Ф-22.05-04.01/125.00.01/Б-2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Кібербезпека

Першого (бакалаврського) рівня вищої освіти
галузі знань 12 «Інформаційні технології»
спеціальності 125 «Кібербезпека»
Кваліфікація: бакалавр з кібербезпеки

ЗАТВЕРДЖЕНО

Вченою радою Державного університету «Житомирська політехніка»

Голова Вченої ради

_____ Віктор ЄВДОКИМОВ

(протокол від «31» серпня 2020 р № 6)

Освітня програма вводиться в дію з 1 вересня 2020 р.

Ректор

_____ Віктор ЄВДОКИМОВ

(наказ від «31» серпня 2020 р № 380/од1)

Житомир – 2020

ПЕРЕДМОВА

Освітньо-професійну програму «Кібербезпека» розроблено відповідно до Стандарту вищої освіти України за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти (затверджено і введено в дію наказом Міністерства освіти і науки України № 1074 від 10 жовтня 2018 р.) робочою групою у складі:

1. Єфіменко А.А., к.т.н., завідувач кафедри комп'ютерної інженерії та кібербезпеки – гарант освітньої програми.
2. Лобанчикова Н.М., к.т.н., доцент, декан факультету інформаційно-комп'ютерних технологій, доцент кафедри комп'ютерної інженерії та кібербезпеки
3. Семенець С.П., д.пед.н., професор, професор кафедри фізики та вищої математики
4. Байлюк Є.М., старший викладач кафедри комп'ютерної інженерії та кібербезпеки
5. Покотило О.А., старший викладач кафедри комп'ютерної інженерії та кібербезпеки

Рецензії зовнішніх стейкхолдерів:

1. Новицький О.В., ТОВ «Treolabs».
2. Пилипчук О., Відділ протидії кіберзлочинам в Житомирській області Департаменту кіберполіції Національної поліції України
3. Молодецька К.В., Поліський національний університет

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

1 – Загальна інформація	
Повна назва закладу вищої освіти та структура підрозділу	Державний університет «Житомирська політехніка», факультет інформаційно-комп'ютерних технологій
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Перший (бакалаврський) рівень вищої освіти Кваліфікація – «бакалавр з кібербезпеки»
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	Відсутня
Цикл /рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Повна загальна середня освіта або наявність освітньо-кваліфікаційного рівня «Молодший спеціаліст»
Мова(и) викладання	Українська
Термін дії освітньої програми	Постійно
Інтернет-адреса постійного розміщення опису освітньої програми	https://ztu.edu.ua
2 – Мета освітньої програми	
Професійна підготовка фахівців з кібербезпеки, набуття ними компетентностей в застосуванні принципів, методів та засобів забезпечення кібербезпеки.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація)	12 – Інформаційні технології 125 – Кібербезпека
Орієнтація освітньої програми	Освітньо-професійна
Основний фокус освітньої програми та спеціалізації	Вища освіта в галузі інформаційних технологій. Програма фокусується на питанням забезпечення кібербезпеки сучасних комп'ютерних систем та мереж. Ключові слова: кібербезпека, комп'ютерна система, комп'ютерна мережа, інформаційна система, інформаційно-телекомунікаційна система, операційна система, адміністрування систем, прикладне та системне програмування, вразливість, атака, ризик, компрометація, протидія, захист інформації, тестування на проникнення, моніторинг, розслідування інциденту, міжмережне екранування, система виявлення та попередження вторгнень, кібероперації, спеціальні системи забезпечення кібербезпеки.

Особливості програми	Тісна співпраця з державними та приватними організаціями з метою отримання практичних навичок безпечної експлуатації, адміністрування, забезпечення захисту комп'ютерних систем та мереж, навичок розробки прикладного та системного програмного забезпечення, проходження практичної підготовки з розробки нових і вдосконалення існуючих комп'ютерних та інформаційних систем з подальшим впровадженням науково-практичних розробок у діяльність організацій та установ.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Працевлаштування в організаціях та підприємствах будь-якої форми власності на посадах: I. Згідно ДК 003:2010 3439 (24771). Фахівець із організації інформаційної безпеки. 2149.2 Фахівець (сфера захисту інформації) 1495 Менеджери (управителі) систем з інформаційної безпеки II. Згідно http://www.cyberdegrees.org/ P01 Chief Infosec Officer P02 Security Manager P03 Security Director P04 Security Auditor P05 Vulnerability Assessor P06 Penetretion Tester P07 Security Code Auditor P08 Forensics Expert P09 Security Architect P10 Security Analyst P11 Security Specialist P12 Security Administrator P13 Security Engineer P14 Incident Responder P15 Cryptographer P16 Security Software Developer P17 Security Consultant
Подальше навчання	Можливість навчання за програмою другого (магістерського) рівня
5 – Викладання та оцінювання	
Викладання та навчання	Викладання здійснюється на засадах студентоцентрованого навчання, самонавчання, проблемно-орієнтованого навчання тощо
Оцінювання	Поточне опитування, тестовий контроль, презентація індивідуальних завдань, звіти команд, звіти з практики. Підсумковий контроль – екзамени та заліки з

	урахуванням накопичених балів поточного контролю. Атестація – підготовка та публічний захист кваліфікаційної роботи/проекту
6 - Програмні компетентності	
Інтегральна компетентність	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.

7 - Результати навчання
РН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 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; РН 5. адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12. Розробляти моделі загроз та порушника; РН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 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; РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;
РН 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;
РН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційнотелекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
РН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
РН 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);
РН 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;
РН 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;
РН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
РН 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;
РН 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;
РН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
РН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
РН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
РН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
РН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
РН 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;
РН 36. Виявляти небезпечні сигнали технічних засобів;

РН 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;
РН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
РН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
РН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
РН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;
РН 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;
РН 45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
РН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
РН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
РН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;
РН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;
РН 50. Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
РН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;
РН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;
РН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
РН 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	У реалізації даної освітньої програми задіяно 1 доктор наук, професор, 8 кандидатів наук, доцентів, 2 кандидати наук. Таким чином, кадрове забезпечення освітньої програми відповідає ліцензійним вимогам щодо надання освітніх послуг у сфері вищої світи і є достатнім для забезпечення якості освітнього процесу
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення відповідає ліцензійним вимогам щодо надання освітніх послуг у сфері вищої світи і є достатнім для забезпечення якості освітнього процесу
Інформаційне та навчально-методичне забезпечення	Інформаційне та навчально-методичне забезпечення освітньої програми з підготовки фахівців зі спеціальності 125 «Кібербезпека» відповідає ліцензійним вимогам, має актуальний змістовий контент, базується на сучасних інформаційно-комунікаційних технологіях. В університеті функціонують Мережна академія Cisco, Центр підтримки академій Cisco, Центр підготовки інструкторів Cisco, ресурси яких доступні для студентів (за умови реєстрації).
9 – Академічна мобільність	
Національна кредитна мобільність	Реалізується в межах спільної діяльності з Національним технічним університетом «КПІ імені Ігоря Сікорського», Хмельницьким національним університетом, Запорізьким національним університетом, Житомирським військовим інститутом імені С.П. Корольова, Житомирським державним університетом імені Івана Франка, Поліським національним університетом, Національним університетом водного господарства та природокористування, Харківським національним університетом радіоелектроніки, Харківським національним університетом ім. В. Каразіна згідно укладених договорів про співпрацю.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Державним університетом «Житомирська політехніка» та зарубіжними закладами вищої освіти.
Навчання іноземних здобувачів вищої освіти	На навчання приймаються іноземні громадяни на умовах контракту, які мають документ про повну загальну середню освіту.

2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1. Перелік компонент освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти/ роботи, практики кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК1	Іноземна мова	24	Заліки, екзамен
ОК2	Розвиток комунікаційних навичок та групова динаміка	3	Залік
ОК3	Лінійна алгебра та аналітична геометрія	3	Залік
ОК4	Українська мова (за професійним спрямуванням)	3	Екзамен
ОК5	Фізика	4	Залік
ОК6	Математичний аналіз	8	Залік, Екзамен
ОК7	Теорія ймовірностей і математична статистика	3	Залік
ОК8	Комп'ютерна дискретна математика	3	Екзамен
ОК9	Екологія та безпека життєдіяльності	3	Залік
ОК10	Філософія	3	Екзамен
ОК11	Архітектура комп'ютера	4	Екзамен
ОК12	Основи програмування	7	Екзамен
ОК13	Пакети прикладних програм	3	Екзамен
ОК14	Об'єктно-орієнтоване програмування	7	Екзамен, Курсова робота
ОК15	Web-технології Ч.1	4	Залік
ОК16	Теорія електричних і магнітних кіл	5	Екзамен
ОК17	Електроніка	4	Залік
ОК18	Основи кібербезпеки	4	Екзамен
ОК19	Бази даних	4	Екзамен
ОК20	Комп'ютерна схемотехніка	4	Екзамен
ОК21	Адміністрування та захист баз та сховищ даних	6	Екзамен, Курсова робота
ОК22	Операційні системи	8	Залік, Екзамен
ОК23	Комп'ютерні мережі	11	Залік, Екзамен, Курсовий проект
ОК24	Нормативно-правове забезпечення кібербезпеки	4	Екзамен
ОК25	Захист інформації в комп'ютерних системах та мережах	9	Залік, Екзамен, Курсовий проект
ОК26	Теоретичні засади кібербезпеки	4	Екзамен
ОК27	Системи технічного захисту інформації	4	Екзамен, Курсова робота
ОК28	Кібероперації	7	Залік, Екзамен, Курсовий проект
ОК29	Навчальна практика	3	Диф. залік
ОК30	Технологічна практика	3	Диф. залік

ОК31	Виробнича практика	6	Диф. залік
ОК32	Переддипломна практика	6	Диф. залік
ОК33	Кваліфікаційна робота	6	Кваліфікаційна атестація
Загальний обсяг обов'язкових компонент:		**180**	
Вибіркові компоненти ОП			
Вибірковий блок 1 *(вибіркові навчальні дисципліни університет, перелік навчальних дисциплін ВК1.Х затверджуються наказом ректора щорічно, студенти обирають 4 навчальні дисципліни загальним обсягом 12 кредитів)*			
ВК1.Х	Дисципліна №1	3	Залік
ВК1.Х	Дисципліна №2	3	Залік
ВК1.Х	Дисципліна №3	3	Залік
ВК2.1	Історія України	3	Залік
ВК2.2	Політологія		
ВК2.3	Психологія		
ВК2.4	Соціологія		
Вибірковий блок 2 *(обираються навчальні дисципліни загальним обсягом 48 кредитів)*			
ВК3.1	Web-технології Ч.2	5	Залік
ВК3.2	Інформаційні технології		
ВК3.3	Інформаційно-комунікаційні технології		
ВК4.1	Комп'ютерна графіка	4	Екзамен
ВК4.2	Технології візуалізації даних		
ВК4.3	Конструювання графічних інтерфейсів		
ВК4.4	Гігієна та фізіологія людини		
ВК4.5	Системи комутації та розподілу інформації		
ВК5.1	Програмування мовою Python	4	Екзамен
ВК5.2	Програмування мовою R		
ВК5.3	Технології моделювання		
ВК5.4	Комп'ютерне проектування в галузі інженерії		
ВК6.1	Прикладна криптологія та безпека програмного забезпечення	4	Екзамен
ВК6.2	Прикладна криптологія		
ВК6.3	Криптографія та стеганографія		
ВК7.1	Системний аналіз та теорія прийняття рішень	5	Екзамен
ВК7.2	Системи підтримки прийняття рішень		
ВК7.3	Штучний інтелект в задачах кібербезпеки		
ВК8.1	Безпровідні мережі	4	Екзамен
ВК8.2	Мережі мобільного зв'язку		
ВК8.3	Глобальні мережі		
ВК9.1	Архітектура та технології IoT	4	Екзамен
ВК9.2	Системи контролю і управління доступом		
ВК9.3	Інфраструктура відкритих ключів		
ВК10.1	Управління кібербезпекою	4	Екзамен

ВК10.2	Інформаційно-аналітичне забезпечення систем кібербезпеки		
ВК10.3	Теорія ризиків та її застосування в кібербезпеці		
ВК11.1	Хмарні технології	4	Екзамен
ВК11.2	Технології та засоби сумісної роботи		
ВК11.3	Медична кібернетика		
ВК11.4	Інформаційні радіосистеми та технології		
ВК12.1	Тестування на проникнення, виявлення та розслідування інцидентів кібербезпеки	3	Залік
ВК12.2	Безпека додатків ОС Windows		
ВК12.3	Безпека мобільних та Web-додатків		
ВК13.1	Адміністрування комп'ютерних систем та мереж	7	Залік, Екзамен
ВК13.2	Безпека IoT		
ВК13.3	Комплексні системи захисту інформації		
Загальний обсяг вибіркових компонент:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

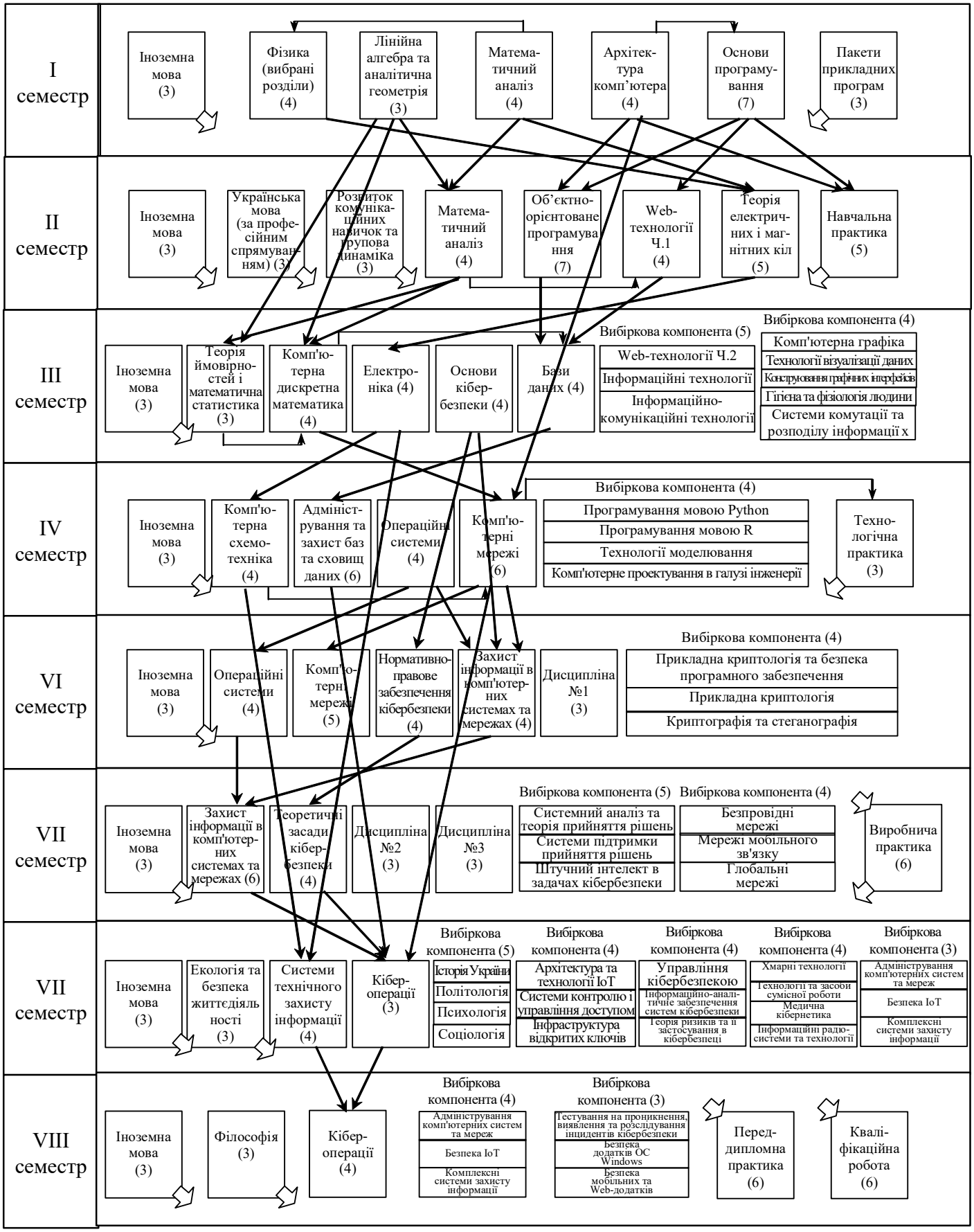
2.2. Структурно-логічна схема освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти/ роботи, практики кваліфікаційна робота)	Кількість кредитів	Загальний обсяг год.	Форма підсумкового контролю
1	2	3	4	
І курс, І семестр				
ОК1	Іноземна мова	3	90	Залік
ОК3	Лінійна алгебра та аналітична геометрія	3	90	Залік
ОК5	Фізика	4	120	Залік
ОК6	Математичний аналіз	4	120	Залік
ОК11	Архітектура комп'ютера	4	120	Екзамен
ОК12	Основи програмування	7	210	Екзамен
ОК13	Пакети прикладних програм	3	90	Екзамен
	Разом	**28**	**840**	
І курс, ІІ семестр				
ОК1	Іноземна мова	3	90	Залік
ОК2	Розвиток комунікаційних навичок та групова динаміка	3	90	Залік
ОК4	Українська мова (за професійним спрямуванням)	3	90	Екзамен
ОК6	Математичний аналіз	4	120	Екзамен
ОК14	Об'єктно-орієнтоване програмування	7	210	Екзамен, Курсова робота
ОК15	Web-технології Ч.1	4	120	Залік
ОК16	Теорія електричних і магнітних кіл	5	150	Екзамен
ОК29	Навчальна практика	3	90	Диф. залік
	Разом	**32**	**960**	
ІІ курс, І семестр				
ОК1	Іноземна мова	3	90	Залік
ОК7	Теорія ймовірностей і математична статистика	3	90	Залік
ОК8	Комп'ютерна дискретна математика	3	90	Екзамен
ОК17	Електроніка	4	120	Залік
ОК18	Основи кібербезпеки	4	120	Екзамен
ОК19	Бази даних	4	120	Екзамен
ВК3.1	Web-технології Ч.2	5	150	Екзамен
ВК3.2	Інформаційні технології			
ВК3.3	Інформаційно-комунікаційні технології			
ВК4.1	Комп'ютерна графіка	4	120	Залік
ВК4.2	Технології візуалізації даних			
ВК4.3	Конструювання графічних інтерфейсів			
ВК4.4	Гігієна та фізіологія людини			
ВК4.5	Системи комутації та розподілу інформації			
	Разом	**30**	**900**	

ІІ курс, ІІ семестр				
ОК1	Іноземна мова	3	90	Залік
ОК20	Комп'ютерна схемотехніка	4	120	Екзамен
ОК21	Адміністрування та захист баз та сховищ даних	6	180	Екзамен, Курсова робота
ОК22	Операційні системи	4	120	Залік
ОК23	Комп'ютерні мережі	6	180	Залік
ОК30	Технологічна практика	3	90	Диф. залік
ВК5.1	Програмування мовою Python	4	120	Екзамен
ВК5.2	Програмування мовою R			
ВК5.3	Технології моделювання			
ВК5.4	Комп'ютерне проектування в галузі інженерії			
	Разом	**30**	**900**	
ІІІ курс, І семестр				
ОК1	Іноземна мова	3	90	Залік
ОК22	Операційні системи	4	120	Екзамен
ОК23	Комп'ютерні мережі	5	150	Екзамен, Курсовий проект
ОК24	Нормативно-правове забезпечення кібербезпеки	4	120	Екзамен
ОК25	Захист інформації в комп'ютерних системах та мережах	3	90	Залік
ОК26	Теоретичні засади кібербезпеки	4	120	Екзамен
ВК1.Х	Дисципліна №1	3	90	Залік
ВК6.1	Прикладна криптологія та безпека програмного забезпечення	4	120	Екзамен
ВК6.2	Прикладна криптологія			
ВК6.3	Криптографія та стеганографія			
	Разом	**30**	**900**	
ІІІ курс, ІІ семестр				
ОК1	Іноземна мова	3	90	Залік
ОК25	Захист інформації в комп'ютерних системах та мережах	6	180	Екзамен, Курсовий проект
ОК31	Виробнича практика	6	180	Диф. залік
ВК1.Х	Дисципліна №2	3	90	Залік
ВК1.Х	Дисципліна №3	3	90	Залік
ВК7.1	Системний аналіз та теорія прийняття рішень	5	150	Екзамен
ВК7.2	Системи підтримки прийняття рішень			
ВК7.3	Штучний інтелект в задачах кібербезпеки			
ВК8.1	Бездротові мережі	4	120	Екзамен
ВК8.2	Мережі мобільного зв'язку			
ВК8.3	Глобальні мережі			
	Разом	**30**	**900**	

IV курс, I семестр				
ОК1	Іноземна мова	3	90	Залік
ОК9	Екологія та безпека життєдіяльності	3	90	Залік
ОК27	Системи технічного захисту інформації	4	120	Екзамен, Курсовий проект
ОК28	Кібероперації	3	90	Залік
ВК2.1	Історія України	3	90	Залік
ВК2.2	Політологія			
ВК2.3	Психологія			
ВК2.4	Соціологія			
ВК9.1	Архітектура та технології IoT	4	120	Екзамен
ВК9.2	Системи контролю і управління доступом			
ВК9.3	Інфраструктура відкритих ключів			
ВК10.1	Управління кібербезпекою	4	120	Екзамен
ВК10.2	Інформаційно-аналітичне забезпечення систем кібербезпеки			
ВК10.3	Теорія ризиків та її застосування в кібербезпеці			
ВК11.1	Хмарні технології	4	120	Екзамен
ВК11.2	Технології та засоби сумісної роботи			
ВК11.3	Медична кібернетика			
ВК11.4	Інформаційні радіосистеми та технології			
ВК13.1	Адміністрування комп'ютерних систем та мереж	3	90	Залік
ВК13.2	Безпека IoT			
ВК13.3	Комплексні системи захисту інформації			
	Разом	**31**	**910**	
IV курс, II семестр				
ОК1	Іноземна мова	3	90	Екзамен
ОК10	Філософія	3	90	Екзамен
ОК28	Кібероперації	4	120	Екзамен
ОК32	Переддипломна практика	6	180	Диф. залік
ОК33	Кваліфікаційна робота	6	180	Кваліфікацій на атестація
ВК13.1	Адміністрування комп'ютерних систем та мереж	4	120	Екзамен
ВК13.2	Безпека IoT			
ВК13.3	Комплексні системи захисту інформації			
ВК12.1	Тестування на проникнення, виявлення та розслідування інцидентів кібербезпеки	3	90	Залік
ВК12.2	Безпека додатків ОС Windows			
ВК12.3	Безпека мобільних та Web-додатків			
	Разом	**31**	**930**	
	Загальний обсяг:	**240**	**7200**	

СТРУКТУРНО-ЛОГІЧНА СХЕМА



Вихідна стрілка, яка розміщена в правому чи лівому нижньому кутку, показує, що ОК забезпечує решту ОК поточного і наступних семестрів;
Вхідна стрілка, яка розміщена у правому чи лівому верхньому кутку, показує, що ОК забезпечується ОК поточного та попередніх семестрів.

3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Поточна атестація студентів здійснюється у формі екзаменів, заліків, диференційованих заліків, захисту курсових робіт та проектів.

Атестація випускників освітньо-професійної програми «Кібербезпека» за спеціальністю 125 «Кібербезпека» проводиться у формі публічного захисту кваліфікаційного проекту/роботи та завершується видачою документу встановленого зразка про присудження йому освітнього ступеня «бакалавр» з присвоєнням кваліфікації: бакалавр з кібербезпеки

Атестація здійснюється відкрито і публічно.

Кваліфікаційний проект/робота оприлюднюється у репозитарії закладу вищої освіти.

4. ВІДПОВІДНІСТЬ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

4.1. Матриця відповідності програмних компетентностей обов'язковим компонентам освітньо-професійної 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	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

5. ЗАБЕЗПЕЧЕНІСТЬ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

5.1. Матриця забезпечення програмних результатів навчання відповідними обов'язковими компонентами освітньо-професійної програми

	РН-1	РН-2	РН-3	РН-4	РН-5	РН-6	РН-7	РН-8	РН-9	РН-10	РН-11	РН-12	РН-13	РН-14	РН-15	РН-16	РН-17	РН-18	РН-19	РН-20	РН-21	РН-22	РН-23	РН-24	РН-25	РН-26	РН-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	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

	РН-28	РН-29	РН-30	РН-31	РН-32	РН-33	РН-34	РН-35	РН-36	РН-37	РН-38	РН-39	РН-40	РН-41	РН-42	РН-43	РН-44	РН-45	РН-46	РН-47	РН-48	РН-49	РН-50	РН-51	РН-52	РН-53	РН-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	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+