МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Львівського національного університету
імені Івана Франка
Голова Вченої ради
_____ Володимир МЕЛЬНИК
(протокол №28/4 від «27» квітня 2022 р.)
Освітня програма в оновленій редакції
вводиться в дію з 01.09.2022

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

першого (бакалаврського) рівня вищої освіти
за спеціальністю 125 Кібербезпека
галузі знань 12 Інформаційні технології

Львів – 2022

Розроблено та оновлено робочою групою спеціальності 125 Кібербезпека у складі:

1. **Венгерський Петро Сергійович** д.фіз.-мат.н., в.о. завідувача кафедри кібербезпеки - гарант освітньої програми
2. **Пелешко Дмитро Дмитрович** д. техн. н., професор, професор кафедри кібербезпеки;
3. **Трушевський Вадерій Миколайович,** . канд. фіз.-мат.н., доцент кафедри кібербезпеки;
4. **Моркун Наталія Володимирівна**, д. техн. наук, професор, професор кафедри кібербезпеки;
5. **Винокурова Олена Анатоліївна**, д. техн. наук, професор, професор кафедри кібербезпеки.
6. **Мусійовський Юрій**, координатор Операційного Центру кібербезпеки компанії СофтСерв;
7. **Фик Максим**, студент четвертого курсу групи ПМк-41 факультету прикладної математики та інформатики.

Рецензії-відгуки зовнішніх стейкхолдерів:

1. Відділ кібербезпеки Департаменту кіберполіції УМВС України;
2. Львів IT Кластер;
3. Компютерна компанія Epam;
4. ТзОВ "Українські інформаційні технології"

Гарант освітньої програми _____ Петро ВЕНГЕРСЬКИЙ

(підпис) (ініціали, прізвище)

УХВАЛЕНО

на засіданні Вченої ради факультету прикладної математики та інформатики

Протокол № 10 від 16 лютого 2022 року

Голова вченої ради _____ Іван ДИЯК

(підпис) (ініціали, прізвище)

Декан

факультету прикладної

математики та інформатики _____ Іван ДИЯК

(підпис) (ініціали, прізвище)

Профіль освітньої програми
зі спеціальності 125 Кібербезпека

1 - Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Львівський національний університет імені Івана Франка, факультет прикладної математики та інформатики
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр бакалавр з кібербезпеки
Офіційна назва освітньої програми	Освітньо-професійна програма “Кібербезпека”
Наявність акредитації	_____
Цикл/рівень	НРК України – 6 рівень, *FQ-EHEA – first cycle, EQF LLL – 6 рівень*
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання – 3 роки 10 місяців
Цикл/рівень	
Передумови	Повна загальна середня освіта або ступінь «молодший бакалавр» (освітньо-кваліфікаційний рівень «молодший спеціаліст»)
Мова викладання	Українська
Термін дії освітньої програми	До повного планового оновлення, не перевищуючи періоду акредитації
1нтернет-адреса постйного розміщення опису освітньої програми	https://ami.lnu.edu.ua/admission/specializations
2 - Мета освітньої програми	
Підготовка висококваліфікованих фахівців, які здатні розробляти та використовувати сучасні методи та засоби захисту інформації, знати основні принципи роботи операційних систем, мати сучасні уявлення про інформаційні технології, володіти спеціалізованими програмними пакетами, щодо захисту даних в інформаційних і телекомунікаційних системах.	
3 - Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність,	12 Інформаційні технології 125 Кібербезпека

спеціалізація (за наявності))	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.
0рієнтація освітньої програми	Освітньо-професійна. Мета освітньої програми полягає у підготовці висококваліфікованих фахівців, які здатні розробляти та використовувати сучасні методи та засоби захисту інформації, знати основні принципи роботи операційних систем, компютерних мереж, володіти спеціалізованими пакетами, щодо захисту даних в телекомунікаційних та інформаційних системах.

Основний фокус освітньої програми та спеціалізації	Отримання комплексу знань для застосування технологій інформаційної безпеки при розробці систем керування базами даних та знань, мережевих додатків та Інтернет-сервісів, захист протоколів передачі та шифрування даних. Освіта в галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека Ключові слова: загроза, вразливість, інцидент, атака, сервісні служби, сканер, антивірус, SIEM системи, тестування на проникнення, SOC центр, аналітика, машинне навчання, аудит системи, ключ шифрування, цифровий підпис.
Особливості програми	
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Перелік первинних посад, що може займати випускник- бакалавр за Державним класифікатором України «Класифікатор професій» за ДК 003:2010: 122 Керівники виробничих та інших основних підрозділів 1236 Керівники підрозділів комп'ютерних послуг 1238 Керівники проектів та програм 1474 Менеджери (управителі) у сфері досліджень та розробок 1495 Менеджери (управителі) систем з інформаційної безпеки 21 Професіонали в галузі фізичних, математичних та технічних наук 2122 Професіонали в галузі статистики 213 Професіонали в галузі обчислень (комп'ютеризації) 2131 Професіонали в галузі обчислювальних систем 2131.1 Наукові співробітники (обчислювальні системи) 2131.2 Розробники обчислювальних систем 2132 Професіонали в галузі програмування 2132.1 Наукові співробітники (програмування) 2132.2 Розробники комп'ютерних програм 2139 Професіонали в інших галузях обчислень (комп'ютеризації) 2139.1 Наукові співробітники (інші галузі обчислень) 2139.2 Професіонали в інших галузях обчислень 23 Викладачі 231 Викладачі університетів та вищих навчальних закладів 232 Викладачі середніх навчальних закладів 2414 Професіонали з питань фінансово-економічної безпеки підприємств, установ та організацій 2414.1 Наукові співробітники (фінансово-економічна безпека підприємств, установ та організацій) 2414.2 Професіонали з фінансово-економічної безпеки 2433 Професіонали в галузі інформації та інформаційного аналізу 2433.1 Наукові співробітники (інформаційна аналітика) 2433.2 Професіонали в галузі інформації та інформаційні аналітики 2447 Професіонали у сфері управління проектами та програмами 2447.1 Наукові співробітники (проекти та програми)

	2447.2 Професіонали з управління проектами та програмами
Подальше навчання	Можливість продовжити навчання за освітньою програмою ступеня магістра. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Застосування проектно-орієнтованого методу навчання з поєднанням індивідуальних завдань з дисциплін курсів та прикладне застосування знань при виконанні мініпроектів. Студентоцентроване навчання, проблемно-орієнтоване викладання, електронне навчання в системі Moodle, самонавчання, колабооративне і проектне навчання на основі виконання кваліфікаційної роботи та виробничої практики. Викладання здійснюється у формі мультимедійних та інтерактивних лекцій, семінарів, практичних та індивідуальних занять, самостійного навчання.
Оцінювання	Усне та письмове опитування, тести, заліки, іспити, презентація наукової роботи, захист курсових робіт, захист бакалаврської кваліфікаційної роботи, складання єдиного державного кваліфікаційного іспиту. Оцінювання навчальних досягнень здобувачів здійснюється за системою ECTS та національною шкалою оцінювання. *Поточний контроль* – усне та письмове опитування, оцінка роботи в малих групах, тестування, захист індивідуальних завдань. *Підсумковий контроль* – екзамени та заліки з урахуванням накопичених балів поточного контролю. *Державна атестація* – підготовка та публічний захист (представлення) кваліфікаційної роботи. Атестація здійснюється у формі публічного захисту.
6 – Програмні компетентності	
Інтегральна компетентність (КІ)	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 реалізовувати 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 України. 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- комунікацтйних 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 в інформаційному просторі та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. КФ 13. Здатність створювати моделі та архітектури програмно-апаратних комплексів, враховуючи умови доступу до даних, шифрування інформації та верифікації користувачів, даних та процесів. КФ 14. Здатність проводити дослідження та аналіз логіки настання кіберінциденту, його умови та причини виникнення та наслідки, завдані в результаті настання інциденту, та перспективи його повторення в майбутньому.
7- Програмні результати навчання	
Програмні результати навчання (ПРН)	ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

	ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; ПРН 4. 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; ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; ПРН 11.Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; ПРН 12. Розробляти моделі загроз та порушника; ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; ПРН 17. 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; ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; ПРН 21. 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; ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); ПРН 25. 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; ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; ПРН 29. 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;

	ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно- 11 телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; ПРН 36. Виявляти небезпечні сигнали технічних засобів; ПРН 37. 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; ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; ПРН 44. 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;

	ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз; ПРН 54. 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	Понад 80% науково-педагогічних працівників, задіяних до викладання професійно-орієнтованих дисциплін зі спеціальності 125 «Кібербезпека» мають наукові ступені та вчені звання, також більше 15% у викладанні приймають участь працівники ІТ-фірм з практичним досвідом у цьому напрямі, більше 10% викладачів проходять спеціалізовані курси для отримання сертифікації з курсів.
Матеріально-технічного забезпечення	Використання сучасного програмного забезпечення провідних компаній у галузі інформаційних технологій та інформаційної безпеки(наприклад, Cisco) а також стандартизованих вітчизняних апаратно-програмних засобів захисту інформації.
Інформаційне та навчально-методичне забезпечення	Використання навчальних класів університету та спеціалізованих лабораторій комп'ютерних фірм для виконання лабораторних та практичних завдань та авторські розробки професорсько-викладацького складу.

9 - Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між університетом та іншими вишами України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між університетом та навчальними закладами країн-партнерів
Навчання іноземних здобувачів вищої освіти	Можливе, після вивчення курсу української мови

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

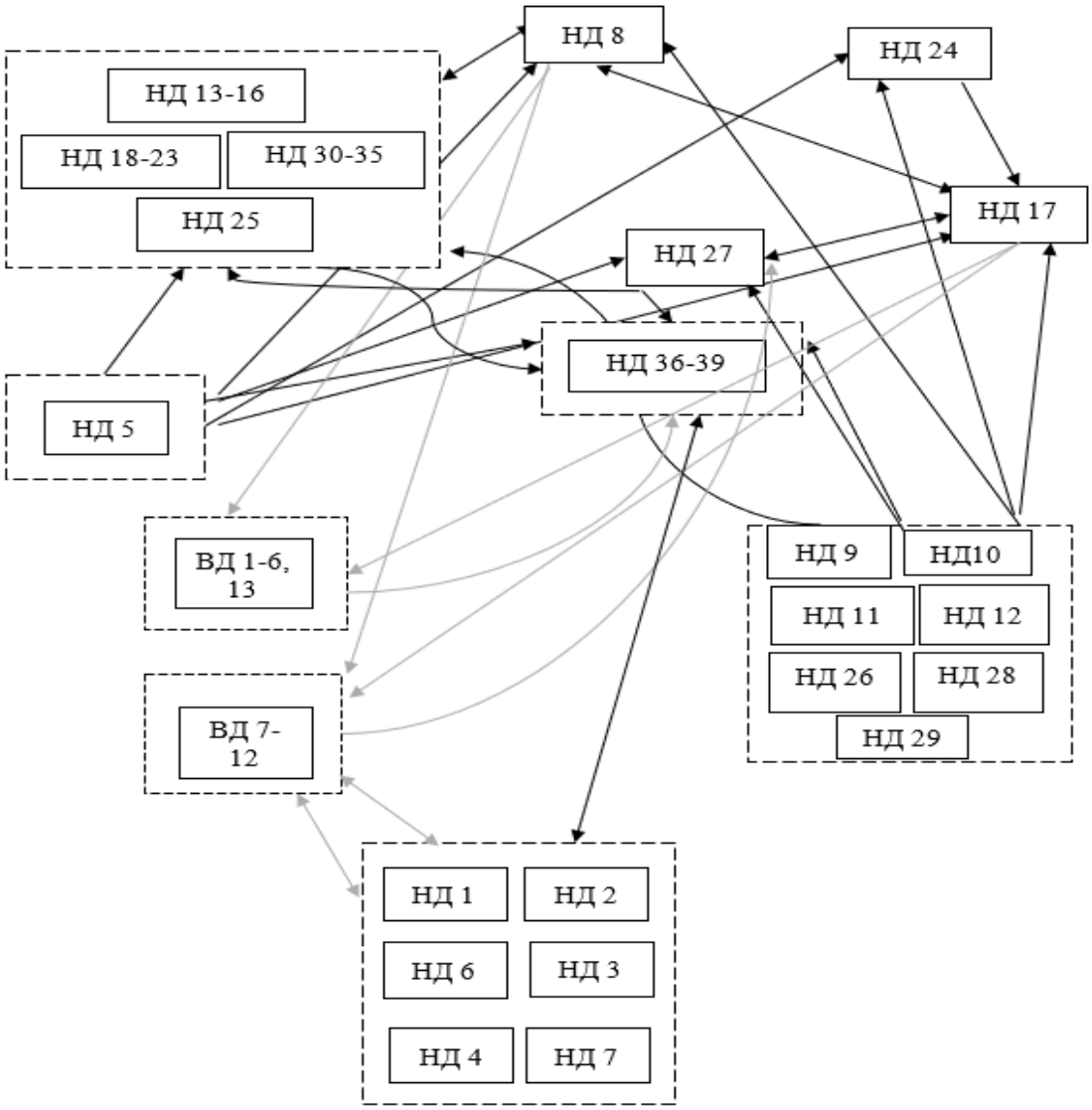
2.1 Перелік компонент ОП

Назва навчальної дисципліни		Загальний обсяг		Форма підсумкового контролю
		Кредити	Години	
1. НОРМАТИВНІ НАВЧАЛЬНІ ДИСЦИПЛІНИ				
НД 1	Українська мова (за професійним спрямуванням)	3	90	залік
НД 2	Історія України	3	90	залік
НД 3	Історія української культури	3	90	залік
НД 4	Філософія	3	90	залік
НД 5	Іноземна мова	16	480	залік + екзамен
НД 6	Фізичне виховання	4	120	залік
НД 7	Безпека життєдіяльності та охорона праці	3	90	залік
НД 8	Основи командної роботи	5	150	залік
НД 9	Основи математичного аналізу та застосування	9	270	екзамен
НД 10	Моделі та методи дискретної математики	4	120	екзамен
НД 11	Обчислювальна геометрія та алгебра	4	120	екзамен
НД 12	Теорія ймовірностей та математична статистика	4	120	екзамен
НД 13	Бази даних	4	120	екзамен
НД 14	Основи операційних систем	8	240	екзамен
НД 15	Безпека комп'ютерних мереж	4	120	екзамен
НД 16	Програмування	16	480	екзамен
НД 17	Менеджмент інформаційної безпеки	8	240	залік+екзамен
НД 18	Комп'ютерна графіка	3	90	екзамен
НД 19	Теорія формальних мов,автоматів та кодів	4	120	екзамен
НД 20	Прикладна криптологія	3	90	залік
НД 21	Системи штучного інтелекту	4	120	екзамен
НД 22	Системні події, їх опрацювання та аналіз	4	120	екзамен

НД 23	Хмарні технології, захист веб-додатків	3	90	екзамен
НД 24	Основи кібербезпеки	4	120	екзамен
НД 25	Алгоритми і структури даних	4	120	залік
НД 26	Застосування дискретної математики в криптології	4	120	екзамен
НД 27	Організація IT на підприємстві(ITIL)	3	90	екзамен
НД 28	Математична логіка	4	120	екзамен
НД 29	Математична криптологія	4	120	екзамен
НД 30	Захист інформації в компютерних мережах	7	210	екзамен
НД 31	Інструменти SecOps 1	3.5	105	екзамен
НД 32	Прикладна статистика	3.5	105	екзамен
НД 33	Програмування паралельних обчислень	3	90	екзамен
НД 34	Інструменти SecOps 2	3	90	екзамен
НД 35	Тестування на проникнення	3	90	екзамен
НД 36	Навчальна (обчислювальна) практика	3	90	залік
НД 37	Виробнича (обчислювальна) практика	3	90	залік
НД 38	Виробнича(переддипломна) практика	3	90	залік
НД 39	Бакалаврська робота та Єдиний державний кваліфікаційний іспит	3	90	екзамен
	Всього	**180**	**5400**	
2. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ				
ВД 1	Дисципліни вільного вибору	12	360	залік
ВД 2.1	Обробка сигналів та зображень	4	120	залік
ВД 2.2	Високорівневе веб-програмування			
ВД 3.1	Технології створення програмних продуктів	5	150	залік
ВД 3.2	Дискретна оптимізація			
ВД 4.1	Технологія кібератак	4	120	залік
ВД 4.2	Застосування Python в кібербезпеці			
ВД 5.1	Методи та системи штучного інтелекту	4	120	залік
ВД 5.2	Теорія ризиків			
ВД 6.1	Компютерний зір	5	150	залік
ВД 6.2	Організація та проведення тестування на проникнення			
ВД 7.1	Комп'ютерна криміналістика	4	120	залік
ВД 7.2	Правові основи інформаційної безпеки			
ВД 8.1	Графічні інформаційні системи та бази даних	4	120	залік
ВД 8.2	Комплексні системи захисту інформації			
ВД 9.1	Моделювання бізнес-процесів безпеки	4	120	залік
ВД 9.2	Методи інтелектуального аналізу даних			

ВД 10.1	Розподілені інформаційно-аналітичні системи	4	120	залік
ВД 10.2	Основи протидії кіберзлочинності			
ВД 11.1	Застосування криптології у віртуальній економіці	4	120	залік
ВД 11.2	Проектування інформаційних систем безпеки			
ВД 12.1	Комп'ютерний проект з кібербезпеки	3	90	залік
ВД 12.2	Комп. проект з безпеки комп'ютерних мереж			
ВД 13	Курсова робота	3	90	
Всього вибіркових навчальних дисциплін		**60**	**1800**	
Всього за час навчання		**240**	**7200**	

2.2. Структурно-логічна схема ОП



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності 125 Кібербезпека проводиться у формі захисту бакалаврської роботи і складанням Єдиного державного кваліфікаційного іспиту та завершується видачею документу встановленого зразка про присудження ступеня бакалавра із присвоєнням кваліфікації: “Бакалавр з кібербезпеки”. Атестація здійснюється відкрито і публічно.

3. Матриця відповідності програмних компетентностей компонентам освітньої програми

	НД 1	НД 2	НД 3	НД 4	НД 5	НД 6	НД 7	НД 8	НД 9	НД 10	НД 11	НД 12	НД 13	НД 14	НД 15	НД 16	НД 17	НД 18	НД 19	НД 20	НД 21	НД 22	НД 23	НД 24	НД 25	НД 26	НД 27	НД 28	НД 29	НД 30	НД 31
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	+	+		+	+	+	+										+	+						+	+						

	НД 32	НД 33	НД 34	НД 35	НД 36	НД 37	НД 38	НД 39	ВД 1	ВД 2.1	ВД 2.2	ВД 3.1	ВД 3.2	ВД 4.1	ВД 4.2	ВД 5.1	ВД 5.2	ВД 6.1	ВД 6.2	ВД 7.1	ВД 7.2	ВД 8.1	ВД 8.2	ВД 9.1	ВД 9.2	ВД 10.1	ВД 10.2	ВД 11.1	ВД 11.2	ВД 12.1	ВД 12.2	ВД 13
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	+	+		+					+	+				+					+	+					+	+		+		+	+	+

4.