МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЛЕСІ УКРАЇНКИ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«ІНФОРМАЦІЙНА БЕЗПЕКА»

першого рівня вищої освіти

за спеціальністю 125 «Кібербезпека»

галузі знань 12 Інформаційні технології

Кваліфікація: бакалавр з кібербезпеки

Професійна кваліфікація : фахівець з організації інформаційної безпеки

ЗАТВЕРДЖЕНО ВЧЕНОЮ
РАДОЮ
Голова вченої ради
_____ /_____/
(протокол №__ від «__» _____2021 р.

Освітня програма вводиться в дію з___ 2021 р.
Ректор _____ /проф. Цьось А.В./
(наказ №__ від «__»_____2021 р.

Луцьк – 2021

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 групою забезпечення ВНУ імені Лесі Українки у складі:

1. Прус Р.Б. – кандидат технічних наук;
2. Глинчук Л. Я. – кандидат фіз.-мат. наук;
3. Сачук Ю. В. – кандидат фіз.-мат. наук;
4. Новосад О.В. – кандидат фіз.-мат. наук.

Програма погоджена вченою радою факультету, 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 в Волинському національному університеті імені Лесі Українки», затверджене Вченою радою ВНУ імені Лесі Українки.

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	Умовна акредитація терміном дії на 1 рік
Цикл/рівень	НРК – 7 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Наявність атестату про повну загальну середню освіту
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 призначена для розвитку професійних умінь та навичок у студентів до розв’язання практичних проблем, які характеризується комплексністю та невизначеністю, на основі методів і засобів забезпечення інформаційної та кібербезпеки. 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 загроз.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань 12 Інформаційні технології Спеціальність 125 «Кібербезпека» 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 зиявлення, 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 кібсрбезпеки. Інструменти та обладнання: • системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; • сучасне програмно-апаратнезабезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Освітньо-професійна
Основний фокус освітньої програми та спеціалізації	Освітня програма передбачає надання загальних і спеціальних знань та професійну підготовку у сфері наук з кібернетичної безпеки, 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	Освітня програма створена на основі аналізу досвіду підготовки фахівців у цій галузі в провідних вузах України, країнах ЄС та США. Існує домовленість про тісну співпрацю у сфері підготовки фахівців з державної безпеки з Поморською академією в м. Слупськ (Польща). Зокрема договір імплементований в рамках програми «Подвійний диплом», що передбачає одно- або двохсеместрове навчання частини студентів у Поморській академії м. Слупськ. З метою підготовки до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації бакалавр з інформаційної безпеки, програма забезпечує підготовку професіоналів, здатних: – виявляти та оцінювати ознаки стороннього кібернетичного впливу; – моделювати можливі ситуації стороннього кібернетичного впливу та прогнозувати їх можливі наслідки;

	– організовувати і підтримувати комплекс заходів щодо забезпечення інформаційної та/або кібербезпеки; – проводити дослідження у напрямах забезпечення інформаційної та/або кібербезпеки національних інтересів України й обґрунтовувати шляхи підвищення їх ефективності; – протидіяти несанкціонованому проникненню протиборчих сторін до власних ІТ систем і мереж, забезпечити стійкість їх роботи, а також відновлення їх нормального функціонування після здійснення кібернападів; – забезпечити криптозахист власного інформаційного ресурсу тощо.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Робочі місця у державних установах та організаціях, приватних та державних підприємствах на посадах фахівців з організації та забезпечення безпеки. Випускники можуть працювати у таких сферах діяльності: 1)адміністрування ОС сімейства Windows/Linux, мережевого обладнання і технологій, провадження політики безпеки ОС; 2)конфігурування засобів антивірусного ПЗ; програмних, клієнт-серверних та хмарних технологій захисту інформації (систем web-фільтрації, систем запобігання вторгнень, систем захисту пошти від вірусів і спам); 3) створення технічної, проектної та експлуатаційної документації інформаційно-комунікаційних систем та систем захисту інформації; 4) налагодження, експлуатації та проведення аналізу системних процесів функціонування мережевих, клієнт-серверних та хмарних технологій; 5) проведення моніторингу несанкціонованої активності в обчислювальних системах; 6) створення, конфігурування, впровадження та експлуатації комплексних систем захисту інформації, в складі інформаційно телекомунікаційних та обчислювальних систем; 7) формування політик та процесів у сфері ІТ безпеки, управління доступом до мережевих ресурсів ІТС та ризиками інформаційної безпеки; 8) проведення розслідувань інцидентів та забезпечення аудиту процесів інформаційної безпеки; 9) підтримка наукових досліджень, педагогічна діяльність тощо. Згідно з Національним класифікатором професій ДК 003-2010 студенти, які здобули освіту за освітньою програмою «Управління інформаційною безпекою» можуть обіймати такі первинні посади: • 2131.2 - адміністратор баз даних • 2131.2 - аналітик комп’ютерних систем • 2132.2 22481 інженер-програміст • 2132.2 - прикладний програміст • 2132.2 - системний програміст • 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) • 2149.2 - професіонал із організації інформаційної безпеки • 1210.1 - керівник підприємства (установи, організації) (сфера захисту інформації) • 1226.2 - керівник структурного підрозділу (сфера захисту інформації) • 2149.2 - фахівець (сфера захисту інформації)
Подальше навчання	Випускник має право продовжити навчання для здобуття освітнього ступеня «магістр». Можливість здобуття освіти за іншими спорідненими (суміжними) спеціальностями галузі знань «Інформаційні технології», що узгоджуються з

	отриманням диплома магістра, іншими міждисциплінарними магістерськими програми з ІТ компонентою. Можливість підвищення кваліфікації та отримання додаткової післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Програма передбачає використання методів проблемно-орієнтованого навчання з проходженням професійно-орієнтованих практик. Викладання та навчання ґрунтуються на принципах студентоцентризму та індивідуально-особистісного підходу; реалізуються через навчання на основі досліджень, посилення практичної орієнтованості та творчої спрямованості у формі комбінації лекцій, практичних занять, самостійної навчальної і дослідницької роботи з використанням елементів дистанційного навчання, розв'язування прикладних задач, виконання проектів, навчальних та виробничих практик, курсових робіт, випускової кваліфікаційної роботи.
Оцінювання	Усні та письмові заліки, екзамени, практики. Накопичувальна бально-рейтингова система, що передбачає оцінювання студентів за всі види аудиторної та позааудиторної освітньої діяльності у вигляді вхідного, поточного, рубіжного та/або семестрового контролю та атестації.
6 –Перелік компетентностей випускинка	
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)	1. Здатність застосовувати знання у практичних ситуаціях. (ЗК 1). 2. Знання та розуміння предметної області та розуміння професії. (ЗК 2). 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. (ЗК 3). 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.. (ЗК4). 5. Здатність до пошуку, оброблення та аналізу інформації. (ЗК 5). 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 з Україні. (ЗК 6). 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. (ЗК 7).
Фахові компетентності (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 1). 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. (ФК 2). 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. (ФК 3). 4. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики безпеки. (ФК 4). 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-

	телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. (ФК 5). 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. (ФК 6). 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 7). 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. (ФК 8). 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою. (ФК 9) 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. (ФК 10). 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. (ФК 11). 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібезбезпеки. (ФК 12).
7 – Програмні результати навчання	
Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. (ПРН 1) Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. (ПРН 2) Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. (ПРН 3) 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 4) Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. (ПРН 5) Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. (ПРН 6) Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. (ПРН 7) Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. (ПРН 8) Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. (ПРН 9) Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. (ПРН 10) Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах. (ПРН 11) Розробляти моделі загроз та порушника. (ПРН 12) Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. (ПРН 13) Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-	

телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. (ПРН 14)

Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. (ПРН 15)

Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. (ПРН 16)

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 17)

Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. (ПРН 18)

Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах. (ПРН 19)

Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. (ПРН 20)

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 21)

Вирішувати задачі управління процедурами ідентифікації, аутентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. (ПРН 22)

Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. (ПРН 23)

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 24)

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 25)

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 26)

Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. (ПРН 27)

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 28)

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 29)

Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. (ПРН 30)

Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем. (ПРН 31)

Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. (ПРН 32)

Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. (ПРН 33)

Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. (ПРН 34)

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 35)

Виявляти небезпечні сигнали технічних засобів. (ПРН 36)

Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. (ПРН37)

Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. (ПРН 38)

Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах дотримання режиму секретності із фіксуванням результатів у відповідних документах. (ПРН 39)

Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних-засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. (ПРН 40)

Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. (ПРН 41)

Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. (ПРН 42)

Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. (ПРН 43)

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 44)

Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. (ПРН 45)

Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. (ПРН 46)

Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. (ПРН 47)

Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. (ПРН 48)

Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. (ПРН 49)

Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). (ПРН50)

Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. (ПРН 51)

Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. (ПРН52) Вирішувати задачі аналізу програмного коду на наявність можливих загроз. (ПРН 53) Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. (ПРН 54) Проводити за заданими алгоритмами і за допомогою ЕОМ розрахунки прогнозованих параметрів та характеристик електронних приладів та пристроїв. (ПРН 55) З заданою електронною схемою, технологічними, економічними та іншими показниками вміти провести топологічне проектування електронних приладів та пристроїв. (ПРН 56) Оцінювати функціонування електронних приладів та пристроїв в системах, визначати відхилення від норми функціонування електронних пристроїв, провадити регулювання відповідних електронних приладів та пристроїв для досягнення нормальних режимів функціонування. (ПРН 57)	
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Заплановано участь у викладанні дисциплін професіоналами, що мають глибокий досвід у сфері теоретико-концептуального осмислення та практичного забезпечення інформаційної та кібербезпеки безпеки, у тому числі на вищому рівні організації.
Матеріально-технічне забезпечення	Використання сучасного матеріально-технічного забезпечення: • комп`ютерна лабораторія С4, системний блок, Intel Dual Core E5300 2.60hz 2Mb; монітор, Asus VH 192DE LCD 5ms; • комп`ютерна лабораторія С9, системний блок, Intel Dual Core E5300 2.60hz 2Mb; монітор, Asus VH 192DE LCD 5ms; • комп`ютерна лабораторія С1, системний блок, Intel Core i3-3220 SRORG 3.3GHz 3Mb; монітор, Asus VH 192DE LCD 5ms; • комп`ютерна лабораторія С2, системний блок, Intel Dual Core E5300 2.60hz 2Mb; монітор, Asus VH 192DE LCD 5ms; • комп`ютерна лабораторія С3, системний блок, Intel Dual Core E5300 2.60hz 2Mb; монітор, Asus VH 192DE LCD 5ms; • лабораторія кіберзахисту: системний блок: Intel Core i3-5400 3.06GHz, Philips 223V5LHSB 5ms; • лабораторія електротехніки; • лабораторія фізики для нефізичних спеціальностей; • лабораторія захисту інформації; • навчальні лабораторії InternetDevels. • Supermicro, 2x Intel(R) Xeon(R) CPU E5507, ОПЗ - 16 Гб, SAS Raid; • IBM BladeCenter на 16 серверів 2x Xeon, ОЗП - 16Gb, SAS Raid; • 2x Xeon, ОЗП - 8Gb, SCSI Raid, SATA Raid. • Arduino Mega2560; • генератор шумових сигналів “Марс-ТЗО-4- 2”; • вібровипромінювач ВІЗ-50 з кріпленням на скло; • вібровипромінювач ВІ4-50 з кріпленням на трубу; Використання сучасного програмного забезпечення: • Microsoft Windows 7 Pro, • Microsoft Security Essentials, • Microsoft Office 2003 Pro, • Microsoft Windows 10 Pro; • Logisim, Code::Blocks; • Virtual Box; VMware Workstation Player;

	• Multisim for Education; • Cisco Packet Tracer; • ME Doc, Nox Player, Victoria, Recuva, R.saver; • CrystalDiskInfo, R-Stuido; • Paragon Partition Manager Free, Cobian Backup, Comodo BackUp, Fbackup; • EaseUS Todo Backup, Wise Data Recovery, Ccproxy, SmallProxy; • TeamViewer, AnyDesk, LogMeIn Hamachi, OpenVPN, uTorrent, Ammyy Admin, Remote Manipulator System; • 1С: Підприємство 8.2; • DriverPack Solution; NVIDIA Forceware; AMD Radeon Software Adrenalin Edition; • Firewall Windows, Outpost Firewall Free, Comodo Firewall; • SpyShelter Free, Zemana AntiLogger, Anti-keylogger, SecureEncrypt's SE-OPS, Malwarebytes Anti-Malware Free, SuperAntiSpyware; • RoboForm, LastPass, KeePass Professional, KeePass Classic, Lazesoft — Recover My Password; • VisualRoute; MathCAD; • Dr.Web LiveDisk; Kaspersky Rescue Disk; ESET SysRescue Live; • TrueCrypt; VeraCrypt; AxCrypt; • FAR Manager, xplorer² LITE, FreeCommander XE; • WinRAR, 7-Zip, Universal Extractor, HaoZip, IZArc; • iCloud, Dropbox, MEGAsync, Google Drive, Microsoft OneDrive; • Auslogics Disk Defrag, Defraggler, Smart Defrag, UltraDefrag; • Deep Freeze, Toolwiz Time Freeze, Reboot Restore Rx, Shadow Defender, Baseline Shield; • Nox App Player, BlueStacks App Player; • Open Server Ultimate.
Інформаційне та навчально-методичне забезпечення	Поєднання лекційних та практичних занять, ознайомчої практики із організації процесу захисту інформації на підприємствах та практики зі спеціалізації, консультування з викладачами та самостійної навчальної роботи. Використання інформаційного пакету навчально-методичних матеріалів в системі управління навчанням Moodle СНУ імені Лесі Українки, хмарних сервісів та авторських розробок науково-педагогічних працівників
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. На основі двосторонніх договорів між СНУ імені Лесі Українки та університетами 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 СНУ імені Лесі Українки та навчальними закладами країн-партнерів. Існує домовленість про тісну співпрацю у сфері підготовки фахівців з державної безпеки з Поморською академією в м. Слупськ (Польща). Зокрема договір імплементований в рамках програми «Подвійний диплом», що передбачає одно- або двохсеместрове навчання частини студентів у Поморській академії м. Слупськ
Навчання іноземних здобувачів вищої освіти	Можливе, після вивчення курсу української мови

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

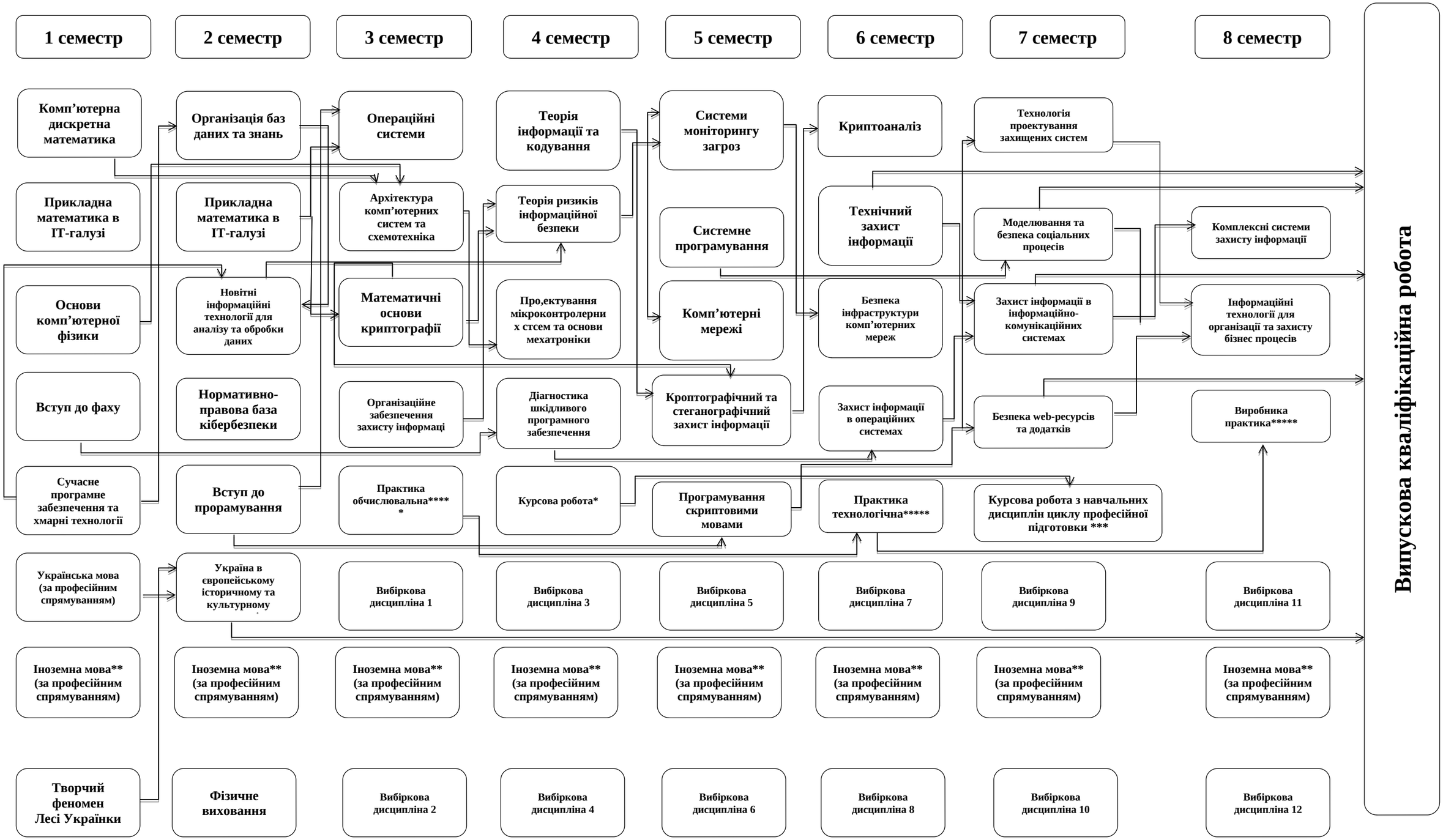
2.1. Перелік компонент ОП

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 технології	4	залік
ОК 10	Організація баз даних та знань	4	залік
ОК 11.	Новітні інформаційні технології для аналізу і обробки даних	5	залік
ОК 12.	Операційні системи	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	4,5	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.	Системне програмування	4	залік

ОК 25.	Комп'ютерні мережі	4	екзамен
ОК 26.	Криптографічний та стеганографічний захист інформації	4,5	екзамен
ОК 27.	Програмування скриптовими мовами	4	екзамен
ОК 28.	Криптоаналіз	4	екзамен
ОК 29.	Технічний захист інформації	4,5	екзамен
ОК 30.	Безпека інфраструктури комп'ютерних мереж	4	екзамен
ОК 31.	Захист інформації в операційних системах	4	екзамен
ОК 32.	Технологія програмування захищених систем	4	залік
ОК 33.	Моделювання та безпека соціальних процесів	4,5	екзамен
ОК 34.	Захист інформації в інформаційно-комунікаційних системах	4,5	екзамен
ОК 35.	Безпека web-ресурсів та додатків	4	екзамен
ОК 36.	Комплексні системи захисту інформації	4,5	екзамен
ОК 37.	Інформаційні технології організації та захисту бізнес процесів	4	екзамен
ОК 38.	Курсова робота*	2	залік
ОК 39.	Курсова робота з навчальних дисциплін циклу професійної підготовки	2	залік
ОК 40	Практика обчислювальна	2	залік
ОК 41	Практика технологічна	2	залік
ОК 42	Практика виробнича	4	залік
Випускова кваліфікаційна робота		3	публічний захист
Загальний обсяг обов’язкових компонент		180 кредитів	
Цикл вибіркових дисциплін			
ВБ. 1	Вибіркова дисципліна 1	4,5	залік
ВБ. 2	Вибіркова дисципліна 2	5	залік
ВБ. 3	Вибіркова дисципліна 3	4,5	залік
ВБ. 4	Вибіркова дисципліна 4	4,5	залік
ВБ. 5	Вибіркова дисципліна 5	4,5	залік
ВБ. 6	Вибіркова дисципліна 6	4	залік
ВБ. 7	Вибіркова дисципліна 7	5	залік
ВБ. 8	Вибіркова дисципліна 8	5	залік
ВБ. 9	Вибіркова дисципліна 9	5	залік
ВБ. 10	Вибіркова дисципліна 10	5	залік
ВБ. 11	Вибіркова дисципліна 11	6,5	залік
ВБ. 12	Вибіркова дисципліна 12	6,5	залік
Загальний обсяг вибіркових компонент		60 кредитів	
Загальний обсяг освітньої програми		240 кредитів	

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

2.2. Структурно-логічна схема ОП



*Курсова робота на основі вивчених нормативних начальних дисциплін: сучасне програмне забезпечення та хмарні технології, організація баз даних та знань, новітні інформаційні технології для аналізу і обробки даних, сучасні методи обчислень, нормативно-правова база кібербезпеки, вступ до програмування, організаційне забезпечення захисту інформації, математичні основи криптографії, архітектура комп'ютерних систем та схемотехніка. ****** - Використовується у багатьох дисциплінах. ***- Курсова робота на основі вивчених навчальних фахових дисциплін циклу професійної підготовки. *****- Різні види практик на основі навчальних фахових дисциплін циклу загальної та професійної підготовки

3. Форми атестації здобувачів вищої освіти

Атестація здобувачів першого (бакалаврського) освітньо-професійного рівня за спеціальністю « 125Кібербезпека» здійснюється у формі публічного захисту кваліфікаційного проекту/роботи та завершується видачею документа встановленого зразка про присудження йому ступеня з освітньою кваліфікацією «Бакалавр з кібербезпеки», з присвоєнням професійної кваліфікації «Фахівець з організації інформаційної безпеки».

На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих здобувачем в процесі навчання згідно «Стандарту вищої освіти за спеціальністю 125 "Кібербезпека" для першого (бакалаврського) рівня вищої освіти №1074 від 10.04.2018 р.». Термін проведення атестації визначається навчальним планом та графіком освітнього процесу.

До атестації допускаються студенти, які виконали всі вимоги програми підготовки.

Кваліфікаційний проект/робота має передбачати розв’язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки. Кваліфікаційний проект/робота має бути перевірений на плагіат та оприлюднений на сайті ЗВО.

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

	ЗК 1	ЗК 2	ЗК 3	ЗК 4	ЗК 5	ЗК 6	ЗК 7
ОК 1.			+				
ОК 2.						+	
ОК 3.			+				
ОК 4.	+				+		
ОК 5.							+
ОК 6.						+	
ОК 7.					+		
ОК 8.					+		
ОК 9.	+	+		+	+		
ОК 10.	+	+		+	+		
ОК 11.	+				+		

OK 12.					+		
OK 13.					+		
OK 14.	+	+		+	+		+
OK 15.	+	+		+	+	+	+
OK 16.	+	+	+		+		
OK 17.	+	+		+	+		
OK 18.	+				+		
OK 19.	+	+					
OK 20.	+	+		+	+		
OK 21.	+						
OK 22.	+	+		+	+		
OK 23.	+	+		+	+		
OK 24.	+			+	+		
OK 25.	+	+		+	+		
OK 26.	+	+		+	+		
OK 27.					+		
OK 28.	+	+		+	+		
OK 29.	+	+		+	+		
OK 30.	+	+		+	+		
OK 31.	+	+		+	+		
OK 32.	+	+		+	+		
OK 33.	+	+		+	+		
OK 34.	+	+		+	+		

ОК 35.		+		+			
ОК 36.	+	+		+	+		
ОК 37.	+	+		+	+		
ОК 38.	+	+			+		
ОК 39.	+	+		+	+		
ОК 40.	+	+		+	+		
ОК 41	+	+		+	+		
ОК 42	+	+		+	+		

5. Матриця відповідності фахових компетентностей (ФК) компонентам освітньо-професійної програми

	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.		+										

OK 11.		+						+				+
OK 12.		+										
OK 13.		+										
OK 14.	+							+				
OK 15.	+						+					
OK 16.		+										
OK 17.	+	+			+		+	+				+
OK 18.								+				+
OK 19.			+			+						
OK 20.								+	+			+
OK 21.			+			+						
OK 22.					+				+			
OK 23.									+		+	+
OK 24.								+				+
OK 25.			+		+	+						
OK 26.			+							+		
OK 27.		+										
OK 28.										+		+
OK 29.			+		+	+	+			+		
OK 30.			+		+	+						
OK 31.					+	+	+		+			

OK 32.							+		+			
OK 33.		+										
OK 34.			+		+	+	+		+		+	
OK 35.					+	+					+	+
OK 36.							+		+			
OK 37.				+					+		+	+
OK 38.								+				
OK 39.		+						+				
OK 40.		+					+				+	
OK 41		+				+	+		+		+	+
OK 42	+	+	+	+	+	+	+	+	+	+	+	+

6. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньо-професійної програми

	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
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.		+	+	+		+																				
ОК 42.		+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	

	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 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.																												
ОК 42.	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		

Гарант освітньої програми програми ст. викл. Прус Р.Б.

Керівник групи забезпечення ст. викл. Сачук Ю.В.