

Вух №11-2  
Від 31.03.2023р.

## РЕЦЕНЗІЯ – ВІДГУК

на програму навчальної дисципліни  
«Спеціальні вимірювання в галузі ТЗІ»  
для підготовки другого (магістерського) рівня вищої освіти  
за спеціальністю 125 – Кібербезпека та захист інформації  
Державного університету інтелектуальних технологій і зв'язку

Програма навчальної дисципліни «Спеціальні вимірювання в галузі ТЗІ» другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» відповідає вимогам до компетенції, знань та умінь, які повинні отримати студенти щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації на об'єктах інформаційної діяльності. Також зміст програми містить теми для формування професійних компетенції, знань, умінь та навичок з професійного стандарту «Фахівець сфери захисту інформації», а саме:

– здійснювати перевірку повноти і відповідності реалізованих заходів із захисту інформації вимогам технічного завдання на створення комплексу технічного захисту інформації (або на створення КСЗІ в інформаційно-комунікаційних системах в частині вимог до захисту інформації від витоку технічними каналами), нормативно-правових актів та нормативних документів системи технічного захисту інформації;

– розробляти проекти комплексних систем захисту інформації та комплексів технічного захисту інформації багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних (відкрита інформація, службова інформація, секретна інформація з різними ступенями секретності);

– виявляти загрози для інформації, що озвучується на об'єктах інформаційної діяльності (обґрунтовувати можливість створення певних технічних каналів витоку інформації, що озвучується на конкретному об'єкті інформаційної діяльності).

Результати навчання корелюють з переліком компетентностей.

Разом з тим, для покращення програми навчальної дисципліни пропонуємо наступне:

1. Відомо що інформаційна безпека досягається впровадженням відповідного набору заходів безпеки, який охоплює політику, процеси, процедури, організаційні структури й програмні та апаратні функції. Ці заходи безпеки необхідно розробити, впровадити, здійснювати моніторинг, переглядати та, за потреби, вдосконалювати для гарантування досягнення певного рівня безпеки та бізнес-цілей організації. На нашу думку необхідно додатково розглянути звіт практик щодо заходів технічного захисту інформації на підприємстві/організації, як це визначено в стандартах серії ISO/IEC 27000.

Вважаємо, що програма навчальної дисципліни «Спеціальні вимірювання в галузі ТЗІ» є актуальною та відповідає вимогам до професійної діяльності фахівців сфери захисту інформації другого (магістерського) рівня вищої освіти.

Заступник Генерального директора



О.В. Ткаченко



Вух №11-4  
Від 31.03.2023р.

## РЕЦЕНЗІЯ – ВІДГУК

на програму навчальної дисципліни  
«Комплексні системи безпеки»  
підготовки магістрів за спеціальністю  
125 – Кібербезпека та захист інформації  
Державного університету інтелектуальних технологій і зв'язку

Навчальна програма дисципліни «Комплексні системи безпеки» підготовки магістрів за спеціальністю 125 – Кібербезпека та захист інформації в цілому відповідає вимогам до компетенцій, знань та умінь, які повинні отримати студенти – магістранти з основних принципів проектування, побудови та оптимізації інтегрованих систем безпеки. Зміст програми також містить теми для формування професійних компетенцій, знань, умінь та навичок з професійного стандарту «Фахівець сфери захисту інформації», наприклад:

- моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, призначених для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації;
- способи провадження апаратних засобів захисту інформації.

В рамках вивчення дисципліни студент повинен отримати знання щодо принципів та технологій побудови комплексних систем безпеки, архітектур, брендів та оптимальних способів застосування тощо. При цьому в рамках компетенцій застосовувати знання в практичних ситуаціях, аналізувати проектні обмеження та можливі компроміси системи безпеки інформації та впроваджувати (налаштовувати) апаратні засоби захисту інформації на об'єктах інформаційної діяльності

Результати навчання в цілому корелюються з переліком компетентностей. Кількість виділених для вивчення дисципліни кредитів 5 ECTS є достатньою. Зміст програми надає випускникові – магістру з кібербезпеки та захисту інформації необхідних компетентностей для фахової та науково-дослідної роботи у галузі комплексних систем безпеки.

Разом з тим, для покращення програми навчальної дисципліни варто відзначити наступне:

1. Потенційно додасть об'єктивності вивчення більшої кількості інтегрованих систем безпеки з оптимальною деталізацією параметрів.
2. Було б доцільним до складу лабораторного курсу включити вивчення сучасних українських систем безпеки з розширеною екосистемою, що дасть можливість вважати їх комплексними системами безпеки з адаптацією до масштабу об'єкта.

В цілому вважаємо, що програма навчальної дисципліни «Комплексні системи безпеки» відповідає низки пунктів як професійного стандарту «Фахівець сфери захисту інформації» та і стандарту вищої освіти України другого (магістерського) рівня за спеціальністю 125 – Кібербезпека. Програма відповідає сучасним тенденціям та вимогам до професійної діяльності фахівців сфери захисту інформації магістерського рівня вищої освіти.

Заступник Генерального директора

О.В. Ткаченко

Вух №11-1  
Від 31.03.2023р.

## РЕЦЕНЗІЯ – ВІДГУК

на програму навчальної дисципліни  
«Кіберфізична безпека об'єктів критичної інфраструктури»  
підготовки магістрів за спеціальністю  
125 – Кібербезпека та захист інформації  
Державного університету інтелектуальних технологій і зв'язку

Програма навчальної дисципліни «Кіберфізична безпека об'єктів критичної інфраструктури», на наш погляд, відповідає вимогам до компетенцій, знань та умінь, які повинні отримати студенти – магістранти з теоретичних основ кіберфізичної безпеки, визначення архітектурних та технічних характеристик об'єктів захисту кіберфізичних систем у критично важливих інфраструктурах, зокрема SCADA (АСУ ТП). Слід відзначити також, що кіберзахист об'єктів критичної інфраструктури України на сьогодні є надзвичайно важливим завданням, тому введення до навчального плану підготовки магістрів присвяченої цим питанням дисципліни є своєчасним та вкрай необхідним.

Програма навчальної дисципліни також містить теми для формування професійних компетенцій, знань, умінь та навичок із професійного стандарту «Фахівець сфери захисту інформації», затвердженого наказом Адміністрації Держспецзв'язку № 715 від 25.11.2022, наприклад:

- концепції архітектури безпеки мережі, включаючи технологію, протоколи, компоненти і принципи ешелонованого захисту (прикладна система ешелонованого захисту);
- мови програмування мікроконтролерів і контролерів відповідно до норм ІЕС 61131-3;
- взаємодія з керівництвом та працівниками технологічних та інших підрозділів підприємства (організації) з технологічних та інших питань, пов'язаних із забезпеченням захисту інформації та кіберзахисту (організовувати та отримувати від технологічних та інших підрозділів інформацію, необхідну для організації захисту інформації та кіберзахисту, узгоджувати та погоджувати технічну документацію на системи та комплекси захисту інформації, доводити до керівництва підрозділів недоліки у захисті інформації та пропозицій до їх усунення, пропозицій про удосконалення систем та комплексів захисту інформації;
- дослідження, розробка і супроводження систем та засобів інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

Кількість виділених для вивчення дисципліни кредитів 5 ECTS, на наш погляд, є достатньою.

Разом з тим, для покращення навчальної програми пропонуємо наступне:

1. Розробити лабораторні роботи по системам забезпечення сталості та неперервності виробничих процесів.

2. Оновити тематику практичних занять новими інтегрованими видами захисту інформації

У цілому вважаємо, що програма навчальної дисципліни «Кіберфізична безпека об'єктів критичної інфраструктури» є актуальною та відповідає сучасним вимогам до професійної діяльності фахівців сфери захисту інформації магістерського рівня вищої освіти.

Заступник Генерального директора



О.В. Ткаченко

Вух №11-5  
Від 31.03.2023р.

## РЕЦЕНЗІЯ – ВІДГУК

на програму навчальної дисципліни  
«Моніторинг та аудит інформаційно-комунікаційних систем»  
другого (магістерського) рівня вищої освіти  
за спеціальністю 125 – Кібербезпека та захист інформації  
Державного університету інтелектуальних технологій і зв'язку

Програма навчальної дисципліни «Моніторинг та аудит інформаційно-комунікаційних систем» підготовки магістрів у цілому відповідає вимогам до компетенцій, знань та умінь, які повинні отримати студенти з основних принципів аналізу, розробки і супроводження систем аудиту та моніторингу інформаційних систем і технологій. Зміст програми також містить теми для формування професійних компетенцій, знань, умінь та навичок з професійного стандарту «Фахівець сфери захисту інформації», затвердженого наказом Адміністрації Держспецзв'язку № 715 від 25.11.2022, наприклад:

- методи та технології моніторингу та аудиту загроз для конфіденційності, цілісності та доступності інформації;
- методи, засоби та інформаційні технології виявлення несанкціонованого доступу до інформації на різних ієрархічних рівнях інформаційно-комунікаційної системи;
- здійснювати моніторинг та аудит загроз для інформації в інформаційних системах та мережах та оцінку ризиків безпеки інформації;
- здійснювати моніторинг та аудит загроз для інформації, що озвучується;
- проводити аудити/огляди систем і комплексів захисту інформації (систем безпеки інформації) та інформаційно-комунікаційних систем.

Програма навчальної дисципліни «Моніторинг та аудит інформаційно-комунікаційних систем» відповідає окремим трудовим функціям стандарту «Фахівець сфери захисту інформації». У результаті вивчення навчальної дисципліни студент повинен отримати знання щодо способів сканування та розпізнавання вразливостей у системах безпеки для інформації в інформаційних системах і мережах та компетенції щодо здатності здійснювати постійний моніторинг та аудит загроз для інформації та відповідну модернізацію систем і комплексів захисту інформації.

Результати навчання в цілому корелюють з переліком компетентностей. Кількість виділених для вивчення дисципліни кредитів 5 ECTS, на наш погляд, є достатньою. Зміст програми надає випускникові – магістру з кібербезпеки та захисту інформації необхідних компетентностей для фахової та науково-дослідної роботи у галузі моніторингу та аудиту інформаційно-комунікаційних систем.

Разом з тим, для покращення програми навчальної дисципліни пропонуємо наступне:

1. В рамках систем моніторингу інформаційно-комунікаційних систем можна було б розглянути центр управління інформаційної безпеки.
2. Було б доцільним розглянути системи автоматизації моніторингу інформаційної безпеки.
3. Треба було більш детально розглянути у курсі лабораторних робіт питання протоколювання процесів у центрі інформаційної безпеки та ведення системного журналу.

Вважаємо, що програма навчальної дисципліни «Моніторинг та аудит інформаційно-комунікаційних систем» є актуальною та відповідає сучасним трендам і вимогам до професійної діяльності фахівців сфери захисту інформації магістерського рівня вищої освіти.

Заступник Генерального директора



О.В. Ткаченко



Вух №11-3  
Від 31.03.2023р.

## РЕЦЕНЗІЯ – ВІДГУК

на програму навчальної дисципліни  
«Управління доступом до інформаційних ресурсів»  
другого (магістерського) рівня вищої освіти  
за спеціальністю 125 – Кібербезпека та захист інформації  
Державного університету інтелектуальних технологій і зв'язку

Програма навчальної дисципліни «Управління доступом до інформаційних ресурсів» підготовки магістрів за спеціальністю 125 – Кібербезпека та захист інформації розроблена відповідно до вимог щодо компетенцій, знань та умінь, які повинні бути надані студентам з основних принципів побудови системи керування безпечного доступу до інформаційних ресурсів інтелектуальної мережі. У програмі передбачається формування низки професійних компетенцій, знань та умінь із затвердженого у 2022 р. професійного стандарту «Фахівець сфери захисту інформації».

Професійні компетенції:

A3. Здатність формувати стратегію і політики безпеки інформації в інформаційно-комунікаційних системах.

A6. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності.

Знання:

A3.32. Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи ешелонованого захисту (прикладна система ешелонованого захисту).

A6.35. Поняття показників захищеності інформації засобів обробки інформації та показників захищеності мовної інформації на об'єкті інформаційної діяльності.

A6.315. Статистична радіотехніка (прийом звісних сигналів на фоні шумів, оцінка параметрів сигналів, що приймаються на фоні шумів).

Уміння та навички:

A3.U1. Обґрунтовувати та розробляти політику безпеки інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

A6.U3. Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі або на об'єкті інформаційної діяльності.

Загальні і фахові компетенції та результати навчання, що отримують студенти у результаті вивчення навчальної дисципліни, відповідають діючому стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для магістерського рівня. Кількість виділених для вивчення дисципліни кредитів ECTS – 4 кредити, на наш погляд, є достатньою. Зміст програми надає випускникові необхідні компетентності для фахової та науково-дослідної роботи у галузі комплексних систем безпеки.

Разом з тим, для покращення навчальної програми пропонуємо наступне:

1. Більше детально освітити існуючі інтелектуальні мережі з аналізом забезпечення вимог по безпечному доступу до інформаційних ресурсів.

2. З урахування воєнного стану в Україні доцільно більш детально розкрити відповідні вимоги до системи управління доступу до інформаційних ресурсів користувачів мережі.

У цілому вважаємо, що програма навчальної дисципліни «Управління доступом до інформаційних ресурсів» відповідає вимогам до професійної діяльності фахівців сфери захисту інформації магістерського рівня вищої освіти.

Заступник Генерального директора

О.В. Ткаченко