МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

КІБЕРБЕЗПЕКА

Другого (магістерського) рівня вищої освіти

за спеціальністю 125 «Кібербезпека та захист інформації»

галузь знань 12 Інформаційні технології

Кваліфікація: магістр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Голова вченої ради

_____ С.М. Шкарлет

(протокол № 14 від "22" грудня 2023 р.)

Освітня програма вводиться в дію з 01 вересня 2024 р.

Ректор _____ О.О. Новомлинець

(наказ № 246/ВС від "22" грудня 2023 р.)

Чернігів 2023

ПЕРЕДМОВА

Розроблено проєктною групою у складі:

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

Розроблена відповідно до стандарту вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для другого (магістерського) рівня вищої освіти, затвердженого наказом МОН України від 18.03.2021 №332

Додаються рецензії зовнішніх стейкходерів:

1. Зайцев С.В., доктор технічних наук, професор, директор ТОВ «Інформаційна безпека».
2. Євсеєв С.П., доктор технічних наук, професор, завідувач кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут».
3. Сорока Б.І., координатор Chernihiv.IT.

1. Профіль освітньої програми зі спеціальності 125 «Кібербезпека та захист інформації»

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Національний університет «Чернігівська політехніка» ННІ електронних та інформаційних технологій. Кафедра кібербезпеки та математичного моделювання
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Магістр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Тип диплому – одиничний. Диплом магістра, одиничний, 90 кредитів ЄКТС., Термін навчання 1 рік 4 місяці
Наявність акредитації	Національне агентство з забезпечення якості вищої освіти. Україна. Сертифікат № 975 від 18.12.2020. Термін дії сертифіката до 01.07.2026.
Цикл/рівень	НРК України - 7 рівень, QF-EHEA – другий цикл, EQF-LLL - 7 рівень
Передумови	Наявність освітнього ступеня бакалавра. Програма фахових вступних випробувань для осіб, що здобули попередній рівень вищої освіти за іншими спеціальностями повинна передбачати перевірку набуття особою компетентностей та результатів навчання, що визначені стандартом вищої освіти зі спеціальності 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти. Університет має право визнати та перезарахувати кредити ЄКТС, отримані за попередньою освітньою програмою підготовки магістра (спеціаліста) за іншою спеціальністю. Максимальний обсяг кредитів ЄКТС, що може бути перезарахований, становить 25% від загального обсягу освітньої програми.
Мова (и) викладання	Українська
Термін дії освітньої програми	До 01 липня 2026 року або до заміни новою
Інтернет адреса постійного розміщення опису освітньої програми	https://op.stu.cn.ua/view/total_view.php
2 – Мета освітньої програми	
Забезпечити здобувачам вищої освіти (ЗВО) фундаментальну підготовку у вигляді поглиблених теоретичних і практичних знань, умінь та навичок за спеціальністю 125 Кібербезпека та захист інформації, достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузях телекомунікацій та інформаційних технологій, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу.	
3 – Характеристика освітньої програми	

Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань – 12 «Інформаційні технології». Спеціальність – 125 «Кібербезпека та захист інформації» *Об'єкти вивчення:* – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. *Цілі навчання:* Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. *Теоретичний зміст предметної області* Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. *Методи, методики та технології* Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. *Інструменти та обладнання.* Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньої програми	Освітньо-професійна програма

Основний фокус освітньої програми та спеціалізації	Загальна: акцент на здатності організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізації, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації.
Особливості програми:	Інтегрована підготовка фахівців до вирішення завдань у сфері інформаційної безпеки, що передбачає розроблення, впровадження та експлуатацію комплексних (інформаційних, телекомунікаційних, технічних) систем захисту інформації на об'єктах інформаційної діяльності, поглиблене вивчення нормативних документів та стандартів з захисту інформації, принципів побудови систем технічного захисту інформації, дій для захисту інформаційних ресурсів організацій і користувачів.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускник з кібербезпеки та захисту інформації може займати первинні посади: • Аналітик загроз безпеки; • Аналітик систем захисту інформації та оцінки вразливостей; • Аналітик з безпеки інформаційно-телекомунікаційних систем; • Уповноважений з авторизації безпеки інформації • Фахівець з юридичних консультацій та адвокації в сфері кібербезпеки • Аудитор програм інформаційних технологій • Аудитор інформаційних технологій (з кібербезпеки) • Експерт з управління інформаційними технологіями • Фахівець з планування політики та стратегії кібербезпеки • Інженер із застосування комп'ютерів • Фахівець з кібердосліджень та розробок систем безпеки • Фахівець з оцінки заходів захисту інформації (кібербезпеки) • Інструктор-методист з інформаційної безпеки та кібербезпеки • Провідний спеціаліст/керівник служби технічного захисту інформації • Дізнавач (сфера кібербезпеки та захисту інформації) Проектна, виробнича, технологічна, управлінська, науково-дослідна; інноваційна, викладацька, експертна та консультативна діяльність у сфері інформаційних технологій/кібербезпеки.
Подальше навчання	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	Ґрунтується на принципах студентоцентризму та індивідуально-особистісного підходу. Реалізується через навчання на основі досліджень, посилення практичної орієнтованості. Викладання проводиться у формі комбінації лекцій, мультимедійної лекції, інтерактивної лекції, практичних, лабораторних, самостійної навчальної та дослідницької роботи з використанням електронного навчання в системі Moodle, розв'язування прикладних задач, виконання курсового проекту (роботи), практики, кваліфікаційної магістерської роботи.
Оцінювання	Оцінювання рівня засвоєння освітньо-професійної програми здійснюється за допомогою поточного, модульного і підсумкового контролю (екзамени, заліки) та за результатами прилюдного захисту

	кваліфікаційної роботи.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності	КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
	КЗ 2. Здатність проводити дослідження на відповідному рівні.
	КЗ 3. Здатність до абстрактного мислення, аналізу та синтезу.
	КЗ 4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
	КЗ 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
	КЗ 6. Здатність до ініціативності, відповідальності та навички до превентивного і аварійного планування, управління заходами безпеки професійної діяльності, уміння приймати рішення у складних та непередбачуваних ситуаціях, лідерські якості та знання міжнародних норм і законодавства України у сфері безпеки життєдіяльності населення, системи управління охороною праці та цивільного захисту
Фахові компетентності	КФ 1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки
	КФ 2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки
	КФ 3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури
	КФ 4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог
	КФ 5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
	КФ 6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
	КФ 7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
	КФ 8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії

	і політики інформаційної безпеки та/або кібербезпеки організації.
	КФ 9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому
	КФ 10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

7 – Програмні результати навчання (ПРН)	
ПРН1.	Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
ПРН2.	Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
ПРН3.	Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
ПРН4.	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
ПРН5.	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
ПРН6.	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
ПРН7.	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
ПРН8.	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
ПРН9.	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
ПРН10.	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
ПРН11.	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
ПРН12.	Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
ПРН13.	Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

ПРН14.	Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
ПРН15.	Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
ПРН16.	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
ПРН17.	Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
ПРН18.	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
ПРН19.	Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
ПРН20.	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
ПРН21.	Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
ПРН22.	Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
ПРН23.	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
ПРН24.	Забезпечувати гарантії збереження здоров'я і працездатності працівників у виробничих умовах через ефективне управління охороною праці та формування відповідальності за колективну та власну безпеку; використовувати методи превентивного та аварійного планування, керувати заходами з безпеки професійної діяльності, приймати рішення у складних та непередбачуваних ситуаціях, вирішувати професійні завдання з урахуванням вимог цивільного захисту та охорони праці

8 – Ресурсне забезпечення реалізації програм	
Кадрове забезпечення	Викладацький склад, який забезпечує реалізацію освітньої програми, відповідає вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності закладів освіти.
Матеріально-технічне забезпечення	Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає потребі. В університеті діють власні об'єкти соціально-побутової інфраструктури. У тому числі: їдальня, буфети, гуртожитки, актові зали, спортивні зали, спортивні майданчики. Заняття та наукові дослідження проводяться у лабораторіях кафедри кібербезпеки та математичного моделювання, кафедри інформаційних і комп'ютерних систем, програмної інженерії та інформаційних технологій. Для проведення інформаційного пошуку та обробки результатів є комп'ютерні класи, де наявне спеціалізоване програмне забезпечення

	та відкритий доступ до Інтернет-мережі.
Інформаційне та навчально-методичне забезпечення	«Навчально-методичне забезпечення навчальних дисциплін (силабуси, конспекти лекцій, методичні матеріали для проведення практичних (лабораторних) занять, самостійної та індивідуальної роботи здобувачів вищої освіти, курсових робіт, завдання для поточного та підсумкового оцінювання знань, перелік рекомендованої літератури тощо) представлено в системі дистанційного навчання MOODLE НУ «Чернігівська політехніка». Здобувачі вищої освіти та викладачі можуть використовувати бібліотечно-інформаційну систему, наукову бібліотеку Університету. Інформаційні ресурси бібліотеки за освітньою програмою формуються відповідно до предметної області та сучасних тенденцій наукових досліджень у галузі. Ресурси Наукової бібліотеки НУ «Чернігівська політехніка» доступні через внутрішню та зовнішню мереж.
9 – Академічна мобільність	
Національна кредитна мобільність	Реалізується в Університеті відповідно до вимог чинного законодавства та регулюється Положенням про академічну мобільність учасників освітнього процесу НУ «Чернігівська політехніка». Здійснюється на основі двосторонніх договорів між НУ «Чернігівська політехніка» та закладами вищої освіти України. Кредити, отримані в інших університетах України, перезараховуються відповідно до Порядку визначення академічної різниці та визнання результатів попереднього навчання в Національному університеті «Чернігівська політехніка».
Міжнародна кредитна мобільність	Реалізується в Університеті відповідно до вимог чинного законодавства та регулюється Положенням про академічну мобільність учасників освітнього процесу НУ «Чернігівська політехніка». Здійснюється на основі двосторонніх договорів між НУ «Чернігівська політехніка» та закладами вищої освіти зарубіжних країн-партнерів. Індивідуальна академічна мобільність можлива за рахунок участі у програмі Еразмус + та інших програмах.
Навчання іноземних здобувачів вищої освіти	Здійснюється згідно з вимогами чинного законодавства, Порядку організації набору та навчання (стажування) іноземців та осіб без громадянства у НУ «Чернігівська політехніка»

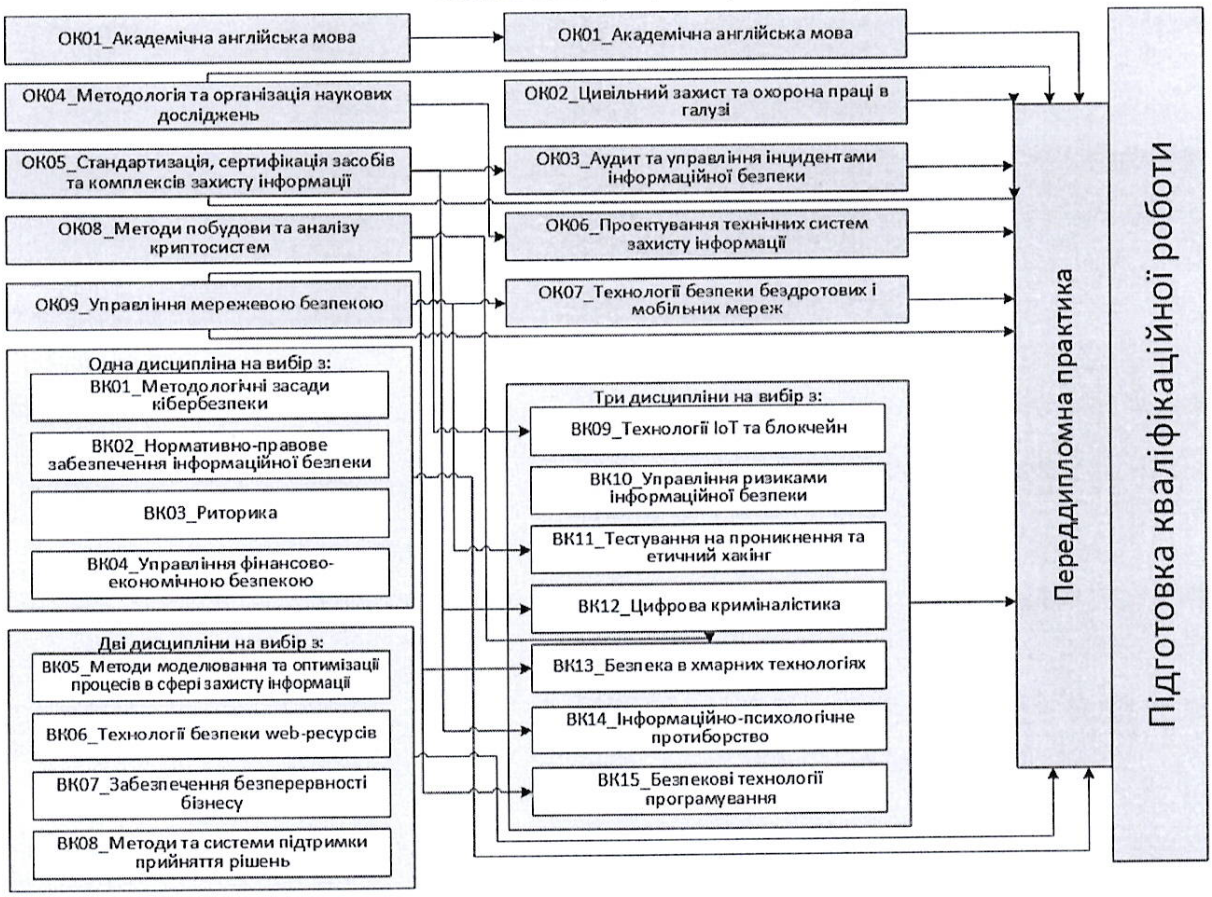
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти(роботи), практики, кваліфікаційна робота	Кількість кредитів	Форма підсумк. контролю
	2	3	4
Обов'язкові компоненти ОП			
ОК 1.	Академічна англійська мова	4	диф.залік
ОК 2.	Цивільний захист та охорона праці в галузі	3	диф.залік
ОК 3.	Аудит та управління інцидентами інформаційної безпеки	4	екзамен
ОК 4.	Методологія та організація наукових досліджень	4	диф.залік
ОК 5.	Стандартизація, сертифікація засобів та комплексів захисту інформації	4	екзамен
ОК 6.	Проектування технічних систем захисту інформації	6	екзамен/КП
ОК 7.	Технології безпеки бездротових і мобільних мереж	3	диф.залік
ОК 8.	Методи побудови та аналізу криптосистем	4	екзамен
ОК 9.	Управління мережевою безпекою	4	екзамен
Загальний обсяг обов'язкових компонент:		**36**	
Вибіркові компоненти ОП			
ВК 1.	Методологічні засади кібербезпеки	4	диф.залік
ВК 2.	Нормативно-правове забезпечення інформаційної безпеки	4	Диф.залік
ВК 3.	Риторика	4	Диф.залік
ВК 4.	Управління фінансово-економічною безпекою	4	Диф.залік
ВК 5.	Методи моделювання та оптимізації процесів в сфері захисту інформації	4	Диф.залік
ВК 6.	Технології безпеки web-ресурсів	4	Диф.залік
ВК 7.	Забезпечення безперервності бізнесу	4	Диф.залік
ВК 8.	Методи та системи підтримки прийняття рішень	4	Диф.залік
ВК 9.	Технології IoT та блокчейн	4	екзамен
ВК 10.	Управління ризиками інформаційної безпеки	4	екзамен
ВК 11.	Тестування на проникнення та етичний хакінг	4	екзамен
ВК 12.	Цифрова криміналістика	4	екзамен
ВК 13.	Безпека в хмарних технологіях	4	екзамен
ВК 14.	Інформаційно-психологічне протиборство	4	екзамен
ВК 15.	Безпекові технології програмування	4	екзамен
Загальний обсяг вибіркових компонент:		**24**	
ОК 10.	Переддипломна практика	16	диф.залік
ОК 11.	Підготовка кваліфікаційної роботи	14	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		90	

2.2. Структурно-логічна схема ОП

Структурно-логічна схема дисциплін ОПП «Кібербзепека» спеціальності 125 Кібербезпека та захист інформації освітньо-ківаліфікаційного рівня магістр



3. Форма атестації здобувачів вищої освіти

Атестація здійснюється у формі публічного захисту кваліфікаційного роботи.

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

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

Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій.

Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації.

Кваліфікаційна робота розміщується у репозитарії Університету.

4.1.Матриця відповідності програмних компетентностей компонентам освітньої програми

Обов'язкові компоненти

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

4.2. Матриця відповідності програмних компетентностей компонентам освітньої програми

Вибіркові компоненти

	ВК 1.	ВК 2.	ВК 3.	ВК 4.	ВК 5.	ВК 6.	ВК 7.	ВК 8.	ВК 9.	ВК 10.	ВК 11.	ВК 12.	ВК 13.	ВК 14.	ВК 15.
КЗ 1.	+	+				+		+	+		+	+	+	+	+
КЗ 2.	+				+				+				+	+	
КЗ 3.		+		+	+	+			+	+		+			+
КЗ 4.						+	+				+	+	+		
КЗ 5.	+		+	+			+				+	+		+	+
КЗ 6.														+	
КФ 1.					+	+		+		+	+		+		+
КФ 2.	+	+									+			+	
КФ 3.											+				+
КФ 4.	+	+		+			+								
КФ 5.				+			+				+				
КФ 6.						+					+		+		
КФ 7.											+	+			
КФ 8.									+						
КФ 9.							+				+				
КФ 10.	+	+	+						+						+

5.1. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми (Обов'язкові компоненти)

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

5.2. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми (Вибіркові компоненти)

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

6. Перелік нормативних документів, на яких базується освітня програма

1. Про вищу освіту. - Закон України від 01.07.2014р. № 1556-VII // ВВРУ від 19.09.2014р., № 37-38, стор. 2716, стаття 2004. URL: https://zakon.rada.gov.ua/laws/show/1556-18
2. Про освіту. - Закон України від 5 вересня 2017р. № 2145-VIII // ВВРУ від 29.09.2017р., №38-39, стор. 5, стаття 380. URL: https://zakon.rada.gov.ua/laws/show/2145-19
3. Національний класифікатор України: «Класифікатор професій» ДК 003:2010 (Редакція від 25.10.2021). URL: http://zakon.rada.gov.ua/rada/show/va327609-10
4. Національна рамка кваліфікацій. - Постанова КМУ від 23 листопада 2011 р. № 1341 // ОВУ від 06.01.2012р., № 101, стор. 15, ст. 3700, код акта 59774/2011. URL: https://zakon.rada.gov.ua/laws/show/1341-2011-п
5. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти. - Постанова КМУ від 29 квітня 2015р. № 266 // ОВУ від 22.05.2015р., №38, стор. 194, ст. 1147, код акта 76797/2015. URL: https://zakon.rada.gov.ua/laws/show/266-2015-п
6. Ліцензійні умови провадження освітньої діяльності. Постанова КМУ від 30 грудня 2015р. № 1187 // ОВУ від 02.02.2016р., № 7, стор. 23, ст. 345, код акта 80480/2016. URL: https://zakon.rada.gov.ua/laws/show/1187-2015-п
7. Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти. URL: https://naqa.gov.ua/wp-content/uploads/2019/07/Додаток-1.-Стандарти-і-рекомендації-щодо-забезпечення-якості-в-Європейському-просторі-вищої-освіти.pdf
8. Методичні рекомендації щодо розроблення стандартів вищої освіти. Наказ Міністерства освіти і науки України від «01» червня 2017 №600. URL: https://mon.gov.ua/storage/app/media/vishcha-osvita/rekomendatsii-1648.pdf
9. Стандарт вищої освіти України другого (магістерського) рівня, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека. Наказ Міністерства освіти і науки України 18.03.2021 р. № 332. URL: https://mon.gov.ua/storage/app/media/vyshcha/standarty/2021/03/19/125%20Kiberbezpeka_mahistr_18_03_21_332.docx