ПРОЄКТ
(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації, автоматизація її обробки»

Другого (магістерського) рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

СМЯ НАУ ОПП 09.01.10 –03– 2021

Освітньо-професійна програма
затверджена Вченою радою Університету
Протокол № ____ від _____ 2021 р.

Вводиться в дію наказом ректора

Ректор
_____ М. Луцький

Наказ № ____ від _____ 2021 р.

КИЇВ

ДІЄ ЯК ТИМЧАСОВА ДО ВВЕДЕННЯ СТАНДАРТУ ВИЩОЇ ОСВІТИ УКРАЇНИ

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

ПОГОДЖЕНО

Науково-методичною радою університету
протокол № _____

від «___» _____ 2021 р.

Голова НМР НАУ
проректор з навчальної роботи

_____ (Полухін А.В.)

ПОГОДЖЕНО

Вченою радою Факультету кібербезпеки, комп'ютерної та програмної інженерії

протокол № _____

від «___» _____ 2021 р.

Голова Вченої ради факультету кібербезпеки, комп'ютерної та програмної інженерії

_____ (_____)

ПОГОДЖЕНО

Кафедрою засобів захисту інформації

протокол засідання № ____

від «___» _____ 2021 р.

Завідувач кафедри

_____ (Козловський В.В.)

ПОГОДЖЕНО

Студентською радою факультету кібербезпеки, комп'ютерної та програмної інженерії

протокол № ____

від «___» _____ 2021 р.

Голова Студентською ради факультету кібербезпеки, комп'ютерної та програмної інженерії

_____ (_____)

ПЕРЕДМОВА

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ (спеціальності 125 «Кібербезпека», рік вступу – 2021-й та наступні до нової редакції освітньої програми) у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

ЛАЗАРЕНКО С.В. – д.т.н., доцент, професор кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії _____
(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

КОЗЛОВСЬКИЙ В.В. – д.т.н., професор, завідувач кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії _____
(підпис)

ТЕМНІКОВ В.О. – д.т.н., доцент, професор кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії _____
(підпис)

ШВЕЦЬ В.А. – к.т.н., доцент, доцент кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії _____
(підпис)

МАРТИНЮК Г.В. – (к.т.н., доцент кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії) _____
(підпис)

_____ _____
(П.І.Б. здобувача вищої освіти) (підпис здобувача вищої освіти)

ЗОВНІШНІ СТЕЙКХОЛДЕРИ

Толюпа С.В. – д.т.н., професор, професор кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

_____
(підпис)

Рецензії, відгуки зовнішніх стейкхолдерів (додаються).

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Контрольний примірник

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	Повна назва закладу вищої освіти та структурного підрозділу	Національний авіаційний університет Факультет кібербезпеки, комп'ютерної та програмної інженерії Кафедра засобів захисту інформації
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр; Магістр з кібербезпеки
1.3.	Офіційна назва освітньо-професійної програми та спеціалізації (за наявності)	Системи технічного захисту інформації, автоматизація її обробки
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці(денна форма навчання)/ 1 рік 4 місяці (заочна форма навчання).
1.5.	Акредитаційна інституція	Міністерство освіти і науки України, рішення Акредитаційної комісії від 12.11.2018 сертифікат серія УД № 11005811
1.6.	Період акредитації	До 01.07.2023 р., чергова
1.7.	Цикл/рівень	7 рівень Національної рамки кваліфікацій України (НРК України), другий цикл Європейського простору вищої освіти (FQ-EHEA), 7 рівень Європейської рамки кваліфікацій для навчання впродовж життя (EQF-LLL).
1.8.	Передумови	Вища освіта зі ступенем бакалавр
1.9.	Форма навчання	Інституційна з елементами дистанційної: очна, заочна, мережева.
1.10.	Мова(и) викладання	Українська
1.11.	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://www.nau.edu.ua http://www.kzzi.nau.edu.ua
Розділ 2. Ціль освітньо-професійної програми		
2.1.	Ціллю ОПП «Системи технічного захисту інформації, автоматизація її обробки» є підготовка висококваліфікованих фахівців, які володіють сучасними загально-науковими й спеціальними знаннями та технологіями інформаційної та/або кібербезпеки, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Опанування специфічних знань особливостей професійної діяльності в авіаційному секторі, застосування яких дозволяє вирішувати практичні завдання підвищення рівня безпеки в авіації. ОПП «Системи технічного захисту інформації, автоматизація її обробки» відповідає місії НАУ, у якій наголошується, щодо внеску НАУ у розвиток суспільства на національному та міжнародному рівнях через генерацію нових знань та інноваційних ідей на основі інтеграції та інтернаціоналізації освіти, досліджень і практики, так і надання високоякісних освітніх та науково-дослідних послуг громадянам України та іноземцям при підготовці фахівців з Кібербезпеки в авіаційно-космічній галузі.	

Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (об'єкт діяльності, теоретичний зміст)	*Об'єкт діяльності*: системи та комплекси технічного захисту інформації на об'єктах інформаційної діяльності; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків). *Теоретичний зміст предметної області*: методи та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі.
3.2.	Орієнтація освітньо-професійної програми	Програма має прикладну орієнтацію. Освітньо-професійна програма базується на загальновідомих наукових результатах в галузі інформаційних технології у рамках яких можлива подальша професійна кар'єра і подальше навчання.
3.3.	Основний фокус освітньо-професійної програми та спеціалізації (за наявності)	Загальна вища освіта та професійна підготовка в галузі 12 – «Інформаційні технології» за спеціальністю 125 – «Кібербезпека». Ключові слова: технічний захист інформації, автоматизовані системи захисту інформації, обробка інформації з обмеженим доступом
3.4.	Особливості освітньо-професійної програми	Програма передбачає: – обов'язкове проходження переддипломної практики; – застосування практичних навичок у сфері технічного захисту інформації; – практичного використання методів та засобів технічного та криптографічного захисту інформації. На відміну від інших освітніх програм увага приділяється автоматизованим системам та комплексам технічного захисту інформації.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Випускники отримують можливість працевлаштування до підприємств (організацій, установ) різних форм власності в галузі «Інформаційних технологій» за спеціальністю «Кібербезпека» на відповідні посади та обіймати посади в інших секторах економіки при наявності сертифікатів про опанування відповідних програм підготовки.
4.2.	Подальше навчання	Продовження навчання для отримання ступеня «Доктор філософії», отримання другої вищої освіти.

Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	Лекції, лабораторні роботи, семінари, практичні заняття, проектна робота в командах, самостійна робота на основі підручників та конспектів, консультації з викладачами, переддипломна практика на підприємствах, підготовка кваліфікаційної магістерської роботи.
5.2.	Оцінювання	Усні, письмові, творчі, тестові та комбіновані екзамени, диференційовані заліки, лабораторні звіти, звіти із практичних робіт та практик, реферати, захист курсових проектів, презентації, поточний контроль, єдиний державний кваліфікаційний екзамен та захист кваліфікаційної роботи.
Розділ 6. Програмні компетентності		
6.1.	Інтегральні Компетентності (ІК)	ІК1. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
6.2.	Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях, професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК2. Знання та розуміння предметної області та розуміння професії, методологічні знання і дослідницькі уміння, що забезпечують виконання завдань науково-дослідної, науково-педагогічної, управлінської і інноваційної діяльності. ЗК3. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням, бути здатним до роботи в команді. ЗК4. Здатність до самостійної науково-дослідної діяльності, пошуку, оброблення та аналізу інформації. ЗК5. Здатність до критики й самокритики, креативність, адаптивність і комунікабельність, наполегливість у досягненні мети, толерантність.
6.3.	Фахові компетентності (ФК)	ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності

6.3.	Фахові компетентності (ФК)	в галузі інформаційної та/або кібербезпеки. ФК2. Здатність до використання сучасних інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. ФК3. Здатність до використання програмних, апаратних та програмно-апаратних комплексів засобів захисту інформації на об’єктах інформаційної діяльності. ФК4. Здатність виконувати роботи з проектування складних комплексів засобів захисту та охорони об’єктів інформаційної діяльності відповідно до сфери їх застосування. ФК5. Здатність до керівництва проектами зі створення інформаційних ресурсів обмеженого доступу. ФК6. Здатність до організації розроблення, впровадження та експлуатації систем автоматизованого оброблення інформації з обмеженим доступом. ФК7. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК8. Здатність проводити ліцензування, атестацію та сертифікацію об’єктів інформаційної діяльності. ФК9. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному/кібернетичному простору та інформаційним ресурсам. ФК10. Здатність розробляти проектну документацію, програми та методики випробувань та організовувати тестування і налагодження комплексів засобів захисту і охорони об’єктів інформаційної діяльності. ФК11. Здатність представляти результати досліджень у вигляді звітів, публікацій. ФК12. Здатність розробляти проекти методичних і нормативних документів, технічної документації, а також пропозиції та заходи з реалізації розроблених проектів.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання (ПРН)	ПРН1. Здійснювати професійну діяльність на основі законодавчої та нормативно-правової бази держави, а також у відповідності до вітчизняних і міжнародних вимог і стандартів в галузі інформаційної безпеки і \або

7.1.	Програмні результати навчання (ПРН)	кібербезпеки; приймати участь у розробці нормативних документів, концепцій, політик, внутрішніх стандартів, положень, інструкцій, рекомендацій, готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки. ПРН2. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних та наукоємних технологій та методів; забезпечувати професійну діяльність на основі знань і навичок про архітектуру інформаційної системи на основі визначення інформаційних суб'єктів та об'єктів інформаційної діяльності, корпоративної архітектури, периметру безпеки (контрольованої зони), політики безпеки, привілеїв. ПРН3. Використовувати методи аналізу й діагностики стану програмних, апаратних та програмно-апаратних засобів і систем захисту інформації; забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. ПРН4. Визначати відомості, які відносяться до інформації з обмеженим доступом, організовувати допуск та доступ персоналу до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки. ПРН5. Організовувати внутрішньо-об'єктовий та пропускний режими на підприємстві. ПРН6. Організовувати контроль за станом захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності. ПРН7. Забезпечувати систему безперервності бізнес процесів та відновлення штатного функціонування комплексів засобів захисту інформації на основі встановленої процедури планування, вимог, правил безпеки з урахуванням аналізу небезпечних впливів, превентивних мір, стратегій відновлення інфраструктури, резервування різних типів; перегляду цілей, стратегій, планів після реалізації загроз порушником, здійснення кібератак, збоїв та відмов різних класів, що

7.1.	Програмні результати навчання (ПРН)	привело до порушень штатного функціонування комплексів засобів захисту інформації. ПРН8. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованим вторгненням до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН9. Здатність продемонструвати знання та вміння забезпечувати систему виявлення, ідентифікації, аналізу та реагування на інциденти з метою забезпечення захисту інформації від різного класу загроз та кібератак; застосовувати національні та міжнародні регулюючі акти, процедури та положення в сфері інформаційної безпеки та/або кібербезпеки для збору доказів і проведення розслідування інцидентів порушення безпеки інформації. ПРН10. Вирішувати задачі захисту інформації, що обробляється в АС (ІТС) з використанням сучасних методів та засобів криптографічного та стеганографічного захисту інформації. ПРН11. Здатність здійснювати оцінювання захищеності інформації усіх видів, що циркулює на об’єкті інформаційної діяльності. ПРН12. Здатність забезпечення функціонування системи моніторингу управління доступом до інформації на об’єктах інформаційної діяльності і процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем в умовах реалізації загроз різних класів та протидії порушникам. ПРН13. Здатність застосування систем виявлення та протидії несанкціонованим вторгненням на об’єкти інформаційної діяльності. ПРН14. Здатність продемонструвати знання та розуміння сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ПРН15. Здатність продемонструвати знання та навички складання звітів, публікацій, розроблення технічної документації. ПРН16. Здатність володіння англійською мовою, використовувати спеціальну термінологію для проведення літературного пошуку.

Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	Кадрове забезпечення відповідає ліцензійним вимогам. Всі науково-педагогічні працівники, що забезпечують освітньо-професійну програму за кваліфікацією відповідають профілю і напряму дисциплін, що викладаються, мають необхідний стаж педагогічної роботи та досвід практичної роботи. В процесі організації навчального процесу залучаються професіонали з досвідом дослідницької, управлінської, інноваційної, творчої та фахової роботи, іноземні лектори.
8.2.	Матеріально-технічне забезпечення	Матеріально-технічна база випускової кафедри засобів захисту інформації дозволяє забезпечити підготовку фахівців на першому (бакалаврському) рівні вищої освіти за ОПП: – забезпеченість комп'ютерними робочими місцями та прикладними комп'ютерними програмами достатнє для виконання навчальних планів; – усі комп'ютери кафедри під'єднані до локальної мережі університету з можливістю виходу в глобальну мережу Інтернет; – для ведення документації та забезпечення навчально-методичними матеріалами освітнього процесу кафедра в достатній кількості забезпечена оргтехнікою (принтерами, МФУ, сканерами); – навчальні лабораторії оснащені технічними засобами та спеціалізованим програмним забезпеченням, необхідними приладами та обладнанням (охоронними системами відеоспостереження, засобами та комплексами виявлення закладних пристроїв, засобами просторового та мережевого захисту інформації). Усі приміщення відповідають будівельним та санітарним нормам, гуртожитками забезпечені усі потребуючі, наявна соціальна інфраструктура включає спортивний комплекс, пункти харчування, центр творчості, медпункт і базу відпочинку. З метою якісної підготовки студентів використовуються охоронні системи відеоспостереження, засоби та комплекси виявлення закладних пристроїв, засоби просторового та мережевого захисту інформації.

8.3	Інформаційне та навчально-методичне забезпечення	Забезпечення навчальною та навчально-методичною літературою, доступ до фахових періодичних видань професійного спрямування, упровадження електронного каталогу та можливість роботи з електронними підручниками здійснюється за рахунок фондів Науково-технічної бібліотеки НАУ. Всі студенти забезпечені підручниками та навчальними посібниками з компонентів ОПП. Відповідне інформаційне та навчально-методичне забезпечення розташоване на освітніх платформах Google Classroom, Moodle (Modular Object-Oriented Dynamic Learning Environment). Всі ресурси науково-технічної бібліотеки доступні через сайт університету: http://www.lib.nau.edu.ua Читальний зал забезпечений бездротовим доступом до мережі Інтернет. Електронний репозитарій наукової бібліотеки НАУ: http://er.nau.edu.ua
Розділ 9. Академічна мобільність		
9.1.	Національна кредитна мобільність	Національна кредитна мобільність здобувачів вищої освіти, наукових і науково-педагогічних працівників, у т.ч. навчання, стажування, проведення наукових досліджень, викладання та підвищення кваліфікації організовується на підставі партнерських угод про співпрацю між Національним авіаційним університетом та закладами вищої освіти в Україні: – Національним технічним університетом України «Київським політехнічним інститутом імені Ігоря Сікорського»; Харківським національним університетом радіоелектроніки.
9.2.	Міжнародна кредитна мобільність	У рамках Еразмус+К1 договір про співробітництво між Національним авіаційним університетом та навчальними закладами ЕС.
9.3.	Навчання іноземних здобувачів вищої освіти	Створено умови для навчання іноземних здобувачів вищої освіти.

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

2.1. Перелік компонент

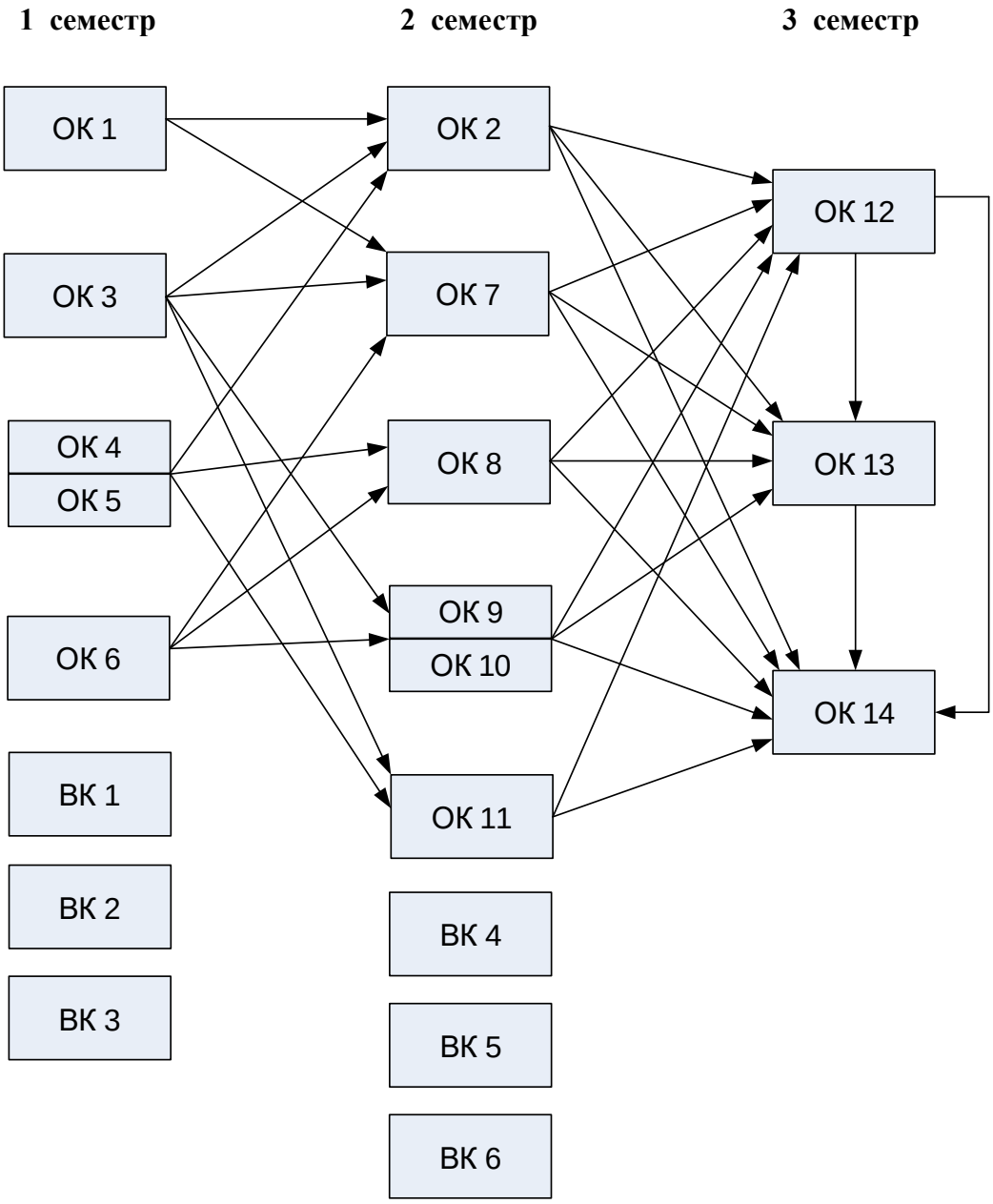
Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Семестр
1	2	3	4	5
Обов'язкові компоненти				
ОК1.	Ділова іноземна мова	3,5	Екзамен	1
ОК2.	Наукові комунікації у фаховій діяльності	3,5	Диферен-ційований залік	2
ОК3.	Методи побудови та аналізу криптосистем	3,5	Екзамен	1
ОК4.	Методологія прикладних досліджень у сфері кбербезпеки	2,5	Диферен-ційований залік	1
ОК5.	Курсовий проект з Методології прикладних досліджень у сфері кбербезпеки	1,5	Захист	1
ОК6.	Моделювання та оптимізація безпекових процесів авіаційної галузі	3,5	Екзамен	1
ОК7.	Безпека в кібернетичному просторі	3,5	Екзамен	2
ОК8.	Спеціальні вимірювання	6,0	Екзамен	2
ОК9.	Автоматизація обробки інформації з обмеженим доступом	6,0	Диферен-ційований залік	2
ОК10.	Курсова робота з Автоматизації обробки інформації з обмеженим доступом	1,0	Захист	2
ОК11.	Науково-дослідна практика у сфері систем технічного захисту інформації, автоматизації її обробки	4,5	Диферен-ційований залік	2
ОК12.	Переддипломна практика	6,0	Диферен-ційований залік	3
ОК13.	Єдиний державний кваліфікаційний іспит	3,0	Екзамен	3
ОК14.	Кваліфікаційна робота	18,0	Захист	3
Загальний обсяг обов'язкових компонент:		66 кредитів ЄКТС		
Вибіркові компоненти*				
ВК1.		4,0	Диферен-ційований залік	
ВК2.		4,0	Диферен-ційований залік	
ВК3.		4,0	Диферен-ційований залік	

1	2	3	4	5
ВК4.		4,0	Диферен-ційований залік	
ВК5.		4,0	Диферен-ційований залік	
ВК6.		4,0	Диферен-ційований залік	
Загальний обсяг вибіркових компонент*		24 кредити ЄКТС		
Загальний обсяг освітньо-професійної програми		90 кредитів ЄКТС		

* *Реалізація права здобувачів вищої освіти на вільний вибір навчальних дисциплін та створення індивідуальної освітньої траєкторії регламентується законом України «Про вищу освіту» та внутрішніми нормативними актами НАУ.*

Вибіркові компоненти обираються здобувачами вищої освіти із каталогів рекомендованих та альтернативних вибіркових дисциплін.

2.2. Структурно-логічна схема освітньо-професійної програми



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів ОС «Магістр» здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної магістерської роботи і завершується видачою документу встановленого зразку про присудження їм освітнього ступеня «Магістр» із присвоєнням освітньої кваліфікації: Магістр з кібербезпеки, за спеціальністю 125 «Кібербезпека».
Вимоги єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит повинен виявляти рівень засвоєння студентом навчального матеріалу, передбаченого навчальними програмами окремих дисциплін, та вміння випускника використовувати знання, набуті в процесі теоретичної підготовки, для вирішення професійних та соціально-виробничих завдань, з якими може зустрітись і які повинен уміти вирішувати майбутній фахівець під час своєї професійної діяльності, а також його підготовленість до продовження навчання за більш високими освітніми ступенями або в системі післядипломного навчання з урахуванням загальних вимог, передбачених стандартами вищої освіти.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота магістра повинна бути самостійною логічно завершеною теоретичною або експериментальною науково-дослідною роботою, пов'язаною з вирішенням актуальної науково-технічної або іншої проблеми у сфері Кібербезпеки. Кваліфікаційна робота магістра не повинна містити академічного плагіату, у тому числі некоректних текстових запозичень, фабрикації та фальсифікації. Кваліфікаційна робота має бути розміщена на сайті Університету або його структурного підрозділу, або у репозитарії.
Вимоги до публічного захисту (демонстрації)	Публічний захист кваліфікаційної магістерської роботи відбувається на засіданні екзаменаційної комісії. Порядок захисту передбачає представлення здобувача й поданих документів; виступ здобувача; відповіді здобувача на запитання членів екзаменаційної комісії та присутніх. Виступ здобувача має супроводжуватись презентацією.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компоненти / Компетентності	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6
ІК1	+	+	+	+	+	+	+	+	+	+	+	+	+	+						
ЗК1	+	+				+	+	+	+	+	+	+	+	+						
ЗК2	+	+	+	+	+	+	+	+	+	+	+	+	+	+						
ЗК3	+	+		+	+	+	+				+	+	+	+						
ЗК4	+	+		+	+	+	+	+			+	+	+	+						
ЗК5		+									+	+		+						
ФК1	+	+	+	+	+	+	+		+	+	+	+	+	+						
ФК2	+	+	+	+	+	+	+	+	+	+	+	+	+	+						
ФК3	+		+				+	+	+	+	+	+	+	+						
ФК4		+		+	+	+						+		+						
ФК5		+		+	+	+	+					+		+						
ФК6		+	+			+	+		+	+	+	+		+						
ФК7							+				+	+	+	+						
ФК8							+				+	+		+						
ФК9	+					+	+	+	+	+	+	+	+	+						
ФК10	+	+	+	+	+		+	+			+	+		+						
ФК11	+	+	+	+	+	+	+	+			+	+	+	+						
ФК12		+	+	+	+	+	+	+	+	+	+	+		+						

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньо-професійної програми

Компоненти / Програмні результати навчання	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6
ПРН1	+	+	+	+	+	+	+		+	+	+	+	+	+						
ПРН2	+	+	+	+	+	+	+	+	+	+	+	+	+	+						
ПРН3		+	+	+	+	+	+				+	+	+	+						
ПРН4						+	+		+	+	+	+	+	+						
ПРН5						+	+		+	+	+	+	+	+						
ПРН6						+	+	+	+	+	+	+	+	+						
ПРН7	+	+		+	+	+	+	+	+	+	+	+	+	+						
ПРН8			+	+	+		+		+	+	+	+	+	+						
ПРН9	+	+				+	+				+	+	+	+						
ПРН10		+	+								+	+	+	+						
ПРН11			+	+	+		+	+	+	+	+	+	+	+						
ПРН12	+			+	+	+	+		+	+	+	+	+	+						
ПРН13						+	+	+			+	+	+	+						
ПРН14	+	+	+	+	+	+	+	+	+	+	+	+	+	+						
ПРН15	+	+	+	+	+	+	+	+	+	+	+	+	+	+						
ПРН16	+	+	+	+	+	+	+	+	+	+	+	+	+	+						

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ пор.	Прізвище ім'я по-батькові	Підпис ознайомленої особи	Дата ознайом-лення	Примітки

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	Зміненого	Заміненого	Нового	Анульо-ваного			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				
Узгоджено				