МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Чернігівський національний технологічний університет
Навчально-науковий інститут технологій
Кафедра кібербезпеки та математичного моделювання

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

КІБЕРБЕЗПЕКА

Першого рівня вищої освіти

за спеціальністю 125 «Кібербезпека»

галузь знань 12 Інформаційні технології

Кваліфікація: бакалавр з кібербезпеки

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Голова вченої ради

_____ /С.М. Шкарлет/

(протокол № 3 від «25» березня 2019 р.)

Освітня програма вводиться в дію з 01 вересня 2019 р.

Ректор _____ / С.М. Шкарлет /

(наказ № 37 від «25» березня 2019р)

Чернігів 2019 р.

ПЕРЕДМОВА

Розроблено робочою групою (науково-методичною комісією спеціальності № 125 «Кібербезпека») у складі:

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

Розроблено відповідно до стандарту вищої освіти України за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології», затверджено наказом МОН від 04.10.2018 р. №1074.

1. Профіль освітньої програми зі спеціальності 125 «Кібербезпека»

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Чернігівський національний технологічний університет. ННІ Технологій. Факультет 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	Ліцензія: наказ МОН №1415л від 10.06.2015 року Первинна акредитація
Цикл/рівень	НРК України - 7 рівень, QF-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
Мова (и) викладання	Українська, англійська
Термін дії освітньої програми	До заміни новою
Інтернет адреса постійного розміщення опису освітньої програми	https://www.stu.cn.ua/staticpages/perelikrivniv/
2 – Мета освітньої програми	
підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань 12 Інформаційні технології Спеціальність 125 «Кібербезпека»
Орієнтація освітньої програми	Освітньо-професійна - бакалавра

Основний фокус освітньої програми та спеціалізації	Загальна: 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.
Особливості програми:	Формування відповідних 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, електронне навчання в системі Moodle, самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді: лекцій, мультимедійних лекцій, семінарів, практичних занять, лабораторних робіт, самостійного навчання, індивідуальних занять.
Оцінювання	Усні та письмові екзамени, практика, 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 основ економіки та підприємницької діяльності
	КЗ 9 Здатність до 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 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 ІТС 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 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 ІТС;
ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС;
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 ІТС 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 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 згідно встановленої політики інформаційної і/або кібербезпеки;
ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в ІТС та ефективності використання КЗЗ в умовах реалізації загроз різних класів;
ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів ІТС.;
ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів ІТС;
ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування ІТС 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 ІТС 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 ІТС;
ПРН 47. Вирішувати задачі захисту інформації, що обробляється в ІТС 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 ІТС;
ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в ІТС;

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 ІТС; 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 програм	
Кадрове забезпечення	Професор-3, доктор наук-1, кандидати наук – 3, доцент – 4, старший викладач – 1, викладач-1
Матеріально-технічне забезпечення	Сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій, комп'ютерні класи, мультимедійний комплекс, сучасна оргтехніка
Інформаційне та навчально-методичне забезпечення	Система MOODLE, паперовий та електронний варіант навчально-методичного забезпечення навчального процесу Фонд наукової бібліотеки нараховує 561597 примірників книг, брошур, періодичних видань, в т.ч.: навчальних видань – 338108 примірників, українською мовою – 315281 примірників. На одного студента в середньому припадає 48 примірників навчальної літератури.
9 – Академічна мобільність	
Національна кредитна мобільність	Допускаються індивідуальні угоди про академічну мобільність для навчання та проведення досліджень в університетах та наукових установах України.
Міжнародна кредитна мобільність	Академічна мобільність студентів здійснюється на підставі укладення угод про співробітництво між іноземним або вітчизняним вищим навчальним закладом та Університетом (далі – «ВНЗ-партнери»), за узгодженими та затвердженими в установленому порядку індивідуальними навчальними планами студентів та програмами навчальних дисциплін.
Навчання іноземних здобувачів вищої освіти	

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 1.	Історія України	4	екзамен
ОК 2.	Фахова українська мова та основи ділової комунікації	3	залік
ОК 3.	Філософія	4	екзамен
ОК 4.	Іноземна мова	16	залік
ОК 5.	Основи академічного письма	3	залік
ОК 6.	Безпека життєдіяльності та основи охорони праці	3	залік
ОК 7.	Громадянська освіта	3	залік
ОК 8.	Економіка підприємства	3	залік
ОК 9.	Історія української культури	3	залік
ОК 10.	Фізичне виховання	12	залік
ОК 11.	Вища математика	9	екзамен
ОК 12.	Фізика	3	залік
ОК 13.	Інформатика	5	екзамен
ОК 14.	Інформаційна безпека держави	3	залік
ОК 15.	Інтернет-технології	4	екзамен
ОК 16.	Технології програмування	12	екзамен/ КП
ОК 17.	Прогнозування та моделювання	5	екзамен
ОК 18.	Основи криптографічного захисту інформації	5	екзамен
ОК 19.	Комп'ютерна графіка	5	екзамен
ОК 20.	Архітектура комп'ютерних систем	4	екзамен
ОК 21.	Операційні системи	11	екзамен
ОК 22.	Бази даних	6	екзамен/ КР
ОК 23.	Комп'ютерна схемотехніка	5	екзамен
ОК 24.	Комплексні системи захисту інформації	12	екзамен
ОК 25.	Менеджмент інформаційної безпеки	4	екзамен
ОК 26.	Спеціальні глави математики	12	залік, екзамен
Загальний обсяг обов'язкових компонент:		159	
Вибіркові компоненти ОП			
ВБ 1.	Основи національної безпеки/ Організаційно-правове забезпечення національної безпеки України	3	залік
ВБ 2.	Організація спеціального діловодства /Діловодство	4	екзамен
ВБ 3.	Системи штучного інтелекту / Експертні системи	3	залік
ВБ 4.	Програмний захист інформації/ Програмні засоби захисту інформації	5	екзамен
ВБ 5.	Цифрова обробка сигналів/ Цифрова обробка та передача інформації	4	екзамен
ВБ 6.	Основи технічного захисту інформації / Система технічного захисту інформації	5	екзамен

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти(роботи), практики, кваліфікаційна робота	Кількість кредитів	Форма підсумк. контролю
ВБ 7.	Імітаційне моделювання / Емпіричні дослідження	5	екзамен
ВБ 8.	Програмування мобільних пристроїв/ Основи наукового дослідження/	4	екзамен
ВБ 9.	Електронний документообіг / ECM – системи	4	екзамен
ВБ 10.	Соціальна інженерія/ Забезпечення інформаційної безпеки держави	5	екзамен
ВБ 11.	Організація комп'ютерних мереж/ Комп'ютерні мережі	6	екзамен/КР
ВБ 12.	Основи тестування програмного забезпечення / Організаційне забезпечення захисту інформації	3	залік
ВБ 13.	Теорія ризиків/ Теорія ризиків інформаційної безпеки	5	екзамен
ВБ 14.	Безпека інформації в інформаційно-комунікаційних системах / Комплексні системи захисту інформації в інформаційно-телекомунікативних системах	4	залік
ВБ 15.	Система охорони державної таємниці/ Захист прав та свобод людини в медіапросторі	3	залік
Загальний обсяг вибіркових компонент:		63	
	Навчальна	3	
	Навчальна	3	
	Технологічна практика	3	
	Виробнича практика	3	
	Підготовка до атестації	6	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

2.2. Структурно-логічна схема ОП

Семестр 1	Семестр 2	Семестр 3	Семестр 4	Семестр 5	Семестр 6	Семестр 7	Семестр 8
Іноземна мова	Іноземна мова	Іноземна мова	Іноземна мова	Іноземна мова	Іноземна мова	Іноземна мова	Іноземна мова
Вища математика	Вища математика	Спеціальні глави математики	Спеціальні глави математики	Спеціальні глави математики	Теорія ризиків/ Теорія ризиків інформаційної безпеки	Економіка підприємства	
Фізика		Комп'ютерна схемотехніка	Основи технічного захисту інформації /Системи технічного захисту інформації		Цифрова обробка сигналів/ Цифрова обробка та передача інформації	Комплексні системи захисту інформації	Комплексні системи захисту інформації
Інформатика		Технології програмування	Технології програмування		Основи тестування програмного забезпечення / Організаційне забезпечення захисту інформації	Програмування мобільних пристроїв/ Основи наукового дослідження	
Інформаційна безпека держави				Основи національної безпеки/Організаційно правове забезпечення національної безпеки України		Система охорони державної таємниці/ Захист прав та свобод людини в медіапросторі	
				Internet технології		Менеджмент інформаційної безпеки	
Комп'ютерна графіка				Електронний документообіг / ECM-системи			
Архітектура комп'ютерних систем	Операційні системи	Операційні системи					
	Історія України	Історія української культури	Філософія		Громадянська освіта		
	Основи академічного письма			Фахова українська мова та основи ділової комунікації			Організація спеціального діловодства / Діловодство
	Бази даних				Основи криптографічного захисту інформації	Програмний захист інформації/ Програмні засоби захисту інформації	Безпека інформації в інформаційно-комунікаційних системах/ Комплексні системи захисту інформації в інформаційно-телекомунікативних системах
				Організація комп'ютерних мереж/ Комп'ютерні мережі		Системи штучного інтелекту/Експертні системи	Соціальна інженерія / Забезпечення інформаційної безпеки держави
			Безпека життєдіяльності				
				Прогнозування та моделювання	Імітаційне моделювання/ Емпіричні дослідження		
Фізичне виховання	Фізичне виховання	Фізичне виховання	Фізичне виховання				
	Навчальна практика		Навчальна практика		Технологічна практика		Виробнича практика
							Підготовка до атестації

3. Форма атестації здобувачів вищої освіти

Атестація здійснюється у формі публічного захисту кваліфікаційного проекту/роботи.

На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за даним стандартом.

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

4.Матриця відповідності програмних компетентностей компонентам освітньої програми
Обов'язкові компоненти/ Вибіркові компоненти

	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.	ВБ 1.	ВБ 2.	ВБ 3.	ВБ 4.	ВБ 5.	ВБ 6.	ВБ 7.	ВБ 8.	ВБ 9.	ВБ 10.	ВБ 11.	ВБ 12.	ВБ 13.	ВБ 14.	ВБ 15.
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

	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.	ВБ 1.	ВБ 2.	ВБ 3.	ВБ 4.	ВБ 5.	ВБ 6.	ВБ 7.	ВБ 8.	ВБ 9.	ВБ 10.	ВБ 11.	ВБ 12.	ВБ 13.	ВБ 14.	ВБ 15.
ПРН 1.		+		+	+				+																															
ПРН 2.								+																+	+														
ПРН 3.																+	+	+					+	+				+	+	+	+	+	+	+			+	+		+
ПРН 4.			+								+	+			+		+							+	+	+			+	+	+	+	+				+			+	
ПРН 5.						+	+						+				+							+	+	+								+	+	+	+	+	+	
ПРН 6.			+				+						+												+															
ПРН 7.						+	+	+						+										+	+		+	+		+		+				+	+			+
ПРН 8.														+										+	+		+										+			+	+
ПРН 9.																								+	+					+		+					+				
ПРН 10.													+							+	+	+	+															+	+		+
ПРН 11.													+							+	+	+	+											+				+			
ПРН 12.														+										+	+					+		+							+	+
ПРН 13.																				+	+	+	+																		+
ПРН 14.																		+						+	+					+		+									+
ПРН 15.											+	+	+		+	+	+	+	+	+	+	+	+	+						+	+	+	+	+	+	+	+	+			+
ПРН 16.																								+						+		+									+
ПРН 17.																		+		+				+	+					+		+									+
ПРН 18.																		+						+						+		+									+
ПРН 19.														+				+						+	+					+		+					+				+
ПРН 20.																		+						+						+		+									+
ПРН 21.																								+						+		+									+
ПРН 22.																					+	+	+	+	+					+		+									+
ПРН 23.																					+	+	+	+	+					+		+									+
ПРН 24.																									+					+		+									+
ПРН 25.																								+	+					+		+									+
ПРН 26.																								+	+					+		+									+
ПРН 27.																								+	+					+		+									+

	ОК 1.	ОК 2.	ОК 3.	ОК 4.	ОК 5.	ОК 6.	ОК 7.	ОК 8.	ОК 9.	ОК 10.	ОК 11.	ОК 12.	ОК 13.	ОК 14.	ОК 15.	ОК 16.	ОК 17.	ОК 18.	ОК 19.	ОК 20.	ОК 21.	ОК 22.	ОК 23.	ОК 24.	ОК 25.	ОК 26.	ВБ 1.	ВБ 2.	ВБ 3.	ВБ 4.	ВБ 5.	ВБ 6.	ВБ 7.	ВБ 8.	ВБ 9.	ВБ 10.	ВБ 11.	ВБ 12.	ВБ 13.	ВБ 14.	ВБ 15.
ПРН 28.																								+	+					+		+									+
ПРН 29.																								+	+					+		+									+
ПРН 30.																								+	+					+		+									+
ПРН 31.														+				+						+	+					+		+					+				+
ПРН 32.																								+	+					+		+									+
ПРН 33.								+																															+	
ПРН 34.														+											+		+										+				+
ПРН 35.																								+	+					+		+									+
ПРН 36.													+								+	+	+							+		+									+
ПРН 37.																								+						+		+									+
ПРН 38.																								+						+		+									+
ПРН 39.														+													+										+			+	
ПРН 40.																								+						+		+									+
ПРН 41.																					+		+	+	+					+											+
ПРН 42.																								+	+					+		+									+
ПРН 43.														+											+		+			+		+									+
ПРН 44.								+																			+													+	
ПРН 45.														+											+																+
ПРН 46.														+								+	+	+	+	+															+
ПРН 47.																		+																							
ПРН 48.																		+																							
ПРН 49.													+								+	+	+	+	+																
ПРН 50.																								+	+				+		+									+
ПРН 51.						+																		+	+				+		+									+
ПРН 52.						+							+								+	+	+	+	+															
ПРН 53.																								+	+				+		+									+
ПРН 54.	+						+																																	