(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО –ПРОФЕСІЙНА ПРОГРАМА

«Аудит кібербезпеки»
(найменування ОПП)

Першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека
(шифр та найменування спеціальності)
галузі знань 12 Інформаційні технології
(шифр та найменування галузі)
освітня кваліфікація: Бакалавр з кібербезпеки
(найменування кваліфікації)

СМЯ НАУ ОПП 14.01.04 – 01 – 2018

Затверджено Вченою радою
Голова Вченої ради
_____ В. Ісаєнко
(протокол № 5 від 26.06 2018р.)

Освітньо-професійна програма
вводиться в дію наказом ректора
Ректор
_____ В. Ісаєнко
(наказ № _____ від _____ 2018р.)

КИЇВ

ДІЄ ЯК ТИМЧАСОВА ДО ВВЕДЕННЯ СТАНДАРТУ ВИЩОЇ ОСВІТИ УКРАЇНИ

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

ПОГОДЖЕНО

Науково-методичною радою університету

протокол № 5

від "04" 06 2018 р

Проректор НАУ з навчальної роботи

Голова НМР НАУ

_____ (Гудманян А.Г.)

ПОГОДЖЕНО

Вченою радою Навчально-наукового інституту інформаційно-діагностичних систем

протокол № 5

від "22" травня 2018 р

Голова Вченої ради Навчально-наукового інституту інформаційно-діагностичних систем

_____ (Гумен М.Б.)

ПОГОДЖЕНО

Кафедрою засобів захисту інформації

протокол засідання № 5

від "05" березня 2018 р

Завідувач кафедри

_____ (Козловський В. В.)

ПОГОДЖЕНО

Науково-методично-редакційною радою

Навчально-наукового інституту інформаційно-діагностичних систем

протокол № 5

від "15" травня 2018 р

Голова НМР Навчально-наукового інституту інформаційно-діагностичних систем

_____ (Павленко П.М.)

ПЕРЕДМОВА

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ (спеціальності 125 Кібербезпека) у складі:

КЕРІВНИК РОБОЧОЇ ГРУПИ:

НІМЧЕНКО Т.В., к.т.н., доцент, доцент кафедри засобів захисту інформації Навчально-наукового інституту інформаційно-діагностичних систем _____
(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

КОЗЛОВСЬКИЙ В.В., д.т.н., проф., завідувач кафедри засобів захисту інформації Навчально-наукового інституту інформаційно-діагностичних систем _____
(підпис)

ШВЕЦЬ В.А., к.т.н., доцент, доцент кафедри засобів захисту інформації Навчально-наукового інституту інформаційно-діагностичних систем _____
(підпис)

ТЕМНІКОВ В.О., к.т.н., доцент, доцент кафедри засобів захисту інформації Навчально-наукового інституту інформаційно-діагностичних систем _____
(підпис)

ЛАЗАРЕНКО С.В., к.т.н., доцент, доцент кафедри засобів захисту інформації Навчально-наукового інституту інформаційно-діагностичних систем _____
(підпис)

Рецензент Оксіюк О.Г., завідувач кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, доктор технічних наук, професор.

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, Навчально-науковий інститут інформаційно-діагностичних систем Кафедра засобів захисту інформації
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр; Бакалавр з кібербезпеки.
1.3.	Офіційна назва освітньо-професійної програми	Освітньо-професійна програма Аудит кібербезпеки
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 4 роки
1.5.	Наявність акредитації	Акредитаційна комісія, Міністерство освіти і науки України, сертифікат серія НД №1193809 від 31.10.2017.
1.6.	Цикл/рівень	FQ-EHEA – перший цикл, НРК – 7 рівень
1.7.	Передумови	Повна загальна середня освіта
1.8.	Мова(и) викладання	Українська
1.9.	Термін дії освітньо-професійної програми	-
1.10	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://www.nau.edu.ua http://www.iids.nau.edu.ua
Розділ 2. Мета освітньо-професійної програми		
2.1.	Мета освітньої програми полягає в оволодінні студентами знаннями, вміннями та навичками використовувати і впроваджувати технології інформаційної та/або кібербезпеки	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань: 12 Інформаційні технології Спеціальність: 125 Кібербезпека
3.2.	Орієнтація освітньо-професійної програми	Освітньо-професійна, 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	Загальна вища освіта
3.4.	Особливості освітньо-професійної програми	Програма передбачає вивчення: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – теорії, моделей та принципів проведення аудиту об'єктів захисту; – методів та засобів проведення аудиту та

		сертифікації інформаційної та/або кібернетичної безпеки; – методів та засобів оцінки захищеності інформації; – методів оцінка ефективності системи аудиторського контролю у галузі управління операційною діяльністю та підтримкою ІТ; – встановлення рівня відповідності інформаційних систем визначеним критеріям стандартів аудиту кібербезпеки.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Випускники підготовлені до роботи за національним класифікатором України : - фахівець з питань безпеки підприємств, установ та організацій; -фахівець із організації інформаційної та/або кібернетичної безпеки; - фахівець з керування ризиками підприємств; - фахівець у галузі інформаційних технологій; - фахівець з безпеки інформаційних систем; - фахівець з інформаційних та операційних ризиків; - фахівець у галузі інформації та інформаційного аналізу; - фахівець з внутрішнього контролю та ІТ аудиту.
4.2.	Подальше навчання	Продовження навчання за програмою другого рівня вищої освіти (магістр).
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання	Лекції, лабораторні роботи, семінари, практичні заняття, проектна робота в командах, самостійна робота на основі підручників та конспектів, консультації з викладачами, виробнича та переддипломна практика на підприємствах, підготовка дипломної роботи.
5.2.	Оцінювання	Усні та письмові екзамени, лабораторні звіти, курсові роботи, презентації, поточний контроль, захист дипломного проекту.
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. ЗК2. Знання та розуміння предметної області та розуміння професії.

6.2.	Загальні компетентності (ЗК)	ЗК3. Здатність професійною спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК5. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК6. 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. ЗК7. 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. ЗК8. Здатність до критики й самокритики, креативність, адаптивність і комунікабельність, наполегливість у досягненні мети, толерантність. ЗК9. Здатність використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
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 в галузі інформаційної та/або кібербезпеки. ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ФК3. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК4. Здатність до планування та проведення аудиту інформаційної та/або кібербезпеки. ФК5. Здатність оцінювати захищеність інформації усіх видів, що циркулює на об'єктах інформаційної діяльності.

6.3.	Фахові компетентності (ФК)	ФК6. Здатність здійснювати розробку, впровадження та моніторинг системних і логічних засобів контролю інформаційної та/або кібербезпеки. ФК7. Здатність визначати інформаційні і технічні ресурси, а також об'єкти інформаційної діяльності, які підлягают захисту. ФК8. Здатність здійснювати процедури управління ризиками та інцидентами інформаційних технологій, проводити розслідування, надавати їм оцінку. ФК9. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). ФК10. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. ФК11. Здатність застосовувати методи та засоби організаційного напрямку, щодо захисту інформації на об'єктах інформаційної діяльності. ФК12. Здатність здійснювати обстеження, облік та атестацію об'єктів інформаційної діяльності. ФК13. Здатність використовувати теоретичні знання та практичні навички з підготовки аудиторської звітності. ФК14. Здатність використовувати теоретичні знання та практичні навички з підготовки технічної документації, брати участь у підборі та розстановці персоналу і розробленні для нього посадових обов'язків.
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 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

7.1.	Програмні результати навчання (ПРН)	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 суб'єктів та об'єктів інформаційної діяльності, корпоративної архітектури, периметру безпеки (контрольованої зони), політики безпеки, привілеїв. ПРН3. Здатність продемонструвати знання та вміння з організації, планування та проведення аудиту інформаційної та/або кібербезпеки. ПРН4. Здатність продемонструвати знання та вміння управління ризиками в інформаційних системах; забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів. ПРН5. 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. ПРН6. Організовувати контроль за станом захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності. ПРН7. 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 та\або кібербезпеки; ПРН8. 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 та/або кібербезпеки для збору доказів і проведення розслідування інцидентів порушення безпеки інформації. ПРН9. Здатність здійснювати оцінювання захищеності інформації усіх видів, що циркулює на об'єкті інформаційної діяльності. ПРН10. Здатність забезпечення функціонування системи моніторингу управління доступом до

7.1.	Програмні результати навчання (ПРН)	інформації на об'єктах інформаційної діяльності і процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем в умовах реалізації кіберзагроз різних класів та протидії порушникам. ПРН11. Здатність продемонструвати знання та розуміння основ побудови систем захисту інформації на об'єктах інформаційної діяльності та описати в загальних поняттях і термінах архітектуру, характеристики та принципи їх дії. ПРН12. Здатність проводити атестацію об'єктів інформаційної діяльності (спираючись на облік та обстеження територій, зон, приміщень) в умовах додержання встановленої політики безпеки із фіксуванням результатів у відповідних документах. ПРН13. Здатність продемонструвати знання та розуміння сучасних методів і моделей інформаційної та/або кібербезпеки. ПРН14. Здатність продемонструвати знання та розуміння захисту інформації на об'єктах інформаційної діяльності та обґрунтовано обирати і застосовувати на практиці методи виявлення інформаційних/кібернетичних загроз; методи протидії спробам несанкціонованого доступу до інформаційних ресурсів; організаційні та адміністративні заходи підвищення рівня інформаційної та/або кібербезпеки. ПРН15. Здатність продемонструвати знання та навички складання аудиторської звітності та технічної документації. ПРН16. Оволодіння навичками працювати самостійно при виконанні курсових робіт, курсових проектів, дипломних робіт. ПРН17. Здатність володіння англійською мовою, використовувати спеціальну термінологію для проведення літературного пошуку.
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	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	Навчальні приміщення, комп'ютерні робочі місця, мультимедійні класи дозволяють повністю забезпечити освітній процес протягом усього циклу підготовки за освітньою програмою.
8.3	Інформаційне та навчально-методичне забезпечення	Офіційний веб-сайт www.nau.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Матеріали навчально-методичного забезпечення освітньої програми викладені в репозитарії НАУ за посиланням: http://er.nau.edu.ua/handle/NAU/9190 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	Двосторонні договори між Національним авіаційним університетом та Технічним університетом України (КПІ) та 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 ОПП

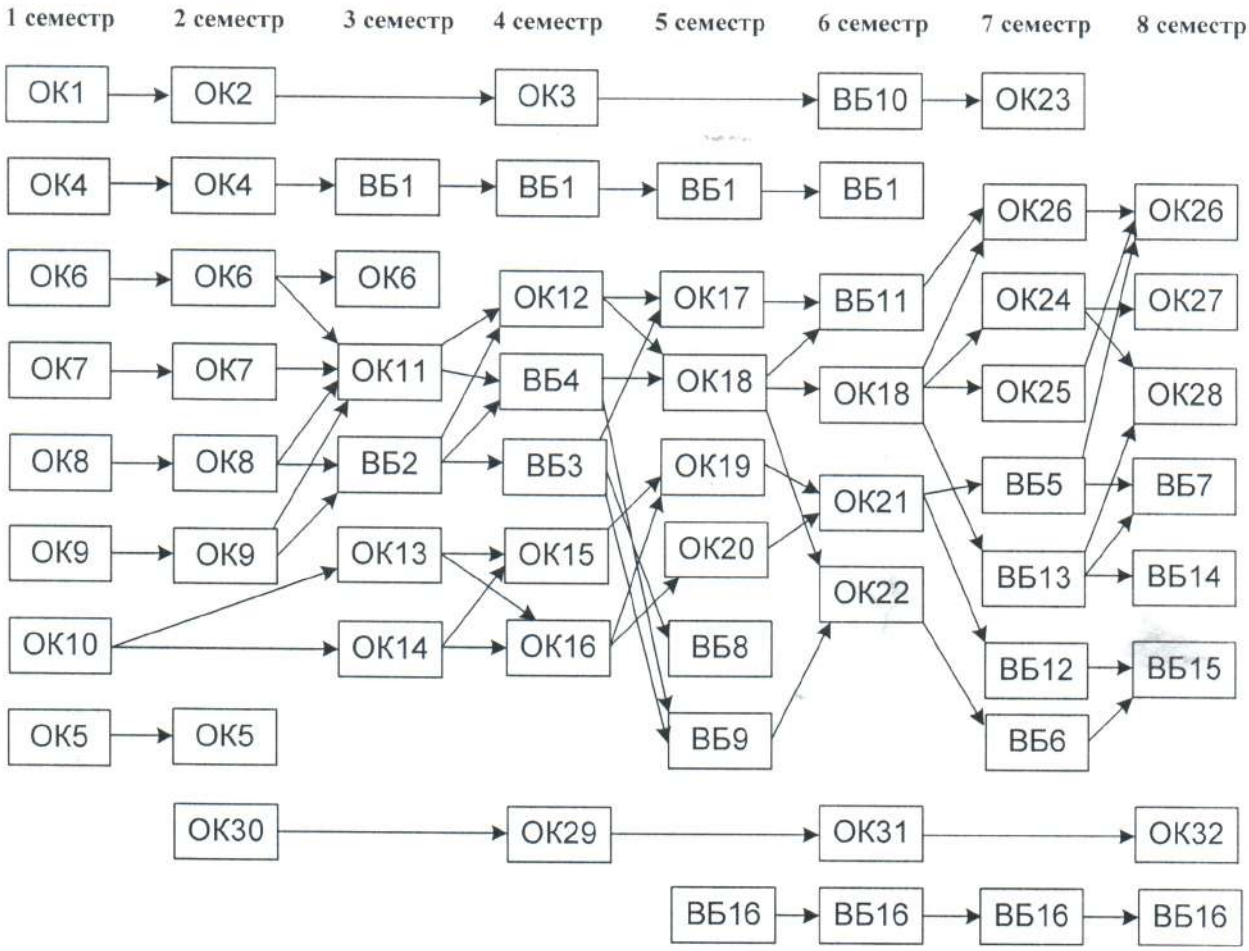
Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОПП			
ОК1.	Українська мова	3.0	Екзамен
ОК2.	Історія та культура України	3.0	Екзамен
ОК3.	Філософія	3.0	Екзамен
ОК4.	Іноземна мова	4.0	Екзамен, Диференційований залік
ОК5.	Фізичне виховання	3.0	Диференційований залік
ОК6.	Вища математика	17	Екзамен, Диференційований залік
ОК7.	Фізика	10.0	Диференційований залік
ОК8.	Інформаційні технології + КР (курсова робота)	12.5	Екзамен
ОК9.	Комп'ютерна графіка	6.0	Екзамен, Диференційований залік
ОК10.	Основи інформаційної безпеки держави	4.0	Екзамен
ОК11.	Операційні системи + КР (курсова робота)	7.0	Екзамен
ОК12.	Бази данних	5.5	Екзамен
ОК13.	Політики, стандарти і процедури інформаційної безпеки + КР (курсова робота)	5.0	Екзамен
ОК14.	Стандарти аудиту інформаційних технологій	4.5	Екзамен
ОК15.	Оцінка ризиків інформаційних технологій	5.0	Екзамен
ОК16.	Стратегія аудиту інформаційних технологій	5.0	Екзамен
ОК17.	Кіберзагрози та уразливості інформаційних систем + КР (курсова робота)	5.0	Екзамен
ОК18.	Захист інформації + КП (курсовий проект)	13.0	Екзамен
ОК19.	Планування аудиту кібербезпеки	4.5	Екзамен
ОК20.	Аудиторська звітність	4.5	Диференційований залік

1	2	3	4
ОК21.	Технології збору та аналізу даних аудиту	4.0	Диференційований залік
ОК22.	Доступ до об'єктів інформаційної діяльності	6.0	Екзамен
ОК23.	Основи охорони праці	3.0	Диференційований залік
ОК24.	Управління ризиками в інформаційних системах	3.0	Диференційований залік
ОК25.	Процеси зберігання, вилучення, транспортування та утилізації інформаційних ресурсів	5.0	Екзамен
ОК26.	Розробка, впровадження та моніторинг системних і логічних засобів контролю безпеки + КП (курсовий проект)	10.0	Екзамен
ОК27.	Кібербезпека хмарних технологій + КР (курсова робота)	3.5	Диференційований залік
ОК28.	Управління інцидентами кібербезпеки	3.0	Диференційований залік
ОК29.	Фахово-ознайомлювальна практика	3.0	Диференційований залік
ОК30.	Комп'ютерна практика	3.0	Диференційований залік
ОК31.	Технологічна практика	4.5	Диференційований залік
ОК32.	Дипломне проектування	7.5	Захист
Загальний обсяг обов'язкових компонент:		180 кредитів	
Вибіркові компоненти ОПП			
ВБ1.	Іноземна мова (за професійним спрямуванням)	8.0	Диференційований залік
ВБ2.	Інформаційні системи	4.0	Диференційований залік
ВБ3.	Комп'ютерні мережі	4.0	Диференційований залік
ВБ4.	Апаратне забезпечення інформаційних систем	3.5	Диференційований залік
ВБ5.	Експертні методи дослідження	4.0	Диференційований залік
ВБ6.	Кіберкриміналістика	4.0	Диференційований залік
ВБ7.	Кризовий менеджмент	3.5	Екзамен
ВБ8.	Економіка інформаційної безпеки*	3.5	Диференційований залік
ВБ9.	Системи платіжної та банківської безпеки*	3.5	Диференційований залік
ВБ10.	Управління персоналом та соціотехніка*	3.0	Диференційований залік

1	2	3	4
ВБ11.	Комплексні системи захисту інформації*	4.5	Екзамен
ВБ12.	Аналітична обробка даних*	3.5	Диференційований залік
ВБ13.	Управління проектами*	3.5	Диференційований залік
ВБ14.	Якість та тестування ПЗ*	3.0	Екзамен
ВБ15.	Системи штучного інтелекту*	4.5	Диференційований залік
ВБ16.	Військова підготовка	29.0	Екзамен, Диференційований залік
Загальний обсяг вибіркових компонент		60 кредитів	
Загальний обсяг освітньо-професійної програми		240 кредитів	

* - дисципліни альтернативні військовій підготовці

2.2. Структурно-логічна схема ОПП



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньо-професійної програми проводиться у формі захисту дипломної роботи та завершується видачею документу встановленого зразка про присудження йому освітнього ступеня бакалавра із присвоєнням освітньої кваліфікації: Бакалавр з кібербезпеки за спеціальністю 125 Кібербезпека.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної 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	ВБ 1	ВБ 2	ВБ 3	ВБ 4	ВБ 5	ВБ 6	ВБ 7	ВБ 8	ВБ 9	ВБ 10	ВБ 11	ВБ 12	ВБ 13	ВБ 14	ВБ 15
ІК1										+			+	+	+		+	+						+		+	+	+	+	+	+	+				+	+	+					+	+	+		+
ЗК1						+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			+	+	+	+	+	+		+	+	+	+	+	+		+	+	+	+		+	+	+
ЗК2								+		+			+	+	+	+	+	+	+					+			+	+								+	+	+			+		+				+
ЗК3	+			+																												+												+			
ЗК4											+		+	+	+	+	+	+	+				+	+			+	+	+	+	+	+		+	+	+	+	+	+					+			+	+
ЗК5	+			+				+					+	+							+				+								+	+	+								+			+
ЗК6	+									+			+	+																							+	+				+					
ЗК7	+	+	+					+		+			+	+			+	+						+			+	+										+				+					
ЗК8			+																																							+			+		
ЗК9					+																																											
ФК1	+			+									+	+	+																		+				+	+	+								
ФК2						+	+	+		+	+	+									+				+		+		+	+	+	+		+	+										+	+
ФК3								+		+			+	+	+	+	+	+	+				+	+			+	+										+	+	+	+	+	+	+				+
ФК4								+	+				+	+	+	+	+	+	+	+	+			+			+	+										+	+	+	+	+		+				+
ФК5								+		+			+	+	+	+	+	+				+		+			+	+	+	+	+	+						+	+					+				+
ФК6						+	+	+	+	+	+	+						+			+	+			+	+							+										+	+		+	+
ФК7								+		+	+	+	+	+	+		+	+			+	+					+		+	+	+	+		+	+								+	+			+
ФК8							+	+		+			+	+	+		+				+			+				+						+	+								+	+			
ФК9									+	+			+	+	+		+	+				+														+								+	+		+	
ФК10										+			+	+	+		+				+	+					+		+	+	+	+		+	+	+								+		+	+
ФК11										+			+	+	+		+	+				+															+							+	+			
ФК12									+				+	+				+					+						+	+	+	+											+				
ФК13													+	+					+	+	+								+	+	+	+				+								+				
ФК14									+	+			+	+				+																			+									+		+		

Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньо-професійної 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	ВБ 1	ВБ 2	ВБ 3	ВБ 4	ВБ 5	ВБ 6	ВБ 7	ВБ 8	ВБ 9	ВБ 10	ВБ 11	ВБ 12	ВБ 13	ВБ 14	ВБ 15
ПРН1	+			+						+			+	+				+	+					+			+					+				+	+					+				+
ПРН2						+	+	+	+		+	+									+			+				+	+	+	+		+	+	+								+			
ПРН3	+			+		+				+			+	+	+	+	+		+	+	+			+		+		+	+	+	+	+	+	+	+	+							+	+	+	
ПРН4						+		+		+	+	+			+		+							+	+	+	+	+						+	+								+	+	+	
ПРН5	+									+			+					+				+							+	+	+	+										+	+				
ПРН6								+		+			+				+	+				+	+				+		+	+	+	+										+	+	+			+
ПРН7						+	+	+	+	+	+		+				+	+				+	+						+	+	+	+		+	+	+							+	+			+	
ПРН8	+			+				+		+	+	+	+	+	+		+	+						+			+					+	+	+	+	+	+			+		+	+				
ПРН9							+	+		+			+				+	+				+					+		+	+	+	+										+	+	+			+
ПРН10								+		+			+				+	+				+							+	+	+	+		+	+	+							+	+	+	+	+	
ПРН11								+		+			+		+		+	+				+					+							+	+	+	+			+		+	+			+	
ПРН12									+	+			+				+	+				+	+						+	+	+	+					+					+	+	+		
ПРН13							+	+		+	+	+	+	+	+	+	+	+	+		+			+			+	+	+	+	+	+		+	+	+	+	+	+	+	+		+	+	+	+	+
ПРН14								+		+			+	+	+	+	+	+	+		+	+		+	+	+	+	+								+	+	+	+	+	+	+	+		+	+
ПРН15	+								+	+			+	+		+		+	+	+	+	+							+	+	+	+										+	+	+			
ПРН16	+			+				+	+	+	+	+	+	+	+		+	+											+	+	+	+	+	+	+	+				+		+	+	+	+	
ПРН17	+			+				+		+			+	+				+									+					+							+	+	+		+	+			+

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки
1		09.07.18	Кожокевич І.П.		

(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				