

Міністерство освіти і науки України



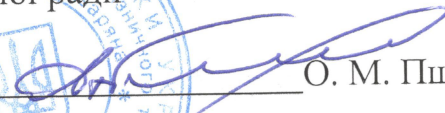
ДНІПРОВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЗАЛІЗНИЧНОГО ТРАНСПОРТУ
імені академіка В. ЛАЗАРЯНА

Схвалено

Вченою радою університету

«25» 02 2019 р. протокол № 8

Голова вченої ради

Професор  О. М. Пшінько

Введено в дію наказом ректора

від 26.02.2019 р. № 79-к

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

назва «Кібербезпека»

першого (бакалаврського) рівня вищої освіти

спеціальність 125 Кібербезпека
(код та назва)

галузь знань 12 Інформаційні технології
(шифр та назва)

кваліфікація Бакалавр з кібербезпеки

Дніпро-2019

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

першого (бакалаврського) рівня вищої освіти

(рівень вищої освіти: перший (бакалаврський) або другий (магістерський))

спеціальності 125 Кібербезпека

(назва освітньо-професійної програми)

1 Методична комісія факультету « Технічна кібернетика »

« 25 » 03 2019 р.

Голова комісії

протокол № 4


(підпис)

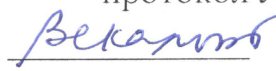
О. Г. Горюнов
ПІБ

2 Вчена рада факультету « Технічна кібернетика »

« 18 » 02 2019 р.

Голова вченої ради

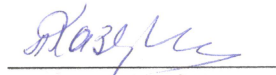
протокол № 4


(підпис)

В. В. Скарозук
ПІБ

3 Навчально-методичний відділ

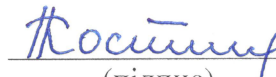
Начальник НМВ


(підпис)

Л. С. Казаріна

« 20 » 02 2019 р.

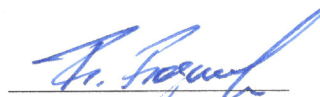
4 Голова комісії ВР


(підпис)

М. О. Костін

« 21 » 02 2019 р.

5 Перший проректор


(підпис)

Б. Є. Боднар

« 22 » 02 2019 р.

ПЕРЕДМОВА

освітньо-професійної програми

першого (бакалаврського) рівня вищої освіти

(рівень вищої освіти: перший (бакалаврський) або другий (магістерський))

спеціальності 125 Кібербезпека

(назва освітньо-професійної програми)

Програму складено на підставі стандарту вищої освіти за спеціальністю 125 «Кібербезпека»), що затверджений наказом Міністерства освіти і науки України від «19» _11_ 2018р. № 1262

ВНЕСЕНО

Кафедрою Електронні обчислювальні мвшини

«21» 01 2019 р.

протокол № 8

Завідувач кафедри

І.В. Жуковицький

(підпис)

Розробники програми:

1. Жуковицький І.В., д.т.н, проф., зав.кафедрою ЕОМ
2. Хмарський Ю.І. к.т.н., доц
3. Остапець Д.О ,к.т.н, доц..
4. Єгоров О.Й к.т.н.,доц.

1. Профіль освітньо-професійної програми
спеціальність 125 Кібербезпека

1.1 - Загальна інформація	
Повна назва закладу вищої освіти	Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Кваліфікація – Бакалавр з Кібербезпеки
Офіційна назва освітньої програми	ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА «Кібербезпека» першого (бакалаврського) рівня вищої освіти
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, кредитів ЄКТС - 240, термін навчання 3 роки 10 місяців (на базі повної загальної середньої освіти) або кредитів ЄКТС - 120, термін навчання 2 роки 10 місяців (на базі освітньо-кваліфікаційного рівня «молодший спеціаліст»)
Наявність акредитації	Міністерство освіти і науки України, ДООУ «Навчально-методичний центр з питань якості освіти» 2013-2023 рр.
Рівень	НРК України - 7 рівень / перший (бакалаврський) рівень вищої освіти
Передумови	Вимоги щодо попередньої освіти: - Повна загальна середня освіта або ступінь «молодший бакалавр» (освітньо-кваліфікаційний рівень «молодший спеціаліст») - Решта вимог визначаються правилами прийому на освітньо-професійну програму бакалавра
Мова(и) викладання	Українська мова
Термін дії освітньої програми	5 років
Інтернет-адреса постійного розміщення опису освітньої програми	www.diit.edu.ua E-mail: evm@diit.edu.ua або dnuzt@diit.edu.ua (кафедра ЕОМ)
1.2 - Мета освітньої програми	
Мета (цілі) освітньої програми: формування особистості фахівця, здатного вирішувати типові та складні професійні завдання в галузі Кібербезпеки	
1.3 - Характеристика освітньої програми	
Предметна область	<u>Об'єкти професійної діяльності випускників:</u> - об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси й інформаційні технології; - технології забезпечення безпеки інформації об'єктів різного рівня (система, об'єкт системи, компонент об'єкта), що пов'язані з інформаційними, інформаційно-комунікаційними технологіями, що використовуються для

	забезпечення функціонування цих об'єктів; – процеси управління інформаційною і кібербезпекою об'єктів, що підлягають захисту. Цілями навчання є формування компетентностей (загальних 7, фахових 12) та здобуття програмних результатів навчання - 54, що необхідні для виконання професійних обов'язків в рамках об'єктів професійної діяльності у складі колективу з урахуванням особливостей майбутньої професії і можливих первинних посад бакалавра з комп'ютерної інженерії. Обсяг кредитів ЄКТС, необхідний для здобуття зазначеного ступеня вищої освіти на базі повної загальної середньої освіти становить 240 кредитів ЄКТС, загальна підготовка становить 91 кредит (38%), професійна підготовка – 149 кредити (62%)	
Орієнтація освітньої програми	Освітньо-професійна Види професійної діяльності , до виконання яких готуються випускники, що освоїли програму бакалавра: проектно-технологічна; виробничо-технологічна; організаційно-управлінська; науково-дослідна; інноваційна	
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта в галузі « Інформаційні технології » за спеціальністю « Кібербезпека ». Ключові слова: • Апаратні засоби забезпечення безпеки комп'ютерних систем; • Програмні засоби забезпечення безпеки комп'ютерних систем; • Безпека комп'ютерних систем та мереж.	
1.4. Придатність випускників до працевлаштування та подальшого навчання		
Придатність до працевлаштування	3	Фахівці
	31	Технічні фахівці в галузі прикладних наук та техніки
	312	Технічні фахівці в галузі обчислювальної техніки
	3121	Техніки-програмісти
	3123	Контролери та регулювальники промислових роботів
	3114	Технік із конфігурованої комп'ютерної системи
	3114	24947 Технік обчислювального (інформаційно-обчислювального) центру
	3114	24971 Технік-конструктор (електроніка)
	3114	25041 Технік-технолог (електроніка)
	3114	Фахівець інфокомунікацій
	3121	25036 Технік-програміст

	3121	Фахівець з інформаційних технологій
	3121	Фахівець з комп'ютерної графіки (дизайну)
	3121	Фахівець з розробки та тестування програмного забезпечення
	3121	Фахівець з розроблення комп'ютерних програм
Подальше навчання	Можливість навчання за програмою другого циклу за цією галуззю знань (що узгоджується з отриманим дипломом бакалавра) або суміжною – магістерською (освітньо-професійною) програмою вищої освіти.	
1.5. Викладання та оцінювання		
Викладання та навчання	Студентоцентроване навчання, самонавчання, проблемно-орієнтоване навчання, навчання через лекції, лабораторні роботи, практичні заняття, курсове проектування тощо.	
Оцінювання	Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль. Форми контролю: усне та письмове опитування, тестові завдання, захист лабораторних та практичних робіт, захисти курсових проектів та робіт, випусковий атестаційний іспит тощо	
1.6. Програмні компетентності		
Інтегральна компетентність	Здатність особи розв'язувати складні спеціалізовані задачі та вирішувати практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки у професійній діяльності або у процесі навчання, що передбачає застосування теорії та методів відповідних наук і характеризуються комплексністю та неповною невизначеністю умов.	
Загальні компетентності (КЗ)	К31. Здатність застосовувати знання у практичних ситуаціях. К32. Знання та розуміння предметної області та розуміння професії. К33. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. К34. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. К35. Здатність до пошуку, оброблення та аналізу інформації. К36. 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. К37. 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.
Фахові компетентності спеціальності (КФ)	КФ1. 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. КФ2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
1.7. Програмні результати навчання (ПРН)	
Комунікація	ПР1. Застосовувати знання державної та іноземних мов з

	метою забезпечення ефективності професійної комунікації;
Автономія і відповідальність	ПР2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПР3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; ПР4. 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;
Уміння, знання	ПР5. Адаптуватися в умовах часткої зміни технологій професійної діяльності, прогнозувати кінцевий результат; ПР6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; ПР7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; ПР8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; ПР9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; ПР10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; ПР11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; ПР12. Розробляти моделі загроз та порушника; ПР13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; ПР14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; ПР15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; ПР16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; ПР17. 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; ПР18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; ПР19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; ПР20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; ПР21. 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; ПР22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки; ПР23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; ПР24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно - телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); ПР25. 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; ПР26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; ПР27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; ПР28. 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; ПР29. 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; ПР30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; ПР31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; ПР32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; ПР33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; ПР34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; ПР35. 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; ПР36. Виявляти небезпечні сигнали технічних засобів; ПР37. Вимірювати параметри небезпечних та задових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоків технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; ПР38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; ПР39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; ПР40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
--	---

	ПР41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; ПР42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; ПР43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; ПР44. 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; ПР45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; ПР46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; ПР47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; ПР48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; ПР49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; ПР50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); ПР51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; ПР52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; ПР53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз;
Відповідальність	ПР54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
1.8. Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідає ліцензійним умовам
Матеріально-технічне	Лекційні аудиторії, що мають мультимедійне

забезпечення	обладнання; Лабораторії, що мають обладнання, яке відповідає предметній галузі (вимірювальні пристрої, комп'ютери, мережеве обладнання, стенди, тощо). У цілому матеріально-технічне забезпечення освітнього процесу відповідає ліцензійним умовам
Інформаційне та навчально-методичне забезпечення	Інформаційно-технологічне забезпечення освітнього процесу Бібліотека: - використання бібліотечного фонду університету, онлайн-ресурсів та баз даних; - інформаційне забезпечення студентів, які працюють над проектами та дипломами Навчальні ресурси: - довгострокові і короткострокові позики книг, доступ до онлайн-ресурсів, міжбібліотечні позики, відеотека; - продовження терміну позики та бронювання книг онлайн; - доступ до електронних журналів; - доступ до електронних бібліотечних ресурсів світу; - доступ до електронного навчального середовища Moodle; - технологічне і матеріально-технічне забезпечення освітнього процесу Академічна підтримка – - консультації з вибору програми, окремих вибіркових дисциплін, - проектування індивідуальних навчальних траєкторій - Персональне консультування
1.9. Академічна мобільність	
Національна кредитна мобільність	Національна кредитна мобільність регламентується «Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу», затвердженого наказом ректора.
Міжнародна кредитна мобільність	Міжнародна кредитна мобільність здійснюється на основі договорів між іноземними університетами та ДНУЗТ і регламентується «Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу», затвердженого наказом ректора.
Навчання іноземних здобувачів вищої освіти	Навчання іноземних громадян здійснюється за даним ОПП, за виключенням обов'язкових компонент ОК1 – ОК4.

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

2.1 Перелік компонентів ОП

Код навчальної дисципліни	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1.Обов'язкові компоненти (ОК)			
1.1.Компоненти загальної підготовки.			
OK1	Історія і культура України	5	Екзамен
OK2	Українська мова (за професійним спрямуванням)	3	Залік
OK3	Філософія	4	Екзамен
OK4	Іноземна мова	9	Екзамен
OK5	Вища математика	11	Екзамен
OK6	Фізичне виховання*	—	Залік
OK7	Фізика	6	Екзамен
OK8	Теорія ймовірності та математична статистика	4	Екзамен
OK9	Основи екології та безпека життєдіяльності	4	Залік
OK10	Основи охорони праці	3	Екзамен
OK11	Програмні засоби загального користування	4	Залік
OK12	Комп'ютерна дискретна математика	4	Екзамен
OK13	Основи програмування	9	Екзамен
OK14	Проектний практикум	4	Залік
OK15	Алгоритми та структури даних	4	Екзамен
1.2.Обов'язкові компоненти професійної підготовки			
OK16	Системи технічного захисту інформації	5	Екзамен
OK17	Прикладна криптологія (+ курсовий проект)	9	Екзамен
OK18	Методи та засоби захисту інформації	6	Екзамен
OK19	Математичні основи інформаційної безпеки	4	Екзамен
OK20	Комп'ютерні мережі	5	Екзамен
OK21	Локальні мережі	5	Екзамен
OK22	Управління інформаційною безпекою	4	Екзамен
OK23	Нормативно-правове та організаційне забезпечення систем захисту інформації	4	Залік

OK24	Захист інформації в комп'ютерних мережах	5	Екзамен
OK25	Комплексні системи захисту інформації	5	Екзамен
OK26	Теорія електричних та магнітних кіл	5	Екзамен
OK27	Архітектура комп'ютерних систем	8	Екзамен
OK28	Вступ до спеціальності	3	Залік
OK29	Практика проектування комп'ютерних мереж (+ курсовий проект)	4	Залік
OK30	Навчальна практика	4	Залік
OK31	Навчально-технологічна практика	4	Залік
OK32	Дипломування	15	Захист проекту
2.Вибіркові компоненти			
2.1. Вибіркові компоненти загальної підготовки .			
ВБ1.1	Теорія інформації та кодування	4	Залік
ВБ1.2	Бази даних	5	Екзамен
ВБ1.3	Фізика (спеціальні розділи)	4	Екзамен
ВБ1.4	Теорія радіо кіл	4	Залік
або			
ВБ2.1.	Основи управління на залізничному транспорті	5	Екзамен
ВБ2.2	Економіка залізничного транспорту	4	Залік
ВБ2.3	Фізичні основи електротехніки	4	Екзамен
ВБ2.4	Інженерна графіка	4	Залік
2.2. Вибіркові компоненти професійної підготовки			
ВБ1.5	ІНТЕРНЕТ технології	6	Залік
ВБ1.6	Системне програмування	7	Екзамен
ВБ1.7	Системне програмне забезпечення	7	Екзамен
ВБ1.8	Комп'ютерна електроніка	4	Екзамен
ВБ1.9	Комп'ютерна схемотехніка	6	Екзамен
ВБ1.10	Арифметичні та логічні основи ЕОМ (+ курсовий проект)	7	Екзамен
ВБ1.11	Проектування засобів захисту інформації на ПЛІС	4	Залік
ВБ1.12	Проектування мікропроцесорних систем захисту	5	Залік
ВБ1.13	Мобільні пристрої та додатки	4	Залік

ВБ1.14	Логічні основи штучного інтелекту	4	Екзамен
<i>або</i>			
ВБ2.5	Побудова мікропроцесорних систем захисту	5	Екзамен
ВБ2.6	Інтелектуальні системи аналізу даних	4	Екзамен
ВБ2.7	Операційні системи	6	Екзамен
ВБ2.8	Схемотехніка функціонально захищених систем	6	Екзамен
ВБ2.9	Основи дискретної електроніки (+ курсовий проект)	7	Екзамен
ВБ2.10	Побудова систем захисту залізничної автоматики	4	Залік
ВБ2.11	Теорія обчислювальних процесів і структур	7	Екзамен
ВБ2.12	Основи стеганографії	4	Залік
ВБ2.13	Комп'ютерна графіка	4	Залік
ВБ2.14	Програмування апаратних засобів	7	Залік
3. Цикл додаткових дисциплін за вибором студента			
ВБ3.1	Військова підготовка	29	Екзамен
ВБ3.2	Комплексні практичні заняття з вивчення курсу первинної військово-професійної підготовки	5	Залік

Примітка*: дисципліна є позакредитною.

2.2. Розділ змісту освітньо-професійної програми за групами компонентів та циклами підготовки

Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів / %)		
	обов'язкові компоненти	вибіркові компоненти	всього за весь термін навчання
Цикл загальної підготовки	74/31	17/7	91/38
Цикл професійної підготовки	95/39,5	54/22,5	149/62
Всього за весь термін навчання	169/70,5	71/29,5	240/100

2.3. Структурно-логічна схема освітньої програми

Код навчальної дисципліни	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Код навчальної дисциплін, яка забезпечується зазначеною в стовпчику 1
1	2	
1. Обов'язкові компоненти (ОК)		
ОК1	Історія і культура України	ОК2
ОК2	Українська мова (за професійним спрямуванням)	ОК1
ОК3	Філософія	ОК1, ОК2
ОК4	Іноземна мова	
ОК5	Вища математика	ОК18
ОК6	Фізичне виховання *	
ОК7	Фізика	ОК5, ВБ1.12
ОК8	Теорія ймовірності та математична статистика	ОК5
ОК9	Основи екології та безпека життєдіяльності	ОК10
ОК10	Основи охорони праці	ОК9
ОК11	Програмні засоби загального користування	ОК8, ОК13, ОК11
ОК12	Комп'ютерна дискретна математика	ОК5
ОК13	Основи програмування	ОК8, ОК11, ОК12
ОК14	Проектний практикум	ОК8, ОК13
ОК15	Алгоритми та структури даних	ОК8, ОК13, ОК11
ОК16	Системи технічного захисту інформації	ОК17, ОК18, ОК19, ОК

OK17	Прикладна криптологія (+ курсовий проект)	OK11,ВБ1.3,ВБ1.8
OK18	Методи та засоби захисту інформації	OK14,ВБ1.7,ВБ1.8,
OK19	Математичні основи інформаційної безпеки	OK8,OK17-OK24
OK20	Комп'ютерні мережі	OK16,OK17,OK18
OK21	Локальні мережі	OK17,ВБ2.3,OK11
OK22	Управління інформаційною безпекою	OK20, OK17,ВБ2.3,OK11
OK23	Нормативно-правове та організаційне забезпечення систем захисту інформації	OK20,OK21,OK16,ВБ2.3
OK24	Захист інформації в комп'ютерних мережах	OK25,OK19, OK16,
OK25	Комплексні системи захисту інформації	OK25,OK24
OK26	Теорія електричних та магнітних кіл	OK16, ВБ1.4, ВБ1.8, ВБ1.9
OK27	Архітектура комп'ютерних систем	OK20,OK21, ВБ2.3
OK28	Вступ до спеціальності	OK11, OK12, OK13, ВБ1.10
OK29	Практика проектування комп'ютерних мереж (+ курсовий проект)	OK20, OK21
OK30	Навчальна практика	OK13
OK31	Навчально-технологічна практика	OK25,OK21,OK19
OK32	Дипломовання	
2. Вибіркові компоненти (Блок1)		
ВБ1.1	Теорія інформації та кодування	OK8,ВБ1.4,ВБ1.14
ВБ1.2	Бази даних	OK13
ВБ1.3	Фізика (спеціальні розділи)	OK7,ВБ1.4
ВБ1.4	Теорія радіо кіл	OK9
ВБ1.5	ІНТЕРНЕТ технології	OK19,OK20
ВБ1.6	Системне програмування	OK19,OK20
ВБ1.7	Системне програмне забезпечення	ВБ1.7, OK19,OK20
ВБ1.8	Комп'ютерна електроніка	OK17,ВБ1.7,ВБ1.8,ВБ2.2
ВБ1.9	Комп'ютерна схемотехніка	OK17,ВБ1.7,ВБ2.3
ВБ1.10	Арифметичні та логічні основи ЕОМ (+ курсовий проект)	OK13,OK25 OK20,OK21,OK16,ВБ2.3
ВБ1.11	Проектування засобів захисту інформації на ПЛІС	OK20,OK21,OK16,ВБ2.3

ВБ1.12	Проектування мікропроцесорних систем захисту	ВБ1.9,ВБ1.10,ВБ1.13
ВБ1.13	Мобільні пристрої та додатки	ОК13, ОК26, ВБ1.6, ВБ1.12
ВБ1.14	Логічні основи штучного інтелекту	ОК12, ВБ1.10
3. Вибіркові компоненти (Блок2)		
ВБ2.1.	Основи управління на залізничному транспорті	ВБ1.2
ВБ2.2	Економіка залізничного транспорту	ВБ1.1
ВБ2.3	Фізичні основи електротехніки	ВБ2.3,ВБ1,6
ВБ2.4	Інженерна графіка	ОК13,ОК26
ВБ2.5	Побудова мікропроцесорних систем захисту	ОК20,ОК21,ОК16,ВБ2.3
ВБ2.6	Інтелектуальні системи аналізу даних	ОК17,ВБ1.7,ВБ1.8,ВБ2.2
ВБ2.7	Операційні системи	ОК17,ВБ1.7,ВБ2.3
ВБ2.8	Схемотехніка функціонально захищених систем	ОК20,ОК21,ОК16,ВБ2.3
ВБ2.9	Основи дискретної електроніки (+ курсовий проект)	ОК17,ВБ2.3,ОК11
ВБ2.10	Побудова систем захисту залізничної автоматики	ВБ2.1, ВБ2.5
ВБ2.11	Теорія обчислювальних процесів і структур	ОК15
ВБ2.12	Основи стеганографії	ОК15, ОК18
ВБ2.13	Комп'ютерна графіка	ОК13, ОК26
ВБ2.14	Програмування апаратних засобів	ОК16

3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності **125 Кібербезпека** проводиться у формі захисту кваліфікаційної дипломної роботи та завершується видачею документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації: Бакалавр з кібербезпеки.

Атестація здійснюється відкрито та публічно.

Кваліфікаційна дипломна робота має бути перевірена на плагіат.

4. Матриця відповідності програмних компетентностей основним та вибіркоким компонентам освітньої програми

	OK1	OK2	OK3	OK4	OK5	OK6	OK7	OK8	OK9	OK10	OK11	OK12	OK13	OK14	OK15	OK16	OK17	OK18	OK19	OK20	OK21	OK22	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	BB1.1	BB1.2	BB1.3	BB1.4	BB1.5	BB1.6	BB1.7	BB1.8	BB1.9	BB1.10	BB1.11	BB1.12	BB1.13	BB1.14		
K31														+											+					+	+																	
K32													+																+																			
K33		+		+																														+														
K34																+	+	+				+			+	+																						
K35					+		+	+			+	+	+	+	+				+				+			+	+	+	+				+			+	+										+	
K36	+		+																																													
K37	+	+	+		+	+	+	+	+	+		+														+							+		+													
KΦ1																						+	+		+																							
KΦ2																	+	+		+	+	+		+					+																+			
KΦ3											+	+	+	+	+	+		+																			+	+	+	+	+	+	+	+				
KΦ4																						+		+	+					+					+													
KΦ5																		+				+		+	+										+											+		
KΦ6																				+	+											+					+	+		+				+				
KΦ7																	+	+				+	+		+																							
KΦ8																						+						+					+															
KΦ9																						+										+																
KΦ10																+	+	+	+					+	+																							
KΦ11																				+	+			+														+							+			
KΦ12																+								+	+				+																			

5. Матриця відповідності програмних результатів навчання основним та вибіркоким компонентам освітньої програми

	OK1	OK2	OK3	OK4	OK5	OK6	OK7	OK8	OK9	OK10	OK11	OK12	OK13	OK14	OK15	OK16	OK17	OK18	OK19	OK20	OK21	OK22	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	BB1.1	BB1.2	BB1.3	BB1.4	BB1.5	BB1.6	BB1.7	BB1.8	BB1.9	BB1.10	BB1.11	BB1.12	BB1.13	BB1.14		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47		
ПР1		+		+																																												
ПР2																																+																
ПР3																																+																
ПР4					+		+	+	+	+		+													+	+		+	+			+			+	+			+									
ПР5																						+																										
ПР6					+		+	+				+					+	+	+					+		+		+							+	+				+								
ПР7																							+																									
ПР8																							+																									
ПР9																						+	+																									
ПР10																				+	+						+													+	+	+	+			+		
ПР11																				+	+			+					+				+															
ПР12																+								+	+																							
ПР13																		+		+	+			+			+									+												
ПР14																+		+						+	+																							
ПР15											+									+	+															+		+							+			
ПР16																									+																							
ПР17																+		+						+			+																					
ПР18																		+						+	+																					+		

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47			
ПР19																	+	+	+					+																									
ПР20													+	+	+		+		+																			+	+										
ПР21																		+						+	+																								
ПР22																	+	+						+																									
ПР23																+								+																									
ПР24																		+				+																											
ПР25																		+						+																									
ПР26																				+	+			+						+															+	+	+		
ПР27																	+	+		+				+						+				+															
ПР28																						+																											
ПР29																						+			+																								
ПР30																	+							+																									
ПР31																	+	+	+	+				+										+															
ПР32																		+				+		+																									
ПР33																						+																											
ПР34																						+	+																										
ПР35																						+			+																								
ПР36																	+		+	+	+			+	+			+													+	+	+	+	+	+			
ПР37							+										+									+										+			+										
ПР38							+										+									+										+			+										
ПР39																						+	+																										
ПР40							+										+									+										+			+										

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47			
ПР41																		+					+																										
ПР42																						+																											
ПР43																						+	+																										
ПР44																						+	+																										
ПР45																						+																											
ПР46																						+																											
ПР47																		+		+																													
ПР48																		+		+				+																									
ПР49																		+					+																+										
ПР50																		+					+																					+	+		+		
ПР51																		+					+																					+	+		+		
ПР52																		+					+						+										+							+	+		
ПР53											+	+	+	+	+		+		+										+		+	+		+	+					+	+	+	+	+	+				
ПР54	+	+	+			+			+	+																																							