від "26" червня 2024 р.)

Тернопіль – 2024

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

«КІБЕРБЕЗПЕКА»

другого (магістерського) рівня вищої освіти

за спеціальністю 125 Кібербезпека та захист інформації

галузі знань 12 Інформаційні технології

Проректор з
науково-педагогічної роботи *Віктор ОСТРОВЕРХОВ*

Директор навчально-наукового центру
моніторингу якості освіти
та методичної роботи *Сергій ШАНДРУК*

В.о.декана факультету комп'ютерних
інформаційних технологій *Ігор ЯКИМЕНКО*

Голова ГЗС *Василь ЯЦКІВ*

Гарант ОПП *Василь ЯЦКІВ*

ПЕРЕДМОВА

Розроблено робочою групою у складі:

1. Василь ЯЦКІВ, доктор технічних наук, професор, завідувач кафедри кібербезпеки ЗУНУ;

2. Михайло КАСЯНЧУК, доктор технічних наук, професор, професор кафедри кібербезпеки ЗУНУ;

3. Ігор ЯКИМЕНКО, кандидат технічних наук, доцент, доцент кафедри кібербезпеки ЗУНУ;

4. Степан ІВАСЬЄВ, кандидат технічних наук, доцент, доцент кафедри кібербезпеки ЗУНУ;

5. Богдан БАРАННІК, викладач кафедри кібербезпеки, випускник освітньо - професійної програми.

Відгуки та рецензії на освітньо-професійну програму:

1. Олена НЄМКОВА, д.т.н., професор, професор кафедри безпеки інформаційних технологій, Національний університет «Львівська політехніка»;

2. Юрій ФРАНКО, к.т.н., доцент, завідувача кафедри комп'ютерних технологій Тернопільського національного педагогічного університету імені Володимира Гнатюка;

3. Олена ВОЛОЩУК, к.т.н., доцент, керівник освітнього департаменту Distributed Lab.

4. Павло КРАСНИЦЬКИЙ, т.в.о. начальника відділу протидії кіберзлочинам в Тернопільській області ДКП Національної поліції України.

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

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Західноукраїнський національний університет, кафедра кібербезпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр, магістр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Освітньо-професійна програма «Кібербезпека»
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці
Наявність акредитації	Освітня програма акредитована Національним агентством із забезпечення якості вищої освіти, рішення від 13.01.2020 р.
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня вищої освіти «бакалавр»
Мова(и) викладання	Українська
Термін дії освітньої програми	5 років
Інтернет-адреса постійного розміщення опису освітньої програми	https://www.wunu.edu.ua/master_fcit_op/
2 – Мета освітньої програми	
Підготовка висококваліфікованих, конкурентоспроможних фахівців здатних проводити наукові дослідження в галузі інформаційної безпеки та/або кібербезпеки, які мають теоретичні знання та сформоване критичне мислення достатні для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки; володіють сучасними методами та технологіями тестування на проникнення; методами цифрової криміналістики; вміють безконфліктно та продуктивно працювати в командах щодо розв'язання проблем та прийняття рішень.	
3 - Характеристика освітньої програми	
Опис предметної області	**Об'єкти вивчення:** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій,

	інших бізнес-операційних процесів на об’єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об’єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. **Цілі навчання:** Підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. **Методи, методики та технології** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання**. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об’єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.

Орієнтація освітньої програми	Освітньо-професійна програма з кібербезпеки. Враховуючи збільшення кібератак на підприємства та організації ОПП орієнтується на поглиблене вивчення систем моніторингу та управління інформаційною безпекою та також сучасних методів та технологій тестування на проникнення.
Основний фокус освітньої програми	Підготовка фахівців для проведення досліджень та науково-технічних розробок у галузі інформаційної безпеки та\або кібербезпеки. Ключові слова: інформаційна безпека, кібербезпека, цифрова криміналістика, тестування безпеки, реверс інжиніринг, блокчейн, безпека Інтернет речей.
Особливості програми	Програма забезпечує підвищення рівня знань та навичок в галузі безпеки ІТ шляхом викладання новітніх дисциплін, спрямованих на отримання якісно нових знань стосовно комплексного аналізу інформаційної та кібербезпеки. ОП передбачає студентську мобільність.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Згідно з Національним класифікатором професій ДК 003:2010 випускники можуть обіймати такі первинні посади, як: – розробник систем захисту інформації 2132.2; – фахівець сфери захисту інформації 2139.2; – аналітик з безпеки інформаційно-телекомунікаційних систем 2139.2; – фахівець з питань безпеки (інформаційно-комунікаційні технології) 2139.2; – інструктор-методист з інформаційної безпеки та кібербезпеки 2139.2; – аудитор/пентестер безпеки комп’ютерних систем; – викладач вищого навчального закладу.
Подальше навчання	Можливість здобуття освіти на третьому (освітньо-науковому) рівні вищої освіти за спеціальністю 125 «кібербезпека» або іншими спеціальностями галузі знань «Інформаційні технології», іншими міждисциплінарними магістерськими програми з ІТ компонентою. Можливість підвищення кваліфікації та отримання додаткової післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Основні підходи: студенто-центроване навчання, самонавчання, проблемно-орієнтоване навчання, інтерактивне навчання, навчання через практику. Методи та технології: загальнонаукові, математично-статистичні, інформаційно-комунікаційні технології, методи науково-дослідницької діяльності та презентації результатів. Викладання проводиться у формі: лекції, мультимедійної лекції, інтерактивної лекції, семінарів, практичних занять, самостійного

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

	рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
7 –Результати навчання	
	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

	РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього

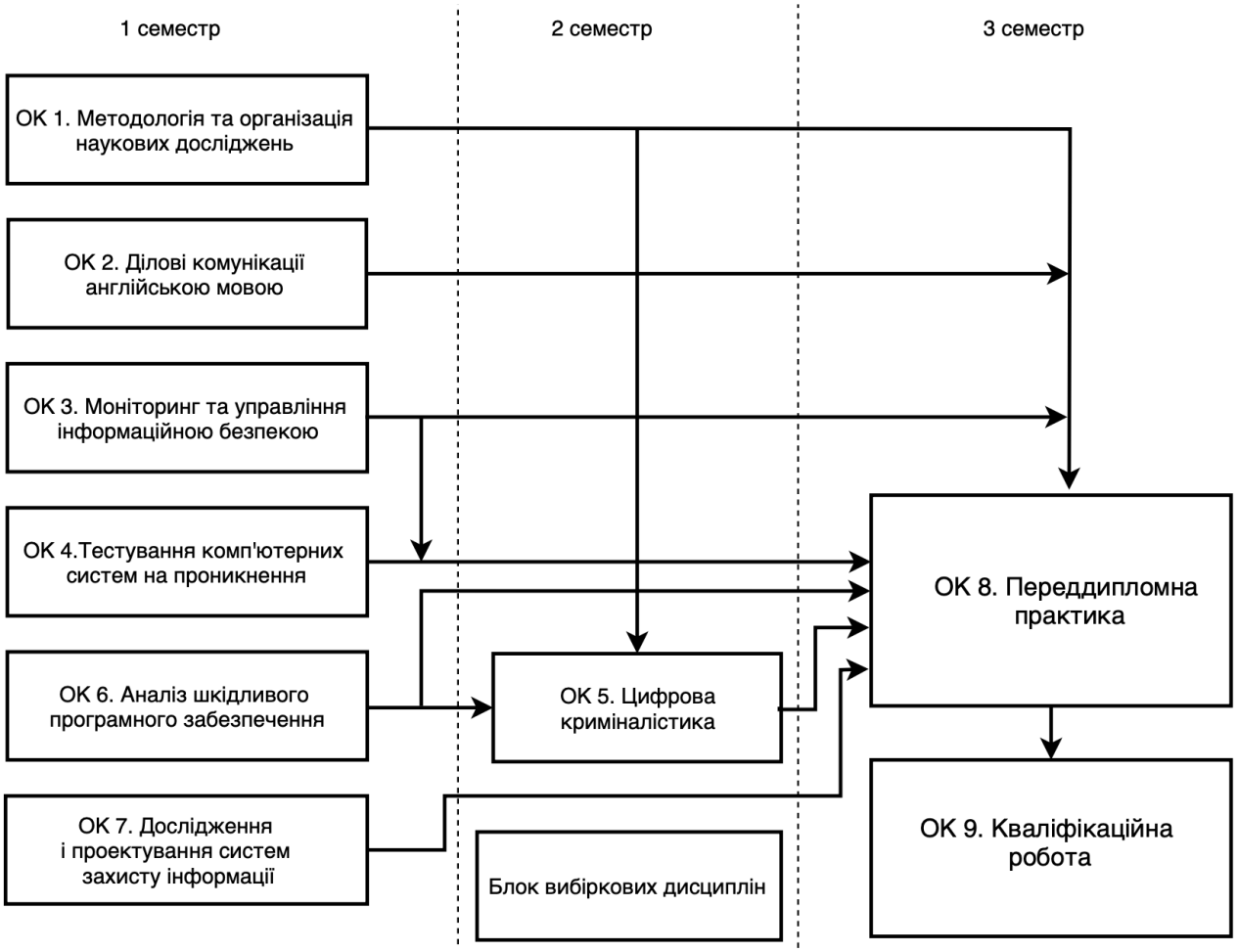
	придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
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 спеціалізованим обладнанням (сервер, маршрутизатори, керовані комутатори, міжмережні екрани, генератор віброакустичного зашумлення, генератори завад, пристрій захисту від електромагнітних завад), мультимедійною, комп'ютерною технікою та спеціалізованим програмним забезпеченням, з можливістю постійного доступу до мережі Internet та внутрішньої мережі ЗУНУ.
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.wunu.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 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 компонентів освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонентів ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти освітньої програми			
Цикл загальної підготовки			
ОК 1	Методологія наукових досліджень	5	екзамен
ОК 2	Ділові комунікації англійською мовою	5	залік
Цикл професійної підготовки			
ОК 3	Моніторинг та управління інформаційною безпекою	5	екзамен
ОК 4	Тестування комп'ютерних систем на проникнення	5	екзамен
ОК 5	Цифрова криміналістика	5	залік
ОК 6	Аналіз шкідливого програмного забезпечення	5	екзамен
ОК 7	Дослідження і проектування систем захисту інформації	5	екзамен
ОК 8	Переддипломна практика	15	залік
ОК 9	Кваліфікаційна робота	15	захист
Загальний обсяг обов'язкових компонентів:		65	
Загальний обсяг вибіркових компонентів:		25	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		90	

2.2. Структурно-логічна схема освітньо-професійної програми «Кібербезпека»



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена у репозитарії ЗУНУ. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1	**ОК 2**	**ОК 3**	**ОК 4**	**ОК 5**	**ОК6**	**ОК 7**	**ОК 8**	**ОК 9**
КЗ 1		+						+	+
КЗ 2	+					+			+
КЗ 3	+								
КЗ 4			+					+	
КЗ 5		+						+	
КФ 1	+			+	+			+	
КФ 2			+	+	+			+	+
КФ 3							+		
КФ 4			+						
КФ 5			+	+		+			+
КФ 6				+					
КФ 7			+		+	+			+
КФ 8							+		+
КФ 9			+						
КФ10	+			+				+	

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

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК6	ОК 7	ОК 8	ОК 9
РН 1		+						+	+
РН 2								+	+
РН 3	+					+	+		+
РН 4	+		+				+		+
РН 5	+					+			+
РН 6			+	+		+			
РН 7				+		+		+	
РН 8							+		+
РН 9			+					+	
РН 10			+	+		+			
РН 11			+						
РН 12			+		+				
РН 13							+		
РН 14			+						
РН 15	+	+						+	
РН 16			+	+					+
РН 17								+	+
РН 18			+					+	+
РН 19							+	+	+
РН 20								+	+
РН 21			+		+				
РН 22	+				+				
РН 23		+			+		+	+	+