МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»

першого рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: Бакалавр, Кібербезпека,

Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ

Голова вченої ради

_____ / В.В. Семенець /

(протокол № 2 від "24" лютого 2020 р.)

зі змінами

протокол № 1 від "28" січня 2021 р.

Освітня програма вводиться в дію з 01.09.2020 р.

Ректор_____ / В.В. Семенець /

(наказ № 117 від "27" лютого 2020 р.)

зі змінами

наказ № 46 від "02" лютого 2021 р.

Харків 2021 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«Безпека інформаційних і комунікаційних систем»
першого рівня вищої освіти
за спеціальністю 125 Кібербезпека

УЗГОДЖЕНО

Перший проректор
_____ І.В. Рубан
«26» 01 2021 р.

В.о. начальника відділу ЛА та ВСЗЯО
_____ С.Б. Макашев
«26» 01 2021 р.

Начальник навчального відділу
_____ А.В. Міхнова
«25» 01 2021 р.

Розглянуто на засіданні Вченої ради факультету КІУ
Протокол № 5 від 25.01.2021 р.
Декан факультету КІУ
_____ О.С. Ляшенко

Розглянуто на засіданні кафедри БІТ
Протокол № 6 від 04.01.2021 р.
Завідувач кафедри БІТ
_____ Г.З. Халімов

Представники роботодавців

Кравченко Володимир Дмитрович
Виконавчий директор ПрАТ «ІІТ» В.Д. Кравченко

РОЗРОБЛЕНО

Проектна група:

керівник проектної групи:

Гріненко Тетяна Олексіївна, к.т.н., доц.,
доц. кафедри БІТ, ХНУРЕ _____ Т.О. Гріненко

члени проектної групи:

Ликов Юрій Володимирович, к.т.н., доц.,
доцент кафедри КРіСТЗІ, ХНУРЕ _____ Ю.В. Ликов

Снігуров Аркадій Владиславович, к.т.н., доц.,
доц. каф. ІКІ, декан факультету ІК, ХНУРЕ _____ А.В. Снігуров

Ляшенко Олексій Сергійович, к.т.н., доц.,
доц. каф. ЕОМ, декан факультету КІУ, ХНУРЕ _____ О.С. Ляшенко

Представник студентського самоврядування
Голова студентського сенату факультету КІУ _____ М.Е. Бондаренко

ПЕРЕДМОВА

Розроблено проектною групою у складі:

1. Гріненко Тетяна Олексіївна (керівник проектної групи)	- кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки
2. Ликов Юрій Володимирович	- кандидат технічних наук, доцент, доцент кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації Харківського національного університету радіоелектроніки
3. Снігуров Аркадій Владиславович	- кандидат технічних наук, доцент, декан факультету інфокомунікацій, доцент кафедри інфокомунікаційної інженерії ім. В.В. Поповського Харківського національного університету радіоелектроніки
4. Ляшенко Олексій Сергійович	- кандидат технічних наук, доцент, декан факультету комп'ютерної інженерії та управління, доцент кафедри електронних обчислювальних машин Харківського національного університету радіоелектроніки

1. Профіль освітньої програми «Безпека інформаційних і комунікаційних систем» за спеціальністю 125 Кібербезпека

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Харківський національний університет радіоелектроніки. Факультет комп'ютерної інженерії та управління (КІУ). Кафедра безпеки інформаційних технологій (БІТ)
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Бакалавр, Кібербезпека, Безпека інформаційних і комунікаційних систем
Офіційна назва освітньої програми	Безпека інформаційних і комунікаційних систем
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС термін навчання 3 роки 10 місяців, (2 роки 10 місяців)
Наявність акредитації	Сертифікат про акредитацію спеціальності МОН України УД№21001341 від 24.07.2015 року Строк дії сертифіката до 01.07.2025 року
Цикл/рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Повна загальна середня освіта (або освітньо-кваліфікаційний рівень молодшого спеціаліста)
Мова(и) викладання	Українська, англійська для іноземних студентів
Термін дії освітньої програми:	До повного завершення періоду навчання або наступного оновлення програми.
Інтернет-адреса постійного розміщення опису освітньої програми	https://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-125-kiberbezpeka/bakalavr-125-kiberbezpeka/osvitnja-programa-bezpeka-informacijnih-i-komunikacijnih-sistem
2- Мета освітньої програми	
Забезпечити підготовку висококваліфікованих фахівців в галузі інформаційних технологій зі спеціальності 125 Кібербезпека, здатних вирішувати складні спеціалізовані задачі та практичні проблеми інформаційної безпеки, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	12 Інформаційні технології 125 Кібербезпека

Орієнтація освітньої програми	Освітньо-професійна програма Акцент програми зроблений на набуття знань, умінь, компетенцій в галузі професійної діяльності, що передбачає застосування певних теорій та методів відповідних наук і характеризується комплексністю та невизначеністю умов
Основний фокус освітньої програми та спеціалізації	Загальна спеціальна освіта першого (бакалаврського) рівня вищої освіти в галузі інформаційних технологій за спеціальністю 125 Кібербезпека. ***Ключові слова***: кібербезпека, інформаційна безпека, криптографічний захист інформації, технічний захист інформації, захист персональних даних, антивірусний захист, захист інформації від несанкціонованого доступу, електронний цифровий підпис, захист від технічних розвідок
Особливості освітньої програми	Інтеграція програмно-апаратних засобів виявлення, моніторингу та забезпечення інформаційної безпеки сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності. Підготовка висококваліфікованих фахівців на високому методичному та професійному рівні.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлашту-вання	Випускники підготовлені до роботи за національним класифікатором України: Класифікатор професій (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
Подальше навчання	Можливість навчатися за програмою другого (магістерського) рівня вищої освіти
5 - Викладання та оцінювання	
Викладання та навчання	Лекції, практичні та лабораторні заняття, самонавчання, проектно-орієнтоване навчання, консультації із науково-педагогічними співробітниками, проведення наукових досліджень, підготовка кваліфікаційної роботи
Оцінювання	Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано); 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F)
6 – Програмні компетентності	
Інтегральна компетент-ність	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 компетент-ності (ЗК)	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області та розуміння професії. ЗК 3. Здатність спілкуватися рідною та другою іноземною мовою 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.
Спеціальні (фахові, предметні) 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 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. 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 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, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; ПРН-23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; ПРН-24 вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); ПРН-25 забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; ПРН-26 впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; ПРН-27 вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; ПРН-28 аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та 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 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	Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями та вченими званнями, які мають великий досвід навчально-методичної, науково-дослідної роботи та відповідають кваліфікації відповідно до спеціальності згідно ліцензійних умов.

Матеріально-технічне забезпечення	1.Забезпеченість приміщеннями для проведення навчальних занять та контрольних заходів. 2. Забезпеченість мультимедійним обладнанням для одночасного використання в навчальних аудиторіях. 3. Наявність соціально-побутової інфраструктури. 4. Забезпеченість здобувачів вищої освіти гуртожитком. 5. Забезпеченість комп'ютерними робочими місцями, лабораторіями, полігонами, обладнанням, устаткуванням, необхідними для виконання навчальних планів. 6.Забезпеченість комп'ютерною технікою, контрольно-вимірювальними приладами, програмно-технічними засобами автоматизації та системами автоматизації проектування. Засоби обчислювальної техніки з прикладним та спеціалізованим програмним забезпеченням, спеціальні радіовимірювальні пристрої, засоби технічного захисту інформації, спеціалізовані апаратно-програмні комплекси. Високий рівень практичної підготовки фахівців забезпечується розвиненою міжнародною співпрацею в науковій і освітніх сферах, наявністю спеціалізованих лабораторій: основ захисту інформації, технічних і програмно-апаратних засобів захисту і обробки інформації в інформаційно-комунікаційних системах, аналізу захищених децентралізованих блокчейн систем, моніторингу та виявлення каналів витоку інформації.
Інформаційне та навчально-методичне забезпечення	1. Забезпеченість вітчизняними та закордонними фаховими періодичними виданнями в галузі інформаційної безпеки та кібербезпеки, в тому числі в електронному вигляді. 2. Наявність доступу до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. 3. Наявність офіційного веб-сайту закладу освіти (http://nure.ua/) та кафедри (http://its.nure.ua/), на якому розміщена основна інформація про діяльність (структура, ліцензії та сертифікати про акредитацію, освітня/освітньо-наукова/ видавнича/ атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація). 4. Наявність електронного ресурсу закладу освіти, який містить навчально-методичні матеріали з дисциплін навчального плану, в тому числі в системі дистанційного навчання, також надання доступу до правової БД "Ліга: Закон"; електронних версій підручників видавництва «Центр учбової літератури»; електронних журналів: «Захист інформації. INSIDE»; «Information Security»; online-журнали з наукової бібліотеки eLIBRARY. Специфічними характеристиками інформаційного та навчально-методичного забезпечення є: - використання методів, моделей, методик та технологій створення, обробки, передачі, приймання, знищення, відображення та кіберзахисту інформаційних ресурсів; - використання методів та моделей розробки прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та кібербезпеки; - використання сукупності нормативно-правових (національні та міжнародні стандарти) та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі.

9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та закладами вищої освіти України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та закладами вищої освіти зарубіжних країн-партнерів.
Навчання іноземних здобувачів вищої освіти	На основі договорів (угод) між Харківським національним університетом радіоелектроніки та закладами вищої освіти іноземних країн.

2. Перелік компонентів освітньо-професійної програми та їх логічна послідовність

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проекти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
Обов'язкові компоненти ОП			
Гуманітарні та соціально-економічні дисципліни			
ОК 1.	Українське фахове мовлення	4	залік
ОК 2.	Філософія	4	екзамен
ОК 3.	Іноземна мова	8	екзамен
ОК3*	Українська мова як іноземна	8	залік
ОК 4.	Основи права	2	залік
ОК 5.	Фізичне виховання (за рахунок вільного часу студентів)		залік
ОК 5*	Українська мова як іноземна		залік
Всього		*18*	
Природничо-наукові (фундаментальні) дисципліни			
ОК 6.	Вища математика	12	екзамен
ОК 7.	Фізика	6	екзамен
Всього		*18*	
Дисципліни базової (професійної) підготовки за спеціальністю			
ОК 8.	Безпека життєдіяльності	3	залік
ОК 9.	Економіка та бізнес	3	залік
ОК 10.	Інформаційні технології	4	залік
ОК 11.	Вища математика (спец. розділи)	4	залік
ОК 12.	Архітектура комп'ютерних систем	4	екзамен
ОК 13.	Схемотехніка	4	залік
ОК 14.	Основи теорії кіл	4	екзамен
ОК 15.	Електрорадіовимірювання	4	залік
ОК 16.	Програмування	18	екзамен
ОК 17.	Нормативно-правове забезпечення інформаційної безпеки	4	залік
ОК 18.	Теорія інформації і кодування	5	екзамен
ОК 19.	Введення в спеціальність	4	залік
ОК 20.	Організація та управління захистом інформації	4	екзамен
ОК 21.	Інформаційно-комунікаційні системи	9	екзамен
ОК 22.	Операційні системи	4	екзамен
Всього		*78*	
Дисципліни професійної та практичної підготовки за ОПП			
ОК 23.	Теорія ймовірностей	4	залік
ОК 24.	Додаткові розділи вищої математики	3	залік
ОК 25.	Теорія елиптичних кривих	3	залік
ОК 26.	Прикладна криптологія	8,5	екзамен
ОК 27.	Комплекси ТЗІ	4	екзамен
ОК 28.	Захист від ТР	3,5	екзамен
ОК 29.	Комплексні системи ЗІ	7	екзамен
ОК 30.	Захист інформації в ІКС	6	екзамен

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проекти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ОК 31.	Криптосистеми і протоколи	6	екзамен
ОК 32.	Об'єктно-орієнтоване програмування	3	залік
ОК 33.	Виробнича практика	4,5	залік
ОК 34.	Передатестаційна практика	4,5	залік
ОК 35.	Кваліфікаційна робота	9	екзамен
Всього		*66*	
	Загальний обсяг обов'язкових компонент	**180**	
Вибіркові компоненти ОП			
Гуманітарні та соціально-економічні дисципліни			
ВБ 1.1	Психологія сприйняття та переробки інформації	3	залік
ВБ 1.2	Інформаційне суспільство	3	залік
ВБ 1.3	Правові основи професійної діяльності	3	залік
ВБ 1.4	Соціальна психологія та конфліктологія	3	залік
ВБ 1.5	Імідж сучасного спеціаліста	3	залік
ВБ 1.6	Soft skills: соціально-психологічні аспекти професійної компетентності	3	залік
ВБ 1.7	Психологія управління	3	залік
ВБ 2.1	Логіка	3	залік
ВБ 2.2	Політичні проблеми сучасного суспільства	3	залік
ВБ 2.3	Демократія: від теорії до практики	3	залік
ВБ 2.4	Ґендерні проблеми сучасного суспільства	3	залік
ВБ 2.5	Організація управління умовами праці	3	залік
ВБ 2.6	Етичні проблеми сучасного суспільства	3	залік
ВБ 2.7.	Екологічна безпека	3	залік
ВБ 3.1	Іноземна мова для професійної комунікації	6	залік
ВБ3.1*	Українська мова як іноземна	6	залік
ВБ 3.2	Академічна іноземна мова. Практичний курс	5	залік
Всього		*6*	
Дисципліни професійної та практичної підготовки			
ВБ 4.1	Мікроконтролери та мікропроцесори	4,5	залік
ВБ 4.2	Системи та засоби автентифікації	4,5	залік
ВБ 4.3	Теорія складності обчислень	4	залік
ВБ 4.4	Програмування криптопримітивів	4	залік
ВБ 4.5	Оптимізовані криптографічні кодування	4	залік
ВБ 4.6	Апаратні засоби захисту інформації	4	залік
ВБ 4.7	Захищені ІТС	4	залік
ВБ 4.8	Аналіз систем та криптопротоколів	4	залік
ВБ 4.9	Експертиза, стандартизація та сертифікація систем та засобів захисту інформації	4	екзамен
ВБ 4.10	Безпека електронної комерції, банківських та платіжних систем	4	екзамен
ВБ 4.11	Основи кібербезпеки	4	залік
ВБ 4.12	Захищені децентралізовані блокчейн системи	4	залік
ВБ 4.13	Системний аналіз процесів та систем захисту інформації	4	залік
ВБ 4.14	Аналіз криптопровайдерів	4	екзамен
ВБ 4.15	Безпека бездротових мереж	4	екзамен
ВБ 4.16	Проектування та тестування криптопримітивів	4	залік

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проекти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ВБ 4.17	Антивірусний захист	4	залік
ВБ 4.18	Методи досягнення консенсусу в розподілених системах	4	залік
ВБ 4.19	Технічний захист інформації в ході будівельно-монтажних робіт	5	залік
ВБ 4.20	Захист баз даних	5	залік
ВБ 4.21	Захищені операційні системи та безпечне програмування	7,5	залік
ВБ 4.22	Алгоритмічні основи еліптичної криптографії	5	залік
ВБ 4.23	Стеганографія	5	залік
ВБ 4.24	Методи аналізу захищених інформаційних систем	7,5	залік
Всього		54	
	Загальний обсяг вибіркових компонент	*60*	
	ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ	**240**	

* - для іноземних здобувачів вищої освіти.

2.2 Структурно логічна схема наведена на рисунку 1.

3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Безпека інформаційних і комунікаційних систем» спеціальності 125 Кібербезпека проводиться у формі захисту кваліфікаційної роботи та завершується видачою документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації: Бакалавр, Кібербезпека, Безпека інформаційних і комунікаційних систем.

Атестація здійснюється відкрито і публічно.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

Складається з двох частин у таблицях:

4.1. Матриця відповідності програмних компетентностей обов’язковим компонентам освітньої програми. Може корегуватися за рішенням Вченої ради факультету КІУ.

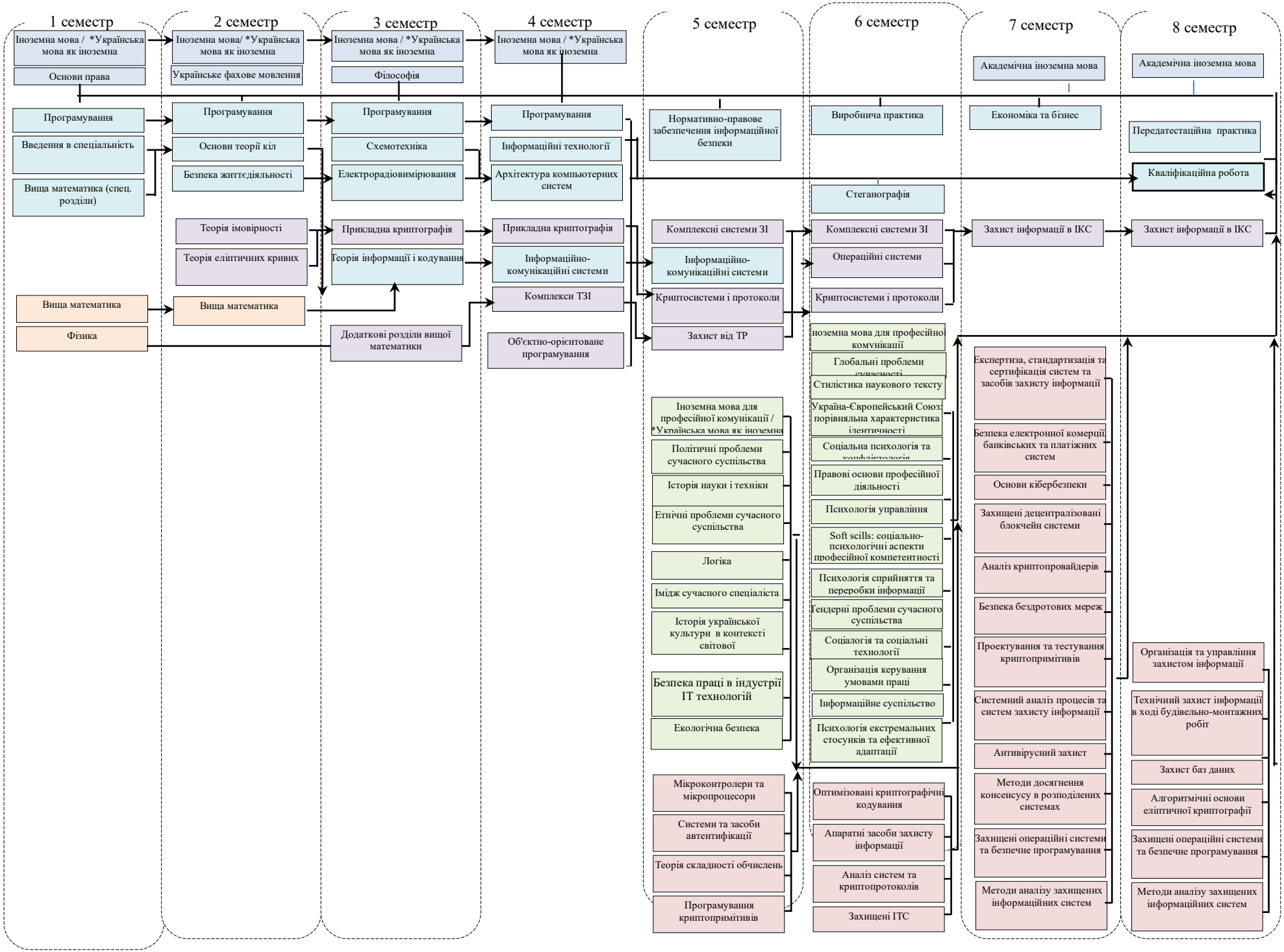
4.2. Матриця відповідності програмних компетентностей варіативним компонентам освітньої програми. Може корегуватися за рішенням кафедри БІТ.

5. Матриця забезпечення програмних результатів навчання компонентам освітньої програми

Складається з двох частин у таблицях:

5.1. Матриця забезпечення програмних результатів навчання обов’язковими компонентами освітньої програми. Може корегуватися за рішенням Вченої ради факультету КІУ.

5.2. Матриця забезпечення програмних результатів навчання вибірковими компонентами освітньої програми. Може корегуватися за рішенням кафедри БІТ


1 семестр
2 семестр
3 семестр
4 семестр
5 семестр
6 семестр
7 семестр
8 семестр
Іноземна мова / *Українська мова як іноземна
Іноземна мова/ *Українська мова як іноземна
Іноземна мова / *Українська мова як іноземна
Іноземна мова / *Українська мова як іноземна
Основи права
Українське фахове мовлення
Філософія
Академічна іноземна мова
Академічна іноземна мова
Програмування
Програмування
Програмування
Програмування
Нормативно-правове забезпечення інформаційної безпеки
Виробнича практика
Економіка та бізнес
Передатестаційна практика
Введення в спеціальність
Основи теорії кіл
Схемотехніка
Інформаційні технології
Кваліфікаційна робота
Вища математика (спец. розділи)
Безпека життєдіяльності
Електрорадіовимірювання
Архітектура компьютерних систем
Стеганографія
Теорія імовірності
Прикладна криптографія
Прикладна криптографія
Комплексні системи ЗІ
Комплексні системи ЗІ
Захист інформації в ІКС
Захист інформації в ІКС
Теорія еліптичних кривих
Теорія інформації і кодування
Інформаційно-комунікаційні системи
Інформаційно-комунікаційні системи
Операційні системи
Вища математика
Вища математика
Комплекси ТЗІ
Криптосистеми і протоколи
Криптосистеми і протоколи
Фізика
Додаткові розділи вищої математики
Об'єктно-орієнтоване програмування
Захист від ТР
іноземна мова для професійної комунікації
Глобальні проблеми сучасності
Стилістика наукового тексту
Експертиза, стандартизація та сертифікація систем та засобів захисту інформації
Україна-Європейський Союз: порівняльна характеристика ідентичності
Іноземна мова для професійної комунікації / *Українська мова як іноземна
Соціальна психологія та конфліктологія
Безпека електронної комерції банківських та платіжних систем
Політичні проблеми сучасного суспільства
Правові основи професійної діяльності
Основи кібербезпеки
Історія науки і техніки
Психологія управління
Захищені децентралізовані блокчейн системи
Етнічні проблеми сучасного суспільства
Soft scills: соціально-психологічні аспекти професійної компетентності
Аналіз криптопровайдерів
Логіка
Психологія сприйняття та переробки інформації
Безпека бездротових мереж
Імідж сучасного спеціаліста
Ґендерні проблеми сучасного суспільства
Проектування та тестування криптопримітивів
Організація та управління захистом інформації
Історія української культури в контексті світової
Соціалогія та соціальні технології
Системний аналіз процесів та систем захисту інформації
Технічний захист інформації в ході будівельно-монтажних робіт
Безпека праці в індустрії ІТ технологій
Організація керування умовами праці
Антивірусний захист
Захист баз даних
Інформаційне суспільство
Екологічна безпека
Психологія екстремальних стосунків та ефективної адаптації
Мікроконтролери та мікропроцесори
Оптимізовані криптографічні кодування
Методи досягнення консенсусу в розподілених системах
Алгоритмічні основи еліптичної криптографії
Системи та засоби автентифікації
Апаратні засоби захисту інформації
Захищені операційні системи та безпечне програмування
Захищені операційні системи та безпечне програмування
Теорія складності обчислень
Аналіз систем та криптопротоколів
Методи аналізу захищених інформаційних систем
Методи аналізу захищених інформаційних систем
Програмування криптопримітивів
Захищені ІТС

4.1 Матриця відповідності програмних компетентностей обов'язковим компонентам освітньої програми

	ОК1	ОК2	ОК3	ОК*3	ОК4	ОК5	ОК*5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35
ЗК1								+	+		+	+	+	+	+	+	+		+	+		+	+	+	+	+	+	+	+	+	+	+		+	+	+
ЗК2												+	+	+				+	+		+	+					+	+	+	+	+	+	+	+	+	+	+
ЗК3	+		+	+			+																														
ЗК4					+			+	+	+	+				+	+									+										+	+	
ЗК5												+		+				+		+		+	+	+	+			+						+	+	+	+
ЗК6			+		+																																
ЗК7			+		+	+																															
ФК1	+												+						+		+	+						+			+		+		+	+	+
ФК2												+		+						+		+	+			+	+	+	+			+		+	+	+	+
ФК3														+										+				+		+	+	+					+
ФК4											+																		+		+	+	+				
ФК5																				+		+	+	+				+	+		+	+			+	+	+
ФК6																								+					+		+	+					
ФК7																												+			+						+
ФК8																						+						+			+						
ФК9																						+						+									
ФК10																						+							+	+		+	+				
ФК11																						+	+									+					
ФК12																						+									+						+

4.2 Матриця відповідності програмних компетентностей вибірковим компонентам освітньої програми

	ВБ4.1	ВБ4.2	ВБ4.3	ВБ4.4	ВБ4.5	ВБ4.6	ВБ4.7	ВБ4.8	ВБ4.9	ВБ4.10	ВБ4.11	ВБ 4.12	ВБ4.13	ВБ4.14	ВБ4.15	ВБ4.16	ВБ 4.17	ВБ 4.18	ВБ4.19	ВБ4.20	ВБ4.21	ВБ4.22	ВБ4.23	ВБ4.24
ЗК1		+	+	+	+	+	+	+	+			+		+	+	+	+	+	+	+		+		+
ЗК2	+	+						+		+	+	+			+		+	+	+		+		+	+
ЗК3																								
ЗК4			+	+	+		+			+		+	+				+		+	+			+	
ЗК5	+	+						+	+	+					+			+		+	+	+		
ЗК6																								
ЗК7																								
ФК1		+				+	+		+	+							+		+					
ФК2	+	+					+	+		+	+	+		+	+	+	+	+		+	+			
ФК3			+			+	+	+			+						+							
ФК4												+	+											
ФК5								+					+		+			+						+
ФК6											+						+			+	+			
ФК7							+																	+
ФК8										+							+							
ФК9							+			+														
ФК10		+										+					+							
ФК11												+			+			+						+
ФК12								+		+					+					+	+			+

5.1. Матриця забезпечення програмних результатів навчання обов'язковими компонентами освітньої програми

	ОК1	ОК2	ОК3	ОК*3	ОК4	ОК5	ОК*5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35
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																		+															+	+			+

	ОК1	ОК2	ОК3	ОК*3	ОК4	ОК5	ОК*5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35
ПРН 32																								+					+		+						
ПРН 33																						+			+	+						+					
ПРН 34																			+			+													+	+
ПРН35															+																+				+	+	
ПРН36																	+			+									+	+							
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		+			+						+																										

5.2. Матриця забезпечення програмних результатів навчання вибірковими компонентами освітньої програми

	ВБ4.1	ВБ4.2	ВБ4.3	ВБ4.4	ВБ4.5	ВБ4.6	ВБ4.7	ВБ4.8	ВБ4.9	ВБ4.10	ВБ4.11	ВБ 4.12	ВБ4.13	ВБ4.14	ВБ4.15	ВБ4.16	ВБ 4.17	ВБ 4.18	ВБ4.19	ВБ4.20	ВБ4.21	ВБ4.22	ВБ4.23	ВБ4.24
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		+			+										+								+	

	ВБ4.1	ВБ4.2	ВБ4.3	ВБ4.4	ВБ4.5	ВБ4.6	ВБ4.7	ВБ4.8	ВБ4.9	ВБ4.10	ВБ4.11	ВБ 4.12	ВБ4.13	ВБ4.14	ВБ4.15	ВБ4.16	ВБ 4.17	ВБ 4.18	ВБ4.19	ВБ4.20	ВБ4.21	ВБ4.22	ВБ4.23	ВБ4.24
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										+														