**ПРОГРАМА**

кваліфікаційного екзамену

за напрямом 6.170103 «Управління інформаційною безпекою»

|  |  |
| --- | --- |
| **Компетенції**  **(з використанням матеріалу модуля вступник повинен вміти)** | **Змістові модулі** |
| Готувати пропозиції до проектів нормативно-правових актів щодо забезпечення інформаційної безпеки.  Вирішувати окремі завдання забезпечення системи інформаційної безпеки на всіх циклах її існування.  Використовувати професійно профільовані знання, уміння й навички для формування системи (органів, підрозділів), що забезпечує інформаційну безпеку.  Використовувати знання, уміння й навички з метою розроблення системи менеджменту інформаційної безпеки. | **1 Менеджмент інформаційної безпеки**  1.1. Система законодавства у сфері інформаційних відносин. Загальні принципи внутрішньої та зовнішньої політики держави у сфері інформаційних відносин.  1.2. Об'єкти та суб'єкти Інформаційних відносин, основні права й обов'язки учасників зазначених відносин.  1.3. Види інформації, загальні принципи охорони інформації з обмеженим доступом.  1.4. Система менеджменту інформаційної безпеки. |
| Характеризувати основні властивості інформації, інформаційних ресурсів та технологій, як об’єктів інформаційної безпеки.  Застосовувати програмно-апаратні засоби захисту даних та оцінювати якість прийнятих рішень.  Застосовувати засоби захисту інформації в операційних системах та давати оцінку якості прийнятих рішень.  Визначати характеристики системи захисту інформації відповідно до стандартів з оцінки захищених систем. | **2 Безпека інформації в інформаціно-комунікаційних системах**  2.1. Основні загрози інформації в ІКС.  2.2. Апаратно-програмні методи та засоби захисту інформації в ІКС.  2.3. Організаційно-режимні аспекти захисту інформації в ІКС.  2.4. Структура й обов'язки підрозділу технічного захисту інформації в ІКС. |
| Оцінювати рівень загроз для інформації в автоматизованих системах та ефективність комплексних систем захисту інформації.  Обґрунтовувати вимоги до комплексних систем захисту інформації.  Визначати цілі та розробляти документи на всіх етапах розробки комплексної системи захисту інформації.  Визначати характеристики комплексів засобів захисту .  Експлуатувати комплексні системи захисту інформації. | **3 Комплексні системи захисту інформації**  3.1 Передпроектні роботи із створення комплексних систем захисту інформації.  3.2 Проектні роботи із створення комплексних систем захисту інформації  3.3 Випробування та державна експертиза комплексних систем захисту інформації.  3.4 Супровід та експлуатація комплексних систем захисту інформації експлуатація. |
| Аналізувати та визначати сутність основних понять в галузі технічного захисту інформації.  Класифікувати, аналізувати особливості технічних каналів витоку інформації на об’єктах інформаційної діяльності.  Обгрунтовувати вибір методів технічного захисту інформації.  Обгрунтовувати вибір засобів технічного захисту інформації. | **4 Основи технічного захисту інформації**  4.1. Понятійна база технічного захисту інформації.  4.2. Технічні канали витоку інформації .  4.3. Методи технічного захисту інформації.  4.4. Технічні засоби захисту інформації. |
| Прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники.  Розробляти, організовувати розробку та здійснення побудови системи організаційно-службових і спеціальних заходів із забезпечення інформаційної безпеки.  Надавати консультативну допомогу громадянам, представникам органів влади, громадських організацій із питань діяльності іноземних політичних, економічних, військових, розвідувальних й інформаційних структур, спрямованих проти інтересів України в інформаційній сфері.  Здійснювати оцінювання ефективності реалізації основних засад розвитку інформаційного суспільства в Україні та світі. | **5 Інформаційна безпека держави**  5.1.Поняття інформаційної безпеки держави, суспільства та особи. Небезпеки для інформаційної безпеки держави, особи та суспільства.  5.2.Обмеження свободи слова і доступу громадян до інформації. Негативні чинники впливу на інформаційну безпеку у сфері суспільної моралі.  5.3. Основи державної політики у сфері забезпечення інформаційної безпеки держави. Інститути громадянського суспільства як суб'єкти забезпечення інформаційної безпеки.  5.4.Правові засади забезпечення інформаційної безпеки держави. Юридична відповідальність за правопорушення у сферах забезпечення інформаційної безпеки держави та інформаційних технологій. |

**Рекомендована література**

1. Богуш В.М., Юдин О.К. Інформаційна безпека держави. – К.: «МК-Прес», 2005.-432с.

2. ДСТУ 3396.1-96, НД ТЗІ 3.7-003-05; НД ТЗІ 1.1-005-07; НД ТЗІ 3.1-001-07; НД ТЗІ 3.3-001-07; НД ТЗІ 1.1-002-99; НД ТЗІ 2.1-001-2001; НД ТЗІ 2.5-004-99; НД ТЗІ 2.5-005-99; НД ТЗІ 3.6-001-2000; НД ТЗІ 3.7-001-99; НД ТЗІ 2.5-008; НД ТЗІ 2.5-010-2003; НД ТЗІ 1.1-005-07; НД ТЗІ 1.4-001-00.

3. Головань С.М. та ін. Документаційне забезпечення робіт із захисту інформації з обмеженим доступом: Підручник. –Львів: Видавництво Національного університету «Львівська по-літехніка», 2005.-288с.

4. Інформаційна безпека держави: підручник, в 2 т. / за заг. ред. В.М. Петрика. – К. : Вид-во ІСЗЗІ НТУУ «КПІ», 2015. – 316 с.

5. Хорев А.А. Защита информации от утечки по техническим каналам. Ч.1. Технические каналы утечки информации. Учебное пособие. – М.: 1998.-320с.

6. Щеглов А.Ю., Защита компьютерной информации от несанкционированного доступа С-Пб.: НиТ, 2004. 384 с.

7. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група ВНV, 2009. – 608 с.

8. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. Пособие для ВУЗов. – М: Горячая линия – Телеком, 2004 – 280 с.

Завідувач кафедри БІТ Корнієнко В.І.