(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО –ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації, автоматизація її обробки»
(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 – 2019

Затверджено Вченою радою
Голова Вченої ради
_____ В. Ісаєнко
(протокол № 4 від 24.04.2019 р.)

Освітньо-професійна програма
вводиться в дію наказом ректора
Ректор
_____ В. Ісаєнко
(наказ № 184 від 25.04.2019 р.)

КИЇВ

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

ПОГОДЖЕНО

Науково-методичною радою університету

протокол № 3

від «18» 04 2019 р

Проректор НАУ з навчальної роботи

Голова НМР НАУ

_____ (Гудманян А.Г.)

ПОГОДЖЕНО

Вченою радою Навчально-наукового інституту інформаційно-діагностичних систем

протокол № 1

від «21» лютого 2019 р

Голова Вченої ради Навчально-наукового інституту інформаційно-діагностичних систем

_____ (Гумен М.Б.)

ПОГОДЖЕНО

Кафедрою засобів захисту інформації

протокол засідання № 4

від «18» лютого 2019 р

Завідувач кафедри

_____(Лазаренко С.В.)

ПОГОДЖЕНО

Науково-методично-редакційною радою

Навчально-наукового інституту інформаційно-діагностичних систем

протокол № 1

від «18» лютого 2019 р

Голова НМР Навчально-наукового інституту інформаційно-діагностичних систем

_____ (Квасніков

ПЕРЕДМОВА

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ (спеціальності 125 Кібербезпека) у складі:

КЕРІВНИК РОБОЧОЇ ГРУПИ:

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

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

ВОЙТЕНКО С.Д., 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)

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

ЩЕРБАК Т.Л., 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-наукового інституту 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	Системи технічного захисту інформації, автоматизація її обробки
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	Акредитаційна комісія, Міністерство освіти і науки України, сертифікат серія НД-ІІ № 1181256 від 18.01.2017
1.6.	Цикл/рівень	FQ-EHEA – перший рівень, 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.kzzi.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, системи та комплекси технічного захисту інформації на об'єктах інформаційної діяльності	
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 за спеціальністю Кібербезпека. Ключові слова: інформаційна безпека, кібербезпека, захист інформації.
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 інформаційної та/або кібербезпеки;

3.4.	Особливості освітньо-професійної програми	– теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення та локалізації каналів витоку інформації; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів виявлення закладних пристроїв; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування.
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 безпеки; – фахівець із організації захисту інформації з обмеженим доступом; – фахівець з режиму секретності; – фахівець з досліджень та розробок; – 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 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. ЗК2. Знання та розуміння предметної області та розуміння професії. 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. ЗК6. Здатність використовувати технічні засоби захисту та охорони інформаційних ресурсів і баз даних обмеженого доступу. ЗК7. Здатність організовувати функціонування системи організаційно-службових і спеціальних (охоронних) заходів із забезпечення інформаційної та/або кібербезпеки установ, підприємств, організацій. ЗК8. 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. ЗК9. 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, 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.

6.3.	Фахові компетентності (ФК)	ФК2. Здатність до використання 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 та в інформаційно-телекомунікаційних (автоматизованих) системах. ФК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК5. Здатність оцінювати захищеність інформації усіх видів, що циркулює на об'єктах інформаційної діяльності. ФК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем та комплексів технічного захисту інформації після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК7. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. ФК8. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). ФК9. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. ФК11. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. ФК12. Здатність виявляти та блокувати канали витоку інформації, методи несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію, здійснювати пошук закладних пристроїв. ФК13. Здатність оцінювати та визначати фізичні процеси, які висвітлюють характеристики та параметри напівпровідникових активних елементів, а також проводити лінійний та

6.3.	Фахові компетентності (ФК)	нелінійний аналіз електричних схем, схемотехніки різноманітних підсилювальних каскадів, операційних підсилювачів та елементів логіки. ФК14. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. ФК15. Здатність використовувати теоретичні знання та практичні навички з підготовки технічної документації.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання (ПРН)	ПРН1. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ПРН2. Застосувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН3. Використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН5. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних у галузі інформаційної та\або кібербезпеки. ПРН6. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки; впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПРН7. Розробляти моделі загроз та порушника. ПРН8. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

7.1.	Програмні результати навчання (ПРН)	ПРН9. Використовувати програмні та рограмно-апаратні комплекси захисту інформаційних ресурсів. ПРН10. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН11. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН12. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів. ПРН13. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. ПРН14. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем. ПРН15. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної та\або кібербезпеки. ПРН16. Виявляти небезпечні сигнали технічних засобів. ПРН17. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН18. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

7.1.	Програмні результати навчання (ПРН)	ПРН19. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ПРН20. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН21. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів. ПРН22. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН23. 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. ПРН24. Організовувати внутрішньо-об'єктовий та пропускний режими на підприємстві. ПРН25. Вирішувати задачі забезпечення та супроводу комплексу технічного захисту інформації на об'єкті інформаційної діяльності. ПРН26. Складати звітність та вести технічну документацію.
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. 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	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 Національним технічним університетом України «Київським політехнічним інститутом імені Ігоря Сікорського» 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.	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

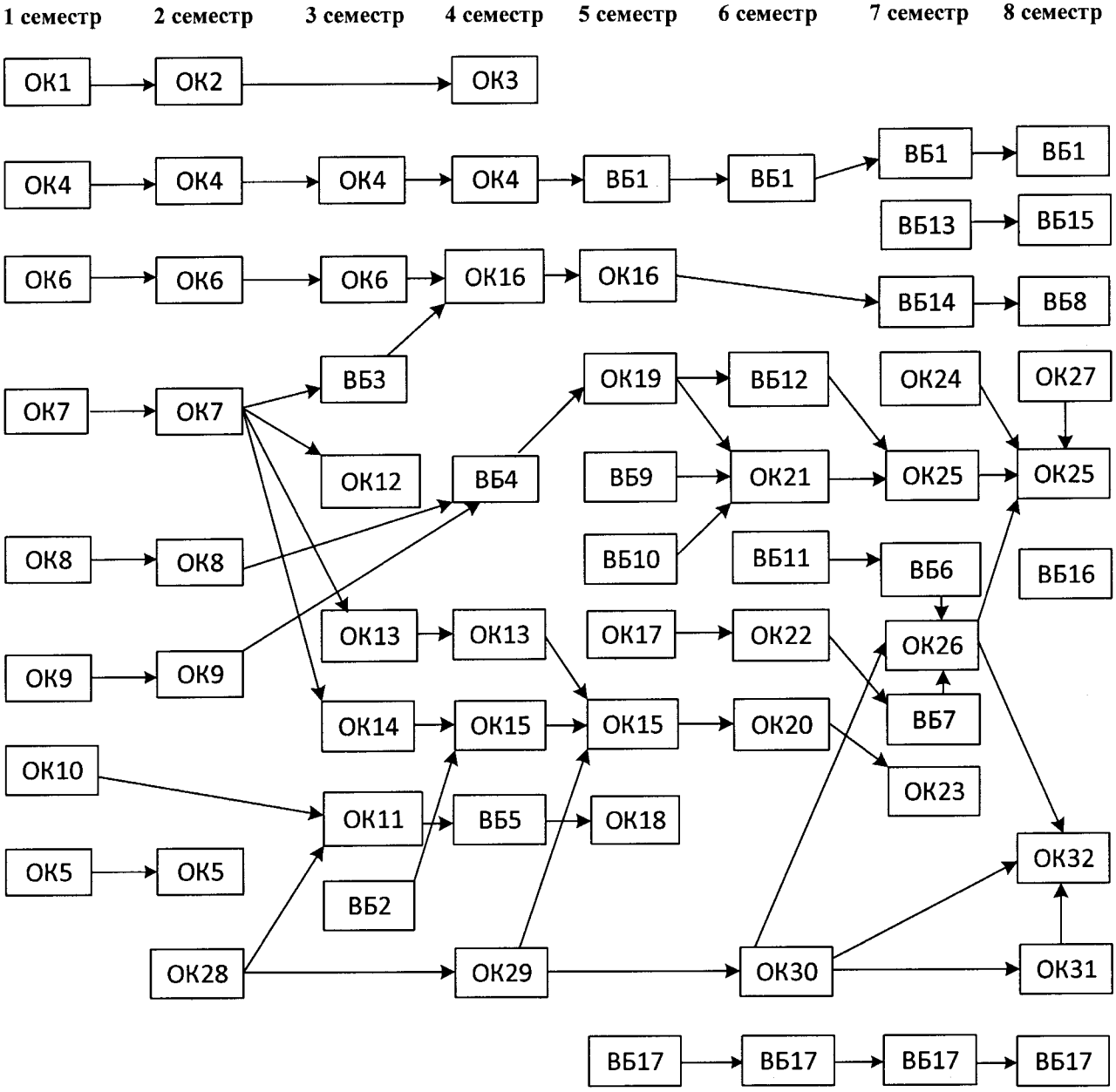
1	2	3	4
ОК6.	Вища математика	15.5	Екзамен, Диференційований залік
ОК7.	Фізика	11.0	Диференційований залік
ОК8.	Інформаційні технології та основи програмування + КР (курсова робота)	13.0	Екзамен
ОК9.	Комп'ютерна графіка	6.5	Екзамен, Диференційований залік
ОК10.	Основи інформаційної безпеки держави	3.5	Екзамен
ОК11.	Основи проектування систем технічного захисту інформації	4.5	Екзамен
ОК12.	Метрологія та вимірювання	4.0	Екзамен
ОК13.	Основи теорії кіл, сигналів та процесів в системах технічного захисту інформації + КР (курсова робота)	10.5	Екзамен
ОК14.	Компонентна база засобів технічного захисту інформації	4.5	Екзамен
ОК15.	Схемотехніка пристроїв технічного захисту інформації + КР (курсова робота)	10.0	Екзамен Диференційований залік
ОК16.	Поля і хвилі в системах технічного захисту інформації + КР (курсова робота)	11.0	Екзамен
ОК17.	Засоби передавання інформації в системах технічного захисту інформації	4.5	Екзамен
ОК18.	Теорія інформації та кодування	3.5	Диференційований залік
ОК19.	Безпека інформаційно-комунікаційних систем	3.0	Екзамен
ОК20.	Мікропроцесори в системах технічного захисту інформації	5.0	Екзамен
ОК21.	Управління інформаційною безпекою	3.5	Екзамен
ОК22.	Засоби приймання та обробки сигналів в системах технічного захисту інформації + КП (курсовий проект)	6.0	Екзамен
ОК23.	Цифрова обробка сигналів	4.0	Диференційований залік
ОК24.	Технічні засоби охорони об'єктів + КП (курсовий проект)	5.0	Екзамен
ОК25.	Методи та засоби технічного захисту інформації	8.0	Екзамен
ОК26.	Проектування систем технічного захисту інформації	5.0	Екзамен
ОК27.	Криптографія та стеганографія	3.0	Диференційований залік
ОК28.	Фахово-ознайомлювальна практика	3.0	Диференційований залік
ОК29.	Навчальна схемотехнічна практика	3.0	Диференційований залік

1	2	3	4
ОК30.	Технологічна практика	3.0	Диференційований залік
ОК31.	Переддипломна практика	3.0	Диференційований залік
ОК32.	Кваліфікаційна робота	7.5	Захист
Загальний обсяг обов'язкових компонент:		180 кредитів	
Вибіркові компоненти ОПП			
ВБ1.	Іноземна мова професійного спрямування	4.0	Екзамен, Диференційований залік
	Іноземна мова спеціальності	4.0	Екзамен, Диференційований залік
	Іноземна мова ділової комунікації	4.0	Екзамен, Диференційований залік
ВБ2.	Пристрої електроживлення систем технічного захисту інформації	4.0	Диференційований залік
	Електроживлення систем технічного захисту інформації	4.0	Диференційований залік
	Соціологія	4.0	Диференційований залік
ВБ3.	Спеціальні розділи фізики	3.0	Диференційований залік
	Фізика складних систем	3.0	Диференційований залік
	Соціологія науки і техніки	3.0	Диференційований залік
ВБ4.	Комп'ютерні мережі	4.0	Диференційований залік
	Комп'ютерні системи та мережі	4.0	Диференційований залік
	Основи політичної аналітики	4.0	Диференційований залік
ВБ5.	Системи запису і відтворення інформації	4.0	Диференційований залік
	Системи аудіо- та відеофіксації інформації	4.0	Диференційований залік
	Психологія професійної діяльності	4.0	Диференційований залік
ВБ6.	Організаційне забезпечення технічного захисту інформації	4.0	Диференційований залік
	Організаційно-технічне забезпечення захисту інформації	4.0	Диференційований залік
	Психологія лідерства	4.0	Диференційований залік

1	2	3	4
ВБ7.	Системи технічного захисту інформації	4.0	Диференційований залік
	Пристрої технічного захисту інформації	4.0	Диференційований залік
	Основи охорони праці	4.0	Диференційований залік
ВБ8.	Радіопротидія	4.0	Екзамен
	Пристрої, системи та комплекси радіопротидії	4.0	Екзамен
	Проектування та інженерно-технічне забезпечення пристроїв радіопротидії	4.0	Екзамен
ВБ9.	Економіка інформаційної безпеки*	3.5	Диференційований залік
ВБ10.	Системи банківської безпеки*	3.5	Диференційований залік
ВБ11.	Нормативно-правове забезпечення інформаційної безпеки*	3.5	Диференційований залік
ВБ12.	Комплексні системи захисту інформації*	4.0	Екзамен
ВБ13.	Аналітична обробка даних*	3.5	Диференційований залік
ВБ14.	Електромагнітна сумісність і завадостійкість систем технічного захисту інформації*	3.5	Диференційований залік
ВБ15.	Аудит інформаційної безпеки*	3.0	Екзамен
ВБ16.	Кібербезпека хмарних технологій*	4.5	Диференційований залік
ВБ17.	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 кваліфікаційної роботи та завершується видачою 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	ВБ 16
ІК1	+			+		+	+	+	+	+	+		+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+
ЗК1	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК2								+		+	+	+		+	+			+	+	+	+		+	+	+	+	+	+	+	+	+		+		+	+	+	+	+	+	+	+	+	+	+	+
ЗК3	+			+															+	+								+	+	+	+	+										+		+				
ЗК4	+			+		+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК5	+	+				+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК6							+	+		+									+		+				+	+		+	+	+	+	+				+		+	+			+		+				
ЗК7							+	+		+				+					+		+			+	+	+		+	+	+	+	+					+	+	+			+		+				
ЗК8	+	+	+																									+	+	+	+											+						
ЗК9	+	+	+		+					+																																+	+					+	
ФК1	+			+						+	+								+		+			+	+	+		+	+	+	+	+	+		+	+	+	+	+	+		+	+	+	+	+
ФК2				+		+	+	+		+	+	+	+	+	+	+	+		+	+	+		+			+		+	+	+	+	+	+	+	+	+				+	+	+	+	+	+	+
ФК3						+	+	+			+			+	+			+	+	+	+		+		+	+	+	+	+	+	+		+		+		+	+	+				+	+	+		
ФК4								+	+	+	+		+	+	+	+		+	+	+	+		+	+	+	+	+	+	+	+	+		+		+	+	+	+	+	+	+	+	+	+	+	
ФК5							+			+		+							+		+			+	+			+	+	+	+	+			+	+	+				+	+				
ФК6											+			+	+		+			+		+		+	+	+				+	+		+		+	+	+	+						+		
ФК7								+			+	+	+	+	+	+	+	+	+	+	+	+	+			+	+	+		+	+	+		+		+						+	+			
ФК8								+	+		+			+	+		+	+	+	+	+	+	+		+	+		+		+	+	+		+		+		+	+				+	+		
ФК9								+		+								+	+		+		+					+		+	+	+				+					+	+	+	+	+		+	+
ФК10						+	+																		+		+			+	+				+			+	+								
ФК11								+		+	+	+		+	+	+		+	+	+	+		+		+	+		+		+	+	+		+		+		+	+	+	+	+	+	+	+	+
ФК12							+				+	+	+	+	+	+	+		+	+	+	+		+	+	+		+		+	+	+		+	+	+	+	+	+	+				+		
ФК13						+	+		+			+	+	+	+	+	+			+		+		+				+	+	+	+	+		+	+		+			+				+		
ФК14								+					+					+	+		+							+	+	+	+	+				+								+		+	
ФК15	+			+					+		+	+		+	+		+			+		+		+	+	+		+	+	+	+	+	+	+			+	+	+			+	+	+		

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	ВБ 16
ПРН1	+	+	+	+	+					+																							+															
ПРН2	+			+																					+			+	+	+	+	+	+														+	+				+	
ПРН3						+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН4	+			+		+	+	+		+	+			+		+	+	+	+	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН5	+			+						+	+								+		+			+	+	+	+	+	+	+	+	+					+	+	+		+	+	+	+			+	
ПРН6	+			+						+	+								+		+				+	+						+					+	+		+	+	+				+	
ПРН7	+			+		+	+		+	+	+								+		+				+	+				+	+	+	+		+			+	+				+	+			+	
ПРН8											+			+			+		+	+	+	+			+	+				+	+	+		+				+	+	+		+		+	+			
ПРН9						+	+	+			+			+	+		+	+	+	+	+	+	+	+	+	+			+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+			+
ПРН10									+					+	+		+		+	+	+	+		+						+	+	+		+			+			+	+							
ПРН11											+			+			+		+	+	+	+		+	+	+	+			+	+	+		+			+	+	+	+		+	+	+		+		+
ПРН12								+			+							+	+		+		+		+	+	+			+	+	+				+		+	+			+	+	+	+			+
ПРН13										+	+								+		+			+	+	+				+	+	+					+	+	+			+	+	+			+	
ПРН14						+	+	+		+								+	+		+		+				+	+	+	+	+				+	+	+						+	+	+	+	+	+
ПРН15	+			+						+	+			+	+		+		+	+	+	+		+	+	+		+		+	+	+	+			+	+	+	+	+	+	+	+		+	+	
ПРН16							+					+	+		+	+				+								+		+	+				+												
ПРН17						+	+					+	+			+									+			+	+	+	+				+			+	+				+			+		
ПРН18							+					+	+			+															+	+				+												
ПРН19	+			+					+		+	+													+	+				+	+	+	+					+	+			+	+	+				
ПРН20						+					+	+			+														+		+	+			+											+		
ПРН21	+			+						+	+	+	+			+			+		+			+	+	+	+	+		+	+	+	+				+	+	+		+	+	+	+		+	+	+
ПРН22										+	+								+		+					+	+			+	+	+														+		
ПРН23										+	+								+		+				+	+				+	+	+						+	+			+	+	+			+		
ПРН24									+		+			+			+					+		+	+	+		+		+	+	+		+			+	+	+			+	+					
ПРН25									+		+	+		+	+		+			+		+		+	+	+				+	+	+		+			+	+	+		+	+	+				
ПРН26	+			+					+		+	+			+					+				+	+	+		+	+	+	+	+	+			+	+	+		+	+	+	+		+		

(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				