МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ЛЕСІ УКРАЇНКИ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

ІНФОРМАЦІЙНА БЕЗПЕКА

першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Освітня кваліфікація: Бакалавр з кібербезпеки

Професійна кваліфікація : Фахівець з організації інформаційної безпеки

ЗАТВЕРДЖЕНО

Вченою радою ВНУ імені Лесі Українки

(протокол № 7 від 28.05 2021)

ПЕРЕЗАТВЕРДЖЕНО

Вченою радою ВНУ імені Лесі Українки

Голова Вченої ради

_____ Цьось А. В.

(протокол № 1 від від 27 січня 2022)

Освітня програма вводиться в дію з_____ 2022 р.

Ректор _____ Анатолій ЦЬОСЬ

наказ № 24з від 27 січня 2022 р.

Луцьк – 2022

ПЕРЕДМОВА

Освітньо-професійна програма є нормативним документом, який регламентує нормативні, компетентнісні, кваліфікаційні, організаційні, навчальні та методичні вимоги у підготовці бакалаврів у галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека.

Освітньо-професійна програма заснована на компетентнісному підході підготовки спеціаліста у галузі знань 12 Інформаційні технології спеціальності 125 «Кібербезпека».

Освітньо-професійна програма розроблена та змінена за результатами зауважень експертів під час акредитації 2021 р., із врахуванням змін до стандарту вищої освіти за спеціальністю 125 Кібербезпека від 2022 р. робочою групою ВНУ імені Лесі Українки у складі:

1 Прус Р.Б. – кандидат технічних наук; старший викладач кафедри комп'ютерних наук та кібербезпеки.
2 Глинчук Л. Я. – кандидат фіз.-мат. наук; доцент кафедри комп'ютерних наук та кібербезпеки.
3 Сачук Ю. В. – кандидат фіз.-мат. наук; старший викладач кафедри комп'ютерних наук та кібербезпеки.
4 Головко В. А., доктор технічних наук, професор кафедри комп'ютерних наук та кібербезпеки.
5 Новосад О. В. – кандидат фіз.-мат. наук, доцент кафедри експериментальної фізики, інформаційних та освітніх технологій.
6 Антіпова М. – здобувач першого (бакалаврського) рівня вищої освіти ОП Інформаційна безпека.
7 Слупко О. М. – директор веб-студії «WEBMAESTO».

Рецензії та відгуки роботодавців, стейкхолдерів:

1. Марчук М. В. – професор, доктор фізико-математичних наук, завідувач відділу моделювання композитних структур і складних систем, Інститут прикладних проблем механіки і математики імені Я. С. Підстригача НАН України, лауреат Державної премії України в галузі науки і техніки.
2. Савченко В. А. – професор, доктор технічних наук, директор навчально-наукового інституту захисту інформації Державного університету телекомунікацій.
3. Паленко А. В. – підполковник, начальник відділу протидії кіберзлочинам у Волинській області Департаменту кіберполіції Національної поліції України.
4. Баландін Т. І. – головний менеджер з ІТ ГО «Центр жіночих ініціатив «Марія».

Програма погоджена Вченою радою факультету інформаційних технологій та математики, схвалена Науково-методичною радою та затверджена Вченою радою Волинського національного університету імені Лесі Українки.

Порядок розробки, експертизи, затвердження і внесення змін у освітню програму регулюється «Положенням про освітні програми підготовки фахівців різних ступенів вищої освіти у Волинському національному університеті імені Лесі Українки».

Лист погодження освітньо-професійної програми

Голова методичної комісії
факультету інформаційних
технологій і математики _____ Валентина ЮНЧИК

Завідувач кафедри математичного
аналізу та статистики _____ Оксана МЕКУШ

Завідувач кафедри теорії функцій
та методики навчання математики _____ Світлана ГЕМБАРСЬКА

Завідувач кафедри комп'ютерних
наук та кібербезпеки _____ Тетяна ГРИШАНОВИЧ

Завідувач кафедри загальної математики
та методики навчання інформатики _____ Марія ХОМЯК

Голова вченої ради
факультету інформаційних
технологій і математики _____ Світлана ЯЦЮК

1. Профіль освітньої програми зі спеціальності 125 Кібербезпека

1 – Загальна інформація	
Ступінь вищої освіти	Бакалавр
Освітня кваліфікація	Бакалавр з кібербезпеки
Професійна кваліфікація	Фахівець з організації інформаційної безпеки
Офіційна назва освітньої програми	Інформаційна безпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, 240 кредитів ЄКТС, Термін навчання 3 роки 10 місяців
Наявність акредитації	Відсутня
Цикл/рівень	НРК – 7 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Наявність атестата про повну загальну середню освіту, диплома молодшого спеціаліста, диплома молодшого бакалавра, фахового молодшого бакалавра.
Мови викладання	Українська мова
Термін дії освітньої програми	4 роки
Інтернет адреса постійного розміщення опису освітньої програми	https://vnu.edu.ua/uk/faculties-and-institutes/fakultet-informaciynikh-tekhnologiy-i-matematiki
2 – Мета освітньої програми	
ОП спрямована на підготовку фахівців, здатних розробляти, впроваджувати та супроводжувати системи захисту в інформаційно-телекомунікаційних технологіях, вирішувати прикладні і наукові завдання проектування та побудови комплексних систем захисту інформації, а також керування процесами управління інформаційною та кібербезпекою в різного роду загрозах.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань 12 Інформаційні технології Спеціальність 125 Кібербезпека
Орієнтація освітньої програми	Освітньо-професійна
Основний фокус освітньої програми	Освітня програма передбачає надання загальних і спеціальних знань та професійну підготовку у сфері наук з кібернетичної безпеки,

та спеціалізації	необхідних для подальшої професійно-наукової діяльності, вона включає дослідження в області захисту інформації, організації та забезпечення інформаційної та/або кібербезпеки об'єктів, що підлягають захисту. **Ключові слова:** кібернетична безпека, інформаційна безпека, забезпечення захисту інформації.
Особливості програми	Особливість програми полягає у врахуванні регіональних особливостей ринку праці, сформованого, переважно, представниками малого та середнього бізнесу, які зацікавленні у поєднанні компетенцій суміжних ІТ спеціальностей в одному фахівці. ОП покликана підготувати фахівців з кіберзахисту, які спроможні також поєднати функції системного адміністратора, інженера з комп'ютерних систем тощо.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Працевлаштування в організаціях та підприємствах будь-якої форми власності на посадах (згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010): 1495 менеджер (управитель) систем з інформаційної безпеки 1229.7 керівник (директор, начальник та ін.) підрозділу (служби, управління, департаменту та ін.) з безпеки (фінансово-економічної, інформаційної) 210.1 керівник підприємства (установи, організації) (сфера захисту інформації) 226.2 керівник структурного підрозділу (сфера захисту інформації) 2149.2 фахівець (сфера захисту інформації) 3121 фахівець з інформаційних технологій 3439 фахівець із організації захисту інформації з обмеженим доступом 3439 фахівець із організації інформаційної безпеки
Подальше навчання	Можливість продовжити навчання за освітньою програмою ступеня магістра.
5 – Викладання та оцінювання	
Викладання та навчання	Викладання та навчання ґрунтуються на принципах студентоцентризму та індивідуально-особистісного підходу, що реалізуються через навчання на основі досліджень, посиленні практичної орієнтованості та творчої спрямованості у формі комбінації лекцій, практичних та лабораторних занять, самостійної навчальної і дослідницької роботи з використанням елементів дистанційного навчання, розв'язування прикладних задач, виконання проектів, навчальних та виробничих практик, курсових робіт.
Оцінювання	Оцінювання навчальних досягнень здійснюється на основі принципів академічної доброчесності згідно з Положенням про

	поточне та підсумкове оцінювання знань студентів ВНУ імені Лесі Українки та враховує всі види аудиторної та позааудиторної освітньої діяльності і має таку структуру: поточний контроль (усне та письмове опитування, захист лабораторних робіт, виступи на практичних заняттях, комп'ютерне тестування, контрольні роботи), підсумковий контроль (модульні контрольні роботи, тестування, індивідуальне науково-дослідне завдання, залік, екзамен, захист практики, захист курсової роботи), державна атестація (єдиний державний кваліфікаційний іспит).
6 –Перелік компетентностей випускника	
Інтегральна компетентність (ІК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	**ЗК 1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК 2.** Знання та розуміння предметної області та розуміння професії. **ЗК 3.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **ЗК 4.** Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **ЗК 5.** Здатність до пошуку, оброблення та аналізу інформації. **ЗК 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. **ЗК 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 (ФК)	**ФК 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. **ФК 2.** Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. **ФК 3.** Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. **ФК 4.** Здатність забезпечувати неперервність бізнес-процесів згідно

	встановленої політики безпеки. **ФК 5.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. **ФК 6.** Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. **ФК 7.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). **ФК 8.** Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **ФК 9.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою. **ФК 10.** Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. **ФК 11.** Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. **ФК 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	
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, аутентифікації, 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 інформаційно-телекомунікаційних (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- 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 дотримання 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	Науково-педагогічні працівники, які залучені до підготовки бакалаврів за спеціальністю 125 Кібербезпека, відповідають ліцензійним вимогам, мають науковий ступінь, вчене звання за відповідною або спорідненою спеціальністю, систематично здійснюють наукову і навчально-методичну діяльність, регулярно проходять стажування (підвищують кваліфікацію), у тому числі й за кордоном; їх базова освіта відповідає профілю дисциплін, які вони викладають.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення освітньо-професійної програми відповідає чинним технологічним вимогам до впровадження освітньої діяльності у сфері вищої освіти, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 (чинний) в редакції від 23.05.2018 р. № 347: навчальні корпуси, лекційні аудиторії (окремі з них обладнані мультимедійними проекторами), аудиторії для практичних занять, комп'ютерні класи, лабораторії (комп'ютерна лабораторія InternetDevels, лабораторія захисту інформації), спеціалізовані кабінети обладнані відповідно до потреб навчального процесу, комп'ютерне, мережеве та програмне забезпечення, мультимедійне обладнання, бібліотека, інклюзивний ХАБ, бездротовий доступ до інтернету в усіх корпусах університету та бібліотеці, соціально-побутова та спортивно-оздоровча інфраструктура.
Інформаційне та навчально-методичне забезпечення	Наявність офіційного веб-сайту ВНУ імені Лесі Українки, сторінок факультету та кафедр, на яких розміщена основна інформація про наукову та навчально-методичну діяльність (освітньо-професійні програми, навчальні плани, силабуси з навчальних дисциплін тощо). Сайт бібліотеки (http://library.vnu.edu.ua), фонди бібліотеки, інституційний репозитарій (https://evnuir.vnu.edu.ua/), фонд кваліфікаційних робіт, наукова періодика, навчально-методичні розробки НПП, які доступні також і у репозитарії університету. На період навчання здобувачеві безкоштовно надається корпоративний обліковий запис у Office365. Існує кілька локальних комп'ютерних мереж і точок бездротового доступу до мережі інтернет в ЗВО. Дистанційні курси навчальних дисциплін розміщено на платформах Moodle https://moodle.vnu.edu.ua, http://cs.vnu.edu.ua/moodle/ (сервер кафедри). Мережа комп'ютерних класів факультету є відділеною від загальної мережі університету та забезпечує кожен комп'ютер виходом в інтернет через сервер-шлюз (він же файл-сервер). Працює VPN-сервер, що дозволяє віддалено працювати з мережею класів факультету. Також є додатковий сервер кафедри з системою тестування OpenTest та хмарним сховищем OwnCloud (testcs.vnu.edu.ua). Функціонують

	точки доступу wi-fi в кожному із комп'ютерних класів факультету.
9 – Академічна мобільність	
Національна кредитна мобільність	Регламентується Постановою КМУ №579 «Про затвердження Положення про порядок реалізації права на академічну мобільність» від 12 серпня 2015 р. та Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу ВНУ імені Лесі Українки. На основі двосторонніх договорів між ВНУ імені Лесі Українки та ЗВО України.
Міжнародна кредитна мобільність	Регламентується Постановою КМУ №579 «Про затвердження Положення про порядок реалізації права на академічну мобільність» від 12 серпня 2015 р. У рамках програми ЄС Еразмус+ на основі двосторонніх договорів між ВНУ імені Лесі Українки та навчальними закладами країн-партнерів.
Навчання іноземних здобувачів вищої освіти	Можливе, після вивчення курсу української мови.

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

2.1. Перелік компонент ОП

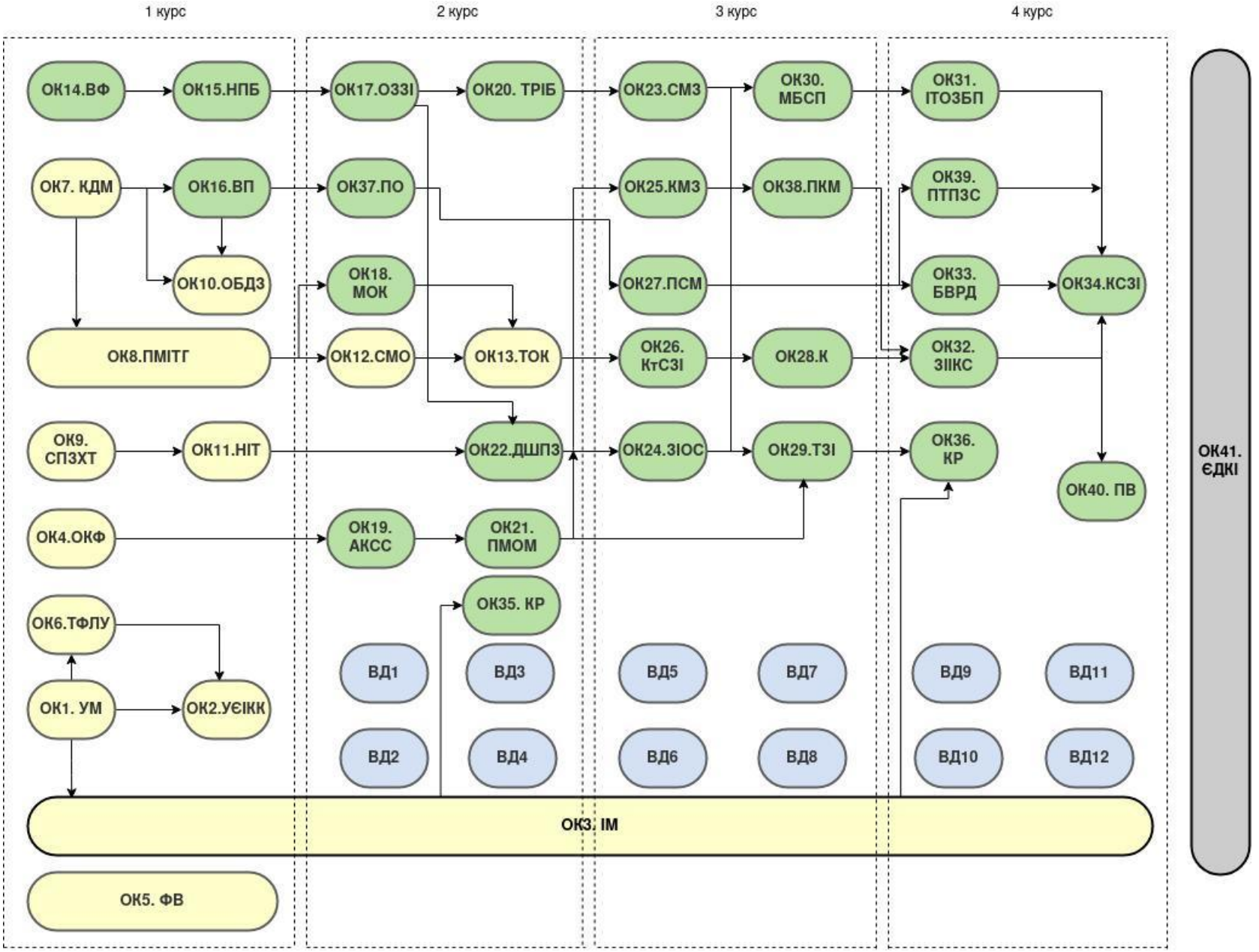
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОП			
Цикл загальної підготовки			
ОК 1.	Українська мова (за професійним спрямуванням)	4	екзамен
ОК 2.	Україна в європейському історичному та культурному контекстах	4	екзамен
ОК 3.	Іноземна мова (за професійним спрямуванням)	10	залік, екзамен
ОК 4.	Основи комп'ютерної фізики	4	залік
ОК 5.	Фізичне виховання	2	залік
ОК 6.	Творчий феномен Лесі Українки	2	залік
ОК 7.	Комп'ютерна дискретна математика	4,5	екзамен
ОК 8.	Прикладна математика в ІТ-галузі	10	залік, екзамен
ОК 9.	Сучасне програмне забезпечення та хмарні	4	залік

	технології		
ОК 10	Організація баз даних та знань	4	залік
ОК 11.	Новітні інформаційні технології для аналізу і обробки даних	5	залік
ОК 12.	Сучасні методи обчислень	4	залік
ОК 13.	Теорія інформації та кодування	4,5	залік
Цикл професійної підготовки			
ОК 14.	Вступ до фаху	4,5	екзамен
ОК 15.	Нормативно-правова база кібербезпеки	4	екзамен
ОК 16.	Вступ до програмування	5	екзамен
ОК 17.	Організаційне забезпечення захисту інформації	4,5	екзамен
ОК 18.	Математичні основи криптографії	4,5	екзамен
ОК 19.	Архітектура комп'ютерних систем та схемотехніка	4,5	екзамен
ОК 20.	Теорія ризиків інформаційної безпеки	4	екзамен
ОК 21.	Проектування мікроконтролерних систем та основи мехатроніки	4,5	екзамен
ОК 22.	Діагностика шкідливого програмного забезпечення	4,5	екзамен
ОК 23.	Системи моніторингу загроз	4	екзамен
ОК 24.	Захист інформації в операційних системах	4	залік
ОК 25.	Комп'ютерні мережі та їх захист	4	екзамен
ОК 26.	Криптографічний та стеганографічний захист інформації	4	екзамен
ОК 27.	Програмування скриптовими мовами	4	екзамен
ОК 28.	Криптоаналіз	4	екзамен
ОК 29.	Технічний захист інформації	4	екзамен
ОК 30.	Моделювання та безпека соціальних процесів	4	екзамен
ОК 31.	Інформаційні технології організації та захисту бізнес процесів	4	екзамен
ОК 32.	Захист інформації в інформаційно-комунікаційних мережах	4	екзамен
ОК 33.	Безпека web-ресурсів та додатків	4	екзамен
ОК 34.	Комплексні системи захисту інформації	4	екзамен
ОК 35.	Курсова робота*	2	залік
ОК 36.	Курсова робота з навчальних дисциплін циклу професійної підготовки	2	залік
ОК 37.	Практика обчислювальна	2	залік
ОК 38.	Практика з організації, налагодження та захисту комп’ютерних мереж	7	залік
ОК 39.	Практика з технологій програмування захищених систем	5	залік
ОК 40.	Практика виробнича	10	залік

ОК 41.	Єдиний державний кваліфікаційний іспит	2	
Загальний обсяг обов'язкових компонент		**180 кредитів**	
Цикл вибіркових дисциплін			
ВД. 1	Вибіркова дисципліна 1	4,5	залік
ВД. 2	Вибіркова дисципліна 2	5	залік
ВД. 3	Вибіркова дисципліна 3	4,5	залік
ВД. 4	Вибіркова дисципліна 4	4,5	залік
ВД. 5	Вибіркова дисципліна 5	4,5	залік
ВД. 6	Вибіркова дисципліна 6	4	залік
ВД. 7	Вибіркова дисципліна 7	5	залік
ВД. 8	Вибіркова дисципліна 8	5	залік
ВД. 9	Вибіркова дисципліна 9	5	залік
ВД. 10	Вибіркова дисципліна 10	5	залік
ВД. 11	Вибіркова дисципліна 11	6,5	залік
ВД. 12	Вибіркова дисципліна 12	6,5	залік
Загальний обсяг вибіркових компонент		**60 кредитів**	
Загальний обсяг освітньої програми		**240 кредитів**	

*Курсова робота з нормативних навчальних дисциплін: сучасне програмне забезпечення та хмарні технології, організація баз даних та знань, новітні інформаційні технології для аналізу і обробки даних, сучасні методи обчислень, вступ до програмування, організаційне забезпечення захисту інформації, математичні основи криптографії, архітектура комп'ютерних систем та схемотехніка.

2.2. Структурно-логічна схема ОП



3. Форми атестації здобувачів вищої освіти

Атестація здобувачів першого (бакалаврського) освітньо-професійного рівня за спеціальністю 125 Кібербезпека здійснюється у формі єдиного державного кваліфікаційного іспиту (наказ Міністерства освіти і науки України від 13.01.2022р. №26) та завершується видачею документа встановленого зразка про присудження їм ступеня бакалавра з освітньою кваліфікацією «Бакалавр з кібербезпеки», з присвоєнням професійної кваліфікації «Фахівець з організації інформаційної безпеки».

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених Стандартом вищої освіти за спеціальністю 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти» (наказ МОН від 04 жовтня 2018 року №1074) та освітньою програмою.

4. Матриця відповідності загальних компетентностей (ЗК) та фахових компетентностей (ФК) компонентам освітньо-професійної програми

	ЗК 1	ЗК 2	ЗК 3	ЗК 4	ЗК 5	ЗК 6	ЗК 7		ФК 1	ФК 2	ФК 3	ФК 4	ФК 5	ФК 6	ФК 7	ФК 8	ФК 9	ФК 10	ФК 11	ФК 12
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	+	+		+	+										+		+			
ОК 35	+	+			+											+				
ОК 36	+	+		+	+					+						+				
ОК 37	+	+		+	+					+					+				+	
ОК 38	+	+		+	+					+				+	+		+		+	+
ОК 39	+	+		+	+					+				+	+		+		+	+
ОК 40	+	+		+	+				+	+	+	+	+	+	+	+	+	+	+	+
ОК 41	+	+								+				+	+		+		+	+

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньо-професійної 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	ОК 35	ОК 36	ОК 37	ОК 38	ОК 39	ОК 40	ОК 41
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		+			+	+																																			+	+

Гарант освітньої програми програми Прус Р. Б.