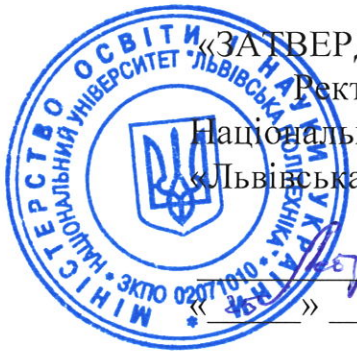
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ЛЬВІВСЬКА ПОЛІТЕХНІКА»



«ЗАТВЕРДЖУЮ»
Ректор
Національного університету
«Львівська політехніка»
_____ /Бобало Ю.Я./
«__24__» _____11_____ 2020 р.

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

“Адміністрування систем кібербезпеки”

другого (магістерського) рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: Магістр з кібербезпеки

за спеціалізацією адміністрування систем кібербезпеки

Розглянуто та затверджено
на засіданні Вченої ради
Університету
від «24» _____11_____ 2020 р.
протокол № 67

Львів 2020 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Рівень вищої освіти	Другий (магістерський)
ГАЛУЗЬ ЗНАНЬ	12 Інформаційні технології
СПЕЦІАЛЬНІСТЬ	125 Кібербезпека
Спеціалізації	125.4 Адміністрування систем кібербезпеки
Кваліфікація	Магістр з кібербезпеки за спеціалізацією адміністрування систем кібребезпеки

РОЗРОБЛЕНО І СХВАЛЕНО

Науково-методичною комісією
спеціальності 125 Кібербезпека
Протокол № 2
від «20» 10 2020 р.

Голова НМК спеціальності
_____ В.Б.Дудикевич

ПОГОДЖЕНО

Проректор з науково-педагогічної
роботи Національного університету
«Львівська політехніка»

_____О.Р. Давидчак
«18» XI 2020 р.

Начальник Навчально-методичного
відділу університету

_____В.М. Свірідов
«18» XI 2020 р.

РЕКОМЕНДОВАНО

Науково-методичною радою
університету
Протокол № 52
від «19» 11 2020 р.

Голова НМР університету
_____А.Г. Загородній

Директор ІКТА

_____ М.М.Микийчук
«21» 10 2020 р.

ПЕРЕДМОВА

Розроблено проектною групою науково-методичної комісії спеціальності 125 «Кібербезпека» у складі:

Опірський І.Р.	– д.т.н., проф., – гарант освітньо-професійної програми
Дудикевич В.Б.	– д.т.н., проф., завідувач кафедри ЗІ
Максимович В.М.	– д.т.н., проф., завідувач кафедри БІТ
Гарасимчук О.І.	– к.т.н., доцент кафедри ЗІ
Журавель І.М.	– д.т.н., проф. кафедри БІТ
Тимошик Н.П.	– директор ПП Under Defence
Бабенцов Г.А.	– студент КБУІ-11

гарант освітньо-професійної програми _____ /Опірський І.Р./

Проект освітньо-професійної програми обговорений та схвалений на засіданні Вченої ради навчально-наукового інституту комп'ютерних технологій, автоматики та метрології

Протокол № 2 від « 22 » 10 2020 р.

Голова Вченої ради ІКТА _____ М.М. Микийчук
(підпис) (прізвище, ініціали)

Затверджено та надано чинності

Наказом ректора Національного університету «Львівська політехніка»

від « 27 » 11 2020 р. № 626-т-10

Ця освітньо-професійна програма не може бути повністю або частково відтворена, тиражована та розповсюджена без дозволу Національного університету «Львівська політехніка».

Профіль освітньо-професійної програми "Адміністрування систем кібербезпеки" магістра зі спеціальності 125 "Кібербезпека"

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Національний університет «Львівська політехніка»
Офіційна назва освітньої програми	Адміністрування систем кібербезпеки Administration of cybersecurity systems
Повна назва кваліфікації мовою оригіналу	Магістр з кібербезпеки за спеціалізацією адміністрування систем кібербезпеки
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 120 кредитів ЄКТС, термін навчання 2 роки
Наявність акредитації	Акредитована
Цикл/рівень	НРК України – 8 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра
Мова(и) викладання	Українська мова
Основні поняття та їх визначення	У програмі використано основні поняття та їх визначення відповідно до Закону України «Про вищу освіту»
2 – Мета освітньої програми	
	Надати теоретичні знання та практичні уміння і навички, достатні для успішного виконання професійних обов'язків за спеціальністю 125 «Кібербезпека» та підготувати студентів для подальшого працевлаштування за обраною спеціальністю.
3 - Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	Інформаційні технології, кібербезпека
Орієнтація освітньої програми	Освітньо-професійна програма базується на загальновідомих положеннях та результатах сучасних наукових досліджень з інформаційних технологій, методів управління інформаційною безпекою, безпеки інформаційних та телекомунікаційних систем, систем технічного захисту інформації, автоматизації обробки інформації, правових засад захисту інформації, комп'ютерних мереж, архітектури комп'ютерних систем, теорії та практики криптографічного захисту інформації, адміністрування безпеки комп'ютерних систем та мереж в рамках яких можлива подальша професійна та наукова кар'єра за даними напрямками.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта та професійна підготовка в області кібербезпеки. ***Ключові слова:*** кібербезпека, безпека інформаційних систем, організація інформаційної безпеки, безпека комп'ютерних мереж, управління інформаційною безпекою, системи технічного захисту інформації, захист інформації, адміністрування систем кібербезпеки.

Особливості програми	
4 – Здатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Робочі місця в державному та приватному секторах у сфері інформаційних технологій, комп'ютерних систем та телекомунікацій, розробка і обслуговування систем інформаційної безпеки, зокрема: спеціаліст по захисту інформації державних та приватних підприємств, професіонал із організації інформаційної безпеки, професіонал із організації захисту інформації з обмеженим доступом, професіонал з режиму секретності, інспектор із організації захисту секретної інформації, менеджер з інформаційної безпеки, професіонал з аудиту мереж передач даних, експерт з безпеки програмного забезпечення; провідний інженер з інформаційної безпеки, професіонал відділу контролю інформаційних ризиків, адміністратор комп'ютерних мереж, професіонал з підтримки інформаційних сервісів, аналітик кібербезпеки.
Подальше навчання	Докторські програми в інформаційних технологіях, інформаційній безпеці, безпеці держави, кібербезпеці.
5 – Викладання та оцінювання	
Викладання та навчання	Поєднання лекцій, практичних занять, консультацій, самостійної роботи із розв'язування проблем; виконання проектів, лабораторні роботи, консультації із викладачами, підготовка магістерської роботи.
Оцінювання	Екзамени, заліки, лабораторні звіти, усні презентації, поточний контроль, захист курсових проектів (робіт), захист кваліфікаційної магістерської роботи.
6 – Програмні компетентності	
Інтегральна компетентність (ІНТ)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми під час професійної діяльності у галузі інформаційних технологій, захисту інформації, що передбачає застосування форм і методів наукового пізнання у галузі інформаційної безпеки, безпеки інформаційно-комунікаційних систем, організацію процесу дослідження у галузі інформаційної безпеки та захисту інформації, обґрунтування та реалізація системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності, режимних територіях (зонах), приміщеннях, тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

Загальні компетентності (ЗК)	ЗК 1. Здатність до письмової та усної комунікації українською та англійською (чи іншою) мовами. ЗК 2. Здатність навчатися, сприймати набуті знання в предметній області та інтегрувати їх із уже наявними, потенціал до подальшого навчання. ЗК 3. Здатність здійснювати пошук та аналізувати інформацію з різних джерел, ефективно використовувати на практиці різні теорії в області навчання та адміністрування. ЗК 4. Набуття гнучкого способу мислення, який дає можливість зрозуміти й розв'язати проблеми та задачі, зберігаючи при цьому критичне відношення до усталених наукових концепцій. ЗК 5. Уміння проводити дослідження на відповідному рівні, мати дослідницькі навички, що виявляються у здатності формувати (роблячи презентації, або представляючи звіти) нові продукти в обраній галузі, вибирати належні напрями і відповідні методи для їх реалізації, беручи до уваги наявні ресурси. ЗК 6. Уміння працювати самостійно і в команді, здатність комунікації з колегами з питань галузі щодо наукових досягнень, як на загальному рівні, так і на рівні спеціалістів. ЗК 7. Уміння думати абстрактно, здатність до аналізу та синтезу, що дозволяє формулювати висновки (діагноз) для різних типів складних управлінських задач, здійснювати планування, аналіз, контроль та оцінювання власної роботи та роботи інших осіб. ЗК 8. Підприємницький дух, ініціативність через здатність ефективно використовувати на практиці різні теорії в управлінні наукою та в області ділового адміністрування. ЗК 9. Мати навички розроблення та управління проектами для забезпечення високого рівня ефективності реалізації різних видів проектів в предметній області. ЗК 10. Визначеність та наполегливість при виконанні отриманих завдань та відповідальність за якість виконуваної роботи. ЗК 11. Навички використання інформаційних та комунікативних технологій, впровадження комп'ютерних програм та використання існуючих. ЗК 12. Уміння адаптуватися та працювати в нових ситуаціях, креативність, здатність до системного мислення
Фахові компетентності спеціальності (ФК)	ФК 1. Базові знання фундаментальних наук та інформаційних технологій, в обсязі, необхідному для освоєння загально-професійних дисциплін. ФК 2. Базові знання наукових понять, теорій і методів, необхідних для розуміння принципів роботи та функціонального призначення устаткування засобів захисту інформації та безпеки інформаційно-комунікаційних систем. ФК 3. Базові знання основних нормативно-правових актів та довідкових матеріалів, чинних стандартів і технічних умов, інструкцій та інших нормативно-розпорядчих документів з інформаційної безпеки. ФК 4. Базові знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації систем технічного захисту інформації та технологій безпеки інформаційно-комунікаційних систем. ФК 5. Уміння застосовувати та інтегрувати знання і розуміння дисциплін інших інженерних галузей.

	ФК 6. Здатність планувати й реалізувати відповідні заходи, щодо захисту інформації в інформаційних і комунікаційних системах. ФК 7. Знання з обчислювальної техніки та програмування, володіння навичками роботи з комп'ютером та апаратними засобами для вирішення задач по спеціальності. ФК 8. Здатність використовувати та впроваджувати нові технології, брати участь в модернізації та реконструкції обладнання, пристроїв, систем та комплексів, зокрема з метою підвищення їх енергоефективності та удосконалення захищеності. ФК 9. Здатність розуміти і враховувати соціальні, екологічні, етичні, економічні аспекти, що впливають на формування технічних рішень. ФК 10. Здатність застосовувати професійно-профільовані знання й практичні навички для розв'язання типових задач спеціальності, а також експлуатації систем і засобів забезпечення захисту інформації та безпеки інформаційно-комунікаційних систем. ФК 11. Здатність використовувати знання й уміння для розрахунку, дослідження, вибору, впровадження, ремонту, та проектування програмно-апаратних засобів і систем захисту інформації та безпеки інформаційних технологій. ФК 12. Здатність використовувати уміння по виявленню й блокуванню каналів і методів несанкціонованого доступу до інформації та комунікаційних систем, джерел і способів дестабілізуючого впливу на них. ФК 13. Уміння ідентифікувати, класифікувати та описувати роботу інформаційних систем і їх складових шляхом використання аналітичних методів і сучасних методів моделювання. ФК 14. Здатність використовувати уміння по участі в підготовці технічної документації; здійсненню технічної експлуатації СЗІ на об'єктах професійної діяльності, призначених для збору, обробки, зберігання й передачі інформації. ФК 15. Уміння проектувати системи захисту і безпеки інформації та їх елементи з урахуванням усіх аспектів поставленої задачі, включаючи створення, налагодження, експлуатацію, технічне обслуговування та утилізацію. ФК 16. Уміння аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати та захищати прийняті рішення. ФК 17. Знання основ охорони праці, виробничої санітарії і пожежної безпеки при реалізації систем технічного захисту інформації. ФК 18. Уміння ідентифікувати, класифікувати та описувати роботу, пов'язану з захистом інформації та безпекою інформаційно-комунікаційних систем, шляхом використання аналітичних методів і методів моделювання.
Фахові компетентності професійного спрямування (ФКС)	**0401*: Адміністрування систем кібербезпеки*** ФКС 1. Здатність використовувати адміністративно-організаційні, управлінські, технічні та правові методи, засоби й заходи із побудови систем забезпечення кібернетичної безпеки.

	ФКС 2. Уміння проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ФКС 3. Здатність і готовність застосовувати знання форм і методів наукового пізнання у галузі інформаційної безпеки; ФКС 4. Здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій, проводити криміналістичну експертизу слідів кібератак в кібернетичному просторі. ФКС 5. Уміння здійснювати програмування базових об'єктів захисту інформації, криптосистем и криптопротоколів. **0402*: Адміністративний менеджмент у сфері кібербезпеки*** ФКС 6. Здатність до проведення аналізу інцидентів інформаційної безпеки, виконання їх оцінювання, визначення пріоритетів та здійснення їх усунення чи запобігання. ФКС 7. Уміння здійснювати вибір організаційних, технічних і програмних засобів для ефективного впровадження захисту сховищ даних та баз даних. ФКС 8. Уміння здійснювати оцінку відповідності системи захисту інформації автоматизованої системи своєму призначенню відповідно до вимог діючих стандартів. ФКС 9. Уміння здійснювати адміністрування підсистем інформаційної безпеки об'єкта, а також підсистем передачі даних. ФКС 10. Уміння проводити атестацію об'єктів, приміщень, технічних засобів, систем, програм і алгоритмів на предмет відповідності вимогам державних або корпоративних нормативних документів щодо захисту інформації.
7 – Програмні результати навчання	
Знання (ЗН)	1. Володіння достатніми знаннями в галузях пов'язаних з інформаційними технологіями, кібербезпекою, інформаційною безпекою, що дасть можливість критично аналізувати ситуацію в даних галузях та визначати ключові тенденції їх розвитку. 2. Знання сучасних досягнень інноваційних технологій в галузі інформаційних технологій, інформаційно-комунікаційних систем, систем захисту інформації, кібербезпеки та управління. 3. Розуміння інструментів, наукових принципів та стратегій, що мають відношення до діагностування та аналізу стану розвитку кібербезпеки на рівні, що дозволить працевлаштування за фахом, здатність ефективно використовувати на практиці теоретичні знання при управлінні інформаційно безпекою. 4. Володіння методами загальнонаукового аналізу у сфері інформаційних технологій та кібербезпеки, володіння фактами, їх розуміння та інтерпретація результатів досліджень у вигляді звітів, публікацій на державній та одній з іноземних мов. 5. Володіння правовими та науково-організаційними основами проведення ліцензування, атестації та сертифікації об'єктів захисту інформації. 6. Здатність до ділових комунікацій у професійній сфері, знання основ ділового спілкування, навички роботи в команді, сучасні уміння вести дискусію й викладати основи інформаційної безпеки. 7. Знання математичних моделей завдань забезпечення інформаційної безпеки та захисту інформації.

	8. Знання основних підходів до організації типових комплексів та засобів захисту інформації в інформаційних і комунікаційних системах. 9. Знання основних моделей уразливостей, загроз та атак для обґрунтування варіантів побудови автоматизованої системи моніторингу інформаційної безпеки для інформаційних і комунікаційних систем та її основних складових. 10. Знання технологій створення систем захисту комп'ютерних систем та мереж для розробки та визначення загальних принципів побудови систем захисту, завдань та вихідних даних, які необхідно враховувати при проектуванні систем захисту. 11. Знання методик аналізу, синтезу, оптимізації та прогнозування якості процесів функціонування інформаційних процесів та технологій в розподілених інформаційно-комунікаційних системах. 12. Знання математичних методів оптимізації з метою одержання найкращих характеристик функціонування засобів та систем. 13. Володіння типовими підходами та методологіями до проектування та модернізації захищених об'єктів інформаційної діяльності відповідно до нормативних вимог чинних стандартів і технічних умов. 14. Здатність планувати та здійснювати власне наукове дослідження, присвячене суттєвій проблемі сучасної науки у галузі захисту інформації з обмеженим доступом; 15. Здобуття адекватних знань та розумінь, що відносяться до спеціальності 125 «Кібербезпека», масштаб яких буде достатнім, щоб успішно організовувати та проводити дослідження з інформаційної безпеки, формувати та репрезентувати результати професійної діяльності.
Уміння (УМ)	1. Вміння проводити бібліографічну роботу із залученням сучасних інформаційних технологій, формувати цілі дослідження, складати техніко-економічне обґрунтування досліджень, що проводяться, вибирати необхідні методи дослідження, модифікувати існуючі та розробляти нові методи, виходячи із завдань конкретного дослідження, застосовувати сучасні методи проведення експерименту в конкретній галузі знань. 2. Уміти здійснювати оцінку відповідності системи захисту інформації автоматизованої системи своєму призначенню відповідно до вимог діючих стандартів. 3. Уміння виконувати аналіз ризиків та джерел загроз, розробляти модель загроз, розробляти модель порушника. 4. Застосовувати набуті знання і розуміння для ідентифікації, формулювання і вирішення завдань захисту інформації, використовуючи відомі методи, системно мислити та застосовувати творчі здібності до формування принципово нових ідей в сфері інформаційної безпеки; 5. Розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем; 6. Поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань сфери

	захисту інформації з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів; 7. Уміння виконувати відповідні дослідження та застосовувати дослідницькі навички в управлінні інформаційною безпекою та в системах технічного захисту інформації. 8. Уміння виконувати аналіз і вибір дисципліни обслуговування заявок для комп'ютерних систем (КС) з врахуванням режимів роботи, вимог стосовно обслуговування заявок, інтенсивності потоків заявок, дисперсії часу очікування; 9. Надавати пропозицій для заключення угод і договорів з іншими установами, організаціями й підприємствами для проведення робіт в області захисту інформації. 10. Уміти проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. 11. Вміння проектувати моделюючі алгоритми, використовуючи методи сумісної роботи аналітичних і імітаційних компонентів. 12. Обґрунтовувати та реалізовувати системи захисту розподілених інформаційних ресурсів у інформаційно-комунікаційних системах. 13. Здійснювати вибір засобів захисту інформації для складових інформаційно-комунікаційних систем: операційні системи, активне мережне обладнання, системи мобільних програмних компонентів тощо. 14. Розробляти комплекси засобів захисту інформаційно-комунікаційних систем. 15. Здійснювати вибір засобів, необхідних для реалізації та компонування криптографічних систем. 16. Застосовувати стандарти у галузі криптографічного захисту інформації та здійснювати вибір конкретних параметрів криптографічних алгоритмів, впроваджувати та використовувати програмні комплекси, що забезпечують підтримку та функціонування інфраструктури відкритих ключів. 17. Розраховувати, конструювати, проектувати, досліджувати, експлуатувати, ремонтувати, налагоджувати типове для обраної спеціалізації обладнання. 18. Уміння застосовувати знання технічних характеристик, конструкційних особливостей, призначення і правил експлуатації устаткування та обладнання для вирішення технічних задач спеціальності.
Комунікація (КОМ)	1. Уміння спілкуватись, включаючи усну та письмову комунікацію українською та іноземною мовами (англійською, німецькою, польською, італійською, французькою, іспанською); 2. Здатність використання різноманітних методів, зокрема сучасних інформаційних технологій, для ефективно спілкування на професійному та соціальному рівнях.
Автономія і відповідальність (АіВ)	1. Здатність адаптуватись до нових ситуацій та приймати відповідні рішення; 2. Здатність усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань;

	3. Здатність відповідально ставитись до виконуваної роботи, самостійно приймати рішення, досягати поставленої мети з дотриманням вимог професійної етики; 4. Здатність демонструвати розуміння основних екологічних засад, охорони праці та безпеки життєдіяльності та їх застосування.
8 – Ресурсне забезпечення реалізації програми	
Специфічні характеристики кадрового забезпечення	Понад 90% науково-педагогічних працівників, задіяних до викладання професійно-орієнтованих дисциплін зі спеціальності 125 «Кібербезпека» мають наукові ступені та вчені звання, з практичним досвідом роботи > 20 %.
Специфічні характеристики матеріально-технічного забезпечення	Використання сучасного обладнання провідних компаній у галузі інформаційних технологій та інформаційної безпеки, зокрема Xilinx, Altera, а також стандартизованих вітчизняних апаратно-програмних засобів захисту інформації, центр сертифікації ключів, виробництва «Інституту інформаційних технологій» (м.Харків), а також використання сучасних прикладних програм для ефективного вирішення задач з технічного захисту інформації та автоматизації її обробки.
Специфічні характеристики інформаційно-методичного забезпечення	Використання віртуального навчального середовища Національного університету «Львівська політехніка» та авторських розробок науково-педагогічних працівників.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Національним університетом «Львівська політехніка» та університетами України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Національним університетом «Львівська політехніка» та навчальними закладами країн-партнерів
Навчання іноземних здобувачів вищої освіти	Можливе, після вивчення курсу української мови.

2. Розподіл змісту освітньо-професійної програми за групами компонентів та циклами підготовки

	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів / %)		
		Обов'язкові компоненти освітньо-професійної програми	Вибіркові компоненти освітньо-професійної програми	Всього за весь термін навчання
1	2	3	4	5
1.	Цикл загальної підготовки	3/2,5	3/2,5	6/5
2.	Цикл професійної підготовки	85/70,8	29/24,2	114/95
Всього за весь термін		88/73,3	32/26,7	120/100

навчання			

5. Перелік компонент освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти спеціальності			
1. Цикл загальної підготовки			
СК1.1.	Педагогіка і методика викладання у вищій школі	3	диф. залік
Всього за цикл:		**3**	
2. Цикл професійної підготовки			
СК2.1.	Комп'ютерні методи аналізу та проектування електронних засобів	5	екзамен
СК2.2.	Комплексні системи санкціонованого доступу	6	екзамен
СК2.3.	Основи інтернету речей та його безпека	4	екзамен
СК2.4.	Основи наукових досліджень та організація науки	5	диф. залік
СК2.5.	Технології протидії шкідливому програмному коду	4	екзамен
СК2.6.	Безпека розподілених мереж і хмарних технологій	5	екзамен
СК2.7.	Комп'ютерні методи високорівневого проектування пристроїв захисту	5	екзамен
СК2.8.	IT аудит кібербезпеки	5	екзамен
СК2.9.	Концепція побудови безпечного міста	5	екзамен
СК2.10.	Безпека розподілених мереж і хмарних технологій (КР)	2	диф. залік
СК2.11.	Комп'ютерні методи аналізу та проектування електронних засобів (КП)	3	диф. залік
СК2.12.	Комплексні системи санкціонованого доступу (КП)	3	диф. залік
СК2.13.	Комп'ютерні методи високорівневого проектування пристроїв захисту (КП)	3	диф. залік
СК2.14.	Науково-дослідницька практика	9	
СК2.15.	Практика за темою магістерської кваліфікаційної роботи	6	диф. залік
СК2.16.	Виконання магістерської кваліфікаційної роботи	12	диф. залік
СК2.17.	Захист магістерської роботи	3	
Всього за цикл		**85**	
Всього за групу компонентів		**88**	
Вибіркові компоненти освітньо-професійної програми			
Вибіркові блоки компонентів			
1. Цикл загальної підготовки			
Всього:		**3**	
2. Цикл професійної підготовки			
Вибіркові компоненти блоку 0401: Адміністрування систем кібербезпеки			
ВБ0401.1	Високорівневе програмування систем захисту комп'ютерних мереж	4	екзамен
ВБ0401.2	Математичні методи моделювання та оптимізації процесів	3	диф. залік
ВБ0401.3	Інтелектуальний аналіз даних	5	екзамен
ВБ0401.4	Системи безпеки інтелектуальних об'єктів	4	екзамен

ВБ0401.5	Сучасні криптографічні алгоритми, протоколи та технології	5	екзамен
ВБ0401.6	Системи безпеки інтелектуальних об'єктів (КП)	3	диф. залік
Вибіркові компоненти блоку 0402: Адміністративний менеджмент у сфері кібербезпеки			
ВБ0402.1	Міжнародні стандарти із кібербезпеки	4	екзамен
ВБ0402.2	Безпека Web-додатків	3	диф. залік
ВБ0402.3	Адміністрування та захист баз даних	5	екзамен
ВБ0402.4	Моделювання та оцінка ефективності засобів захисту інформації	5	екзамен
ВБ0402.5	Проектування систем безпеки об'єктів критичної інфраструктури та держ. таємниці	5	екзамен
ВБ0402.6	Проектування систем безпеки об'єктів критичної інфраструктури та держ. таємниці (КР)	2	диф. залік
Всього:		**24**	
Вибіркові компоненти інших освітньо-професійних програми			
Всього:		**5**	
Всього за вибіркові компоненти:		**32**	
Всього зо освітньо-професійну програму:		**120**	

4. Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи та завершується видачею документів встановленого зразка про присудження йому ступеня магістра . На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою в процесі навчання за даним стандартом. До атестації допускаються студенти, які виконали всі вимоги програми підготовки.
Вимоги до кваліфікаційної роботи/проекту	Кваліфікаційна робота має передбачати розв'язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки. Кваліфікаційна робота виконується з грифом ДСК та зберігається у філії РСО кафедри.

5. Матриця відповідності програмних компетентностей навчальним компонентам

	СК1.1.	СК2.1.	СК2.2.	СК2.3.	СК2.4.	СК2.5.	СК2.6.	СК2.7.	СК2.8.	СК2.9.	СК2.10.	СК2.11.	СК2.12.	СК2.13.	СК2.14.	СК2.15.	СК2.16.	СК2.17.
ІНТ				•		•		•	•		•							
ЗК1	•	•											•	•	•	•		
ЗК2							•	•			•	•		•	•	•		
ЗК3	•														•	•	•	•
ЗК4							•	•			•	•					•	•
ЗК5													•	•	•	•	•	•
ЗК6													•	•				
ЗК7				•											•	•		
ЗК8	•	•					•	•			•	•						
ЗК9			•	•	•		•	•		•		•						
ЗК10							•	•			•	•	•	•	•	•		

ЗК11			•			•			•	•								
ЗК12	•	•					•	•			•	•		•	•	•		
ФК1			•	•	•	•			•	•								
ФК2	•					•			•									
ФК3				•				•										
ФК4				•	•			•										
ФК5			•	•	•		•	•		•	•	•			•			
ФК6									•		•				•			
ФК7			•			•	•					•						
ФК8				•	•		•	•							•			
ФК9	•	•		•			•								•			
ФК10							•	•			•	•	•	•	•	•		
ФК11							•	•			•	•			•			
ФК12				•		•		•	•		•							
ФК13	•					•												
ФК14							•	•			•	•			•			
ФК15			•	•				•		•		•			•			
ФК16	•															•	•	•
ФК17				•				•							•		•	•
ФК18	•		•				•			•		•						

6. Матриця відповідності фахових компетентностей спеціалізації (ФКС) навчальним компонентам

	ВБ0301.1.	ВБ0301.2	ВБ0301.3	ВБ0301.4	ВБ0301.5	ВБ0301.6	ВБ0302.1	ВБ0302.2	ВБ0302.3	ВБ0302.4	ВБ0302.5	ВБ0302.6
ФКС1				•	•	•						
ФКС2		•	•		•							
ФКС3					•							
ФКС4	•											
ФКС5		•			•	•						
ФКС6								•		•		
ФКС7									•		•	•
ФКС8							•			•	•	•
ФКС9								•	•			
ФКС10							•				•	•

Логічно-структурна схема освітньо-професійної програми “Адміністрування систем кібербезпеки” магістра зі спеціальності 125 “Кібербезпека”