(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО –ПРОФЕСІЙНА ПРОГРАМА

«Управління інформаційною безпекою»
(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 освітньої кваліфікації)

СМЯ НАУ ОПП 14.01.05 – 01 – 2019

Затверджено Вченою радою
Голова Вченої ради
_____ В.Ісаєнко
(протокол №____від_____2019 р.)

Освітньо-професійна програма
вводиться в дію наказом ректора
Ректор
_____ В.Ісаєнко
(наказ №____від_____2019 р.)

КИЇВ

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

ПОГОДЖЕНО

Науково-методичною радою університету

протокол №_____

від "_____"_____2019 р

Проректор НАУ з навчальної роботи

Голова НМР НАУ

_____(Гудманян А.Г.)

ПОГОДЖЕНО

Вченою радою Навчально-наукового інституту інформаційно-діагностичних систем

протокол №_____

від "_____"_____2019 р

Голова Вченої ради Навчально-наукового інституту Інформаційно-діагностичних систем

_____(Гумен М.Б.)

ПОГОДЖЕНО

Кафедрою безпеки інформаційних технологій

протокол засідання №_____

від "_____"_____2019 р

Завідувач кафедри

_____(Корченко О.Г.)

ПОГОДЖЕНО

Науково-методично-редакційною радою Навчально-наукового інституту інформаційно-діагностичних систем

протокол №_____

від "_____"_____2019 р

Заступник голови НМР Навчально-наукового інституту Інформаційно-діагностичних систем

_____(Квасніков В.П.)

ПЕРЕДМОВА

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ (спеціальності 125 Кібербезпека, Управління інформаційною безпекою) у складі:

КЕРІВНИК РОБОЧОЇ ГРУПИ:

ХОХЛАЧОВА Ю.Є., к.т.н., доц., доцент кафедри безпеки інформаційних технологій _____

(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

ЗАРІЦЬКИЙ О.В., д.т.н., доцент кафедри безпеки інформаційних технологій _____

(підпис)

КОРЧЕНКО А.О., к.т.н., доц., доцент кафедри безпеки інформаційних технологій _____

(підпис)

ІВАНЧЕНКО І.С., к.т.н., доцент кафедри безпеки інформаційних технологій _____

(підпис)

Рецензент Хлапонін Ю.І., завідувач кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури, 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 безпеки інформаційних технологій
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр з кібербезпеки
1.3.	Офіційна назва освітньо-професійної програми	Управління інформаційною безпекою
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
1.5.	Наявність акредитації	Акредитовано, сертифікат про акредитацію НД 1193809 від 31 жовтня 2017 року
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 липня 2027 р.
1.10	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://www.nau.edu.ua http://www.iids.nau.edu.ua http://www.bit.nau.edu.ua
Розділ 2. Мета освітньо-професійної програми		
2.1.	Мета освітньої програми полягає в оволодінні студентами знаннями, вміннями та навичками розробляти і впроваджувати системи управління інформаційною безпекою	
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 загально-відомих наукових в практичних результатах в галузі інформаційної безпеки, у рамках яких можлива подальша професійна кар'єра і подальше навчання.
3.3.	Основний фокус освітньо-професійної програми та спеціалізації	Загальна вища освіта першого (бакалаврського) рівня спеціальності 125 Кібербезпека
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; – принципів впровадження і супроводу систем управління інформаційною безпекою; – теорії, моделей та принципів управління доступом до інформаційних ресурсів;

		– теорії систем управління інформаційною безпекою; – методів та засобів виявлення, управління та ідентифікації ризиків та інцидентів інформаційної безпеки; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів і засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих засобів проектування систем управління інформаційною безпекою.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Випускники підготовлені до роботи за національним класифікатором України : -фахівець із організації інформаційної безпеки; -фахівець із організації захисту інформації з обмеженим доступом; -фахівець з режиму секретності ; -фахівець з розробки та тестування програмного забезпечення; -фахівець з розроблення комп'ютерних програм; -фахівець з інформаційних технологій; -інспектор з організації захисту секретної інформації.
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 кваліфікаційної роботи.
5.2.	Оцінювання	Усні та письмові екзамени, лабораторні звіти, курсові роботи, презентації, поточний контроль, кваліфікаційний екзамен, захист кваліфікаційної роботи.
Розділ 6. Програмні компетентності		
6.1.	Інтегральні компетентності	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі інформаційної безпеки.
6.2.	Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та

		розуміння професії. ЗК3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК4. Здатність до пошуку, оброблення та аналізу інформації. ЗК5. 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. ЗК6. 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, стандарти і рекомендовані практики з метою здійснення професійної діяльності в галузі інформаційної безпеки. ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. ФК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК4. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики інформаційної безпеки підприємства. ФК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-комунікаційних системах з метою реалізації інформаційної безпеки підприємства. ФК6. Здатність відновлювати штатне функціонування інформаційно-комунікаційних систем після реалізації кіберзагроз, здійснення кібератак, збоїв та відмов різних класів і походження. ФК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації. ФК8. Здатність здійснювати процедури управління інцидентами інформаційної безпеки, проводити розслідування, надавати їм оцінку. ФК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою. ФК10. Здатність застосовувати методи та засоби криптографічного і технічного захисту

		інформації. ФК11. Здатність виконувати моніторинг процесів функціонування інформаційно-комунікаційних систем згідно встановленої політики інформаційної безпеки підприємства. ФК12. Здатність аналізувати, виявляти та оцінювати можливі кіберзагрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам підприємства (галузі, регіону, держави). ФК13. Здатність застосовувати методи теорії інформації та кодування, обробки та захисту інформації при наявності завад в каналах передачі даних. ФК14. Здатність застосовувати теоретичні знання та практичні навички із побудови, керування, модернізації, моніторингу та аналізу продуктивності сучасних інформаційно-комунікаційних систем. ФК15. Здатність застосовувати теоретичні знання та практичні навички з організації та функціонування сучасних операційних систем, уміння зі створення та використання ефективного програмного забезпечення для керування обчислювальними ресурсами в багато користувальницьких операційних системах. ФК16. Здатність застосовувати методи та засоби організаційного характеру для побудови системи управління інформаційною безпекою. ФК17. Здатність застосовувати методи та засоби стеганографічного захисту інформації.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання	ПРН1. Розв’язувати задачі інформаційної безпеки за рахунок використання сучасних методів і засобів криптографічного захисту інформації. ПРН2. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня інформаційної безпеки. ПРН3. Визначати відомості, які відносяться до різних видів конфіденційної інформації, організовувати допуск та доступ персоналу до конфіденційної інформації згідно встановленої політики інформаційної безпеки підприємства. ПРН4. Організовувати внутрішньо об’єктовий та пропускний режими на підприємстві. ПРН5. Організовувати контроль за станом безпеки конфіденційної інформації на підприємстві згідно відповідної політики безпеки.

		ПРН6. Здатність продемонструвати знання та розуміння архітектури комп'ютерів та описати в загальних поняттях і термінах структуру комп'ютера та його апаратних компонентів, принципів їх взаємодії; систему команд; протоколи за засоби обміну даними; систему переривань; методику проектування арифметичних та управляючих пристроїв; засоби підвищення продуктивності та надійності цифрової обчислювальної техніки. ПРН7. Здатність продемонструвати знання та розуміння основ побудови систем управління інформаційною безпекою та описати в загальних поняттях і термінах архітектуру, характеристики та принципи їх дії. ПРН8. Здатність продемонструвати знання та розуміння основ побудови комп'ютерних мереж та описати в загальних поняттях і термінах принципи та методи організації мережевих комунікацій; архітектуру та функціонування локальних, комбінованих і глобальних комп'ютерних мереж; систему мережевих стандартів, способи адресації та протоколи маршрутизації; інтерфейси та методи доступу до передавального середовища. ПРН9. Здатність продемонструвати знання та розуміння організації баз даних та розробляти проекти баз даних інформаційних систем, використовуючи сучасні методи і моделі інформаційної безпеки. ПРН10. Здатність продемонструвати знання та розуміння системного програмування та розробляти системні програми, алгоритми обробки різних типів даних та тестування програмного забезпечення. ПРН11. Реалізовувати основи системного підходу, критерії ефективної організації обчислювального процесу для постановки та рішення завдань організації оптимального і безпечного функціонування обчислювальних систем. ПРН12. Вибирати, обґрунтовуючи свій вибір, оптимальні алгоритми керування ресурсами, порівнювати та оцінювати різні методи, що лежать в основі планування і диспетчеризації процесів. ПРН13. Здатність продемонструвати знання та розуміння системного програмного забезпечення та описати в загальних поняттях і термінах процеси функціонування операційних систем та їх складових частин, сучасних

		операційних середовищ та систем програмування, засоби та технології їх експлуатації та адміністрування. ПРН14. Здатність продемонструвати знання та розуміння технологій проектування комп'ютерних систем інформаційної безпеки та виконувати системне, операційне, функціонально-логічне і технічне проектування комп'ютерних пристроїв, використовуючи сучасні засоби автоматизованого проектування. ПРН15. Здатність продемонструвати знання та розуміння діагностування та експлуатації систем інформаційної безпеки та застосовувати на практиці засоби автоматичного контролю і діагностування . ПРН16. Здатність продемонструвати знання та розуміння сучасних методів і моделей інформаційної безпеки. ПРН17. Здатність продемонструвати знання та розуміння інженерії програмного забезпечення та описати в загальних поняттях і термінах процеси, методи і засоби автоматизації проектування, виробництва, випробувань та оцінки якості програмних продуктів; методи організації колективної розробки програмного забезпечення інформаційних систем; мовні засоби і специфікації інтерфейсів об'єктів програмування. ПРН18. Здатність продемонструвати знання та розуміння застосовування методів і засобів криптографічного та технічного захисту інформації. ПРН19. Здатність продемонструвати знання та розуміння професійної діяльності на основі впровадженої системи управління інформаційною безпекою. ПРН20. Здатність продемонструвати знання і розуміння інформаційної безпеки та обґрунтовано обирати і застосовувати на практиці методи виявлення інформаційних загроз; програмні та програмно-апаратні засоби захисту даних та операційних систем; методи протидії спробам несанкціонованого доступу до інформаційних ресурсів; організаційні та адміністративні заходи підвищення рівня інформаційної безпеки. ПРН21. Оволодіння навичками працювати самостійно при виконанні курсових робіт, курсових проектів, дипломних робіт. ПРН22. Здатність володіння англійською мовою, використовувати спеціальну терміно-

		логію 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. У 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/14303 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	У рамках двосторонніх договорів між Національним авіаційним університетом та вітчизняними закладами вищої освіти.
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

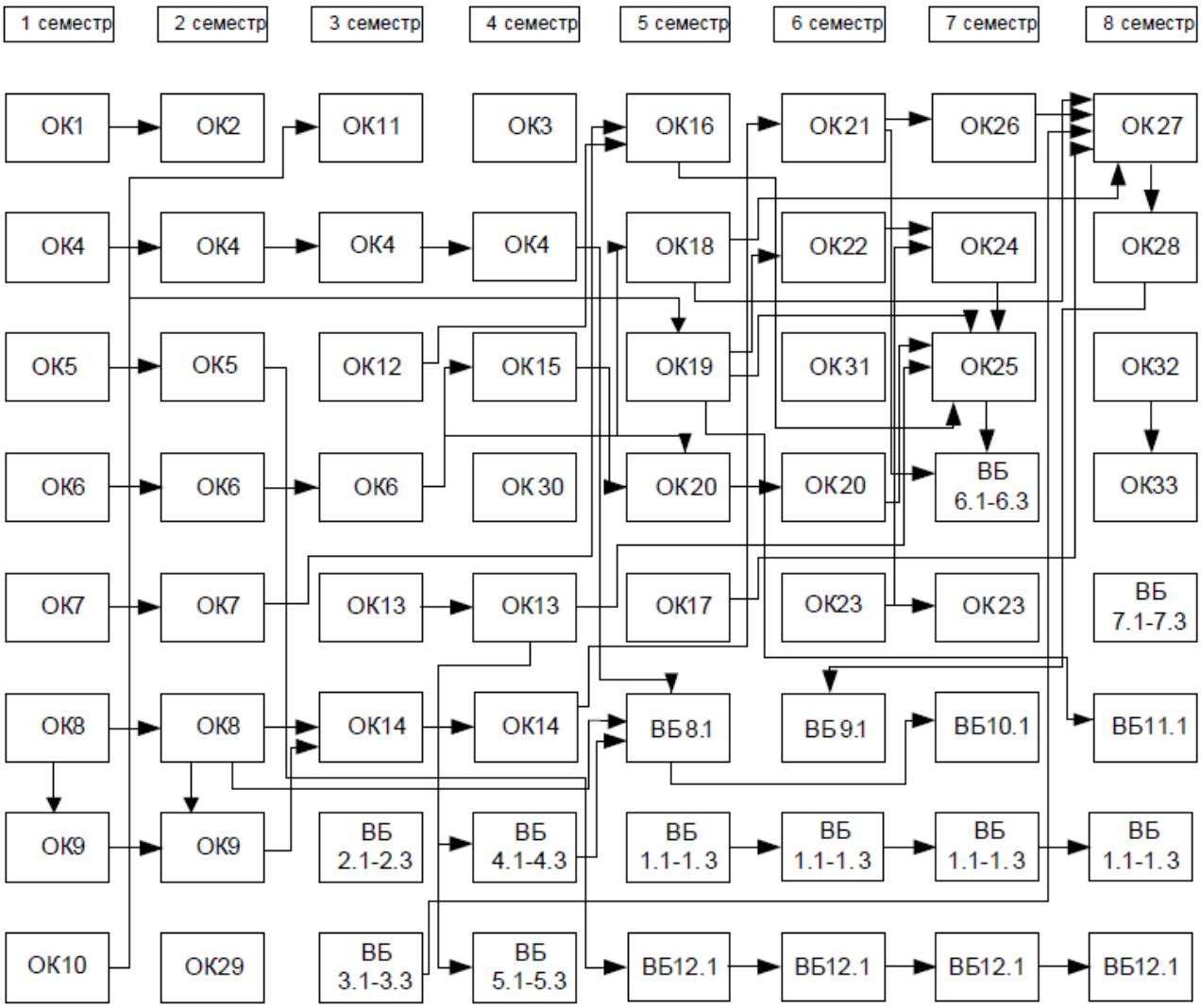
2.1. Перелік компонент ОПП

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.	Історія української державності та культури	3.0	Екзамен
ОК2.	Ділова українська мова	3.0	Екзамен
ОК3.	Філософія сучасного суспільства	3.0	Екзамен
ОК4.	Фахова іноземна мова	4.0	Екзамен Диференційований залік
ОК5.	Фізичне виховання	3.0	Диференційований залік
ОК6.	Вища математика	18.0	Екзамен Диференційований залік
ОК7.	Фізика	10.0	Диференційований залік
ОК8.	Інформаційні технології та основи програмування	12.0	Екзамен
ОК9.	Комп'ютерна графіка	5.5	Екзамен Диференційований залік
ОК10.	Основи інформаційної безпеки держави	4.0	Екзамен
ОК11.	Інформаційно-психологічні впливи у кіберпросторі	4.0	Диференційований залік
ОК12.	Стандарти інформаційної безпеки	3.5	Диференційований залік
ОК13.	Захищені комп'ютерні системи та мережі	8.5	Екзамен Диференційований залік
ОК14.	Технології програмування	8.5	Екзамен Диференційований залік
ОК15.	Дискретна математика	5.0	Екзамен
ОК16.	Технічні засоби охорони об'єктів критичної інфраструктури	4.0	Диференційований залік
ОК17.	Основи системного аналізу	4.0	Екзамен
ОК18.	Оцінка та управління ризиками	5.0	Екзамен

ОК19.	Управління ресурсами інформаційних систем	4.0	Диференційований залік
ОК20.	Криптографія та криптоаналіз	9.5	Екзамен
ОК21.	Операційні системи та системне програмне забезпечення	5.0	Диференційований залік
ОК22.	Технології штучного інтелекту	4.0	Екзамен
ОК23.	Тестування безпеки інформаційних систем	9.5	Екзамен
ОК24.	Технології виявлення уразливостей інформаційних систем	4.5	Диференційований залік
ОК25.	Комплексні системи захисту інформації	5.5	Екзамен
ОК26.	Інформаційне забезпечення управлінської діяльності	4.5	Екзамен
ОК27.	Системи управління інформаційною безпекою	3.5	Екзамен
ОК28.	Інцидент-менеджмент у кіберпросторі	4.0	Екзамен
ОК29.	Фахова ознайомлювальна практика	3.0	Диференційований залік
ОК30.	Навчальний комп'ютерний практикум	3.0	Диференційований залік
ОК31.	Технологічна практика	3.0	Диференційований залік
ОК32.	Переддипломна практика	3.0	Диференційований залік
ОК32	Кваліфікаційна робота	7.5	Захист
Загальний обсяг обов'язкових компонент:		180 кредитів	
Вибіркові компоненти ОПП			
ВБ 1.1.	Іноземна мова (за професійним спрямуванням)	4.0	Екзамен Диференційований залік
ВБ 1.2.	Іноземна мова спеціальності	4.0	Екзамен Диференційований залік
ВБ 1.3.	Іноземна мова ділової комунікації	4.0	Екзамен Диференційований залік
ВБ 2.1.	Архітектура апаратного забезпечення комп’ютера	5.0	Екзамен
ВБ 2.2.	Апаратна і логічна схема комп’ютера	5.0	Екзамен
ВБ 2.3.	Соціологія	5.0	Екзамен
ВБ 3.1.	Організація секретного діловодства	3.0	Диференційований залік
ВБ 3.2.	Особливості організації конфіденційного діловодства	3.0	Диференційований залік
ВБ 3.3.	Психологія професійної діяльності	3.0	Диференційований залік
ВБ 4.1.	Бази даних та знань	4.0	Диференційований залік

ВБ 4.2.	Бази даних та основи SQL	4.0	Диференційований залік
ВБ 4.3.	Технології створення баз даних	4.0	Диференційований залік
ВБ 5.1.	Сучасні системи розмежування доступу	4.5	Екзамен
ВБ 5.2.	Технології розмежування доступу для захисту даних в комп‘ютерних системах;	4.5	Екзамен
ВБ 5.3.	Системи контролю и керування доступом	4.5	Екзамен
ВБ 6.1.	Програмні засоби захисту інформації	3.0	Диференційований залік
ВБ 6.2.	Програмне забезпечення систем захисту інформації	3.0	Диференційований залік
ВБ 6.3.	Основи охорони праці	3.0	Диференційований залік
ВБ 7.1.	Економічна безпека діяльності підприємств	3.5	Диференційований залік
ВБ 7.2.	Економіка інформаційної безпеки	3.5	Диференційований залік
ВБ 7.3.	Економіка в галузі інформаційної безпеки	3.5	Диференційований залік
ВБ 8.1.	Спеціальне системне програмне забезпечення *	7.0	Диференційований залік
ВБ 9.1.	Інтернет-технології *	7.5	Екзамен
ВБ 10.1.	Захищені мережеві протоколи *	7.0	Диференційований залік
ВБ 11.1.	Цифрова криміналістика *	7.5	Екзамен
ВБ 12.1.	Військова підготовка	29.0	Екзамен Диференційований залік
Загальний обсяг вибіркових компонент		60 кредитів	
Загальний обсяг освітньо-професійної програми		240 кредитів	

2.2. Структурно-логічна схема ОПП



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньо-професійної програми проводиться у формі захисту кваліфікаційної роботи та завершується видачею документу встановленого зразка про присудження йому освітнього ступеня бакалавра із присвоєнням освітньої кваліфікації: Бакалавр з кібербезеки.

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	ОК33	ВБ1	ВБ2	ВБ3	ВБ4	ВБ5	ВБ6	ВБ7	ВБ8	ВБ9	ВБ10	ВБ11	ВБ12
ЗК1		+		+	+	+	+	+	+				+	+	+	+		+		+	+			+	+		+	+	+	+	+	+	+						+	+			+	+	+
ЗК2										+	+		+							+	+			+	+		+	+		+	+	+	+		+						+	+		
ЗК3	+	+		+																												+	+												
ЗК4	+		+			+					+				+										+				+	+	+	+	+				+					+				
ЗК5	+											+																																		+
ЗК6					+																																									+
ФК1										+	+	+						+							+		+	+				+				+								
ФК2								+					+						+		+			+	+		+			+	+	+	+								+			
ФК3								+					+	+		+			+		+			+	+	+	+	+		+	+		+		+		+	+	+		+		+		
ФК4										+											+						+	+			+		+											
ФК5													+	+								+			+		+			+	+	+						+						
ФК6																		+	+						+		+	+			+									+					
ФК7																			+						+		+				+						+								
ФК8																												+																	
ФК9																										+	+																		
ФК10																+				+																	+			+						
ФК11																						+	+	+			+																		
ФК12										+	+							+				+	+	+				+				+								+			+		
ФК13													+			+				+											+		+			+									
ФК14													+				+															+	+				+					+	+		
ФК15								+					+							+						+							+				+			+				
ФК16										+															+		+	+			+	+	+											
ФК17																				+													+												

5. 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	ОК33	ВБ1	ВБ2	ВБ3	ВБ4	ВБ5	ВБ6	ВБ7	ВБ8	ВБ9	ВБ10	ВБ11	ВБ12
ПРН1																				+																											
ПРН2						+									+					+																											
ПРН3										+		+													+		+									+									
ПРН4																									+												+									
ПРН5									+																+											+									
ПРН6									+								+				+																+									
ПРН7													+				+					+															+			+						
ПРН8													+				+																					+					+	+		
ПРН9								+											+																			+								
ПРН10								+						+					+		+																		+		+				
ПРН11																	+								+																				
ПРН12								+						+					+		+					+													+						
ПРН13														+							+																				+				
ПРН14													+												+																				
ПРН15																									+		+																		
ПРН16										+	+							+					+	+	+		+																	
ПРН17								+						+							+	+																	+		+				
ПРН18						+									+					+																										
ПРН19																									+	+	+		+	+	+	+													
ПРН20											+		+								+		+	+	+			+													+			+	
ПРН21								+						+						+				+	+		+				+	+			+									
ПРН22				+																														+												

(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				