П Р О Є К Т

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА»

першого (бакалаврського) рівня вищої освіти

галузі знань ***12 Інформаційні технології***
спеціальності ***125 Кібербезпека та захист інформації***
освітня кваліфікація ***Бакалавр з кібербезпеки та захисту інформації***

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Голова вченої ради
_____ Володимир ОНИЩЕНКО
(протокол № ___ від «___» _____ 2024 р.)

Освітньо-професійна програма вводиться в дію з 01.09.2024

Ректор _____ Володимир ОНИЩЕНКО
(наказ № ___ від «___» _____ 2024 р.)

Полтава, 2024

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

«КІБЕРБЕЗПЕКА»

РІВЕНЬ ВИЩОЇ ОСВІТИ	*Перший (бакалаврський) рівень*
СТУПІНЬ ВИЩОЇ ОСВІТИ	*Бакалавр*
ГАЛУЗЬ ЗНАНЬ	*12 Інформаційні технології*
СПЕЦІАЛЬНІСТЬ	*125 Кібербезпека та захист інформації*
ОСВІТНЯ КВАЛІФІКАЦІЯ	*Бакалавр з кібербезпеки та захисту інформації*

ПОГОДЖЕНО
Проректор з науково-педагогічної та навчальної роботи

_____ Анатолій МАРТИНЕНКО
«____» _____ 2024 р.

ПОГОДЖЕНО
Директор департаменту організації навчального процесу, акредитації та ліцензування

_____ Олег МАКСИМЕНКО
«____»_____2024 р.

РЕКОМЕНДОВАНО
Вченою радою
Навчально-наукового інституту інформаційних технологій та робототехніки
Протокол № __ від «__» _____ 2024 р.
Голова вченої ради інституту
_____ Володимир ПЕНЦ

СХВАЛЕНО
Навчально-методичною комісією
Навчально-наукового інституту інформаційних технологій та робототехніки
Протокол № __ від «__» _____ 2024 р.
Голова НМК інституту
_____ Олександр ШЕФЕР

СХВАЛЕНО
Кафедрою комп'ютерних та інформаційних технологій і систем
Протокол № __ від «__» _____ 2024 р.
В.о. завідувача кафедрою
_____ Олена ДВІРНА

РОЗРОБЛЕНО
Проєктною (робочою) групою,
Керівник проєктної (робочої) групи, гарант освітньо-професійної програми
_____ Юрій ЗДОРЕНКО
«____» _____ 2024 р.

ПЕРЕДМОВА

Освітньо-професійна програма розроблена відповідно до Стандарту вищої освіти України першого (бакалаврського) рівня вищої освіти, галузь знань – 12 Інформаційні технології, спеціальність 125 Кібербезпека та захист інформації, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 27.09.2016 №7.

Програму розроблено проєктною (робочою) групою у складі:

Керівник проєктної (робочої) групи:

Здоренко Юрій Миколайович – доцент кафедри комп'ютерних та інформаційних технологій і систем, кандидат технічних наук, доцент;

Члени проєктної (робочої) групи:

Головко Геннадій Вячеславович – доцент кафедри комп'ютерних та інформаційних технологій і систем, кандидат технічних наук, доцент;

Янко Аліна Сергіївна – доцент кафедри комп'ютерних та інформаційних технологій і систем, кандидат технічних наук, доцент

До розробки освітньої програми були долучені:

Ковтун В.В. – керівник навчального центру Software Development Services

Шейко І.О. – директор IT-компанії DIGI CODE

Треумов Д.О. –SEO-спеціаліст компанії IST GrouP

Зовнішні рецензенти:

1. NIXSOLUTIONS, м. Харків
2. Partizan Security Global
3. Харківський IT-кластер

1. Профіль освітньо-професійної програми зі спеціальності 125 Кібербезпека та захист інформації

1.1. Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Національний університет «Полтавська політехніка імені Юрія Кондратюка»; Навчально-науковий інститут інформаційних технологій та робототехніки; Кафедра комп'ютерних та інформаційних технологій і систем
Рівень вищої освіти	Перший (бакалаврський) рівень вищої освіти
Ступінь вищої освіти	Бакалавр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Назва освітньої програми	Кібербезпека
Інтернет-адреса розміщення освітньої програми	https://nupp.edu.ua/page/litsenzuvannya-ta-akreditatsiya.html
Форми навчання	Денна
Освітня кваліфікація	Бакалавр з кібербезпеки та захисту інформації
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – 125 Кібербезпека та захист інформації Освітня програма – «Кібербезпека»
Опис предметної області	**Об'єкт(и) вивчення та діяльності:** 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 складають** 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
Академічні права випускників	Можливість продовження навчання на другому (освітньо-професійному) рівні вищої освіти та здобувати додаткові кваліфікації в системі післядипломної освіти
Обсяг кредитів за Європейською кредитно-трансферною системою, необхідний для здобуття відповідного ступеня вищої освіти	240 кредитів ЄКТС Термін навчання – 3 роки, 10 місяців
Наявність акредитації	Акредитується вперше
Цикл / рівень	НРК України – 6 рівень, QF-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Наявність повної загальної середньої освіти або ступеня молодший бакалавр (молодший спеціаліст)
Мова(и) викладання	Українська мова
Термін дії освітньої програми	Термін дії освітньої програми – до 30.06.2026»
1.2. Мета освітньої програми	
Мета освітньої програми	Мета освітньої програми полягає в підготовці фахівців, здатних вирішувати складні спеціалізовані задачі та практичні проблеми забезпечення інформаційної безпеки та захисту інформаційної та кібернетичної безпеки держави
1.3. Характеристика освітньої програми	
Орієнтація	Освітньо-професійна програма базується має прикладну

освітньої програми	орієнтацію і спрямована на вирішення спеціалізованих та практичних задач з кібербезпеки та захисту інформації.
Основний фокус освітньої програми	Загальна вища освіта в галузі інформаційних технологій, спрямованих на розв'язання задач забезпечення кібернетичної безпеки, набуття професійних навичок фахівця із захисту даних. Акцент на формуванні вмінь застосовувати технології й програмно-технічні засоби проектування, реалізації, впровадження й супроводження програмних засобів різного призначення, комплексних систем захисту інформації, кібербезпеки, комп'ютерних систем і мереж, веб-технологій. Ключові слова: кібербезпека, комп'ютерні системи, комп'ютерні мережі, програмування, захист програмного забезпечення, інформаційно-комунікаційні технології, інформаційна безпека, захист інформації
Особливості та відмінності програми	Характерною особливістю даної програми є надання можливості поглибленого вивчення дисциплін, присвячених інформаційній та кібербезпеці, поглиблено вивчати іноземну мову протягом усього терміну навчання. Студенти мають можливість вибудувати унікальну індивідуальну освітню траєкторію шляхом вибору навчальних дисциплін та поглиблювати знання, обираючи один з двох мейджорів – «Захист корпоративних мереж» або «Блокчейн та безпека банківських систем». Здобувачі вищої освіти за цією освітньою програмою мають можливість брати участь в програмах міжнародної академічної мобільності (тривалістю 1 або 2 семестри).
1.4. Придатність випускників освітньої програми до працевлаштування	
Придатність до працевлаштування	Випускники підготовлені до роботи за національним класифікатором України (ДК 003:2010): 3439 – фахівець із організації інформаційної безпеки, 3439 – фахівець із організації захисту інформації з обмеженим доступом, 3439 – фахівець з режиму секретності, 3439 – інспектор з організації захисту секретної інформації
1.5. Викладання та оцінювання	
Викладання та навчання	Проведення лекційних, практичних та лабораторних занять, організація майстер-класів, наукових конференцій та семінарів; залучення студентів до участі в проєктних роботах, конкурсах, олімпіадах та науково-дослідних заходах. Залучення до проведення занять кваліфікованих фахівців-практиків. Написання та захист кваліфікаційної роботи, яка презентується та обговорюється за участі викладачів, практиків, студентів. Застосовуються інноваційні технології дистанційного навчання з використанням онлайн-платформ для проведення занять

Оцінювання	**Форми контролю:** письмові екзамени (тестування, вирішення проблемних завдань, розв'язання певної прикладної задачі), усне екзаменування, заліки, проміжні контрольні роботи та опитування, презентації, звіти з практик, публічний захист курсових робіт, публічний захист кваліфікаційної роботи. **Види контролю:** поточний та підсумковий контроль **Шкала оцінювання:** оцінювання здійснюється за 100-бальною (рейтинговою) шкалою, шкалою ЄКТС (ECTS), (A, B, C, D, E, FX, F), національною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно»).
1.6. Програмні компетентності	
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)	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Спеціальні (фахові, предметні) компетентності (СК)	КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-

	апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
1.7. Програмні результати (ПР)	
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 та\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 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 ріні 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	
1.8. Ресурсне забезпечення реалізації програми	
Основні характеристики кадрового забезпечення	Заклад вищої освіти забезпечує освітній процес необхідними та доступними для здобувачів вищої освіти кадровими ресурсами. До реалізації освітньої програми залучені науково-педагогічні працівники, з яких 87% мають вчені звання та/або наукові ступені. До викладання професійно-орієнтованих дисциплін залучаються викладачі-практики. Частка лекційних годин науково-педагогічних працівників з практичним досвідом роботи складає більше 16%. Освітня та/або професійна кваліфікація науково-педагогічних працівників, що залучені до реалізації освітніх компонентів освітньої програми, повністю відповідає вимогам Ліцензійних умов провадження освітньої діяльності, затверджених постановою Кабінету Міністрів України від 30.12.2015 р. №1187 (в редакції постанови Кабінету Міністрів України від 24.03.2021 №365)
Основні характеристики матеріально-технічного забезпечення	Використання лекційних аудиторій, обладнаних мультимедійною технікою; навчальних аудиторій для проведення практичних та лабораторних занять з використанням персональних комп'ютерів; спеціалізованих навчальних лабораторій Lenovo, Dell, Asus, HP, Cisco.
Основні характеристики інформаційного та навчально-методичного забезпечення	Усі освітні компоненти забезпечені навчально-методичними розробками науково-педагогічних працівників університету – методичними вказівками, навчальними посібниками або підручниками. Навчальні матеріали з кожного освітнього компонента освітньої програми розміщені на платформі дистанційного навчання Moodle. Студенти отримують повний доступ до електронної бібліотеки університету. Індивідуальний навчальний план та персональний розклад занять доступні в особистому електронному кабінеті студента.
1.9. Академічна мобільність	
Національна кредитна мобільність	Національна кредитна мобільність може здійснюватися відповідно до угод Національного університету «Полтавська політехніка імені Юрія Кондратюка» у закладах вищої освіти (наукових установах) – партнерах Національного університету «Полтавська політехніка імені Юрія Кондратюка» в межах України та згідно з Положенням про порядок реалізації права здобувачів вищої освіти Національного університету «Полтавська політехніка імені Юрія Кондратюка» на академічну мобільність. https://nupp.edu.ua/uploads/files/0/doc/polozhennia/akademichna-

	mobilnist.pdf
Міжнародна кредитна мобільність	Може реалізовуватися здобувачами вищої освіти відповідно до укладених угод Національного університету «Полтавська політехніка імені Юрія Кондратюка» та угоди (Еразмус+К1) у закладах вищої освіти (наукових установах) – партнерах поза межами України та згідно з Положенням про порядок реалізації права здобувачів вищої освіти Національного університету «Полтавська політехніка імені Юрія Кондратюка» на академічну мобільність. https://nupp.edu.ua/uploads/files/0/doc/polozhennia/akademichna-mobilnist.pdf
Навчання іноземних здобувачів вищої освіти	Навчання іноземних студентів може здійснюватися згідно з вимогами чинного законодавства

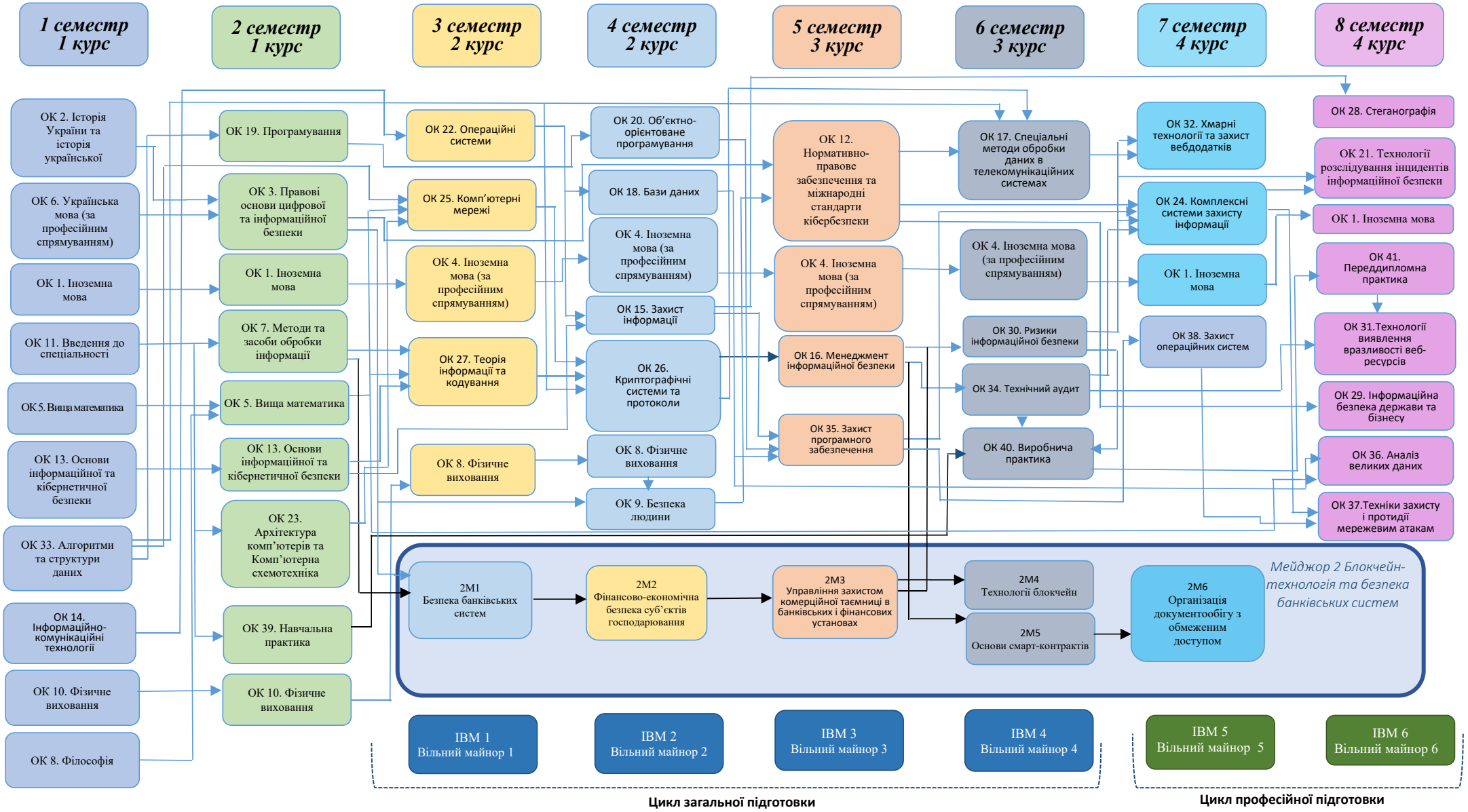
2. Перелік компонент освітньої програми та їх логічна послідовність

2.1. Перелік компонент освітньо-професійної програми

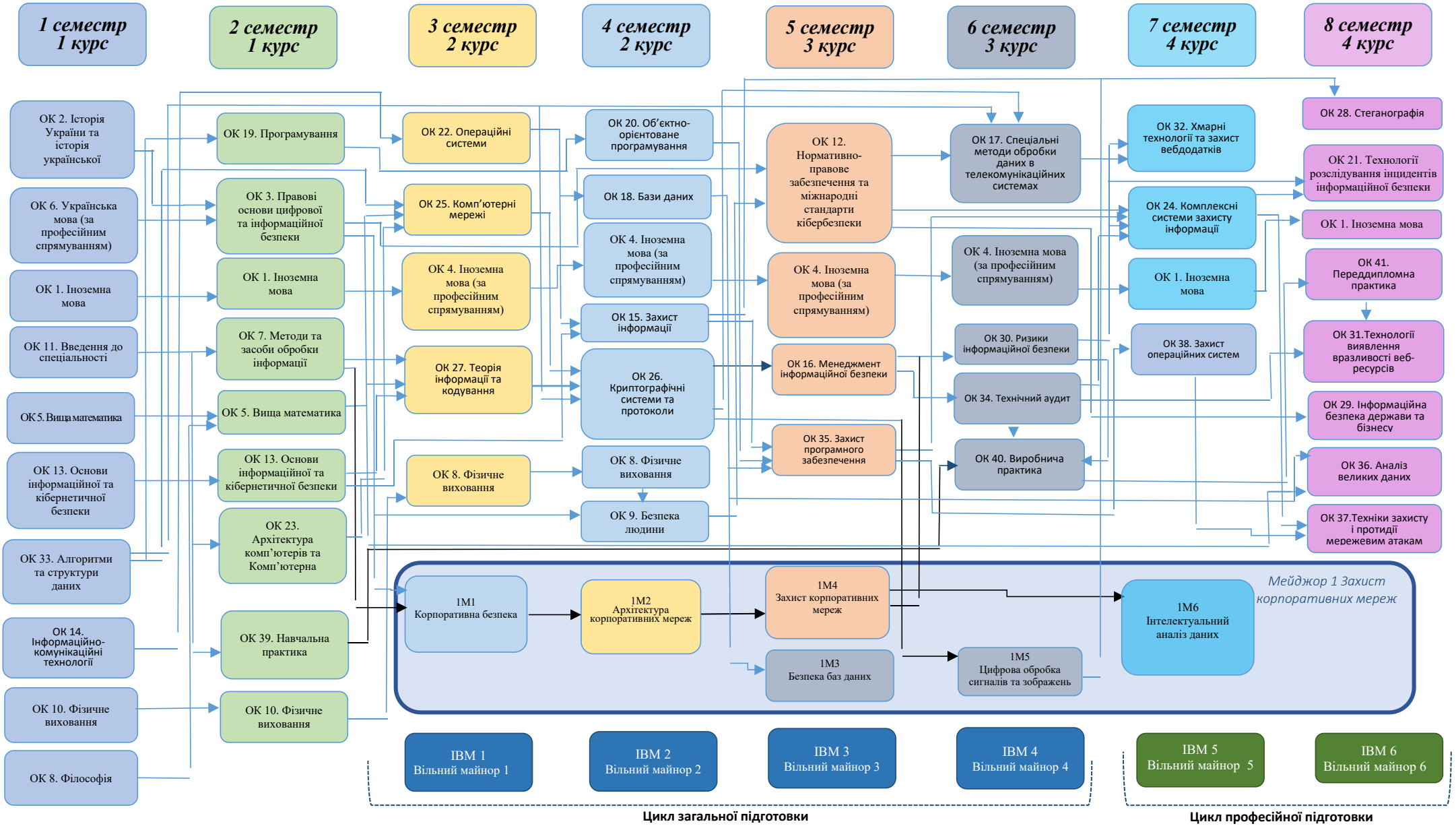
Код о/к	Компоненти освітньої програми (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ			
І. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
ОК 1.	Іноземна мова	8	диф. залік, екзамен
ОК 2	Історія України та української культури	3	диф. залік
ОК 3	Правові основи цифрової та інформаційної безпеки	4	диф. залік
ОК 4.	Іноземна мова за професійним спрямуванням	8	диф. залік, екзамен
ОК 5.	Вища математика	7	екзамен
ОК 6.	Українська мова за професійним спрямуванням	3	екзамен
ОК 7	Методи та засоби обробки інформації	4	диф. залік
ОК 8	Безпека людини	3	екзамен
ОК 9	Філософія	3	екзамен
ОК 10	Фізичне виховання		диф. залік
Загальний обсяг обов'язкових компонент загальної підготовки:		**43**	
ІІ. ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОК 11	Введення до спеціальності	4	екзамен
ОК 12	Нормативно-правове забезпечення та міжнародні стандарти кібербезпеки	4	екзамен
ОК 13	Основи інформаційної та кібернетичної безпеки	5	диф. залік, екзамен
ОК 14	Інформаційно-комунікаційні технології	4	диф. залік
ОК 15	Захист інформації	4	КР, екзамен
ОК 16	Менеджмент інформаційної безпеки	4	екзамен
ОК 17	Спеціальні методи обробки даних в телекомунікаційних системах	5	екзамен
ОК 18	Бази даних	5	екзамен
ОК 19	Програмування	6	диф. залік, екзамен
ОК 20	Об'єктно-орієнтоване програмування	5	екзамен
ОК 21	Технології розслідування інцидентів інформаційної безпеки	4	екзамен
ОК 22	Операційні системи	5	екзамен
ОК 23	Архітектура комп'ютерів та Комп'ютерна схемотехніка	4	диф. залік
ОК 24	Комплексні системи захисту інформації	5	КР, екзамен
ОК 25	Комп'ютерні мережі	5	КР, екзамен
ОК 26	Криптографічні системи та протоколи	4	екзамен
ОК 27	Теорія інформації та кодування	5	екзамен
ОК 28	Стеганографія	4	екзамен
ОК 29	Інформаційна безпека держави та бізнесу	4	екзамен
ОК 30	Ризики інформаційної безпеки	4	екзамен
ОК 31	Технології виявлення вразливості веб-ресурсів	3	диф. залік
ОК 32	Хмарні технології та захист вебдодатків	4	екзамен
ОК 33	Алгоритми та структури даних	6	екзамен
ОК 34	Технічний аудит	3	КР,екзамен
ОК 35	Захист програмного забезпечення	4	КР,екзамен

ОК 36	Аналіз великих даних	4	диф. залік
ОК 37	Техніки захисту і протидії мережевим атакам	4	диф. залік
ОК 38	Захист операційних систем	4	диф. залік
ОК 39	Навчальна практика	3	диф. залік
ОК 40	Виробнича практика	6	диф. залік
ОК 41	Переддипломна практика	6	диф. залік
Загальний обсяг обов'язкових компонент професійної підготовки:		**137**	
Загальний обсяг обов'язкових компонент загальної та професійної підготовки:		**180**	
ВИБІРКОВІ КОМПОНЕНТИ			
І. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
УВМ1	Вільний майнор 1	4	диф. залік
УВМ 2	Вільний майнор 2	4	диф. залік
УВМ 3	Вільний майнор 3	4	диф. залік
УВМ 4	Вільний майнор 4	4	диф. залік
Загальний обсяг вибіркових компонент загальної підготовки:		**16**	
ІІ. ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ІВМ1	Вільний майнор 5	4	
ІВМ2	Вільний майнор 6	4	
Мейджор 1 «Захист корпоративних мереж» (Блок вибіркових дисциплін №1 за освітньою програмою)			
1 ММ 1	Архітектура корпоративних мереж	6	диф. залік
1 ММ 2	Корпоративна безпека	6	диф. залік
1 ММ 3	Безпека баз даних	6	диф. залік
1 ММ 4	Захист корпоративних мереж	6	диф. залік
1 ММ 5	Цифрова обробка сигналів та зображень	6	диф. залік
1 ММ 6	Інтелектуальний аналіз даних	6	диф. залік
Мейджор 2 «Блокчейн-технологія та безпека банківських систем» (Блок вибіркових дисциплін №2 за освітньою програмою)			
2 ММ 1	Безпека банківських систем	6	диф. залік
2 ММ 2	Фінансово-економічна безпека суб'єктів господарювання	6	диф. залік
2 ММ 3	Управління захистом комерційної таємниці в банківських і фінансових установах	6	диф. залік
2 ММ 4	Технології блокчейн	6	диф. залік
2 ММ 5	Основи смарт-контрактів	6	диф. залік
2 ММ 6	Організація документообігу з обмеженим доступом	6	диф. залік
Загальний обсяг вибіркових компонент професійної підготовки:		**44**	
Загальний обсяг вибіркових компонент загальної та професійної підготовки		**60**	
ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ		**240**	

2.2. Структурно-логічна схема ОП (індивідуальна освітня траєкторія за мейджором 1 «Блокчейн-технологія та безпека банківських систем»)



2.2. Структурно-логічна схема ОП (індивідуальна освітня траєкторія за мейджором 2 «Захист корпоративних мереж»)



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом та освітньою програмою.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	КЗ 1.	КЗ 2.	КЗ 3.	КЗ 4.	КЗ 5.	КЗ 6.	КЗ 7.	КФ 1.	КФ 2.	КФ 3.	КФ 4.	КФ 5.	КФ 6.	КФ 7.	КФ 8.	КФ 9.	КФ 10.	КФ 11.	КФ 12.
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 відповідності програмним результатів компонентам освітньої 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
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 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
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 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
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									*							