ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

ЗАТВЕРДЖЕНО
рішенням вченої ради Національного
університету цивільного захисту України
від 28.06.2023 року, протокол № 11

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

за спеціальністю 125 Кібербезпека та захист інформації
галузі знань 12 Інформаційні технології

РІВЕНЬ ВИЩОЇ ОСВІТИ перший

СТУПІНЬ бакалавр

Харків 2023

ПЕРЕДМОВА

Розроблено на основі стандарту вищої освіти за першим (бакалаврським) рівнем вищої освіти в галузі знань 12 Інформаційні технології, спеціальністю 125 Кібербезпека, затвердженого і введеного в дію наказом Міністерства освіти і науки України від 04 жовтня 2018 року № 1074, проєктною групою у складі:

керівник проєктної групи (гарант освітньої програми):

ЛЄВТЄРОВ Олександр Антонович, доцент кафедри управління та організації діяльності у сфері цивільного захисту, доктор технічних наук, старший науковий співробітник.

члени проєктної групи:

ТЮТЮНИК Вадим Володимирович, начальник кафедри управління та організації діяльності у сфері цивільного захисту, доктор технічних наук, професор (рівень володіння іноземною мовою В2);

КОМЯК Валентина Михайлівна, професор кафедри фізико-математичних дисциплін, доктор технічних наук, професор;

ПІКСАСОВ Михайло Михайлович, начальник центру навчально-інформаційних технологій та телекомунікаційних систем, кандидат технічних наук, доцент;

СЕМЕРНІН Дмитро Олександрович, інженер сектору технічного захисту інформації центру навчально-інформаційних технологій та телекомунікаційних систем.

1 Профіль освітньої програми «Управління інформаційною безпекою об'єктів критичної інфраструктури»

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Національний університет цивільного захисту України Факультет пожежної безпеки Кафедра автоматичних систем безпеки та інформаційних технологій
Ступінь вищої освіти та назва кваліфікації (відповідно до стандарту вищої освіти)	Ступінь вищої освіти – бакалавр Освітня кваліфікація – бакалавр з кібербезпеки Спеціалізація - управління інформаційною безпекою
Офіційна назва освітньої програми	«Управління інформаційною безпекою об'єктів критичної інфраструктури»
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС
Наявність акредитації	Освітня програма не акредитована, Національне агентство із забезпечення якості вищої освіти, передбачається подання на акредитацію у 2026 р.
Цикл/рівень вищої освіти	Національна рамка кваліфікацій – 6 рівень. Рамка кваліфікацій Європейського простору вищої освіти – перший цикл вищої освіти
Передумови	Наявність повної загальної середньої освіти Наявність ступеня молодшого бакалавра
Мова(и) викладання	Українська
Термін дії освітньої програми	До наступної акредитації.
Інтернет-адреса постійного розміщення опису освітньої програми	www.nuczu.edu.ua/ розділ «Освітня діяльність», підрозділ «Освітні програми та проєкти освітніх програм»
2 – Мета освітньої програми	
Підготовка фахівців, здатних до управління процесами використання та впровадження технологій інформаційної безпеки та/або кібербезпеки на об'єктах критичної інфраструктури.	
3 – Характеристика освітньої програми	
Предметна область	Об'єктами вивчення та діяльності є: 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 критичної інфраструктури, що підлягають захисту. Теоретичним змістом предметної області є – законодавча, нормативно-правова бази України та вимоги відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципи супроводу систем та комплексів інформаційної та/або кібербезпеки;

	– теорії, моделі та принципи управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методи та засоби виявлення, управління та ідентифікації ризиків; – методи та засоби оцінювання та забезпечення необхідного рівня захищеності інформації; – методи та засоби технічного та криптографічного захисту інформації; – сучасні інформаційно-комунікаційні технології; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; – автоматизовані системи 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 програми	Освітньо-професійна. Акцент на розвиток здатностей, умінь та навичок щодо прогнозування, проектування, оптимізації, системного аналізу та прийняття рішень, аналізу і синтезу даних і знань, пов'язаних з використанням та впровадженням технологій інформаційної безпеки та/або кібербезпеки на об'єктах критичної інфраструктури.
Фокус програми: загальна/спеціальна	Спеціальна освіта та професійна підготовка фахівців з питань використання та впровадження технологій інформаційної безпеки та/або кібербезпеки. Унікальність програми полягає у впровадженні основ ризик-управління інформаційною безпекою об'єктів критичної інфраструктури, з урахуванням правової обґрунтованості, адміністративно-управлінської й технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації. Додатковий акцент на задачі зі сфери захисту інформації, які виникають в підрозділах Державної служби України з надзвичайних ситуацій (підрозділи телекомунікацій, інформаційних технологій та Системи 112, технічного захисту інформації та радіотехнічного контролю, інформаційних технологій та телекомунікаційних систем).
Особливості програми	Реалізація програми передбачає залучення до аудиторних занять професіоналів-практиків, експертів галузі, представників роботодавців, які мають належний досвід у галузі (стейкхóлдерів).
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Відповідно до здобутої освітньої кваліфікації бакалавр здатний виконувати професійні роботи за професіями, зазначеними у ДК 003:2010 Національний класифікатор України, а саме: – Аналітик загроз безпеки, код КП 2139.2; – Аналітик з безпеки інформаційно-комунікаційних систем, код КП 2139.2;

	– Дізнавач (сфера кібербезпеки та захисту інформації), код КП 2139.2; – Експерт криміналіст (сфера кібербезпеки та захисту інформації), код КП 2139.2; – Фахівець з питань безпеки (інформаційно-комунікаційні технології), код КП 2139.2; – Фахівець з підтримки інфраструктури кіберзахисту, код КП 2139.2; – Фахівець сфери захисту інформації, код КП 2139.2.
Подальше навчання	Мають право продовжити навчання на другому (магістерському) рівні вищої освіти та здобувати додаткові кваліфікації в системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	Провідні методи навчання: проблемний, частково-пошуковий та дослідницький. Викладання та навчання проводиться у формі лекцій, серед них інтерактивних та мультимедійних лекцій, практичних занять, навчання через лабораторну практику, самостійного навчання, курсового дослідження.
Система оцінювання	Оцінювання результатів навчання за освітніми компонентами здійснюється за 100-бальною шкалою через такі види контролю: поточний (відповіді (виступи) на аудиторних заняттях; результати виконання практичних, лабораторних, контрольних робіт; результати виконання і захисту завдань самостійної роботи здобувача; результати виконання і захисту інших видів робіт); підсумковий (письмові екзамени, диференційований залік, залікові роботи, захисти звітів з практик); атестація здобувачів вищої освіти (Єдиний державний кваліфікаційний іспит).
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
	ЗК 2. Знання та розуміння предметної області та розуміння професії.
	ЗК 3. Здатність професійно спілкуватися державною та іноземною мовою як усно, так і письмово (українською мовою для іноземних студентів).
	ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
	ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.
	ЗК 6. Здатність реалізовувати свої права і обов’язки як члена суспільства, усвідомлювати цінності та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
	ЗК 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові, предметні) компетентності (СК)	СК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики та стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. СК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. СК 3 Здатність до використання програмних та програмно-апаратних комплексів захисту інформації в інформаційно-комунікаційних (автоматизованих) системах. СК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. СК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. СК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. СК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). СК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. СК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. СК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. СК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. СК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленою політикою інформаційної та/або кібербезпеки. СК13. Здатність до дій в особливих умовах, пов’язаних із високим рівнем фізичного та психологічного навантаження та в умовах воєнного стану.
7 – Програмні результати навчання (ПРН)	
ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації (української мови для іноземних студентів).	
ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.	
ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.	

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
ПРН 11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах.
ПРН 12. Розробляти моделі загроз та порушника.
ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки.
ПРН 23. Реалізувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах.
ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на

основі моделей управління доступом (мандатних, дискреційних, рольових).
ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН 36. Виявляти небезпечні сигнали технічних засобів.
ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи захисту інформації.
ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

ПРН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-комунікаційних 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-комунікаційних 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 громадського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина України.
ПРН 55. Згуртовувати підлеглих навколо ідеї державної незалежності та відповідальності за збереження готовності до виконання завдань в умовах воєнного стану. Визначати фізичні, хімічні, біологічні та психофізіологічні шкідливі чинники в умовах воєнного стану

8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Якісний рівень професійної підготовки бакалаврів забезпечується висококваліфікованими науково-педагогічними працівниками (доктори та кандидати наук, професори, доценти), які мають досвід навчально-методичної, науково-дослідницької роботи та відповідають кваліфікації відповідно до спеціальності згідно ліцензійних умов.
Матеріально-технічне забезпечення	Освітній процес забезпечено приміщеннями для проведення навчальних занять, комп'ютерною технікою, мережевими системами пошуку та обробки інформації; мультимедійним обладнанням; засобами обчислювальної техніки з відповідним програмним забезпеченням, спеціальними радіовимірювальними приладами, засобами технічного захисту інформації, апаратно-програмними комплексами. Високий рівень практичної підготовки фахівців забезпечується розвиненою міжнародною співпрацею в науковій і освітній сферах, наявністю спеціалізованих лабораторій: компанії CISCO, компанії D-Link, компанії Oracle, компаній CS, Avaya, Samsung, Alcatel, Monis, лабораторії супутникового та мобільного зв'язку, безпроводових мереж, моніторингу радіочастотного ресурсу, мереж наступного покоління, систем доступу та комутації, транспортних мереж, хмарних обчислень в Інтернет-технологіях.

Інформаційне та навчально-методичне забезпечення	Інформаційне та навчально-методичне забезпечення складають методичні комплекси дисциплін, а саме: підручники, курси лекцій, методичні розробки до практичних занять, методичні вказівки до самостійної роботи, методичні матеріали до написання курсових робіт, екзаменаційних та тестових запитань різної складності тощо.
9 – Академічна мобільність	
Національна кредитна мобільність	Право на національну кредитну мобільність може бути реалізоване на підставі Закону України «Про вищу освіту» і договорів про співробітництво між Університетом та вітчизняними закладами вищої освіти.
Міжнародна кредитна мобільність	Право на міжнародну кредитну мобільність може бути реалізоване на підставі міжнародних договорів про співробітництво в галузі освіти та науки, міжнародних програм і проектів, а також здобувачами вищої освіти з власної ініціативи, на основі індивідуальних запрошень.
Навчання іноземних здобувачів вищої освіти	Навчання іноземних громадян здійснюється після вивчення ними української мови.

2 Перелік компонентів освітньої програми та їх логічна послідовність

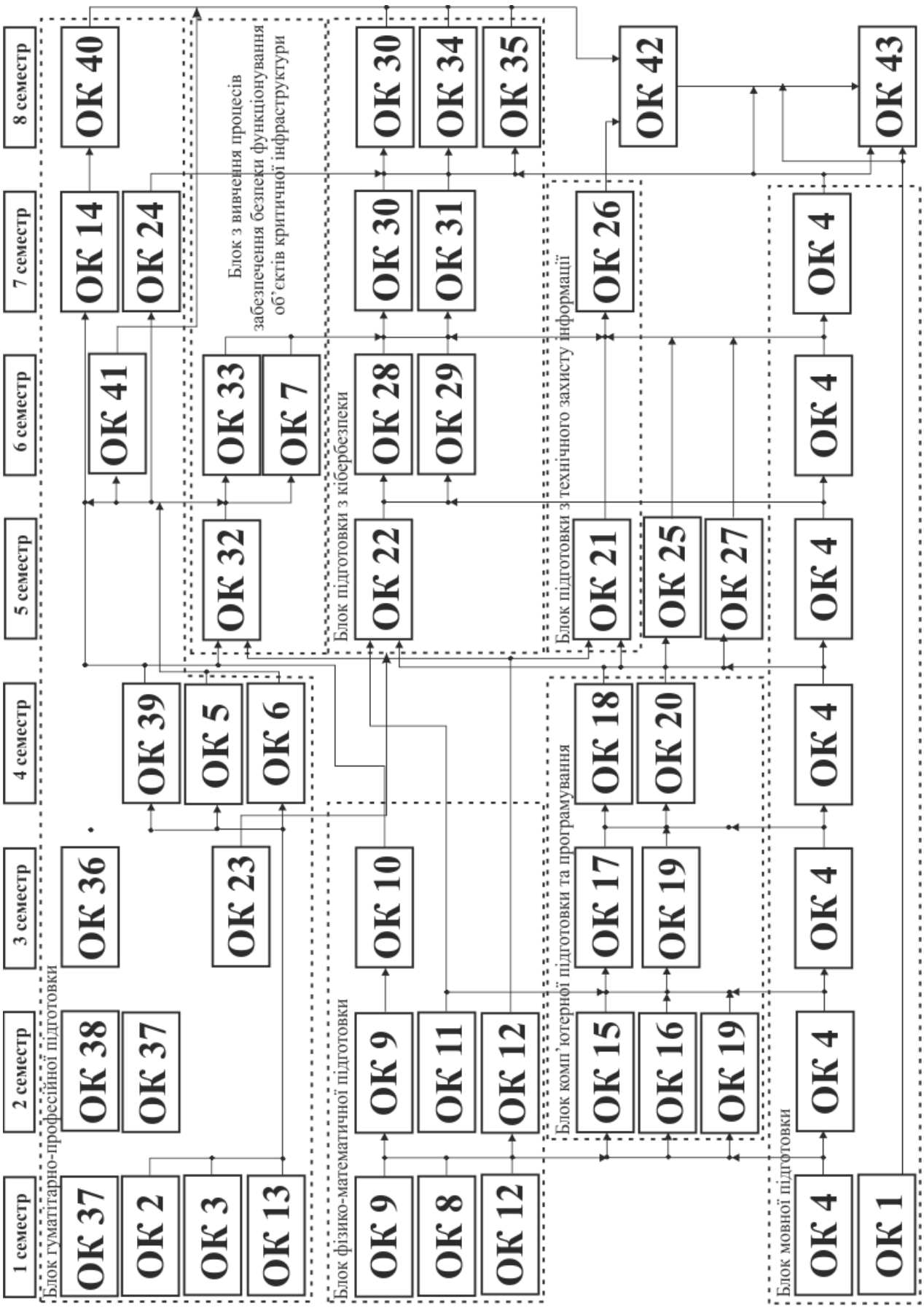
2.1 Перелік компонентів освітньої програми

Код компо-нента	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ЗАГАЛЬНІ ОБОВ'ЯЗКОВІ КОМПОНЕНТИ			
ОК 1	Українська мова (за професійним спрямуванням)	3,0	Екзамен
ОК 2	Історія та культура України	3,0	Екзамен
ОК 3	Філософія	3,0	Екзамен
ОК 4	Іноземна мова	14,5	Диференційовані заліки; екзамен
ОК 5	Правознавство	4,0	Диференційований залік
ОК 6	Психологічне забезпечення професійної діяльності	3,0	Диференційований залік
ОК 7	Політологія	3,0	Диференційований залік
ОК 8	Лінійна алгебра та аналітична геометрія	3,0	Диференційований залік
ОК 9	Математичний аналіз	6,0	Екзамени
ОК 10	Теорія ймовірності та математична статистика	3,0	Екзамен
ОК 11	Спеціальні розділи математики (дискретна математика)	3,0	Екзамен
ОК 12	Фізика	8,0	Диференційований залік; екзамен
ОК 13	Культура безпеки	3,0	Диференційований залік
ОК 14	Гендерні основи безпеки та професійної діяльності	3,0	Диференційований залік
ПРОФЕСІЙНІ ОБОВ'ЯЗКОВІ КОМПОНЕНТИ			
ОК 15	Алгоритми і методи програмування	3,5	Диференційований залік
ОК 16	Теорія інформації в сфері безпеки	3,5	Екзамен
ОК 17	Комп'ютерна логіка	3,0	Екзамен
ОК 18	Бази даних і знань	3,5	Екзамен
ОК 19	Програмування	6,5	Диференційований залік; Екзамен
ОК 20	Операційні системи	3,0	Диференційований залік
ОК 21	Комп'ютерні мережі	4,0	Екзамен
ОК 22	WEB програмування	4,0	Екзамен

ОК 23	Інформаційна безпека держави	5,0	Екзамен
ОК 24	Менеджмент інформаційної безпеки та комп'ютерна криміналістика	3,0	Екзамен
ОК 25	Фізичні основи технічних засобів розвідки	3,5	Диференційований залік
ОК 26	Технічні засоби захисту інформації	3,0	Екзамен
ОК 27	Основи кібербезпеки	4,0	Екзамен
ОК 28	Алгоритмічні основи криптології	3,0	Екзамен
ОК 29	Проектування та захист WEB додатків	3,0	Екзамен
ОК 30	Захист інформації в комп'ютерних мережах	7,0	Диференційований залік; Екзамен
ОК 31	Безпека програмного забезпечення	3,0	Екзамен
ОК 32	Моделювання процесів на об'єктах критичної інфраструктури	3,0	Екзамен
ОК 33	Основи ризико-орієнтованого підходу в безпеці об'єктів критичної інфраструктури	3,0	Диференційований залік
ОК 34	Теорія прийняття рішень	3,0	Екзамен
ОК 35	Комплексні системи захисту інформації на об'єктах критичної інфраструктури	5,0	Екзамен
ОК 36	Підготовка з надання домедичної допомоги	4,0	Екзамен
ОК 37	Рятувальна та загальна фізична підготовка (розділ – Рятувальна підготовка) Рятувальна та загальна фізична підготовка (розділ – Загальна фізична підготовка)	9,0	Диференційовані заліки
ОК 38	Первинна військово-професійна підготовка	4,0	Диференційовані заліки
ОК 39	Дії в надзвичайних ситуаціях та правила пожежної безпеки	3,0	Диференційований залік
ОК 40	Спеціальна підготовка	3,0	Диференційований залік
ОК 41	Навчальна практика	3,0	Диференційований залік
ОК 42	Виробнича практика	9,0	Диференційований залік
Атестація			
ОК 43	Єдиний державний кваліфікаційний іспит	3,0	
Загальний обсяг обов'язкових освітніх компонент:		**180**	
Вибіркові компоненти освітньо-професійної програми *			
Загальний обсяг вибіркових освітніх компонентів:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

* – здобувач вищої освіти має право формувати індивідуальну освітню траєкторію з урахуванням власного творчого потенціалу, особливості зростання та своїх професійних інтересів і здійснювати вибір освітніх компонентів в обсязі, що становить не менш як 25 % загальної кількості кредитів ЄКТС робочого навчального плану, передбачених для відповідної освітньої програми.

2.2 Структурно-логічна схема освітньої програми



3 Форма атестації здобувачів вищої освіти

Атестація здобувачів вищої освіти за освітньою програмою «Управління інформаційною безпекою об’єктів критичної інфраструктури» здійснюється у формі Єдиного державного кваліфікаційного іспиту.

4 Відповідність освітніх компонентів компетентностям та результатам навчання

Компетентності, якими повинен оволодіти здобувач	**Програмні результати навчання**	**Найменування освітніх компонентів**
ЗК 1. Здатність застосовувати знання у практичних ситуаціях	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	ОК7. Політологія ОК 6. Психологічне забезпечення професійної діяльності ОК 13. Культура безпеки ОК 14. Гендерні основи безпеки та професійної діяльності ОК 34. Теорія прийняття рішень ОК 41. Навчальна практика ОК 42. Виробнича практика ОК 43. Єдиний державний кваліфікаційний іспит
ЗК 2. Знання та розуміння предметної області та розуміння професії	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 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності	ОК 3. Філософія ОК 6. Психологічне забезпечення професійної діяльності ОК7. Політологія ОК 13. Культура безпеки ОК 14. Гендерні основи безпеки та професійної діяльності ОК 24. Менеджмент інформаційної безпеки та комп'ютерна криміналістика ОК 25. Фізичні основи технічних засобів розвідки ОК 27. Основи кібербезпеки ОК 30. Захист інформації в комп'ютерних мережах ОК 31. Безпека програмного забезпечення ОК 42. Виробнича практика ОК 43. Єдиний державний кваліфікаційний іспит

Компетентності, якими повинен оволодіти здобувач	Програмні результати навчання	Найменування освітніх компонентів
ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово (українською мовою для іноземних студентів)	ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації (української мови для іноземних студентів) ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат	ОК 1. Українська мова (за професійним спрямуванням) ОК 4. Іноземна мова ОК 41. Навчальна практика ОК 42. Виробнича практика ОК 43. Єдиний державний кваліфікаційний іспит
ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням	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 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	ОК 3. Філософія ОК 6. Психологія професійної діяльності ОК7. Політологія ОК 8. Лінійна алгебра та аналітична геометрія ОК 9. Математичний аналіз ОК 10. Теорія ймовірності та математична статистика ОК 12. Фізика ОК 15. Алгоритми і методи програмування ОК 18. Бази даних і знань ОК 19. Програмування ОК 20. Операційні системи ОК 21. Комп'ютерні мережі ОК 28. Алгоритмічні основи криптології ОК 34. Теорія прийняття рішень ОК 41. Навчальна практика ОК 42. Виробнича практика ОК 43. Єдиний державний кваліфікаційний іспит
ЗК 5. Здатність до пошуку, оброблення та аналізу інформації	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	ОК7. Політологія ОК 8. Лінійна алгебра та аналітична геометрія ОК 9. Математичний аналіз ОК 10. Теорія ймовірності та математична статистика ОК 11. Спеціальні розділи математики(дискретна) ОК 12. Фізика

Компетентності, якими повинен оволодіти здобувач	Програмні результати навчання	Найменування освітніх компонентів
	ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності	ОК 16. Теорія інформації в сфері безпеки ОК 17. Комп'ютерна логіка ОК 18. Бази даних і знань ОК 19. Програмування ОК 26. Технічні засоби захисту інформації ОК 28. Алгоритмічні основи криптології ОК 41. Навчальна практика ОК 42. Виробнича практика ОК 43. Єдиний державний кваліфікаційний іспит
ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства. усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні	ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки ПРН 54. Усвідомлювати цінності громадського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина України	ОК 1. Українська мова (за професійним спрямуванням) ОК 2. Історія та культура України ОК 3. Філософія ОК 5. Правознавство ОК7. Політологія ОК 13. Культура безпеки ОК 14. Гендерні основи безпеки та професійної діяльності ОК 23. Інформаційна безпека держави ОК 27. Основи кібербезпеки
ЗК 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя	ПРН 54. Усвідомлювати цінності громадського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина України	ОК 2. Історія та культура України ОК 3. Філософія ОК 13. Культура безпеки ОК 14. Гендерні основи безпеки та професійної діяльності
СК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики	ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі	ОК7. Політологія ОК 23. Інформаційна безпека держави ОК 24. Менеджмент інформаційної безпеки та

Компетентності, якими повинен оволодіти здобувач	Програмні результати навчання	Найменування освітніх компонентів
і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки	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	комп'ютерна криміналістика ОК 27. Основи кібербезпеки ОК 41 Навчальна практика ОК 42. Виробнича практика ОК 43. Єдиний державний кваліфікаційний іспит
СК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки	ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. ПРН 12. Розробляти моделі загроз та порушника. ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. 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,	ОК 12. Фізика ОК 15. Алгоритми і методи програмування ОК 16. Теорія інформації в сфері безпеки ОК 17. Комп'ютерна логіка ОК 18. Бази даних і знань ОК 19. Програмування ОК 20. Операційні системи ОК 24. Менеджмент інформаційної безпеки та комп'ютерна криміналістика ОК 27. Основи кібербезпеки ОК 35. Комплексні системи захисту інформації на об'єктах критичної інфраструктури ОК 41 Навчальна практика ОК 42. Виробнича практика ОК 43. Єдиний державний кваліфікаційний іспит

Компетентності, якими повинен оволодіти здобувач	Програмні результати навчання	Найменування освітніх компонентів
	процесів для внутрішніх і віддалених компонент. ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах. 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.	
СК 3 Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах	ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів., ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів, 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 50. Забезпечувати функціонування програмних	ОК 11. Спеціальні розділи математики (дискретна математика) ОК 13. Культура безпеки ОК 14. Гендерні основи безпеки та професійної діяльності ОК 15. Алгоритми і методи програмування ОК 16. Теорія інформації в сфері безпеки ОК 17. Комп'ютерна логіка ОК 20. Операційні системи ОК 22. WEB програмування ОК 28. Алгоритмічні основи криптології ОК 30. Захист інформації в комп'ютерних мережах ОК 31. Безпека програмного забезпечення ОК 34. Теорія прийняття рішень ОК 35. Комплексні системи захисту інформації на об'єктах критичної інфраструктури

Компетентності, якими повинен оволодіти здобувач	Програмні результати навчання	Найменування освітніх компонентів
	та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).	
СК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки	ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. ПРН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.	ОК 21. Комп'ютерні мережі ОК 24. Менеджмент інформаційної безпеки та комп'ютерна криміналістика ОК 25. Фізичні основи технічних засобів розвідки ОК 26. Технічні засоби захисту інформації ОК 29. Проектування та захист WEB додатків ОК 30. Захист інформації в комп'ютерних мережах ОК 31. Безпека програмного забезпечення ОК 32. Моделювання процесів на об'єктах критичної інфраструктури ОК 33. Основи ризико-орієнтованого підходу в безпеці об'єктів критичної інфраструктури
СК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки	ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності., ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень., ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.,	ОК 21. Комп'ютерні мережі ОК 24. Менеджмент інформаційної безпеки та комп'ютерна криміналістика ОК 29. Проектування та захист WEB додатків ОК 30. Захист інформації в комп'ютерних мережах ОК 31. Безпека програмного забезпечення ОК 32. Моделювання процесів на об'єктах критичної інфраструктури ОК 33. Основи ризико-орієнтованого підходу в безпеці об'єктів критичної інфраструктури

Компетентності, якими повинен оволодіти здобувач	Програмні результати навчання	Найменування освітніх компонентів
	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 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.	
СК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження	ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.	ОК 21. Комп'ютерні мережі ОК 26. Технічні засоби захисту інформації ОК 30. Захист інформації в комп'ютерних мережах ОК 31. Безпека програмного забезпечення ОК 35. Комплексні системи захисту інформації на об'єктах критичної інфраструктури
СК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту	ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації,	ОК 32. Моделювання процесів на об'єктах критичної інфраструктури ОК 33. Основи ризико-орієнтованого підходу в

Компетентності, якими повинен оволодіти здобувач	Програмні результати навчання	Найменування освітніх компонентів
інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)	аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПРН 21. 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.	безпеці об'єктів критичної інфраструктури ОК 26. Технічні засоби захисту інформації ОК 35. Комплексні системи захисту інформації на об'єктах критичної інфраструктури ОК 42. Виробнича практика ОК 43. Єдиний державний кваліфікаційний іспит
СК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку	ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки, 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.	ОК 23. Інформаційна безпека держави ОК 24. Менеджмент інформаційної безпеки та комп'ютерна криміналістика ОК 33. Основи ризико-орієнтованого підходу в безпеці об'єктів критичної інфраструктури ОК 34. Теорія прийняття рішень ОК 42. Виробнича практика ОК 43. Єдиний державний кваліфікаційний іспит
СК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою	ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки, ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних,	ОК 23. Інформаційна безпека держави ОК 24. Менеджмент інформаційної безпеки та комп'ютерна криміналістика ОК 26. Технічні засоби захисту інформації ОК 32. Моделювання процесів на об'єктах критичної інфраструктури ОК 33. Основи ризико-орієнтованого підходу в безпеці об'єктів критичної інфраструктури

Компетентності, якими повинен оволодіти здобувач	Програмні результати навчання	Найменування освітніх компонентів
	інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем., ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації, ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки	ОК 34. Теорія прийняття рішень ОК 35. Комплексні системи захисту інформації на об'єктах критичної інфраструктури ОК 42. Виробнича практика ОК 43. Єдиний державний кваліфікаційний іспит
СК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності	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.	ОК 11. Спеціальні розділи математики (дискретна математика) ОК 26. Технічні засоби захисту інформації ОК 28. Алгоритмічні основи криптології ОК 29. Проектування та захист WEB додатків ОК 30. Захист інформації в комп'ютерних мережах ОК 31. Безпека програмного забезпечення ОК 32. Моделювання процесів на об'єктах критичної інфраструктури ОК 33. Основи ризико-орієнтованого підходу в безпеці об'єктів критичної інфраструктури
СК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки	ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-комунікаційних системах., ПРН 52. Використовувати інструментарій для	ОК 20. Операційні системи ОК 25. Фізичні основи технічних засобів розвідки ОК 30. Захист інформації в комп'ютерних мережах ОК 31. Безпека програмного забезпечення ОК 32. Моделювання процесів на об'єктах критичної інфраструктури ОК 33. Основи ризико-орієнтованого підходу в

Компетентності, якими повинен оволодіти здобувач	Програмні результати навчання	Найменування освітніх компонентів
	моніторингу процесів в інформаційно-телекомунікаційних системах.	безпеці об'єктів критичної інфраструктури ОК 35. Комплексні системи захисту інформації на об'єктах критичної інфраструктури ОК 41 Навчальна практика ОК 42. Виробнича практика ОК 43. Єдиний державний кваліфікаційний іспит
СК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки	ПРН 12. Розробляти моделі загроз та порушника., 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 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.	ОК 18. Бази даних і знань ОК 25. Фізичні основи технічних засобів розвідки ОК 29. Проектування та захист WEB додатків ОК 32. Моделювання процесів на об'єктах критичної інфраструктури ОК 33. Основи ризико-орієнтованого підходу в безпеці об'єктів критичної інфраструктури ОК 35. Комплексні системи захисту інформації на об'єктах критичної інфраструктури ОК 43. Єдиний державний кваліфікаційний іспит
СК 13 Здатність до дій в особливих умовах, пов’язаних із високим рівнем фізичного та психологічного навантаження та в умовах воєнного стану.	ПРН 55. Згуртовувати підлеглих навколо ідеї державної незалежності та відповідальності за збереження готовності до виконання завдань в умовах воєнного стану. Визначати фізичні, хімічні, біологічні та психофізіологічні шкідливі чинники в умовах воєнного стану	ОК36 Підготовка з надання домедичної допомоги. ОК37 Рятувальна та загальна фізична підготовка. ОК38. Первинна військово-професійна підготовка ОК39. Дії в надзвичайних ситуаціях та правила пожежної безпеки ОК40 Спеціальна підготовка

5 Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37	ОК38	ОК39	ОК40	ОК41	ОК42	ОК43
ЗК1						*	*						*	*																			*							*	*	*
ЗК2			*			*	*						*	*										*	*		*			*	*	*								*	*	*
ЗК3	*			*																																					*	*	*
ЗК4			*			*	*	*	*	*		*			*			*	*	*	*							*						*						*	*	*
ЗК5							*	*	*	*	*					*	*	*	*							*		*													*	*	*
ЗК6	*	*	*		*		*						*	*									*				*																
ЗК7		*	*										*	*																														
СК1							*																*	*			*															*	*	*
СК2												*			*	*	*	*	*	*				*			*								*							*	*	*
СК3											*		*	*	*	*	*			*		*						*		*	*			*	*								
СК4																					*			*	*	*			*	*	*	*	*										
СК5																					*			*					*	*	*	*	*										
СК6																					*					*				*	*				*								
СК7																										*						*	*		*						*	*	*
СК8																							*	*									*	*								*	*	*
СК9																							*	*		*						*	*	*	*							*	*	*
СК10											*															*		*	*	*	*	*	*										
СК11																				*					*					*	*	*	*		*							*	*	*
СК12																		*							*				*			*	*		*									*
СК13																																				*	*	*	*	*			

6 Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37	ОК38	ОК39	ОК40	ОК41	ОК42	ОК43
ПРН1	*			*										*																											*	*	*
ПРН2			*			*					*																														*	*	*
ПРН3			*				*	*			*																							*							*	*	*
ПРН4						*	*						*	*																				*							*	*	*
ПРН5	*			*			*																																		*	*	*
ПРН6																								*	*		*			*	*											*	
ПРН7		*			*		*						*	*									*				*														*	*
ПРН8																							*	*			*														*	*	
ПРН9																							*				*														*	*	
ПРН10																*		*		*																					*			
ПРН11																*		*									*														*			
ПРН12																*		*		*							*															*		
ПРН13																	*	*	*																						*	*		
ПРН14																	*						*		*	*	*														*	*		
ПРН15															*		*		*	*	*	*						*													*	*	*
ПРН16											*																			*		*	*		*						*	*	*
ПРН17																				*	*			*		*															*	*	*	*
ПРН18											*					*			*						*	*	*														*	*	*	*
ПРН19																*		*	*		*		*							*											*	*	*	*
ПРН20															*	*	*	*	*		*					*		*														*	*		
ПРН21													*			*							*	*					*													*	*	*	*
ПРН22																								*			*						*	*	*							*	*	*	*
ПРН23																									*	*				*			*									*	*	*	*
ПРН24																				*				*			*						*		*							*	*	*	
ПРН25					*											*		*		*																									*
ПРН26																							*		*	*	*			*	*										*	*	*	*
ПРН27																*		*		*	*					*	*			*												*		*

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37	ОК38	ОК39	ОК40	ОК41	ОК42	ОК43
ПРН28																*					*		*	*			*			*											*	*
ПРН29																							*		*	*	*			*					*					*	*	*
ПРН30																														*	*	*	*		*						*	*	*
ПРН31																*			*	*	*							*														*	*
ПРН32																*							*	*									*									*	*	*
ПРН33																								*								*	*								*	*	*
ПРН34															*	*															*			*								*	*	*
ПРН35											*					*								*	*	*	*			*	*				*					*	*	*
ПРН36												*													*	*																*		*
ПРН37					*				*			*													*	*																*		*
ПРН38									*	*		*													*			*														*		*
ПРН39					*																		*	*	*	*															*	*	*
ПРН40					*																		*	*	*	*															*		*
ПРН41															*		*		*	*	*			*																				*
ПРН42													*			*							*	*			*															*	*	*
ПРН43					*											*							*		*		*			*											*	*	*
ПРН44																								*								*	*		*							*	*	*
ПРН45																										*				*	*	*	*		*							*	*	
ПРН46										*			*			*		*					*	*			*			*					*							*	*	*
ПРН47										*			*			*		*						*			*	*							*							*	*	*
ПРН48										*			*			*		*	*	*								*							*								*
ПРН49																											*				*	*	*		*							*	*	*
ПРН50											*				*	*			*	*	*		*					*		*					*							*	*	*
ПРН51																			*	*	*						*	*	*	*	*										*	*	*
ПРН52															*		*	*	*	*	*	*						*		*												*	*
ПРН53															*		*		*	*	*																					*	*
ПРН54		*			*																		*								*				*						*	*	*
ПРН55																																				*	*	*	*	*			

7 Матриця відповідності визначених освітньою програмою компетентностей дескрипторам Національної рамки кваліфікацій (НРК)

Класифікація компетентностей за НРК	**Знання** **Зн1** Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень **Зн2** Критичне осмислення проблем у галузі та на межі галузей знань	**Уміння/навички** **Ум1** Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур **Ум2** Здатність інтегрувати знання та розв'язувати складні задачі або мультидисциплінарних контекстах **Ум3** Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	**Комунікація** **К1** Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема, до осіб, які навчаються	**Відповідальність та автономія** **АВ1** Управління робочими або навчальними процесами, які є складними непередбачуваними та потребують нових стратегічних підходів **АВ2** Відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів **АВ3** Здатність продовжувати навчання з високим ступенем автономії
1	2	3	4	5
Загальні компетентності (ЗК)				
ЗК1	Зн2	Ум1		
ЗК2	Зн1		К1	АВ3
ЗК3		Ум3		АВ1
ЗК4	Зн2		К1	АВ2
ЗК5		Ум2		АВ1
ЗК6	Зн1			
ЗК7	Зн1, Зн2	Ум1		
Спеціальні (фахові, предметні) компетентності (СК)				
СК1	Зн1	Ум3	**К1**	АВ1
СК2	Зн2	Ум3	**К1**	
СК3	Зн2	Ум1		

1	2	3	4	5
СК4	Зн2	Ум1, Ум2		АВ2
СК5	Зн2	Ум1		
СК6	Зн2	Ум1		АВ3
СК7	Зн1, Зн2	Ум3		АВ1
СК8			К1	
СК9	Зн2	Ум2		АВ1
СК10			К1	АВ1
СК11	Зн1, Зн2	Ум1, Ум2		
СК12	Зн2	Ум3		АВ2
СК13		Ум3	К1	АВ1

Перелік нормативних документів, на яких базується освітня програма:

1. Закон України від 01.07.2014 р. № 1556-VII «Про вищу освіту».
Режим доступу: https://zakon.rada.gov.ua/laws/show/1556-18.

2. «Кодекс цивільного захисту України».
Режим доступу: http://zakon.rada.gov.ua/go/5403-17.

3. Закон України «Про охорону праці».
Режим доступу: http://zakon.rada.gov.ua/go/2694-12.

4. Постанова Кабінету Міністрів України від 29.04.2015 р. № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти».
Режим доступу: http://zakon4.rada.gov.ua/laws/show/266-2015-п.

5. Постанова Кабінету Міністрів України від 23.11.2011 р. № 1341 «Про затвердження Національної рамки кваліфікацій».
Режим доступу: http://zakon4.rada.gov.ua/laws/show/1341-2011-п.

6. Постанова Кабінету Міністрів України від 19 травня 2021 р. № 497 «Порядок атестації здобувачів ступеня фахової передвищої освіти та ступенів вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях у формі єдиного державного кваліфікаційного іспиту».
Режим доступу: https://zakon.rada.gov.ua/laws/show/497-2021-%D0%BF#Text.

7. Постанова Кабінету Міністрів України від 30.12.2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності» (в редакції постанови Кабінету Міністрів України від 24 березня 2021 р. № 365).
Режим доступу: https://zakon.rada.gov.ua/laws/show/365-2021-%D0%BF#Text.

8. Постанова Кабінету Міністрів України від 9 січня 2014 року № 11 «Про затвердження Положення про Єдину державну систему цивільного захисту» (із змінами).
Режим доступу: https://zakon.rada.gov.ua/laws/show/11-2014-%D0%BF#Text

9. ДК003:2010 Національний класифікатор України «Класифікатор професій», затверджений наказом Держспоживстандарту України від 28.07.2010 № 237 (зі змінами).
Режим доступу: https://zakon.rada.gov.ua/rada/show/va327609-10.

10. «Довідник кваліфікаційних характеристик професій працівників у сфері цивільного захисту України», Вип. 92 (доопрацьований). Наказ ДСНС України від 05.12.2018 р. № 707.

Режим доступу: https://mon.gov.ua/storage/app/media/vyshcha/naukovo-metodychna_rada/2020-metod-rekomendacziyi.docx.

12. Наказ Міністерства освіти і науки України від 25.01.2021 № 102 «Про затвердження форм документів про вищу освіту (наукові ступені) та додатка до них, зразка академічної довідки»

Режим доступу: https://zakon.rada.gov.ua/laws/show/z0122-21#n18.

13. ДСТУ 3891:2013 Безпека у надзвичайних ситуаціях. Терміни та визначення основних понять.

14. ДСТУ 7295:2013 Безпека у надзвичайних ситуаціях. Моніторинг. Терміни та визначення основних понять.