(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

# ОСВІТНЬО –ПРОФЕСІЙНА ПРОГРАМА

**« Безпека інформаційних і комунікаційних систем »**
(найменування ОПП)

**Другого (магістерського) рівня вищої освіти**

**за спеціальністю** _125 Кібербезпека___
(шифр та найменування спеціальності)

**галузі знань** ____12 Інформаційні технології_____
(шифр та найменування галузі)

**кваліфікація:** Науковий співробітник (інформаційна безпека)
Професіонал з безпеки інформаційних і комунікаційних систем
(найменування кваліфікації)

**СМЯ НАУ ОПП 09.01.09 – 01 – 2018**

Затверджено Вченою радою
Голова Вченої ради
_____ В.Ісаєнко
(протокол № 6 від 26.06.2018р.)

Освітньо-професійна програма
Вводиться в дію наказом ректора
_____ 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 "07" 06 2018 р

Проректор НАУ з навчальної роботи

Голова НМР НАУ

_____(Гудманян А.Г.)

ПОГОДЖЕНО

Вченою радою Навчально-наукового інституту Комп'ютерних інформаційних технологій

протокол № 5

від "21" 05 2018 р

Голова Вченої ради Навчально-наукового Комп'ютерних інформаційних технологій

_____(Юдін О.К.)

ПОГОДЖЕНО

Кафедрою комп'ютеризованих систем захисту інформації

протокол засідання № 19

від "23" 04 2018 р

Завідувач кафедри

_____( Корнієнко Б.Я.)

ПОГОДЖЕНО

Науково-методично-редакційною радою Навчально-наукового інституту Комп'ютерних інформаційних технологій

протокол № 9

від "16" 05 2018 р

Голова НМР Навчально-наукового інституту Комп'ютерних інформаційних технологій

_____(Масловський Б.Г.)

Затверджено та надано чинності наказом ректора університету

від «____»_____2018 р. № _____

## ПЕРЕДМОВА

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ (спеціальності 125 Кібербезпека ) у складі:

КЕРІВНИК РОБОЧОЇ ГРУПИ:

КОРНІЄНКО Б.Я. д.т.н., проф., завідувач Кафедри комп'ютеризованих систем захисту інформації _____

(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

ШІМАТОК О.С., к.т.н., доц., доцент кафедри КСЗІ _____

(підпис)

ПЕТРЕНКО А.Б., к.т.н., доц., доцент кафедри КСЗІ _ _____

(підпис)

ІЛЬЄНКО А.В., к.т.н., доц., доцент кафедри КСЗІ _ _____

(підпис)

Рецензент Толюпа С.В., доктор технічних наук, професор кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій Київського національного університету імені Тараса Шевченка,

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 комп'ютерних інформаційних технологій, кафедра комп'ютеризованих систем захисту інформації. |
| 1.2. | Ступінь вищої освіти та назва кваліфікації мовою оригіналу | Магістр; Науковий співробітник (інформаційна безпека), Професіонал з безпеки інформаційних і комунікаційних систем |
| 1.3. | Офіційна назва освітньо-професійної програми | Безпека інформаційних і комунікаційних систем |
| 1.4. | Тип диплому та обсяг освітньо-професійної програми | Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1рік 6 місяців. |
| 1.5. | Наявність акредитації | Акредитаційна комісія, Міністерство освіти і науки України, сертифікат НД № 1191192 від 31.08.2017р. |
| 1.6. | Цикл/рівень | FQ-EHEA – другий цикл, НРК – 8 рівень |
| 1.7. | Передумови | Наявність ступеня бакалавра |
| 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<br>http://www.icit.nau.edu.ua |
| **Розділ 2. Мета освітньо-професійної програми** | | |
| 2.1. | Мета освітньої програми полягає в оволодінні студентами знаннями, вміннями та навичками з проектування, експлуатації, адміністрування та інформаційного захисту комп'ютерних систем, локальних і корпоративних інформаційно-обчислювальних мереж та системного програмного забезпечення. | |
| **Розділ 3. Характеристика освітньо-професійної програми** | | |
| 3.1 | Предметна область (галузь знань, спеціальність, спеціалізація (за наявності)) | Галузь знань: 12 Інформаційні технології<br>Спеціальність: 125 Кібербезпека |
| 3.2. | Орієнтація освітньо-професійної програми | Освітньо-професійна, базується на загальновідомих наукових результатах інформаційних технологій,<br>у рамках яких можлива подальша професійна кар'єра і подальше навчання у галузі безпеки інформаційних і комунікаційних систем. |
| 3.3. | Основний фокус освітньо-професійної програми та спеціалізації | Загальна вища освіта в галузі знань інформаційних технологій з поглибленою спеціальною підготовкою в сфері безпеки інформаційних і комунікаційних систем.<br>Ключові слова: |

| | | |
|---|---|---|
| | | – теоретичні основи методів та засобів технічного та криптографічного захисту інформації;<br>– теорія систем управління інформаційною та/або кібербезпекою;<br>– стандартизація, сертифікація засобів та комплексів захисту інформації;<br>– побудова та експлуатація комп'ютерних систем та мереж;<br>– методи та технологій системного та спеціального програмного забезпечення. |
| 3.4. | Особливості освітньо-професійної програми | Програма передбачає вивчення теоретичних основ та сучасних технологій проектування, експлуатації, адміністрування та інформаційного захисту комп'ютерних систем, інформаційно-обчислювальних мереж та системного програмного забезпечення.<br>Особливістю програми є поглиблене вивчення принципів побудови та експлуатації комп'ютерних систем, технологій системного програмування, загально системного та спеціального програмного забезпечення, теорії систем управління інформаційною та/або кібербезпекою. |
| **Розділ 4. Придатність випускників до працевлаштування та подальшого навчання** | | |
| 4.1. | Придатність до працевлаштування | Випускники підготовлені до роботи за національним класифікатором України ДК003:2010 а саме: наукові співробітники (інформаційна безпека), професіонал з безпеки інформаційних і комунікаційних систем;<br>інженер з безпеки інформаційних і комунікаційних системах;<br>асистент кафедри вищого навчального закладу;<br>молодший науковий співробітник науково-дослідного підрозділу (установи). |
| 4.2. | Подальше навчання | Випускники мають право продовжити навчання на третьому (освітньо-науковому) рівні вищої освіти для отримання ступеня «Доктор філософії» |
| **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 дипломної роботи. |
| **Розділ 6. Програмні компетентності** | | |
| 6.1. | Інтегральні компетентності | Здатність розв'язувати складні задачі і проблеми у певній галузі професійної діяльності або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог. |
| 6.2. | Загальні компетентності (ЗК) | ЗК1. Здатність до абстрактного мислення, аналізу і синтезу<br>ЗК2. Здатність до навчання та самонавчання (пошуку, оброблення та аналізу інформації з різних джерел)<br>ЗК3. Здатність застосовувати знання на практиці<br>ЗК4. Вільне усне і письмове спілкування українською мовою та здатність спілкуватися, читати та писати іноземною мовою<br>ЗК5. Міжособистісні навички та вміння<br>ЗК6. Навички використання інформаційних і комунікаційних технологій<br>ЗК7. Здатність розв'язувати поставлені задачі та приймати відповідні рішення<br>ЗК8. Здатність оцінювати та забезпечувати якість виконуваних робіт<br>ЗК9. Здатність працювати як індивідуально, так і в команді<br>ЗК10. Базові дослідницькі навички і уміння |
| 6.3. | Фахові компетентності (ФК) | ФК1. Знання технічних характеристик, конструктивних особливостей, застосування і правил експлуатації програмних, програмно-технічних засобів, комп'ютерних систем, мереж та програмно-технічних засобів захисту інформації<br>ФК2. Здатність використовувати методи фундаментальних і прикладних дисциплін для опрацювання, аналізу й синтезу результатів професійних досліджень<br>ФК3. Здатність розробляти алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем з використанням сучасних методів і мов програмування, а також засобів і систем |

| | | |
|---|---|---|
| | | автоматизації проектування тощо<br>ФК4. Здатність проектувати та моделювати комп'ютерні системи та мережі різного виду та призначення<br>ФК5. Здатність будувати архітектуру та створювати системне і прикладне програмне забезпечення комп'ютерних систем та мереж.<br>ФК6. Здатність використовувати та впроваджувати нові технології захисту інформації, включаючи технології розумних, мобільних, і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.<br>ФК7. Здатність досліджувати технології, здійснювати їх аналіз, синтез та вибір для створення систем захисту інформації<br>ФК8. Здатність проводити управління та забезпечення якістю продуктів і сервісів інформаційних технологій на протязі їх життєвого циклу.<br>ФК9. Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів, статей і доповідей на науково-технічних конференціях.<br>ФК10. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів технічного та криптографічного захисту інформації, комп'ютерних систем, мереж та їхніх компонентів шляхом використання аналітичних методів і методів моделювання;<br>ФК11. Здатність досліджувати проблему у галузі комп'ютерних та інформаційних технологій, визначати їх обмеження.<br>ФК12. Здатність проектувати системи та їхні компоненти з урахуванням усіх аспектів їх життєвого циклу та поставленої задачі, включаючи створення, налаштування, експлуатацію, технічне обслуговування та утилізацію.<br>ФК13. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати та захищати прийняті рішення. |
| **Розділ 7. Програмні результати навчання** | | |
| 7.1. | Програмні результати навчання | ПРН1. Вирішувати задачі практичного застосування в своїй професійній діяльності криптографічних алгоритмів, протоколів та |

| | | |
|---|---|---|
| | | криптосистем для забезпечення належного рівня інформаційної та кібернетичної безпеки в інформаційно-телекомунікаційних системах.<br>Розробляти та впроваджувати криптографічні системи і використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.<br>ПРН2. Вміння реалізовувати математичні та комп'ютерні моделі для тестування захищеності інформаційної системи шляхом використання спеціалізованих програмних та апаратних засобів забезпечення інформаційної та кібернетичної безпеки<br>ПРН3.Розуміння шляхів самостійного освоєння нових методів дослідження, нового наукового й науково-виробничого профілю діяльності.<br>Здійснювати науково-дослідну роботу в професійній області, зокрема під час розробки нових технологій інформаційної та кібернетичної безпеки<br>Використовувати методи загальнонаукового аналізу у сфері інформаційної та кібернетичної безпеки та демонструвати можливості сучасних природничо-наукових методів дослідження у практиці забезпечення інформаційної безпеки.<br>Здійснювати розробку планів і програм проведення наукових досліджень і технічних розробок, підготовка окремих завдань для виконавців в сфері забезпечення інформаційної та кібернетичної безпеки<br>ПРН4. Здійснювати розробку проектів зі створення і впровадження систем забезпечення інформації та кібернетичної безпеки, а саме засобів захисту інформації, розробляти програми та методики випробувань<br>ПРН5.Здійснювати організацію функціонування інформаційно-комунікаційної систем: формувати опис автоматизованої системи та середовища її функціонування, визначати склад апаратного та програмного забезпечення, здійснювати аналіз обчислювальних процесів та технологій обробки інформації, аналіз складу та характеристик існуючої системи захисту з |

| | | |
|---|---|---|
| | | використанням засобів Cisco.<br>ПРН6. Здатність управляти проектами з забезпечення інформаційної та кібернетичної безпеки, моделювати системи та процеси захисту інформації, здійснювати аналіз об'єктів захисту, приймати експертні рішення<br>Здатність організовувати та проводити роботи щодо розробки та оцінки поточного стану системи інформаційної безпеки, встановлення рівня її відповідності певним критеріям та надання результатів у вигляді рекомендації.<br>Здатність володіти новітніми технологіями розроблення програмних та програмно-апаратних засобів захисту інформації при вирішенні прикладних задач інформації та кібернетичної безпеки.<br>ПРН7. Здійснювати роботу із сертифікації засобів захисту інформації.<br>Здійснювати розробку програм та методик випробувань функціональних послуг безпеки.<br>ПРН8. Розробляти програму та методику випробувань функціональних послуг безпеки та проводити сертифікацію засобів захисту інформації.<br>ПРН9. Здійснювати роботу із сертифікації та атестації комплексів технічного захисту інформації. Здійснювати проводити роботи з первинної, додаткової та контрольної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації.<br>ПРН10. Здійснювати виявлення стороннього кібернетичного впливу.<br>Здійснювати протидію несанкціонованому проникненню протиборчих сторін у власні інформаційні системи, забезпечуючи стійкість їхньої роботи, а також відновлення нормального функціонування після здійснення кібернетичних нападів<br>ПРН11. Обґрунтовувати комплекс завдань із проектування систем кібернетичного захисту.<br>Здійснювати поточний аналіз стану |

| | | |
|---|---|---|
| | | захищеності кіберпростору.<br>ПРН12. Здатність моделювати можливі ситуації кібернетичного впливу та здійснювати прогнозування впливів на кіберінфраструктуру. Розробляти та впроваджувати програмні моделі реалізації методів оцінці захищеності кіберсистем<br>ПРН13. Здійснювати компанування клієнтської та серверної частини Web-додатків та реалізовувати їх механізми взаємодії.<br>Здійснювати проектування Web-додатків, підвищувати продуктивність і забезпечувати балансування навантаження в Web-додатках, застосовувати інструментальний апарат тестування Web-додатків.<br>ПРН14. Вирішувати задачі практичного застосування в своїй професійній діяльності WEB-технологій з метою реалізації сучасних WEB-систем для забезпечення належного рівня інформаційної та кібернетичної безпеки в інформаційно-комунікаційних системах.<br>ПРН15. Розробляти та впроваджувати спроектовані WEB-додатки, використовувати компоненти захисту середовищ розробки WEB-додатків для забезпечення необхідного рівня захищеності інформації в інформаційно-комунікаційних системах.<br>ПРН16.Обґрунтовувати вибір архітектури ІВК з урахуванням завдань, що вирішується на рівні держави, відомства, державних установ, приватних організацій, суспільних організацій.<br>Здійснювати визначення основних функціональних та криптографічних вимог до системи сертифікації.<br>Здійснювати побудову функціональної структури, топологію центрів сертифікації та обґрунтовувати вимоги безпеки до центрів з метою забезпечення кібернетичної безпеки.<br>ПРН17. Визначати функціональну структуру, топологію центрів сертифікації та обґрунтовувати вимоги безпеки до центрів сертифікації з метою забезпечення необхідної якості надання послуг. |

| | | |
|---|---|---|
| | | ПРН18. Обґрунтовувати вибір архітектури інфраструктури відкритих ключів та систем електронного цифрового підпису з урахуванням завдань, що вирішується в інформаційно-телекомунікаційних системах.<br>Розробляти та впроваджувати інфраструктуру відкритих ключів та використовувати центри сертифікації ключів для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.<br>Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.<br>ПРН19. Обґрунтовувати впровадження конкретного алгоритму процедур відновлення та стиснення даних на основі розрахунку показників ефективності алгоритмів стиснення та оцінки ефективності процедур відновлення при певних вимогах замовника.<br>Розробляти та впроваджувати програмні моделі реалізації методів стиснення-відновлення інформаційних даних<br>ПРН20.Вміння оцінювати інформацію, як у кількісному, так і якісному розумінні.<br>Здатність підрахувати кількість інформації у повідомленні та визначати інформативність дискретних і безперервних джерел повідомлень.<br>Здатність оцінювати пропускну здатність каналу зв'язку та визначати швидкість передачі інформації.<br>Здатність оцінювати кількісні втрати інформації при передачі сигналів по реальних каналах зв'язку.<br>Здійснювати вибір, оцінку та розроблення структур інформаційних систем, мереж та їх елементів для ефективної передачі та зберігання інформаційних об`єктів з використанням методів та моделей завадостійкого кодування.<br>ПРН21. Вміння оцінювати основні аудіо характеристики голосу людини, систематизувати й організовувати процедури структурного представлення аудіо сигналів.<br>Здатність оцінювати та класифікувати методи |

| | | |
|---|---|---|
| | | визначення базових характеристик аудіо сигналів у сучасних системах захисту інформації.<br>Вміння розробляти методи ідентифікації керуючих аудіо сигналів захищених інформаційно–телекомунікаційних систем з метою забезпечення цілісності та доступності інформаційного потоку даних.<br>ПРН22. Обґрунтовувати і розробляти системи моніторингу та аудиту інформаційної безпеки за критеріями оцінки ризиків згідно міжнародним стандартам ISA і ISACF.<br>ПРН23. Розуміння науково-організаційних основ проведення аудиту безпеки інформаційних і комунікаційних систем.<br>Забезпечувати належне функціонування систем моніторингу та аудиту інформаційних ресурсів і процесів.<br>Впроваджувати засоби та інструменти для моніторингу процесів в інформаційно-телекомунікаційних системах.<br>ПРН24. Вирішувати в своїй професійній діяльності задачі практичного застосування розслідувань інцидентів порушення інформаційної та кібернетичної безпеки за принципами IOCE/ SWDGE. Забезпечувати конфігурування та функціонування систем моніторингу та аудиту ресурсів та процесів.<br>Вміння спілкуватись, включаючи усну та письмову комунікацію українською мовою та однією з іноземних мов (англійською, німецькою, італійською, французькою, іспанською). |
| **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.<br>Матеріали навчально-методичного забезпечення освітньої програми викладені в репозитарії НАУ за посиланням: http://er.nau.edu.ua/handle/NAU/9162<br>Всі ресурси науково-технічної бібліотеки доступні через сайт університету: http://www.lib.nau.edu.ua<br>Читальний зал забезпечений бездротовим доступом до мережі Інтернет.<br>Електронний репозитарій наукової бібліотеки НАУ: http://er.nau.edu.ua |
| | | |
| 9.1. | Національна кредитна мобільність | Двосторонні договори між НАУ та Технічним університетом України (КПІ) та Харківським національним університетом радіоелектроніки. |
| 9.2. | Міжнародна кредитна мобільність | У рамках Еразмус+К1 договір про співробітництво між НАУ та навчальними закладами ЕС |
| 9.3. | Навчання іноземних здобувачів вищої освіти | Основні навчальні модулі забезпечені навчально-методичним комплексами для іноземних здобувачів вищої освіти. |

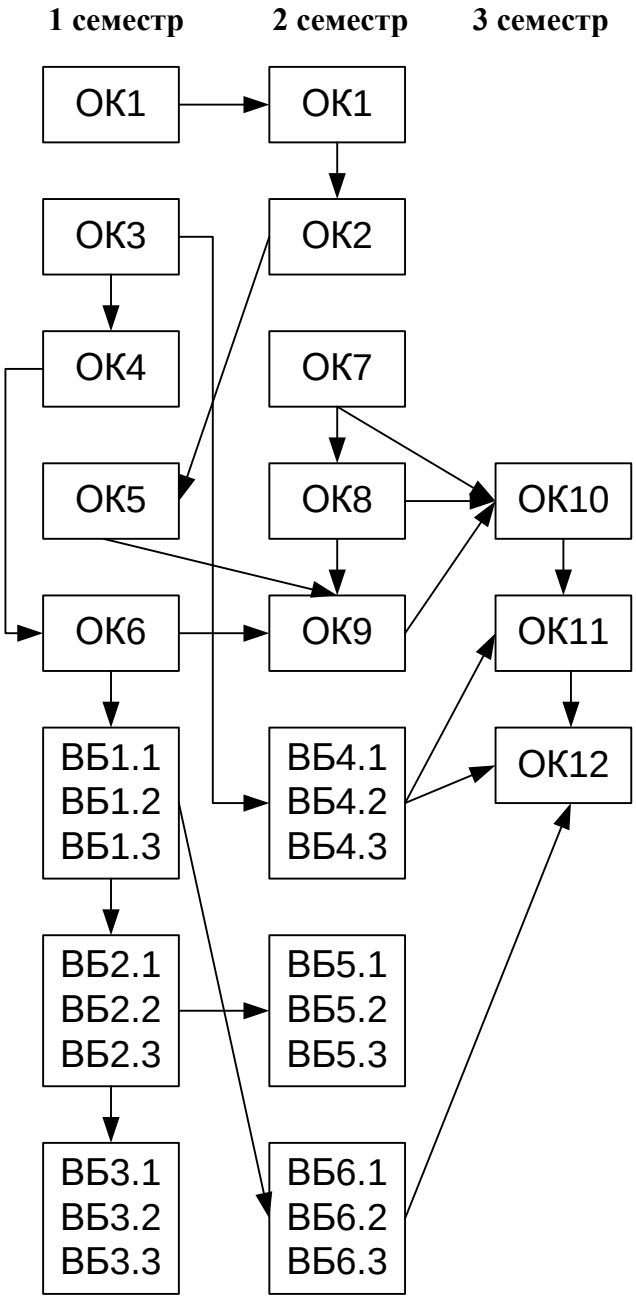
# 2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

## 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. | Ділова іноземна мова | 4.0 | Диф.залік |
| ОК2. | Наукові комунікації у фаховій діяльності | 4.0 | Диф.залік |
| ОК3. | Методи побудови та аналізу криптосистем | 4.0 | Екзамен |
| ОК4. | Методи моделювання та оптимізація процесів в сфері захисту інформації | 4.0 | Екзамен |
| ОК5. | Методологія та організація наукових досліджень | 4.0 | Екзамен |
| ОК6. | Автоматизоване проектування технічних засобів захисту інформації+КП (курсовий проект) | 5.0 | Екзамен |
| ОК7. | Захист комунікаційних мереж засобами Cisco | 4.5 | Екзамен |
| ОК8. | Технології створення та застосування систем захисту кібернетичного простору | 4.5 | Екзамен |
| ОК9. | Науково-дослідна практика (наукове стажування) | 3.0 | Диф.залік |
| ОК10. | Переддипломна практика | 7.5 | Диф.залік |
| ОК11. | Кваліфікаційний екзамен | 1.5 | Екзамен |
| ОК12. | Виконання дипломної роботи | 21.0 | Захист |
| **Загальний обсяг обов'язкових компонент:** | | 67 кредитів | |
| **Вибіркові компоненти ОПП** | | | |
| *Вибірковий блок 1* | | | |
| ВБ 1.1. | Стандартизація, сертифікація засобів та комплексів захисту інформації | 3.5 | Диф.залік |
| ВБ 1.2. | Сертифікація програмних і технічних засобів захисту | 3.5 | Диф.залік |
| ВБ 1.3. | Атестація комплексів технічного захисту інформації | 3.5 | Диф.залік |
| *Вибірковий блок 2* | | | |
| ВБ 2.1. | Методологічні засади кібербезпеки | 3.5 | Диф.залік |
| ВБ 2.2. | Кібернетична безпека | 3.5 | Диф.залік |
| ВБ 2.3 | Захист кіберінфраструктури | 3.5 | Диф.залік |
| *Вибірковий блок 3* | | | |
| ВБ 3.1. | Проектування WEB-додатків | 4.0 | Диф.залік |
| ВБ 3.2. | Організація WEB-додатків загального призначення | 4.0 | Диф.залік |
| ВБ 3.3. | Системи безпеки WEB-додатків | 4.0 | Диф.залік |

| | | | |
|---|---|---|---|
| *Вибірковий блок 4* | | | |
| ВБ 4.1. | Технологія організації інфраструктури відкритих ключів | 4.0 | Екзамен |
| ВБ 4.2. | Інфраструктура відкритих ключів: технології, архітектура та впровадження | 4.0 | Екзамен |
| ВБ 4.3 | Організація та архітектура інфраструктури відкритих ключів | 4.0 | Екзамен |
| *Вибірковий блок 5* | | | |
| ВБ 5.1. | Технології стиску інформаційних потоків | 4.0 | Диф.залік |
| ВБ 5.2. | Методи та моделі завадостійкості кодування | 4.0 | Диф.залік |
| ВБ 5.3. | Теорія та методи ідентифікації аудіо сигналів | 4.0 | Диф.залік |
| *Вибірковий блок 6* | | | |
| ВБ 6.1. | Моніторинг та аудит кібернетичного простору | 4.0 | Диф.залік |
| ВБ 6.2. | Аудит кіберінфраструктури | 4.0 | Диф.залік |
| ВБ 6.3. | Аналіз кібернетичного простору | 4.0 | Диф.залік |
| **Загальний обсяг вибіркових компонент** | | 23 кредита | |
| **Загальний обсяг освітньо-професійної програми** | | 90 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 магістра із присвоєнням кваліфікації:

2149.1 Науковий співробітник (інформаційна безпека)

2149.2 Професіонал з безпеки інформаційних і комунікаційних систем

# 4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

| | ОК1 | ОК2 | ОК3 | ОК4 | ОК5 | ОК6 | ОК7 | ОК8 | ОК9 | ОК10 | ОК11 | ОК12 | ВБ 1.1; ВБ .1.2; ВБ 1.3 | ВБ 2.1; ВБ 2.2; ВБ 2.3 | ВБ 3.1; ВБ 3.2; ВБ 3.3 | ВБ 4.1; ВБ 4.2; ВБ 4.3 | ВБ 5.1; ВБ 5.2; ВБ 5.3 | ВБ 6.1; ВБ 6.2; ВБ 6.3 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ЗК1 | | + | + | | + | | | | | | | | | | | | | |
| ЗК2 | | | | | + | | | | | | | | | + | | | | |
| ЗК3 | | | | | | | + | | + | | | + | + | | | | | |
| ЗК4 | + | | | | + | | | | | | | + | | | | | | |
| ЗК5 | | + | | | | | | | + | | | | | | | | | |
| ЗК6 | | | | | | | + | + | | | | + | | + | + | | + | |
| ЗК7 | | | | | | | | | | | + | + | | | | | | |
| ЗК8 | | | | | | | | | | | | | + | | + | | | + |
| ЗК9 | | | | | + | | | | + | | | | | | | | | |
| ЗК10 | | | | + | + | + | | | | | | | | | | + | | + |
| ФК1 | | | | | | + | + | | + | + | | | + | | + | | | |
| ФК2 | | | + | + | + | | | + | + | | | | | + | | + | + | |
| ФК3 | | | | | | + | | + | | | | | + | + | + | | | |
| ФК4 | | | | | | | + | | + | + | | | | | + | | | |
| ФК5 | | | + | + | | | | | | | | | | | | + | + | |
| ФК6 | | | | | | | | + | + | + | | + | | + | + | + | | |
| ФК7 | | | | + | | + | | | + | | | + | | | | + | + | |
| ФК8 | | | | | | | | + | | | | | + | + | + | | | + |
| ФК9 | | + | | | + | | | | + | | | + | | | | | | |
| ФК10 | | | + | + | | + | | + | | + | | + | | | | + | + | |
| ФК11 | | + | | | + | | | + | | | | | | + | | | | + |
| ФК12 | | | | + | | + | | | + | | | | + | | + | + | + | + |
| ФК13 | | + | | + | + | | | | | | | | | + | | | | |

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

| | ОК1 | ОК2 | ОК3 | ОК4 | ОК5 | ОК6 | ОК7 | ОК8 | ОК9 | ОК10 | ОК11 | ОК12 | ВБ 1.1; ВБ .1.2; ВБ 1.3 | ВБ 2.1; ВБ 2.2; ВБ 2.3 | ВБ 3.1; ВБ 3.2; ВБ 3.3 | ВБ 4.1; ВБ 4.2; ВБ 4.3 | ВБ 5.1; ВБ 5.2; ВБ 5.3 | ВБ 6.1; ВБ 6.2; ВБ 6.3 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**(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 | | | | |

# РЕЦЕНЗІЯ-ВІДГУК
на освітньо-професійну програму
«Безпека інформаційних і комунікаційних систем»

Якісна підготовка здобувачів вищої освіти в сфері забезпечення інформаційної безпеки та/або кібербезпеки, на теперішній час для України є важливим завданням. Така потреба викликана необхідністю забезпечення необхідного рівня захищеності інформації, захисту прав і свобод громадян в сучасних умовах. Національний авіаційний університет має в своєму арсеналі досвід, потужний кадровий потенціал та матеріально-технічну базу аби виконати таке завдання.

Рецензована освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека» щодо підготовки фахівців освітнього ступеня «Магістр» розроблена співробітниками Навчально-наукового інституту комп'ютерних інформаційних технологій після консультацій із науковцями, потенційними роботодавцями, які підтвердили потребу підготовці фахівців цієї спеціальності.

В освітньо-професійній програмі визначені програмні компетентності виходячи із видів і завдань у галузі забезпечення інформаційної безпеки та\або кібербезпеки. Вони розподілені на загальні та фахові компетентності, найбільш відповідні для запропонованої програми. Загальні компетентності не залежать від предметної області, але важливі для успішної подальшої професійної та соціальної діяльності фахівця у галузі забезпечення інформаційної безпеки та\або кібербезпеки. Фахові компетентності в повній мірі залежать від предметної області, та є важливими для успішної професійної діяльності за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека». Фахові компетентності охоплюють технології і процеси забезпечення та управління інформаційною і\або кібербезпекою об'єктів, що підлягають захисту. Чітка характеристика фахових компетентностей відображає сучасні тенденції розвитку інформаційних технологій та забезпечення інформаційної безпеки і\або кібербезпеки, що дозволить максимізувати працевлаштування та конкурентоспроможність випускників на вітчизняному та міжнародному ринку праці.

Навчальний план підготовки щодо підготовки фахівців освітнього ступеня «Магістр» за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека» повністю відповідає завданням освітньо-професійної програми.

Послідовність вивчення дисциплін, план та графік навчального процесу, перелік та обсяг нормативних та вибіркових дисциплін відповідають структурно-логічній схемі підготовки фахівців освітнього ступеня «Магістр» за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека» і покликані сприяти забезпеченню відповідності програмних результатів навчання запитам потенційних роботодавців (стейкхолдерів).

Професор кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, доктор технічних наук, професор. С.В.Толюпа

(Найменування посади керівника) (підпис) (Ініціали, прізвище)