(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО –ПРОФЕСІЙНА ПРОГРАМА

«Адміністративний менеджмент у сфері захисту інформації»
(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 14.01.05 – 01 – 2018

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

Освітньо-професійна програма
вводиться в дію наказом ректора
Ректор
_____ В.Ісаєнко
(наказ №____від_____2018 р.)

КИЇВ

ДІЄ ЯК ТИМЧАСОВА ДО ВВЕДЕННЯ СТАНДАРТУ ВИЩОЇ ОСВІТИ УКРАЇНИ

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

ПОГОДЖЕНО
Науково-методичною радою університету
протокол № 5
від "07" 02 2018 р
Проректор НАУ з навчальної роботи
Голова НМР НАУ
_____(Гудманян А.Г.)

ПОГОДЖЕНО
Вченою радою Навчально-наукового інституту інформаційно-діагностичних систем
протокол № 3
від "13" 03 2018 р
Голова Вченої ради Навчально-наукового інституту Інформаційно-діагностичних систем
_____(Гумен М.Б.)

ПОГОДЖЕНО
Кафедрою безпеки інформаційних технологій
протокол засідання № 2
від "19" 02 2018 р
Завідувач кафедри
_____(Корченко О.Г.)

ПОГОДЖЕНО
Науково-методично-редакційною радою Навчально-наукового інституту інформаційно-діагностичних систем
протокол № 2
від "20" 02 2018 р
Голова НМР Навчально-наукового інституту Інформаційно-діагностичних систем
_____(Павленко П.М.)

ПЕРЕДМОВА

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ (спеціальності 125 Кібербезпека, спеціалізації 125.05 Адміністративний менеджмент у сфері захисту інформації) у складі:

КЕРІВНИК РОБОЧОЇ ГРУПИ:

КОРЧЕНКО О.Г., д.т.н., проф., завідувач кафедри безпеки інформаційних технологій

(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

КІНЗЕРЯВИЙ В.М., к.т.н., доцент кафедри безпеки інформаційних технологій

(підпис)

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

(підпис)

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

(підпис)

Рецензент Лахно В.А., завідувач кафедри кібербезпеки та управління захистом інформаційних систем Європейського університету, доктор технічних наук, професор.

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Врахований примірник №1

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; Бакалавр з кібербезпеки.
1.3.	Офіційна назва освітньо-професійної програми	Освітньо-професійна програма Адміністративний менеджмент у сфері захисту інформації
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 4 роки
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	-
1.10	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, використовувати і впроваджувати сучасні технології та методи захисту інформації на підприємстві	
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 результатах в галузі захисту інформації, 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; – принципів супроводу систем та комплексів захисту інформації; – теорії, моделей та принципів управління

		доступом до інформаційних ресурсів; – теорії систем управління захистом інформації; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних захищених інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування засобів захисту інформації.
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 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 дипломній 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	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення захисту інформації, 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. ЗК3. Здатність професійно 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. 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 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 захисту інформації. ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей захисту інформації. ФК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації. ФК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики безпеки. ФК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-комунікаційних системах з метою реалізації встановленої політики безпеки. ФК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації. ФК8. Здатність здійснювати процедури управління інцидентами безпеки, проводити розслідування, надавати їм оцінку. ФК9. Здатність застосовувати методи та засоби

		криптографічного та технічного захисту інформації. ФК10. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-комунікаційних систем згідно встановленої політики безпеки. ФК11. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою безпеки. ФК12. Здатність застосовувати методи теорії інформації та кодування, обробки та захисту інформації при наявності завад в каналах передачі даних. ФК13. Здатність застосовувати теоретичні знання та практичні навички із побудови, керування, модернізації, моніторингу та аналізу продуктивності, діагностики та розв`язання проблем сучасних інформаційних мереж. ФК14. 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 багатокористувальницьких операційних системах. ФК15. Здатність застосовувати методи та засоби організаційного характеру, щодо захисту інформації.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання	ПРН1. Здійснювати вибір і оцінку систем передачі даних та протоколів, визначати основні параметри каналу зв'язку для подальшої передачі інформації. ПРН2. Вирішувати задачі захисту інформації з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН3. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації. ПРН4. Визначати відомості, які відносяться до різних видів конфіденційної інформації, організовувати допуск та доступ персоналу до конфіденційної інформації. ПРН5. Організовувати внутрішньо об'єктовий та пропускний режими на підприємстві. ПРН6. Організовувати контроль за станом

		захисту конфіденційної інформації на підприємстві. ПРН7. Здатність продемонструвати знання та розуміння основ комп'ютерної схемотехніки та описати в загальних поняттях і термінах характеристики, параметри, фізичні принципи побудови та логічні основи функціонування цифрових елементів; номенклатуру і функціональне призначення інтегральних мікросхем; типові схеми функціональних вузлів комп'ютерів; методику їх аналізу та розрахунку з використанням пакетів програм систем автоматизованого проектування засобів захисту. ПРН8. 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. ПРН9. Здатність продемонструвати знання та розуміння основ побудови комп'ютерних систем захисту інформації та описати в загальних поняттях і термінах архітектуру, характеристики та принципи їх дії. ПРН10. 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; технологію автоматизованого проектування комп'ютерних мереж. ПРН11. Здатність продемонструвати знання та розуміння організації баз даних та розробляти проекти баз даних інформаційних систем, використовуючи сучасні методи і моделі захисту інформації. ПРН12. Здатність продемонструвати знання та розуміння системного програмування та розробляти захищені системні програми, алгоритми обробки різних типів даних та тестування програмного забезпечення.

		ПРН13. Реалізовувати основи системного підходу, критерії ефективної організації обчислювального процесу для постановки та рішення завдань організації оптимального функціонування обчислювальних систем. ПРН14. Вибирати, обґрунтовуючи свій вибір, оптимальні алгоритми керування ресурсами, порівнювати та оцінювати різні методи, що лежать в основі планування і диспетчеризації процесів, розробляти алгоритми прикладних програм на основі архітектури "клієнт-сервер" ПРН15. Здатність демонструвати знання та розуміння безпечного 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. ПРН16. Здатність демонструвати знання та розуміння технологій проектування комп'ютерних систем захисту інформації та виконувати системне, операційне, функціонально-логічне і технічне проектування комп'ютерних пристроїв, використовуючи сучасні засоби автоматизованого проектування. ПРН17. Здатність продемонструвати знання та розуміння діагностування та експлуатації комп'ютерних систем захисту інформації та застосовувати на практиці засоби автоматичного контролю і діагностування . ПРН18. Здатність демонструвати знання та розуміння сучасних методів і моделей захисту інформації. ПРН19. Здатність демонструвати 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. ПРН20. Здатність продемонструвати знання та розуміння застосовування методів та засобів криптографічного та технічного захисту інформації. ПРН21. Здатність демонструвати знання та розуміння професійній діяльності на основі

		впровадженої системи управління захистом інформації. ПРН22. Здатність продемонструвати знання та розуміння захисту інформації у комп'ютерних системах 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 комп'ютерних систем. ПРН23. Оволодіння навичками працювати самостійно при виконанні курсових робіт, курсових проектів, дипломних робіт. ПРН24. 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. 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 вищими навчальними закладами.
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

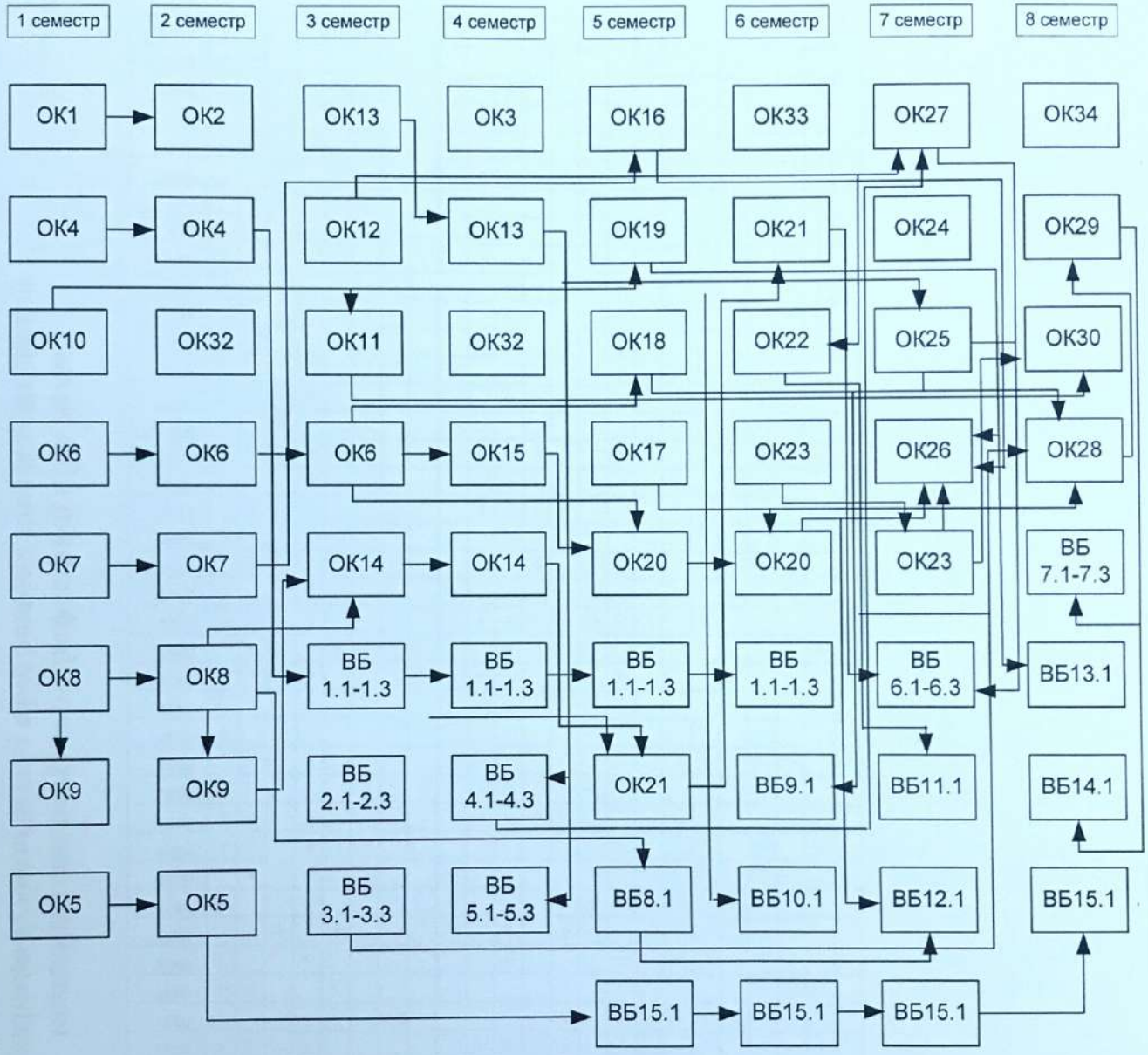
2.1. Перелік компонент ОПП

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 та основи програмування	11.5	Екзамен
ОК9.	Комп'ютерна графіка	3.0	Екзамен Диференційований залік
ОК10.	Основи інформаційної безпеки держави	4.0	Екзамен
ОК11.	Інформаційно-психологічні впливи у кіберпросторі	4.0	Диференційований залік
ОК12.	Інформаційно-аналітичне забезпечення інформаційної безпеки	3.0	Диференційований залік
ОК13.	Захищені комп'ютерні системи та мережі	9.0	Екзамен Диференційований залік
ОК14.	Технології програмування	8.5	Екзамен Диференційований залік
ОК15.	Дискретна математика	3.5	Екзамен
ОК16.	Технічні засоби охорони об'єктів критичної інфраструктури	3.5	Диференційований залік
ОК17.	Захищений електронний документообіг	3.5	Екзамен
ОК18.	Управління ризиками інформаційної безпеки	4.0	Екзамен

ОК19.	Нормативно-правове забезпечення інформаційної безпеки	3.5	Диференційований залік
ОК20.	Криптографія та криптоаналіз	8.0	Екзамен
ОК21.	Операційні системи та системне програмне забезпечення	6.0	Екзамен Диференційований залік
ОК22.	Управління ресурсами інформаційних систем	4.0	Екзамен
ОК23.	Тестування безпеки інформаційних систем	7.5	Екзамен
ОК24.	Основи охорони праці	3.0	Диференційований залік
ОК25.	Технології виявлення уразливостей інформаційних систем	4.5	Диференційований залік
ОК26.	Комплексні системи захисту інформації	5.0	Екзамен
ОК27.	Інформаційне забезпечення управлінської діяльності	4.5	Екзамен
ОК28.	Системи управління інформаційною безпекою	4.5	Екзамен
ОК29.	Інцидент-менеджмент у кіберпросторі	4.0	Екзамен
ОК30.	Соціотехнічна безпека	3.0	Диференційований залік
ОК31.	Фахова ознайомлювальна практика	3.0	Диференційований залік
ОК32.	Навчальний комп'ютерний практикум	3.0	Диференційований залік
ОК33.	Технологічна практика	4.5	Диференційований залік
ОК34.	Дипломне проектування	7.5	Захист
Загальний обсяг обов'язкових компонент:		180 кредитів	
Вибіркові компоненти ОПП			
ВБ 1.1.	Іноземна мова (за професійним спрямуванням)	8.0	Диференційований залік
ВБ 1.2.	Іноземна мова спеціальності	8.0	Диференційований залік
ВБ 1.3.	Іноземна мова (за фахом)	8.0	Диференційований залік
ВБ 2.1.	Апаратне забезпечення інформаційних систем	5.0	Екзамен
ВБ 2.2.	Інфраструктура інформаційних технологій	5.0	Екзамен
ВБ 2.3.	Апаратні складові персонального комп'ютера	5.0	Екзамен
ВБ 3.1.	Організація спеціального діловодства	3.0	Екзамен
ВБ 3.2.	Ведення конфіденційного діловодства	3.0	Екзамен
ВБ 3.3.	Діловодство та режим секретності	3.0	Екзамен
ВБ 4.1.	Організація корпоративних баз даних і знань	4.0	Диференційований залік
ВБ 4.2.	Бази даних та інформаційні системи	4.0	Диференційований

			залік
ВБ 4.3.	Основи баз даних	4.0	Диференційований залік
ВБ 5.1.	Системи ідентифікації, аутентифікації та авторизації	4.5	Екзамен
ВБ 5.2.	Протоколи аутентифікації та обміну ключами	4.5	Екзамен
ВБ 5.3.	Технології забезпечення цілісності та доступності	4.5	Екзамен
ВБ 6.1.	Технології програмного захисту інформації	3.0	Екзамен
ВБ 6.2.	Програмний захист інформації	3.0	Екзамен
ВБ 6.3.	Програмні методи та засоби захисту інформації	3.0	Екзамен
ВБ 7.1.	Економіка інформаційної безпеки	3.5	Диференційований залік
ВБ 7.2.	Економічні аспекти захисту інформації	3.5	Диференційований залік
ВБ 7.3.	Економічна стратегія безпеки підприємства	3.5	Диференційований залік
ВБ 8.1.	Управління спеціальним системним програмним забезпеченням *	7.0	Диференційований залік
ВБ 9.1.	Маркетинг продуктів і послуг інформаційної безпеки *	3.5	Диференційований залік
ВБ 10.1.	Управління веб-контентом *	4.0	Екзамен
ВБ 11.1.	Управління проектами захисту інформації *	3.5	Диференційований залік
ВБ 12.1.	Захищені мережеві технології обробки інформації *	3.5	Диференційований залік
ВБ 13.1.	SEO-технології в управлінській діяльності*	3.0	Диференційований залік
ВБ 14.1.	Криміналістичний аналіз комп'ютерних систем *	4.5	Екзамен
ВБ 15.1.	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 дипломної роботи та завершується видачею документу встановленого зразка про присудження йому освітнього ступеня бакалавра із присвоєнням освітньої кваліфікації: бакалавр з кібербезпеки.

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	ОК34	ВБ1	ВБ2	ВБ3	ВБ4	ВБ5	ВБ6	ВБ7	ВБ8	ВБ9	ВБ10	ВБ11	ВБ12	ВБ13	ВБ14	ВБ15
ЗК1	+			+	+	+	+	+	+				+	+		+		+		+	+			+	+	+		+	+			+	+	+	+	+					+	+			+	+	+	+
ЗК2										+	+	+	+						+	+	+				+	+		+	+	+		+	+	+					+		+			+	+		+	
ЗК3	+	+		+													+									+									+											+	+		+	
ЗК4								+		+	+	+	+			+		+	+	+	+				+	+		+	+			+	+	+		+								+	+			
ЗК5		+	+			+					+	+			+		+										+				+	+	+				+							+			+		
ЗК6		+																																															
ЗК7		+									+																																						
ЗК8					+																																													
ФК1										+	+						+	+	+							+		+	+					+			+							+				
ФК2								+					+								+	+				+	+		+				+	+	+								+	+				
ФК3								+					+	+		+	+				+	+				+	+	+	+	+			+	+	+		+		+	+	+				+	+		
ФК4										+											+							+	+	+			+	+														
ФК5													+	+			+									+		+					+	+					+										
ФК6																		+	+			+				+		+	+					+							+		+		+					
ФК7																						+				+		+						+					+										
ФК8																													+																				
ФК9																+				+																			+										
ФК10																							+		+			+											+										
ФК11										+	+							+					+		+				+	+				+						+		+				+		
ФК12													+			+				+														+	+		+												
ФК13													+																						+					+					+	+	+			
ФК14								+					+							+							+								+					+	+		+				+		
ФК15										+									+							+		+	+					+	+												+		

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	ОК34	ВБ1	ВБ2	ВБ3	ВБ4	ВБ5	ВБ6	ВБ7	ВБ8	ВБ9	ВБ10	ВБ11	ВБ12	ВБ13	ВБ14	ВБ15
ПРН1													+			+																				+									+		+			
ПРН2																				+																													
ПРН3						+									+					+																													
ПРН4										+		+					+		+							+		+																				
ПРН5																										+														+									
ПРН6									+			+					+									+													+										
ПРН7									+				+																																				
ПРН8									+												+																												
ПРН9													+											+													+								+				
ПРН10													+									+																	+										
ПРН11								+														+																		+		+							
ПРН12								+						+							+	+																		+									
ПРН13																										+														+								+	
ПРН14								+						+							+	+					+														+							
ПРН15														+							+																											
ПРН16													+													+		+																				
ПРН17																							+		+	+		+		+														+				
ПРН18										+	+							+					+		+	+		+												+		+						
ПРН19								+						+							+																											
ПРН20						+									+					+				+		+	+	+							+	+	+									+		
ПРН21											+		+								+		+		+		+		+												+		+					+	
ПРН22														+						+			+			+		+							+													
ПРН23								+						+																					+														
ПРН24				+																																														

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки
		09.07.2019	Миколаєвська В.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				