МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

КІБЕРБЕЗПЕКА

Першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузь знань 12 Інформаційні технології

Кваліфікація: бакалавр з кібербезпеки

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
(протокол № 3 від «25» березня 2019 р.)
Освітня програма введена в дію
з «01» вересня 2019р.
(наказ № 37 від «25» березня 2019р.)
Зі змінами,
затвердженими Вченою радою
від «25» жовтня 2021 р., протокол № 10,
наказ № 195 від «25» жовтня 2021 р.;
від «26» вересня 2022 р., протокол № 6,
наказ № 575/ВС від «26» вересня 2022 р.

Голова вченої ради
Ректор _____ /О.О. Новомлинець/

Чернігів 2022

ПЕРЕДМОВА

Розроблено робочою групою спеціальності 125 Кібербезпека у складі:

1. Ткач Ю.М., завідувач, професор кафедри кібербезпеки та математичного моделювання, д.пед.н., професор.
2. Шелест М.Є., професор кафедри кібербезпеки та математичного моделювання, д.т.н., професор.
3. Петренко Т.А., к.т.н., доцент кафедри кібербезпеки та математичного моделювання.

Розроблено відповідно до стандарту вищої освіти України за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології», затвердженого наказом МОН України від 04.10.2018 р. №1074 та з врахуванням змін відповідно до наказу МОН України від 13.01.2022 № 26 «Про внесення змін до деяких стандартів вищої освіти»

Додаються рецензії зовнішніх стейкходерів:

1. Опірський І.Р., професор кафедри захисту інформації Національного університету «Львівська політехніка», доктор технічних наук, професор.
2. Казмірчук С.В., доктор технічних наук, завідувач кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету.
3. Лисиця І.М., директорка Чернігівського ІТ-кластеру

1. Профіль освітньо-професійної програми «Кібербезпека»
зі спеціальності 125 Кібербезпека

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Національний університет «Чернігівська політехніка» ННІ електронних та інформаційних технологій Кафедра кібербезпеки та математичного моделювання
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр. Бакалавр з кібербезпеки
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Тип диплому – одиничний. Диплом бакалавра, одиничний, 240 кредитів ЄКТС. Термін навчання 3 роки 10 місяців
Наявність акредитації	Україна. Акредитаційна комісія. Сертифікат про акредитацію спеціальності 125 Кібербезпека за рівнем вищої освіти бакалавр. Серія УД № 26014082 від 04 листопада 2020 року. Термін дії сертифіката до 01.07.2024 року
Цикл/рівень	НРК України - 6 рівень, FQ-EHEA – перший цикл, EQF-LLL - 6 рівень
Передумови	На базі повної загальної середньої освіти. При вступі на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») може бути визнано та перезараховано результати навчання обсягом не більше ніж 120 кредитів ЄКТС, отримані в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста). При вступі на базі ступеня «бакалавр» за іншими спеціальностями може бути визнано та перезараховано результати навчання, отримані в межах попередньої освітньої програми обсягом не більше ніж 90 кредитів ЄКТС. При вступі на основі ступеня «фаховий молодший бакалавр» може бути визнано та перезараховано не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти». Прийом на основі ступенів «молодший бакалавр», «фаховий молодший бакалавр» або освітньо-кваліфікаційного рівня «молодший спеціаліст» здійснюється за результатами зовнішнього незалежного оцінювання в порядку, визначеному законодавством.
Мова (и) викладання	Українська
Термін дії освітньої програми	До 01.07.2024 року або до заміни новою
Інтернет адреса постійного розміщення опису освітньої програми	https://op.stu.cn.ua/view/total_view.php
2 – Мета освітньої програми	
підготовка фахівців, здатних використовувати технології кібербезпеки, а також впроваджувати у всі сфери діяльності новітні інформаційні технології та програмне забезпечення	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань 12 Інформаційні технології Спеціальність 125 Кібербезпека **Об'єкти професійної діяльності випускників**: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні,

	інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. **Цілі навчання**: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** **Знання** – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного 6 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.
Орієнтація освітньої програми	Освітньо-професійна
Основний фокус освітньої програми та спеціалізації	Загальна освіта в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека. Акцент на системному аналізі здобутків вітчизняних та зарубіжних дослідників для прийняття обґрунтованих професійних рішень за умов невизначеності та мінливості зовнішнього середовища з врахуванням резервів та можливостей інноваційного розвитку внутрішнього середовища підприємства на основі широкого використання сучасних інформаційних технологій. Ключові слова: кібербезпека, інформаційна безпека, інформаційні технології, захист інформації
Особливості програми:	Формування компетентностей в умовах нестабільності інформаційного середовища на основі принципів інноваційного розвитку та сучасних інформаційних технологій.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	*Фахівець з організації інформаційної безпеки і може займати первинні посади:* ● адміністратор інформаційної та кібербезпеки; ● аудитор/пентестер безпеки інформаційно-комунікаційних систем; ● розробник засобів захисту інформації; ● провідний спеціаліст/керівник служби технічного захисту інформації; ● фахівець з розроблення комп'ютерних програм; ● технік із конфігурованої комп'ютерної системи; ● фахівець з організації захисту інформації з обмеженим доступом; ● фахівець з режиму секретності;

	● інспектор з організації захисту секретної інформації; ● технік обчислювального (інформаційно-обчислювального) центру; ● технік із системного адміністрування; ● технік-програміст; ● фахівець з інформаційних технологій; ● фахівець з комп'ютерної графіки (дизайну); ● фахівець з розробки та тестування програмного забезпечення.
Подальше навчання	Можливість продовжити навчання за освітньо-професійною або освітньо-науковою програмою ступеня магістра
5 – Викладання та оцінювання	
Викладання та навчання	Основні підходи, методи та технології, які використовуються у даній програмі: проблемно-орієнтоване навчання, навчання в системі Moodle, самонавчання. Викладання проводиться у вигляді: лекцій, мультимедійних лекцій, семінарів, практичних занять, лабораторних робіт, самостійного навчання, індивідуальних завдань.
Оцінювання	Усні та письмові екзамени, курсові роботи та проекти, презентації тощо.
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	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, верховенство права, прав і свобод людини і громадянина України.
	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.
	КЗ 8. Базові знання з академічної культури і академічної грамотності; основ економіки та підприємницької діяльності; набуття навичок комунікації, лідерство, здатність брати на себе відповідальність і працювати в критичних умовах, вміння залагоджувати конфлікти, працювати в команді.
	КЗ 9. Здатність до ініціативності, відповідальності та навичок до безпечної діяльності відповідно до майбутнього профілю роботи, галузевих норм і правил, а також необхідного рівня індивідуального та колективного рівня безпеки у надзвичайних ситуаціях.
Фахові компетентності	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 встановленої політикою інформаційної та/або кібербезпеки.
7 – Програмні результати навчання (ПРН)	
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, в 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 (ІТС);	

ПРН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;
ПРН 12. Розробляти моделі загроз та порушника;
ПРН 13. Аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних;
ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних систем програмно-апаратними засобами та давати оцінку 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 і/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 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 вітчизняними та міжнародними вимогами і стандартами;
ПРН 45. Застосовувати різні класи політик інформаційної 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.

ПРН 55. Вирішувати професійні задачі діяльності, пов'язані з забезпеченням життя, здоров'я і працездатності під час роботи, оцінювати середовище перебування щодо особистої безпеки, безпеки колективу, суспільства; аналізувати найважливіші тенденції розвитку вітчизняної культури, аналізувати проблеми сучасного культурного розвитку; використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя з метою збереження та зміцнення власного здоров'я. ПРН 56. Вести ділові розмови, визначати й оцінювати причини виникнення труднощів при комунікаціях, формувати власний діловий імідж, конструктивно вирішувати конфліктні ситуації; вести розгорнутий монолог (лекцію) з фахової проблематики, формувати власну стратегію життя, стратегію успіху, аналізувати та створювати медіа-контент; розуміти економічні категорії, закони, причинно-наслідкові та функціональні зв'язки, які існують між процесами та явищами на різних рівнях економічних систем, демонструвати знання теорій, методів і функцій менеджменту, збирати та аналізувати необхідну фінансову інформацію.	
8 – Ресурсне забезпечення реалізації програм	
Кадрове забезпечення	Кадрове забезпечення реалізації освітньої програми повністю відповідає ЛУ провадження освітньої діяльності. Підготовку фахівців спеціальності 125 «Кібербезпека» забезпечують висококваліфіковані науково-педагогічні кадри університету.
Матеріально-технічне забезпечення	Відповідно до ЛУ освітня програма має необхідне матеріально-технічне забезпечення, зокрема аудиторний та бібліотечні фонди, сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій, комп'ютерні класи, мультимедійний комплекс, гуртожитки та об'єкти соціально-побутової інфраструктури. Достатньою для якісної реалізації освітньої програми є забезпеченість лекційними аудиторіями, аудиторіями для проведення практичних занять, а також наукових, виховних заходів та заходів дозвілля.
Інформаційне та навчально-методичне забезпечення	Система MOODLE, паперовий та електронний варіант навчально-методичного забезпечення навчального процесу. Усі ресурси бібліотеки НУ «Чернігівська політехніка» доступні через сайт університету, читальний зал бібліотеки забезпечений бездротовим доступом до мережі Інтернет.
9 – Академічна мобільність	
Національна кредитна мобільність	Реалізується в університеті відповідно до вимог чинного законодавства та регулюється Положенням про академічну мобільність учасників освітнього процесу НУ «Чернігівська політехніка». На основі двосторонніх договорів між НУ «Чернігівська політехніка» та закладами вищої освіти України. Кредити, отримані в інших університетах України, перезараховуються відповідно до довідки про академічну мобільність
Міжнародна кредитна мобільність	Реалізується в університеті відповідно до вимог чинного законодавства та регулюється Положенням про академічну мобільність учасників освітнього процесу НУ «Чернігівська політехніка». Академічна мобільність ЗВО здійснюється на підставі угод про співробітництво між НУ «Чернігівська політехніка» та закладами вищої освіти зарубіжних країн-партнерів, затверджених в установленому порядку індивідуальних навчальних планів та робочих програмам навчальних дисциплін. Індивідуальна академічна мобільність можлива за рахунок участі у програмі «Еразмус+» та інших програм)
Навчання іноземних здобувачів вищої освіти	Здійснюється згідно з вимогами чинного законодавства, Порядку організації набору та навчання (стажування) іноземців та осіб без громадянства у НУ «Чернігівська політехніка»

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

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти(роботи), практики, кваліфікаційна робота	Кількість кредитів	Форма підсумк. контролю
	2	3	4
Обов'язкові компоненти ОП (ОК)			
ОК 1	Історія України	4	екзамен
ОК 2	Фахова українська мова та основи ділової комунікації	3	диференційований залік
ОК 3	Філософія	4	екзамен
ОК 4	Іноземна мова	16	диференційований залік
ОК 5	Основи академічного письма	3	диференційований залік
ОК 6	Безпека життєдіяльності та основи охорони праці	3	диференційований залік
ОК 7	Громадянська освіта	3	диференційований залік
ОК 8	Фізичне виховання	12	залік
ОК 9	Вища математика	9	екзамен
ОК 10	Фізика	3	диференційований залік
ОК 11	Інформатика	5	екзамен
ОК 12	Інформаційна безпека держави	3	диференційований залік
ОК 13	Теорія ризиків	4	екзамен
ОК 14	Технології програмування	4	екзамен
ОК 15	Прогнозування та моделювання	5	екзамен
ОК 16	Основи криптографічного захисту інформації	6	екзамен/ КСР
ОК 17	Комп'ютерна графіка	5	екзамен
ОК 18	Архітектура комп'ютерних систем	4	екзамен
ОК 19	Операційні системи	5	екзамен
ОК 20	Бази даних	6	екзамен/ КСР
ОК 21	Комп'ютерні мережі	6	екзамен/КП
ОК 22	Комплексні системи захисту інформації	5	екзамен

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти(роботи), практики, кваліфікаційна робота	Кількість кредитів	Форма підсумк. контролю
ОК 23	Менеджмент інформаційної безпеки	4	диференційований залік
ОК 24	Спеціальні глави математики	12	диференційований залік, екзамен
ОК 25	Безпека комп'ютерних мереж	6	екзамен
ОК 26	Системи технічного захисту інформації	5	екзамен
ОК 27	Програмний захист інформації	4	екзамен
ОК 28	Соціальна інженерія	4	екзамен
ОК 29	Безпека інформації в інформаційно-комунікаційних системах	3	диференційований залік
ОК 30	Інциденти інформаційної безпеки	6	екзамен
Загальний обсяг обов'язкових компонент:		**162**	
Вибіркові компоненти ОП (ВК)			
ВК 1.1.	Історія української культури	3	диференційований залік
ВК 1.2.	Корпоративна культура	3	диференційований залік
ВК 1.3.	Тренінг-курс «Психологія ділових відносин»	3	диференційований залік
ВК 1.4.	Риторика	3	диференційований залік
ВК 1.5.	Тренінг-курс «Лідерство та «team-building»»	3	диференційований залік
ВК 1.6.	Комунікаційний менеджмент	3	диференційований залік
ВК 1.7.	Тренінг-курс «Креативне мислення та інтелектуальна власність»	3	диференційований залік
ВК 1.8.	Психологія впливу	3	диференційований залік
ВК 1.9.	Психологія успіху	3	диференційований залік
ВК 1.10.	Тренінг-курс «Сучасні медіа»	3	диференційований залік
ВК 1.11.	Generalist-курс	3	диференційований залік
ВК 1.12.	Дисципліна на вибір з іншої ОП, яка формує соціальні навички (soft skills)	3	диференційований залік
Загальний обсяг вибіркових компонент: *(необхідно вибрати 1 дисципліну)*		**3**	
ВК 2.1	Сучасна економіка	3	диференційований залік
ВК 2.2	Управління бізнесом	3	диференційований залік
ВК 2.3	Фінансова грамотність	3	диференційований залік
ВК 2.4	Фінансово-економічна безпека	3	диференційований залік

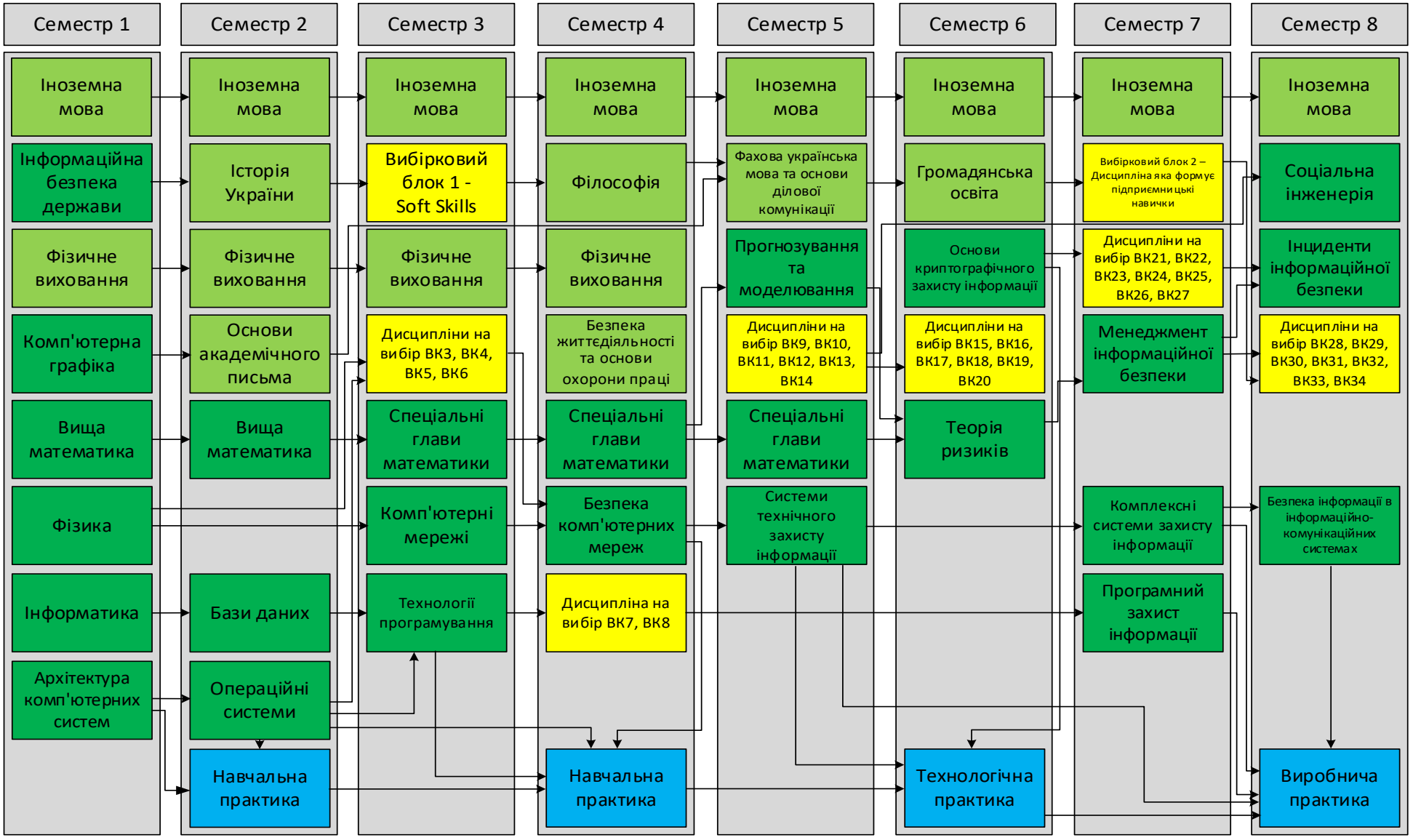
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти(роботи), практики, кваліфікаційна робота	Кількість кредитів	Форма підсумк. контролю
ВК 2.5	Маркетинг	3	диференційований залік
ВК 2.6	Тренінг-курс «Start up creation»	3	диференційований залік
ВК 2.7	Економіка підприємства	3	диференційований залік
ВК 2.8	Дисципліна на вибір з іншої ОП, яка формує підприємницькі навички	3	диференційований залік
Загальний обсяг вибіркових компонент: *(необхідно вибрати 1 дисципліну)*		**3**	
ВК 3	Безпека в Smart технологіях	4	екзамен
ВК 4	Основи наукового дослідження	4	екзамен
ВК 5	Адміністрування Unix-подібних систем	4	екзамен
ВК 6	Комп'ютерна схемотехніка	4	екзамен
ВК 7	Психологія управління	4	екзамен
ВК 8	Об'єктно-орієнтоване програмування	4	екзамен
ВК 9	Web-технології	4	екзамен
ВК 10	Основи національної безпеки	4	екзамен
ВК 11	Системи банківської безпеки	4	екзамен
ВК 12	Електронний документообіг	4	екзамен
ВК 13	ECM – системи	4	екзамен
ВК 14	Фізичні основи технічних засобів розвідки	4	екзамен
ВК 15	Цифрова обробка сигналів	4	екзамен
ВК 16	Імітаційне моделювання	4	екзамен
ВК 17	Емпіричні дослідження	4	екзамен
ВК 18	Основи тестування програмного забезпечення	4	екзамен
ВК 19	Організаційне забезпечення захисту інформації	4	екзамен
ВК 20	Основи стеганографії	4	екзамен
ВК 21	Системи штучного інтелекту	4	екзамен
ВК 22	Експертні системи	4	екзамен
ВК 23	Програмування мобільних пристроїв	4	екзамен
ВК 24	Системне програмування	4	екзамен

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти(роботи), практики, кваліфікаційна робота	Кількість кредитів	Форма підсумк. контролю
ВК 25	Системи охорони державної таємниці	4	екзамен
ВК 26	Технології прикладного програмування	4	екзамен
ВК 27	Захист інформації в телекомунікаційних системах	4	екзамен
ВК 28	Організація та архітектура інфраструктури відкритих ключів	4	екзамен
ВК 29	Управління проєктами	4	екзамен
ВК 30	Організація спеціального діловодства	4	екзамен
ВК 31	Датчики та виконавчі механізми систем безпеки	4	екзамен
ВК 32	Інтернет розвідка	4	екзамен
ВК 33	Blockchain: основи та приклади застосування	4	екзамен
ВК 34	Мережі мобільного зв’язку	4	екзамен
Загальний обсяг вибіркових компонент: *(необхідно вибрати 15 дисциплін)*		**60**	
ОК 31	Навчальна практика	3	диференційований залік
ОК 32	Навчальна практика	3	диференційований залік
ОК 33	Технологічна практика	3	диференційований залік
ОК 34	Виробнича практика	3	диференційований залік
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

2.2. Структурно-логічна схема ОП

Семестр	Види навчальної діяльності
1 семестр 30 кр.	Дисципліни загальної та професійної підготовки: ОК4 (2кр.), ОК8 (3кр.), ОК9 (5кр.), ОК10 (3кр.), ОК11 (5кр.), ОК12 (3кр.), ОК17 (5кр.), ОК18 (4кр.)
2 семестр 30 кр.	Дисципліни загальної та професійної підготовки: ОК1 (4кр.), ОК4 (2кр.), ОК5 (3кр.), ОК8 (3кр.), ОК9 (4кр.), ОК19 (5кр.), ОК20 (6кр.), ОК31 (3кр.)
3 семестр 30 кр.	Дисципліни загальної та професійної підготовки: ОК4 (2кр.), ОК8 (3кр.), ОК14 (4кр.), ОК21 (6кр.), ОК24 (4кр.), ВК1.1-ВК1.11 (3 кр.), ВК3-ВК6 (8 кр.)
4 семестр 30 кр.	Дисципліни загальної та професійної підготовки: ОК3 (4кр.), ОК4 (2кр.), ОК6 (3кр.), ОК8 (3кр.), ОК24 (5кр.), ОК25 (6кр.), ОК32 (3кр.) ВК7-ВК8 (4кр.)
5 семестр 30 кр.	Дисципліни загальної та професійної підготовки: ОК2 (3кр.), ОК4 (2кр.), ОК15 (5кр.), ОК24 (3кр.), ОК26 (5кр.) ВК9-ВК14 (12 кр.)
6 семестр 30 кр.	Дисципліни загальної та професійної підготовки: ОК4 (2кр.), ОК7 (3кр.), ОК13 (4кр.), ОК16 (6кр.), ОК33 (3кр.) ВК15-ВК20 (12 кр.)
7 семестр 30 кр.	Дисципліни загальної та професійної підготовки: ОК4 (2кр.), ОК22 (5кр.), ОК23 (4кр.), ОК27 (4кр.) ВК2.1-ВК2.8 (3кр.), ВК21-ВК27 (12 кр.)
8 семестр 30 кр.	Дисципліни загальної та професійної підготовки: ОК4 (2кр.), ОК28 (4кр.), ОК29 (3кр.), ОК30 (6кр.), ОК34 (3кр.) ВК28-ВК34 (12 кр.)

Структурно-логічна схема дисциплін ОПП спеціальності 125 Кібербезпека освітньо-ківаліфікаційного рівня Бакалавр



3. Форма атестації здобувачів вищої освіти

Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту (ЄДКІ) або атестаційного іспиту у разі не проведення ЄДКІ.

Єдиний державний кваліфікаційний іспит та атестаційний іспит передбачають оцінювання досягнень результатів навчання, визначених відповідним стандартом та цією освітньою програмою.

На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих здобувачем вищої освіти у процесі навчання за даною освітньою програмою.

До атестації допускаються здобувачі вищої освіти, які виконали всі вимоги програми підготовки.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

Обов'язкові компоненти (ОК)

	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.
КЗ 1.									+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
КЗ 2.										+		+	+					+	+	+		+			+	+	+		+	+	+	+	+	+
КЗ 3.		+		+	+																												+	+
КЗ 4.			+										+	+	+	+							+											+
КЗ 5.			+		+				+			+	+											+				+			+	+	+	+
КЗ 6.	+						+					+																+						
КЗ 7.	+					+		+																										
КЗ 8.					+																													
КЗ 9.						+																												
КФ 1.												+	+			+			+			+	+		+	+		+			+	+	+	+
КФ 2.												+			+		+				+	+			+			+	+		+	+	+	+
КФ 3.																+											+		+				+	+
КФ 4.																						+	+											
КФ 5.														+				+	+	+		+			+	+	+		+				+	+
КФ 6.																									+		+		+					
КФ 7.																						+												
КФ 8.																							+							+				
КФ 9.																							+										+	+
КФ 10.																+										+								
КФ 11.													+						+						+									
КФ 12.													+		+							+	+					+						

Вибіркові компоненти (ВК).

	ВК 1.1	ВК 1.2	ВК 1.3	ВК 1.4	ВК 1.5	ВК 1.6	ВК 1.7	ВК 1.8	ВК 1.9	ВК 1.10	ВК 1.11	ВК 1.12	ВК 2.1	ВК 2.2	ВК 2.3	ВК 2.4	ВК 2.5	ВК 2.6	ВК 2.7	ВК 2.8	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8	ВК 9	ВК 10	ВК 11	ВК 12	ВК 13	ВК 14	ВК 15	ВК 16	ВК 17	ВК 18	ВК 19	ВК 20	ВК 21	ВК 22	ВК 23	ВК 24	ВК 25	ВК 26	ВК 27	ВК 28	ВК 29	ВК 30	ВК 31	ВК 32	ВК 33	ВК 34
КЗ 1.		+	+																		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
КЗ 2.												+								+	+			+		+		+		+	+	+			+	+					+	+	+	+	+		+			+	+
КЗ 3.		+		+								+								+																																
КЗ 4.		+	+				+	+	+			+						+		+			+														+	+	+						+						
КЗ 5.							+														+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	
КЗ 6.											+																	+	+																							
КЗ 7.	+	+	+		+	+		+	+	+												+												+															+		
КЗ 8		+		+	+	+	+	+	+	+	+		+	+	+	+	+	+	+																																
КЗ 9																																																+				
КФ 1.																											+	+	+						+											+				
КФ 2.						+															+		+	+		+	+		+	+	+	+	+	+	+	+	+						+			+			+	
КФ 3.																							+			+	+					+	+	+		+														
КФ 4.							+														+																							+							
КФ 5.																																					+	+												+	
КФ 6.																																								+											
КФ 7.																																		+									+	+						
КФ 8.																																		+										+						
КФ 9.																												+															+						
КФ 10.																															+					+											+	
КФ 11.																							+												+														
КФ 12.																					+				+																		+					+	+	

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми.

Обов'язкові компоненти (ОК)

	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.
ПРН 1		+		+	+																									+	+	+	+
ПРН 2			+		+																		+									+	+
ПРН 3			+		+		+		+				+			+	+							+				+			+	+	+	+
ПРН 4										+			+		+													+			+	+	+	+
ПРН 5													+		+																		+	+
ПРН 6			+						+				+		+									+				+			+	+	+	+
ПРН 7												+										+	+		+						+	+	+	+
ПРН 8												+																			+	+	+	+
ПРН 9												+													+				+	+				
ПРН 10																					+				+				+			+	+	+
ПРН 11																					+				+				+				+	+
ПРН 12																						+												
ПРН 13																									+				+		+	+	+	+
ПРН 14														+											+		+							
ПРН 15										+	+			+			+	+	+	+									+				+	+
ПРН 16																						+											+	+
ПРН 17																		+							+				+				+	+
ПРН 18																			+							+	+		+					
ПРН 19																										+	+					+	+	+
ПРН 20														+												+					+	+	+	+
ПРН 21																						+									+	+	+	+
ПРН 22																									+				+		+	+	+	+
ПРН 23																			+						+	+			+					
ПРН 24																			+						+	+			+					
ПРН 25																									+									
ПРН 26																													+					
ПРН 27																										+	+		+					
ПРН 28																						+							+		+	+	+	+
ПРН 29																									+				+					
ПРН 30																						+				+								
ПРН 31												+													+				+					
ПРН 32																			+										+				+	+
ПРН 33													+										+											
ПРН 34												+											+											
ПРН 35																						+												
ПРН 36																										+							+	+
ПРН 37																										+							+	+
ПРН 38																										+								
ПРН 39																										+							+	+

	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.
ПРН 40																										+								
ПРН 41																													+					
ПРН 42																			+										+	+				
ПРН 43												+											+							+	+	+	+	+
ПРН 44													+										+											
ПРН 45													+										+											
ПРН 46													+												+									
ПРН 47																+																		
ПРН 48																+																		
ПРН 49																			+						+									
ПРН 50																											+		+					
ПРН 51																			+						+				+					
ПРН 52																			+															
ПРН 53														+													+						+	+
ПРН 54	+						+					+																+						
ПРН 55	+					+		+																										
ПРН 56		+		+	+																													

Вибіркові компоненти (ВК).

	ВК 1.1.	ВК 1.2.	ВК 1.3.	ВК 1.4.	ВК 1.5.	ВК 1.6.	ВК 1.7.	ВК 1.8.	ВК 1.9.	ВК 1.10.	ВК 1.11.	ВК 1.12.	ВК 2.1.	ВК 2.2.	ВК 2.3.	ВК 2.4.	ВК 2.5.	ВК 2.6.	ВК 2.7.	ВК 2.8.	ВК 2.9.	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8	ВК 9	ВК 10	ВК 11	ВК 12	ВК 13	ВК 14	ВК 15	ВК 16	ВК 17	ВК 18	ВК 19	ВК 20	ВК 21	ВК 22	ВК 23	ВК 24	ВК 25	ВК 26	ВК 27	ВК 28	ВК 29	ВК 30	ВК 31	ВК 32	ВК 33	ВК 34
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																																						+													+			

	ВК 1.1.	ВК 1.2.	ВК 1.3.	ВК 1.4.	ВК 1.5.	ВК 1.6.	ВК 1.7.	ВК 1.8.	ВК 1.9.	ВК 1.10.	ВК 1.11.	ВК 1.12.	ВК 2.1.	ВК 2.2.	ВК 2.3.	ВК 2.4.	ВК 2.5.	ВК 2.6.	ВК 2.7.	ВК 2.8.	ВК 2.9.	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8	ВК 9	ВК 10	ВК 11	ВК 12	ВК 13	ВК 14	ВК 15	ВК 16	ВК 17	ВК 18	ВК 19	ВК 20	ВК 21	ВК 22	ВК 23	ВК 24	ВК 25	ВК 26	ВК 27	ВК 28	ВК 29	ВК 30	ВК 31	ВК 32	ВК 33	ВК 34
ПРН 30																																			+																
ПРН 31																																				+		+	+					+				+			+
ПРН 32																																				+				+				+							
ПРН 33																													+																+	+				
ПРН 34																																				+								+							
ПРН 35																																				+				+				+							
ПРН 36																																	+						+					+	+					
ПРН 37																																	+				+							+						
ПРН 38																									+												+							+				+		
ПРН 39																												+																							
ПРН 40																									+												+							+				+		
ПРН 41																							+																												
ПРН 42																												+				+																	+	
ПРН 43																												+	+							+								+				+		
ПРН 44																													+																			+	+			
ПРН 45																													+							+												+			
ПРН 46																																							+											+		
ПРН 47																											+				+	+			+		+													
ПРН 48																																+				+	+										+			
ПРН 49																													+							+														
ПРН 50																																+																		
ПРН 51																																				+				+	+						+			
ПРН 52																						+														+											+			
ПРН 53																											+					+																		
ПРН 54											+														+			+	+																					
ПРН 55	+																																																		
ПРН 56		+	+	+	+			+	+	+	+	+		+	+	+	+	+	+	+	+									+																				

6. Перелік нормативних документів, на яких базується освітня програма

1. Про вищу освіту. - Закон України від 01.07.2014р. № 1556-VII // ВВРУ від 19.09.2014р., № 37-38, стор. 2716, стаття 2004. URL: https://zakon.rada.gov.ua/laws/show/1556-18
2. Про освіту. - Закон України від 5 вересня 2017р. № 2145-VIII // ВВРУ від 29.09.2017р., №38-39, стор. 5, стаття 380. URL: https://zakon.rada.gov.ua/laws/show/2145-19
3. Національний класифікатор України: «Класифікатор професій» ДК 003:2010 (Редакція від 25.10.2021). URL: http://zakon.rada.gov.ua/rada/show/va327609-10
4. Національна рамка кваліфікацій. - Постанова КМУ від 23 листопада 2011 р. № 1341 // ОВУ від 06.01.2012р., № 101, стор. 15, ст. 3700, код акта 59774/2011. URL: https://zakon.rada.gov.ua/laws/show/1341-2011-п
5. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти. - Постанова КМУ від 29 квітня 2015р. № 266 // ОВУ від 22.05.2015р., №38, стор. 194, ст. 1147, код акта 76797/2015. URL: https://zakon.rada.gov.ua/laws/show/266-2015-п
6. Ліцензійні умови провадження освітньої діяльності. Постанова КМУ від 30 грудня 2015р. № 1187 // ОВУ від 02.02.2016р., № 7, стор. 23, ст. 345, код акта 80480/2016. URL: https://zakon.rada.gov.ua/laws/show/1187-2015-п
7. Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти. URL: https://naqa.gov.ua/wp-content/uploads/2019/07/Додаток-1.-Стандарти-і-рекомендації-щодо-забезпечення-якості-в-Європейському-просторі-вищої-освіти.pdf
8. Методичні рекомендації щодо розроблення стандартів вищої освіти. Наказ Міністерства освіти і науки України від «01» червня 2017 №600. URL: https://mon.gov.ua/storage/app/media/vishcha-osvita/rekomendatsii-1648.pdf
9. Стандарт вищої освіти України першого (бакалаврського) рівня, галузі знань 2 Інформаційні технології, спеціальності 125 Кібербезпека. Наказ Міністерства освіти і науки України 04.10.2018 р. № 1074 (зі змінами та доповненнями). URL: https://mon.gov.ua/storage/app/media/vishcha-osvita/2022/Standarty.Vyshchoyi.Osvity/Zatverdzheni.Standarty/01/31/125-Kiberbezpeka-bak.31.01.22.pdf