**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ**

# ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «ТЕХНІЧНІ СИСТЕМИ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ» другого (магістерського) рівня вищої освіти

**Галузь знань** 12 Інформаційні технології
**Спеціальність** 125 Кібербезпека
**Освітня кваліфікація** магістр з кібернетичної безпеки
**Професійна кваліфікація** 2149.2 Професіонал із організації захисту інформації з обмеженим доступом, викладач вищих навчальних закладів

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Голова вченої ради

Протокол № 19 від «13» березня 2017 р.

Освітня програма вводиться в дію з 01.09.2017 р.

Ректор Толубко В.Б. _____/

Наказ № 83 від «15» березня 2017 р.

Київ-2017

**ЛИСТ ПОГОДЖЕННЯ**
**ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ**
**«ТЕХНІЧНІ СИСТЕМИ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ»**
**ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ**

| | |
|---|---|
| **галузь знань** | *12 «Інформаційні технології»* |
| **спеціальність** | *125 «Кібербезпека»* |
| ***спеціалізація*** | *-* |
| **рівень вищої освіти** | *другий (магістерський)* |
| **освітня кваліфікація** | *магістр з кіберентичної безпеки* |
| **професійна квліфікація** | *2149.2 Професіонал із організації захисту інформації з обмеженим доступом, викладач вищих навчальних закладів* |

1. Науково-методична рада протокол № 3 від "21" березня 2017р.

Голова науково-методичної ради _____ В.Б. Толубко

2. Навчально-науковий центр

Директор навчально-наукового центру _____ А.М. Явтушенко

3. Вчена рада Навчально-наукового інституту захисту інформації
протокол № 6 від "22" лютого 2017р.

Голова вченої ради інституту _____ В.С Наконечний

4. Кафедра систем захисту інформації
протокол № 8 від "28" 02 2017р.

Завідувач кафедри _____ С.В.Лазоренко

5. Рецензії від зовнішніх – стейкхолдерів (фірм-партнерів):

1. Державне підприємство Український науково-технічний і впроваджувальний центр комплексного захисту інформації (Український центр «Безпека»)

2. Товариство з обмеженою відповідальністю «Інфосейф ІТ»

**продовження**

# ЛИСТ ПОГОДЖЕННЯ
# ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
# «ТЕХНІЧНІ СИСТЕМИ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ»
## ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

**галузь знань** *12 «Інформаційні технології»*
**спеціальність** *125 «Кібербезпека»*
**рівень вищої освіти** *другий (магістерський)*
**освітня кваліфікація** *магістр з кібернетичної безпеки*
**професійна кваліфікація** *2149.2 Професіонал із організації захисту інформації з обмеженим доступом, викладач вищих навчальних закладів*

Представники професійної асоціації (ринку праці):

1. Державне підприємство «Український науково-технічний і впроваджувальний центр комплексного захисту інформації» (Український центр «Безпека»).

2. Товариство з обмеженою відповідальністю «Інфосейф ІТ».

**«ПОГОДЖЕНО»**

Директор Державного підприємства «Український науково-технічний і впроваджувальний центр комплексного захисту інформації» (Український центр «Безпека»)

_____ В.Г. Глазунов

**«ПОГОДЖЕНО»**

Директор Товариства з обмеженою відповідальністю «Інфосейф ІТ»

_____ В.В. Жора

## Передмова

1. Розроблено проектною групою Державного університету телекомунікацій у складі:

**Керівник – Зибін Сергій Вікторович** – доцент кафедри комп'ютерні системи та мережі Навчально-наукового інституту телекомунікацій та інформатизації, кандидат технічних наук зі спеціальності 125 Кібербезпека ( 05.13.21 – системи технічного захисту інформації), доцент кафедри комп'ютерних систем та мереж;

**Члени проектної групи:**

**Бурячек Володимир Леонідович** – завідувач кафедри інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації, доктор технічних наук зі спеціальності 125 Кібербезпека ( 20.05.01- інформаційна безпека держави), професор кафедри інформаційної та кібернетичної безпеки ;

**Семко Віктор Володимирович** – доцент кафедри інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації, кандидат технічних наук зі спеціальності 255 – Озброєння та військова техніка ( 20.02.14 – озброєння та військова техніка), доцент кафедри інформаційної та кібернетичної безпеки)

## 1. Профіль освітньої програми

| 1 – Загальна інформація | |
|---|---|
| **Повна назва вищого навчального закладу та структурного підрозділу** | Державний університет телекомунікацій, Навчально-науковий інститут захисту інформації |
| **Ступінь вищої освіти та назва кваліфікації мово оригіналу** | Магістр<br>Освітня кваліфікація – магістр з кібернетичної безпеки |
| **Офіційна назва освітньої програми** | Освітньо-професійна програма «Технічні системи інформаційного та кібернетичного захисту» |
| **Тип диплому та обсяг освітньої програми** | Диплом магістра, одиничний<br>Обсяг освітньої програми-90 кредитів ЄКТС; термін навчання 1,5 роки |
| **Наявність акредитації** | Розробляється вперше |
| **Цикл/рівень** | НРК України – 7 рівень/ Магістр,<br>QF-EHEA- другий цикл,<br>EQF-LLL – 7 рівень |
| **Передумови** | Наявність ступеня бакалавра або магістра іншої спеціальності |
| **Мова(и) викладання** | Українська, англійська |
| **Термі дії освітньої програми** | Введена в дію з 01.09.2017 року |
| **Інтернет - адреса постійного розміщення опису освітньої програми** | http://www.dut.edu.ua/ua/1748-pidgotovka-magistriv-kafedra-sistem-informaciynogo-ta-kibernetichnogo-zahistu |

| 2 – Мета освітньої програми |
|---|
| Метою магістерської програми є підготовка висококваліфікованих фахівців магістрів з кібернетичної безпеки, які здатні проводити наукові дослідження, здійснювати професійну діяльність у системі державних та комерційних підприємств пов'язаної з наданням послуг щодо захисту інформації на об'єктах інформаційної діяльності, здійснювати апробацію та практичне впровадження наукових результатів, які володіють інноваційними компетентностями, необхідними для ефективного захисту інформації на об'єктах інформаційної діяльності, і здатні вирішувати практичні та науково-дослідні завдання.<br>Набуті компетентності можуть бути застосовані в дослідницьких, управлінських, освітніх, підриємницьких та інших дисциплінарно-професійних полях. |

| 3 - Характеристика програми | | |
|---|---|---|
| **1** | **Предметна область, Напрям (галузь знань, спеціальність)** | 12 Інформаційні технології<br>125 Кібербезпека |

| | | |
|---|---|---|
| 2 | **Основний фокус освітньої програми та спеціалізації** | Загальна: дослідження в області практики та науки захисту інформації. Акцент на організації та забезпечення інформаційної безпеки на об'єктах інформаційної діяльності |
| 3 | **Орієнтація освітньої програми** | Освітньо-професійна. Програма носить прикладний характер, спрямована на забезпечення потреб ринку праці, зокрема в IT галузі |
| 4 | **Особливості програми** | Програма передбачає обов'язкове курсове професійне навчання з метою отримання майбутнім фахівцем кваліфікації фахівця захисту інформації в інформаційних і комунікаційних системах. Передбачена практика, з метою забезпечення умов підготовки фахівця в реальному середовищі майбутньої професійної діяльності. Залучення до викладацької діяльності керівників та професіоналів, які працюють в системі інформаційної безпеки, а також представників бізнесу, з метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки.<br>Реалізація процесного підходу при конструюванні змісту профільно-орієнтованих навчальних дисциплін.<br>Реалізація студентської мобільності, академічної співпраці та молодіжних обмінів. |
| **4 – Придатність випускників до працевлаштування та подальшого навчання** | | |
| 1 | **Придатність до працевлаштування** | Магістр з кібернетичної безпеки (випускник) здатний виконувати професійні роботи за Державним класифікатором професій ДК 003: 2010:<br>**Основна:**<br>**20289** - Професіонал із організації захисту інформації з обмеженим доступом<br>**Допоміжна:**<br>**20289** - Професіонал із організації інформаційної безпеки<br>**2310.2** – Викладач вищого навчального закладу |
| 2 | **Подальше навчання** | Можливість продовжувати освіту за третім (освітньо-науковим) освітнім рівнем вищої освіти |
| **5 – Викладання та оцінювання** | | |
| **Викладання та навчання** | | **Стиль навчання:**<br>поєднання репродуктивного та творчого стилів навчання як взаємодоповнюючих з домінуючим творчим компонентом;<br>емоційно-ціннісний стиль навчання з поєднанням |

| | |
|---|---|
| | емоційно-імпровізаційного та емоційно-методичного стилів.<br>**Методика навчання:**<br>узгодження декількох навчальних технологій: інформаційної технології навчання; технології моделюючого навчання; розвивальної технології навчання; активізуючої технології навчання; технології виробничого навчання; технології випереджаючого навчання, технології дистанційного навчання.<br>**Організація навчального процесу:**<br>кредитно-модульна система. |
| **Оцінювання** | Письмові та усні екзамени, наукові есе, тестування знань, усні презентації, поточний контроль, звіти про практику, захист магістерської роботи. |
| **6 - Програмні компетенції** | |
| **Загальні компетентності (ЗК)** | **ЗК-1.** Здатність визначати та задовольняти потреби особистого та наукового розвитку, бути критичним і самокритичним.<br>**ЗК-2.** Вміння використовувати інформаційні і комунікаційні технології для впровадження проектів в інформаційній та безпековій сферах.<br>**ЗК-3.** Здатність до організації, планування й оперативного управління охороною праці в структурних підрозділах підприємств.<br>**ЗК-4.** Здатність допомагати через викладання, наставництво та наочні приклади (демонстрацію).<br>**ЗК-5.** Вміння визначати, поважати та керувати етичними, культурними та іншими питаннями, пов'язаними з наявністю тих чи інших відмінностей.<br>**ЗК-6.** Вміння визначати підприємницькі можливості чи вид діяльності або громадського впливу, здатність приймати обґрунтовані рішення, здатність оцінювати та забезпечувати якість виконуваних робіт.<br>**ЗК-7.** Вміння виявляти, ставити та вирішувати проблеми.<br>**ЗК-8.** Вміння розробляти математичні моделі завдань забезпечення інформаційної безпеки та захисту інформації |

| | |
|---|---|
| **Фахові компетентності спеціальності (ПП; ППк)** | **ПП-1.** Здатність до виявлення та формування актуальних наукових проблем, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією.<br>**ПП-2.** Здатність до обґрунтування та реалізації системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності.<br>**ПП-3**. Здійснювати організаційно-правове забезпечення ліцензування діяльності, пов'язаної з проведенням робіт та надання послуг у галузі забезпечення захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності.<br>**ПП-4.** Здатність до використання інформаційні технології як в побуті, так і в професійній діяльності.<br>**ПП-5**. Здатність до накопичення наукових і педагогічних вмінь та навичок (діагностування й інтерпретування ситуацій, планування та здійснення наукових досліджень, викладання у вищому навчальному закладі предметів, що відносяться до галузі інформаційних технологій та захисту інформації); здатність до генерування нових знань з теорії захисту інформації та інформаційної безпеки, з проблем алгоритмізації та програмування процесів в системах кібербезпеки; тощо.<br>**ПП-6.** Здатність до оволодіння спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та без пековими технологіями; здатність до застосування різноманітних, професійно профільованих знань і практичних навичок у сфері захисту інформації.<br>**ПП-7.** Здатність до виробничо-технологічної діяльності (розробки та впровадження раціональних технологій інформаційної безпеки, вибору технології ІБ, устаткування та засобів, використання інформаційних технологій; розробки програм і методик випробувань систем інформаційної та кібербезпеки). |

| | |
|---|---|
| | **ПП-8.** Здатність до планування й реалізації заходів із захисту інформації в ІКС; створення та забезпечення функціонування систем інформаційної та кібербезпеки; здатність до формування правильних висновків, оперативного приймання та реалізації нестандартних рішень тощо.<br>**ПП-9**. Здатність до проектування перспективних систем захисту інформації, застосовувати сучасні методи і засоби їх аналізу та побудови.<br>**ПП-10**. Здатність до підтримання комплексних систем інформаційної та кібербезпеки в стані, необхідному для вирішення завдань захисту інформації.<br>**ПП-11**. Здатність до розробки алгоритмів, методик, моделей та складних програмних комплексів оцінки характеристик і стану систем інформаційної та кібербезпеки.<br>**ПП-12**. Здатність до розробки та впровадження дослідницьких проектів у галузі знань «інформаційні технології» спеціальності «Кібербезпека» для забезпечення безпеки об'єктів інформаційної діяльності.<br>**ПП-13**. Здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем, до обробки та перетворення інформації тощо.<br>**ПП-14**. Здатність до проведення сертифікаційних аудитів на об'єктах інформаційної діяльності.<br>**ПП-15.** Здатність до управління розробкою та впровадженням системи автоматизованого оброблення інформації з обмеженим доступом.<br>**ППк-1.** Здатність до розроблення методик аналізу, синтезу, оптимізації та прогнозування якості процесів захисту конфіденційної інформації на об'єктах інформаційної діяльності.<br>**ППк-2**. Здатність до орієнтування у сучасних концепціях і моделях, методах та засобах управління інцидентами інформаційної боротьби<br>**ППк-3**. Виходячи зі знання теорії інформаційних ресурсів обмеженого доступу здійснювати вибір методів і засобів забезпечення захисту інформації з обмеженим доступом.<br>**ППк-4**. Виходячи із основних характеристик та моделей радіоелектронних каналів витоку інформації здійснювати обґрунтування варіантів |

| | |
|---|---|
| | використання методів та засобів протидії витоку інформації з обмеженим доступом радіоелектронними каналами.<br>**ППк-5**. Здатність спілкуватися результативно в усній і письмовій формах з фахівцями та нефахівцями, здатність спілкуватися другою мовою. |
| **7 - Програмні результати навчання** | |
| | **ПРН-1.** Уміти формувати і аргументовано відстоювати власну<br>позицію з різних проблем філософії науки та методології наукового пізнання.<br>**ПРН-2.** Уміти визначати та задовольняти потреби особистого та наукового розвитку, бути критичним і самокритичним<br>**ПРН-3**. Уміти ставити і вирішувати завдання з проблем самоактуалізації особистості, саморозвитку, самоосвіти, самовиховання та самоорганізації.<br>**ПРН-4**. Уміти вести дискусії і полеміки, здійснювати публічні промови, робити повідомлення і доповіді з питань дисертаційного дослідження, аргументовано викладати власну точку зору державною та іноземною мовою.<br>**ПРН-5**. Уміти читати оригінальну наукову літературу на іноземній мові, опрацьовувати та оформляти інформацію<br>**ПРН-6.** Уміти розробляти логічні схеми, складати план-проспекти та технічні завдання на виконання наукових досліджень.<br>**ПРН-7**. Уміти обґрунтовувати та реалізовувати системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності.<br>**ПРН-8.** Уміти моделювати структуру наукового дослідження, формулювати мету, об'єкт, предмет та наукові задачі, упорядковувати та систематизувати результати дослідження, обґрунтовувати їх достовірність та проводити їх апробацію.<br>**ПРН-9**. Уміти здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на |

| | |
|---|---|
| | об'єктах інформаційної діяльності.<br>**ПРН-10**. Уміти здійснювати оцінку системи захисту інформації автоматизованої системи своєму призначенню відповідно до вимог діючих стандартів та нормативних документів.<br>**ПРН-11**. Володіти вмінням демонструвати своєчасність та плановість у науковому дослідженні, спроможність управляти науковими проектами.<br>**ПРН-12**. Володіти вмінням формувати технології розроблення комплексів засобів захисту інформації з обмеженим доступом та охорони обєктів інформаційної діяльності.<br>**ПРН-13**. Уміти застосовувати тпові підходи до проектування захищених обєктів інформаційної діяльності.<br>**ПРН-14.** Уміти здійснювати обґрунтування варіантів використання методів та засобів радіомоніторингу об'єктів інформаційної безпеки, їх основних складових, узагальнювати і критично оцінювати результати отримані вітчизняними і зарубіжними дослідниками.<br>**ПРН-15**. Уміти обґрунтовувати варіанти використання методів та засобів протидії витоку інформації з обмеженим доступом радіоелектронними каналами.<br>**ПРН-16**. Уміти розробляти проекти комплексів засобів захисту та охорони об'єктів інформаційної діяльності.<br>**ПРН-17**. Уміти розробляти проектну документацію, програми і методики випробувань.<br>**ПРН-18.** Здійснювати розроблення методик аналізу, синтезу, оптимізації та прогнозування якості процесів захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності.<br>**ПРН-19**. Уміти визначати основні параметри інформаційних ресурсів наукового дослідження (навчального процесу), планувати структуру, зміст та процес організації його проведення (лекцій, практично-семінарських занять).<br>**ПРН-20.** Уміти організовувати та здійснювати проведення сертифікації у галузі захисту інформації з обмеженим доступом та охорони об'єктів |

| | |
|---|---|
| | інформаційної діяльності відповідно до міжнародних стандартів.<br>**ПРН-21**. Уміти оформляти аудиторський звіт, що містить оцінку поточного стану рівня безпеки, інформацію про виявлені проблеми, аналіз відповідних ризиків та рекомендації<br>щодо їх усунення.<br>**ПРН-22.** Уміти демонструвати володіння предметною базою знань та сучасними техніками наукового дослідження, здатність створювати та інтерпретувати нові знання.<br>**ПРН-23.** Уміти оформляти документи на одержання сертифікату відповідності.<br>**ПРН-24**. Організовувати та здійснювати збирання даних від замовника, здійснювати їх попередній аналіз та планування заходів з підготовки та проведення сертифікаційного аудиту на об'єктах інформаційної діяльності.<br>**ПРН-25**. Уміти розробляти проекти комплексів засобів захисту та охорони об'єктів інформаційної діяльності.<br>**ПРН-26**. Уміти застосовувати сучасні способи, методи та засоби захисту автоматизованої системи: політику безпеки, архітектуру захисту, механізми захисту та засоби захисту.<br>**ПРН-27**. Уміти проводити інструктажі, наради та технічні заняття з працівниками підприємства чи його підрозділу з питань охорони праці та нових законодавчих і правових актів України з охорони праці, пожежної та промислової безпеки.<br>**ПРН-28**. Уміти розробляти та тестувати імітаційні моделі, використовуючи мову імітаційного моделювання<br>**ПРН-29**. Уміти використовувати математичні методи оптимізації з метою одержання найкращих характеристики функціонування засобів та систем |
| **8 – Ресурсне забезпечення реалізації програми** | |
| **Кадрове забезпечення** | Висококваліфікований науково-педагогічний склад, який включає провідних науковців у напряму захисту інформації |
| **Матеріально-технічне забезпечення** | Використання обладнання для пошуку технічних каналів витоку інформації::<br>скануючий приймач AR8200;<br>скануючи приймач ICR20; |

| | |
|---|---|
| | детектор електромагнітного поля Protect 1206;<br>детектор електромагнітного поля Protect 1210;<br>детектор нелінійних переходів NR 90;<br>програмно-апаратний комплекс DjScan^<br>пошуковий комплекс ST-032. |
| **Інформаційне та навчально-методичне забезпечення** | Всі дисципліни навчального плану забезпечені інформаційними та навчально-методичними матеріалами, у т.ч. засобами системи дистанційного навчання Moodle |
| **9 – Академічна мобільність** | |
| **Національна кредитна мобільність** | Наявність двосторонніх договорів між ДУТ та вищими навчальними закладами України забезпечує національну кредитну мобільність |
| **Міжнародна кредитна мобільність** | Зміст навчання відповідає світовим освітнім стандартам, що дозволяє приймати участь у програмах подвійних дипломів та бути конкурентоспроможним на світовому ринку праці |
| **Навчання іноземних здобувачів вищої освіти** | Дозволяє можливість навчання іноземним громадянам |

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

### 2.1. Зміст підготовки за освітньою програмою компетентності та результатами навчання

| № п.п. | Дисципліна | Шифр | Компетентність | Результат навчання |
|---|---|---|---|---|
| **Цикл дисциплін загальної підготовки** | | | | |
| 1. | Захист професійної діяльності в галузі | ЗК.12.1.01 | ЗК3 | ПРН-27 |
| 2. | Організація проведення наукових досліджень | ЗК.12.1.02 | ЗК-2,<br>ЗК-6, ЗК-7 | ПРН-1,<br>ПРН-11<br>ПРН-19<br>ПРН-8 |
| 3. | Педагогіка та психологія | ЗК.12.1.03 | ЗК-1, ЗК-4,<br>ЗК-5 | ПРН-2 |
| 4. | Математичні методи моделювання та оптимізації | ЗК.12.1.04 | ЗК-8 | ПРН-28<br>ПРН-29 |
| **Цикл дисциплін професійної підготовки** | | | | |
| 1. | Ліцензування, атестація та сертифікація у сфері | ПП.12.2.01 | ПП-3<br>ПП-13 | ПРН-17<br>ПРН-20 |

| | | | | |
|---|---|---|---|---|
| | безпеки обєктів інформаційної діяльності | | ПП-14 | |
| 2. | Автоматизація обробки інформації з обмеженим доступом | ПП.12.2.02 | ПП-15<br>ПП-13<br>ПП-10 | ПРН-10 |
| 3. | Технологія створення та застосування комплексів захисту інформації з обмеженим доступом та охорони обєктів інформаційної діяльності | ПП.12.2.03 | ПП-9<br>ПП-8<br>ПП-2 | ПРН-25<br>ПРН-15<br>ПРН-12 |
| 4. | Теорія захисту інформаційних ресурсів обмеженого доступу | ПП.12.2.04 | ПП-4 | ПРН-7<br>ПРН-26 |
| 5. | Радіомоніторинг і радіопротидія на обєктах інформаційної діяльності | ПП.12.2.05 | ПП-6 | ПРН-14 |
| 6. | Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності | ПП.12.2.06 | ПП-11<br>ПП-12 | ПРН-10<br>ПРН-23 |
| 7. | Науково-педагогічна практика | ПП.12.2.07 | ПП-5 | ПРН-3 |
| 8. | Науково-дослідна практика | ПП.12.2.08 | ПП-1 | ПРН-6<br>ПРН-22 |
| 9. | Переддипломна практика | ПП.12.2.09 | ПП-7 | ПРН-3 |
| 10. | Дипломне проектування, державна атестація | ПП.12.2.10 | ПП-1 | ПРН-25 |
| **Дисципліни вільного вибору студента** | | | | |
| 1. | Іноземна мова (за фаховим спрямуванням) | ППк.12.3.1.01 | ППк-5 | ПРН-5<br>ПРН-4 |
| 2. | Системи контролю та управління доступом на обєкті інформаційної діяльності | ППк.12.3.2.01 | ППк-3 | ПРН-9 |
| 3. | *Технології виявлення уразливостей та протидії злоякісному* | ППк.12.3.2.02 | ППк-3 | ПРН-9 |

| | | | | |
|---|---|---|---|---|
| | *програмному забезпеченню* | | | |
| 4. | Вплив потужних полів на електронні засоби та методи їх захисту | ППк.12.3.2.03 | ППк-4 | ПРН-15 |
| 5. | *Технології виявлення уразливостей та забезпечення безпеки Web-ресурсів* | ППк.12.3.2.04 | ППк-1 | ПРН-26 |
| 6. | Організація захисту конфіденційної інформації | ППк.12.3.2.05 | ППк-1 | ПРН-13 ПРН-16 |
| 7. | *Управління інцидентами інформаційної безпеки* | ППк.12.3.2.06 | ППк-1 | ПРН-13 ПРН-16 |
| 8. | Аналіз та оптимізація процесів і систем технічного захисту інформації | ППк.12.3.2.07 | ППк-2 | ПРН-18 |
| 9. | *Технологія виявлення уразливостей мережевих ресурсів* | ППк.12.3.2.08 | ППк-3 | ПРН-9 ПРН-10, ПРН-12 |

**2.2. Перелік компонент ОП**

| Код н/д | Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота) | Кількість кредитів | Форма підсумк. контролю |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| **Обов'язкові компоненти ОП** | | | |
| **Цикл загальної підготовки** | | | |
| ЗК12.1.01 | Захист професійної діяльності в галузі | 3 | Іспит |
| ЗК12.1.02 | Організація проведення наукових досліджень | 3 | Залік |
| ЗК12.1.03 | Педагогіка та психологія | 3 | Залік |
| ЗК12.1.04 | Математичні методи моделювання та оптимізації | 3 | Залік |
| **Цикл професійної підготовки** | | | |
| ПП12.2.01 | Ліцензування, атестація та сертифікація у сфері безпеки обєктів інформаційної діяльності | 5 | Іспит |
| ПП12.2.02 | Автоматизація обробки інформації з обмеженим доступом | 3 | Іспит |
| ПП12.2.03 | Технологія створення та застосування комплексів захисту інформації з обмеженим доступом та охорони обєктів інформаційної діяльності | 5 | Іспит |
| ПП12.2.04 | Теорія захисту інформаційних ресурсів обмеженого доступу | 4 | Залік |
| ПП12.2.05 | Радіомоніторинг і радіопротидія на обєктах | 4 | Залік |

| | | | |
|---|---|---|---|
| | інформаційної діяльності | | |
| ПП12.2.06 | Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності | 4 | Іспит |
| ПП12.2.07 | Науково-педагогічна практика | 6 | Залік |
| ПП12.2.08 | Науково-дослідницька практика | 6 | Залік |
| ПП12.2.09 | Переддипломна практика | 9 | Залік |
| ПП12.2.10. | Дипломне проектування. Державна атестація | 9 | Іспит |
| **Загальний обсяг обов'язкових компонент:** | | **67** | |
| **Вибіркові компоненти ОП** | | | |
| ПКк.12.3.1.01 | Іноземна мова (за фаховим спрямуванням) | 5 | Залік |
| *Вибірковий блок 1* | | | |
| ПКк.12.3.2.01 | Системи контролю та управління доступом на обєкті інформаційної діяльності | 4 | Залік |
| ПКк.12.3.2.02 | *Технології виявлення уразливостей та протидії злоякісному програмному забезпеченню* | | |
| *Вибірковий блок 2* | | | |
| ПКк.12.3.2.03 | Вплив потужних полів на електронні засоби та методи їх захисту | 4 | Іспит |
| ПКк.12.3.2.04 | *Технології виявлення уразливостей та забезпечення безпеки Web-ресурсів* | | |
| *Вибірковий блок 3* | | | |
| ПКк.12.3.2.05 | Організація захисту конфіденційної інформації | 6 | Іспит |
| ПКк.12.3.2.06 | *Управління інцидентами інформаційної безпеки* | | |
| *Вибірковий блок 4* | | | |
| ПКк.12.3.2.07 | Аналіз та оптимізація процесів і систем технічного захисту інформації | 4 | Залік |
| ПКк.12.3.2.08 | *Технологія виявлення уразливостей мережевих ресурсів* | | Залік |
| **Загальний обсяг вибіркових компонент:** | | **23** | |
| **ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ** | | **90** | |

## 2.3. Структурно-логічна схема ОП

| Цикл | I курс | | | | II курс | | Всього | |
|---|---|---|---|---|---|---|---|---|
| | 1 семестр | | 2 семестр | | 3 семестр | | Кр. | % |
| Цикл загальної підготовки | Захист професійної діяльності в галузі | 3 | | | | | | |
| | | | Організація проведення наукових досліджень | 3 | | | | |
| | | | Педагогіка та психологія у вищій школі | 3 | | | | |
| | | | Математичні методи моделювання та оптимізації | *3* | | | **12** | **13,4** |
| Цикл професійної підготовки | | | Ліцензування, атестація та сертифікація у сфері безпеки обєктів інформаційної діяльності | 5 | | | | |
| | Автоматизація обробки інформації з обмеженим доступом | 3 | | | | | | |
| | Технологія створення та застосування комплексів захисту інформації з обмеженим доступом та охорони обєктів інформаційної діяльності | 5 | | | | | | |
| | Теорія захисту інформаційних ресурсів обмеженого доступу | 4 | | | | | | |
| | | | Радіомоніторинг і радіопротидія на обєктах інформаційної | 4 | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | діяльності | | | | | |
| | | | Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності | 4 | | | | |
| | | | | | Науково-педагогічна практика | 6 | | |
| | | | | | Науково-дослідницька практика | 6 | | |
| | | | | | Переддипломна практика | 9 | | |
| | | | | | Дипломне проектування, ДА | 9 | | |
| | | ***12*** | | ***13*** | | ***30*** | ***55*** | **61** |
| **Вільного вибору студента** | Системи контролю та управління доступом на обєкті інформаційної діяльності/ *Технології виявлення уразливостей та протидії зловісному програмному забезпеченню* | 4 | | | | | | |
| | Іноземна мова (за фаховим спрямуванням) | 3 | Іноземна мова (за фаховим спрямуванням) | 2 | | | | |
| | Вплив потужних полів на електронні засоби та методи їх захисту/ *Технології виявлення уразливостей та забезпечення безпеки Web-ресурсів* | 4 | | | | | | |
| | | | Організація захисту конфіденійної інформації/ *Управління інцидентами інформаційної безпеки* | 6 | | | | |
| | Аналіз та оптимізація процесів і систем технічного захисту | 4 | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | інформації/ *Технологія виявлення уразливостей мережевих ресурсів* | | | | | | | |
| | | *15* | | *8* | | | **23** | **25,6** |
| | **Всього** | **30** | | **30** | | **30** | **90** | **100** |
| | | | | | | | | |

## 3.Форма атестації здобувачів вищої освіти

| | |
|---|---|
| *Форми атестації здобувачів вищої освіти* | Атестація магістрів здійснюється у формі публічного захисту магістерської роботи. |
| *Вимоги до кваліфікаційної роботи* | Атестація здійснюється відкрито і гласно.<br>Кваліфікаційна робота перевіряється на плагіат згідно «Положення про запобігання академічному плагіату у Державному університеті телекомунікацій» |

## 4. Матриця відповідності програмних кометентностей компонентам освітньої програми

| | ЗК12.1.01 | ЗК12.1.02 | ЗК12.1.03 | ЗК12.1.04 | ПП.12.2.01 | ПП.12.2.02 | ПП.12.2.03 | ПП.12.2.04 | ПП.12.2.05 | ПП.12.2.06 | ПП.12.2.07 | ПП.12.2.08 | ПП.12.2.09 | ПП.12.2.10 | ППк.12.3.1.01 | ППк12.3.2.01 | ППк.12.3.2.02 | ППк.12.32.03 | ППк.12.3.2.04 | ППк.12.3.2.05 | ППк.12.3.2.06 | ППк.12.3.2.07 | ППк.12.3.2.08 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ЗК 1** | | | • | | | | | | | | | | | | | | | | | | | | |
| **ЗК 2** | | • | | | | | | | | | | | | | | | | | | | | | |
| **ЗК 3** | • | | | | | | | | | | | | | | | | | | | | | | |
| **ЗК 4** | | | • | | | | | | | | | | | | | | | | | | | | |
| **ЗК 5** | | | • | | | | | | | | | | | | | | | | | | | | |
| **ЗК 6** | | • | | | | | | | | | | | | | | | | | | | | | |
| **ЗК 7** | | • | | | | | | | | | | | | | | | | | | | | | |
| **ЗК-8** | | | | • | | | | | | | | • | | • | | | | | | | | | |
| **ПП 1** | | | | | | • | | | | | | | | | | | | | | | | | |
| **ПП 2** | | | | | | | • | | | | | | | | | | | | | | | | |
| **ПП 3** | | | | | • | | | | | | | | | | | | | | | | | | |
| **ПП 4** | | | | | | | | • | | | | | | | | | | | | | | | |
| **ПП 5** | | | | | | | | | | | • | | | | | | | | | | | | |
| **ПП 6** | | | | | | • | | | • | | | | | | | | | | | | | | |
| **ПП 7** | | | | | | | | | | | | | • | | | | | | | | | | |
| **ПП 8** | | | | | | | • | | | | | | | | | | | | | | | | |
| **ПП 9** | | | | | | | • | | | | | | | | | | | | | | | | |
| **ПП 10** | | | | | | • | | | | | | | | | | | | | | | | | |
| **ПП 11** | | | | | | | | | | • | | | | | | | | | | | | | |
| **ПП 12** | | | | | | | | | | • | | | | | | | | | | | | | |
| **ПП 13** | | | | | • | • | | | | | | | | | | | | | | | • | • | |
| **ПП 14** | | | | | • | | | | | | | | | | | | | | | | | | |
| **ПП-15** | | | | | | • | | | | | | | | | | | | | | | • | • | |
| **ППк 1** | | | | | | | | | | | | | | | | | | | • | • | | | • |
| **ППк 2** | | | | | | | | | | | | | | | | | | | | | | | |
| **ППк 3** | | | | | | | | | | | | | | | | • | • | | | | | | |
| **ППк 4** | | | | | | | | | | | | | | | | | | • | | | | | |
| **ППк 5** | | | | | | | | | | | | | | | • | | | | | | | | |

## 5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

| | ЗК12.1.01 | ЗК12.1.02 | ЗК12.1.03 | ЗК12.1.04 | ПП.12.2.01 | ПП.12.2.02 | ПП.12.2.03 | ПП.12.2.04 | ПП.12.2.05 | ПП.12.2.06 | ПП.12.2.07 | ПП.12.2.08 | ПП.12.2.09 | ПП.12.2.10 | ППк.12.3.1.01 | ППк12.3.2.01 | ППк.12.3.2.02 | ППк.12.32.03 | ППк.12.3.2.04 | ППк.12.3.2.05 | ППк.12.3.2.06 | ППк.12.3.2.07 | ППк.12.3.2.08 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ПРН1 | | • | | | | | | | | | | | | | | | | | | | | | |
| ПРН2 | | | • | | | | | | | | | | | | | | | | | | | | |
| ПРН3 | | | | | | | | | | | • | | • | | | | | | | | | | |
| ПРН4 | | | | | | | | | | | | | | | • | | | | | | | | |
| ПРН5 | | | | | | | | | | | | | | | • | | | | | | | | |
| ПРН6 | | | | | | | | | | | | • | | | | | | | | | | | |
| ПРН7 | | | | | | | | • | | | | | | | | | | | | | | | |
| ПРН8 | | • | | | | | | | | | | | | | | | | | | | | | |
| ПРН9 | | | | | | | | | | | | | | | | • | • | | | | | | • |
| ПРН10 | | | | | | • | | | | • | | | | | | | | | | | | | • |
| ПРН11 | | • | | | | | | | | | | | | | | | | | | | | | |
| ПРН12 | | | | | | | • | | | | | | | | | | | | | | | | • |
| ПРН13 | | | | | | | | | | | | | | | | | | | | • | • | | |
| ПРН14 | | | | | | | | | • | | | | | | | | | | | | | | |
| ПРН15 | | | | | | | • | | | | | | | | | | | • | | | | | |
| ПРН16 | | | | | | | | | | | | | | | | | | | | • | • | | |
| ПРН17 | | | | | • | | | | | | | | | | | | | | | | | | |
| ПРН18 | | | | | | | | | | | | | | | | | | | • | | | • | |
| ПРН19 | | • | | | | | | | | | | | | | | | | | | | | | |
| ПРН20 | | | | | • | | | | | | | | | | | | | | | | | | |
| ПРН21 | | | | | | • | | | | | | | | | | | | | | | | | |
| ПРН 22 | | | | | | | | | | | | • | | | | | | | | | | | |
| ПРН 23 | | | | | • | | | | | • | | • | | | | | | | | | | | |
| ПРН 25 | | | | | | | • | | | | | | | • | | | | | | | | | |
| ПРН 26 | | | | | | | | • | | | | | | | | | | | • | | | | |
| ПРН 27 | • | | | | | | | | | | | | | | | | | | | | | | |
| ПРН 28 | | | | • | | | | | | | | | | | | | | | | | | | |
| ПРН 29 | | | | • | | | | | | | | | | | | | | | | | | | |

**Гарант освітньої програми**
Доцент кафедри комп'ютерних систем та
мереж Навчально-наукового інституту телекомунікацій
та інформатизації, кандидат технічних наук, доцент **С.В.Зибін**

**Рецензія**
**на Освітньо-професійну програму «Технічні системи інформаційного та кібернетичного захисту» другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека»**

На сьогоднішній день серед основних реальних та потенційних загроз національній безпеці України в інформаційній сфері є розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави. Серед загроз, які можуть призвести до розголошення інформації, за своїми небезпечними наслідками особливе місце займають несанкціонований доступ до інформації, яка обробляється та циркулює на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, а також витік інформації технічними каналами.

З метою протидії зазначеним загрозам в Україні створена та функціонує система технічного захисту інформації, яка дозволяє вирішувати практично весь комплекс завдань з технічного захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах державних органів, підприємств, установ та організацій.

Система являє собою сукупність організаційних структур, поєднаних цілями і завданнями захисту інформації, нормативно-правової та матеріально-технічної бази і спрямована на забезпечення конфіденційності, цілісності та доступності інформації інженерно-технічними заходами.

Одним з вищих навчальних закладів України, який безпосередньо займається підготовкою фахівців у сфері технічного захисту інформації є Державний університет телекомунікацій. Особливістю цього навчального закладу є гнучка система підготовки фахівців, заснована на практико-орієнтованому підході.

Освітньо-професійна програма «Технічні системи інформаційного та кібернетичного захисту» другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека» відповідає міжнародним та національним стандартам, враховує вимоги ринку праці, які забезпечуються наданням компетенцій на базі навчальних дисциплін професійної підготовки.

Рівень компетентностей визначених у Освітньо-професійній програмі «Технічні системи інформаційного та кібернетичного захисту» та якісний склад науково-педагогічних працівників Державного університету телекомунікацій дозволяє здійснювати підготовку магістрів зі спеціальності 125 «Кібербезпека».

Директор Державного підприємства «Український науково-технічний і впроваджувальний центр комплексного захисту інформації»
(Український центр «Безпека»)

В.Г. Глазунов

**Рецензія**
**на Освітньо-професійну програму «Технічні системи інформаційного та кібернетичного захисту» другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека»**

Розвиток сучасних інформаційних і комунікаційних технологій формує нову систему відносин у суспільстві. Разом з тим переваги у розвитку економіки нівелюються можливістю впливу на процеси прийняття рішень шляхом несанкціонованого заволодіння інформацією. Від впливу кіберзлочинності не застраховані тепер ні великі підприємства ні пересічні громадяни. При цьому, об'єктами полювання є не лише інформація, віднесена до державної чи комерційної таємниці, а й персональні дані, банківські рахунки тощо. У зв'язку з цим проблема захисту такої інформації виступає сьогодні на передній план.

Підготовкою фахівців з питань технічного захисту інформації в Україні опікується Державний університет телекомунікацій. Він забезпечений відповідною матеріально-технічною базою, науково-педагогічними працівниками високого рівня кваліфікації та реалізує концепцію підготовки, яка заснована на практико-орієнтованому підході. У сфері кібербезпеки здійснюється інтегрована підготовка фахівців до вирішення завдань щодо технічного захисту інформації.

Освітньо-професійна програма «Технічні системи інформаційного та кібернетичного захисту» другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека» розроблена на базі світових та національних освітніх стандартів, враховує вимоги роботодавців ринку праці і забезпечена наданням компетенцій на базі навчальних дисциплін професійної підготовки.

Представлена Освітньо-професійна програма «Технічні системи інформаційного та кібернетичного захисту», враховує вимоги роботодавців та всі тенденції сучасного ринку праці і підготовлена на високому рівні, що підтверджує здатність Державного університету телекомунікацій готувати фахівців рівня магістр зі спеціальності 125 «Кібербезпека».

Директор Товариства з обмеженою відповідальністю «Інфосейф ІТ»


В.В. Жора