Назва дисципліни		Сертифікація, експертиза, аудит інформаційної безпеки			
Рівень вищої освіти		Другий (магістерський) рівень			
Назва спеціальності		Комп'ютерні науки та інформаційні технології			
Назва спеціалізації		Програмне забезпечення систем захисту інформації			
Форма навчання		денна			
Кафедра, що забезпечує		Інформатики та управління захистом інформаційних систем			
курс	5	семестр	9	**Викладач**	Доц. Кононович В.Г.
А	**Мета і задачі дисципліни**				
	Метою дисципліни «Сертифікація, експертиза, аудит інформаційної безпеки» є поглиблене вивчення та формування комплексу знань, пов'язаних із сутністю небезпек інформаційної безпеки та набуття основ практичних навичок використання методів забезпечення інформаційної безпеки, методів державної сертифікації, державної експертизи , внутрішнього та зовнішнього аудиту, методів і алгоритмів дослідження систем інформаційної безпеки з точки зору ризиків інформаційної безпеки, а також особливостей проведення аудиту на державних і комерційних підприємствах. Основними *задачами* дисципліни є: освоїти поняття інформаційної безпеки, сертифікації засобів інформаційної безпеки, державної експертизи систем та об'єктів інформаційної безпеки; навчитися оцінювати загрози для інформаційної безпеки; враховувати небезпеку загроз інформаційній безпеці в процесі проведення експертизи та аудиту; освоїти правові засади сертифікації, експертизи та аудиту інформаційної безпеки, основи державної політики у цій сфері, принципи, алгоритми і прийоми проведення експертизи та аудиту; осмислити юридичну відповідальність за правопорушення у сфері забезпечення інформаційної безпеки; оволодіння методами оцінки ефективності сертифікації, експертизи та аудиту інформаційної безпеки; оволодіння методами рішення теоретичних, науково-технічних і технологічних проблем і задач з розробки та підтримки систем сертифікації, експертизи та аудиту, їх складових, користуючись для цього сучасними математичними теоріями та підходами, зокрема загальним підходом до аналізу стану й технології функціонування систем інформаційної безпеки, теорії ризиків, теорії експертних оцінок; оволодіння методами оцінювання впливів сертифікації, експертизи та аудиту на ризики інформаційної безпеки.				
В	**Тематика дисципліни**				
	1. Основні принципи організації та проведення оцінки інформаційної захищеності в інформаційно-комунікаційних системах. 2. Загальні підходи до оцінки інформаційної захищеності. 3. Правові основи безпеки та оцінки безпеки інформаційно-комунікаційних систем України. 4. Структура обробки інцидентів інформаційної безпеки. Державні центри інформаційної безпеки. 5. Система організації оцінки безпеки інформаційної інфраструктури України. 5.1. Кваліфікаційний аналіз та його види. 5.2. Вимоги до кваліфікаційного аналізу. 5.3. Положення та організація державної експертизи. 5.4. Сертифікація засобів технічного захисту інформації. 5.5. Аудит інформаційної безпеки. 6. Цілі та задачі технічного контролю ефективності заходів захисту інформації. 7. Задачі та законодавчі основи інструментального контролю захищеності інформації. 8. Елементи математичного забезпечення контролю захищеності інформації від витоку технічними каналами: 8.1. Вимірювання частотних та амплітудних характеристик сигналів. 8.2. Визначення небезпечних зон джерел електромагнітних випромінювань. 8.3. Оцінка та розрахунок похибки виконаних вимірювань. 9. Передова практика ОБСЄ з реалізації заходів безпеки в інформаційно-				

	комунікаційних технологіях по зниженню ризиків у кіберпросторі. 10. Модель і методи оцінювання ефективності заходів захисту за Рекомендацією МСЕ-Т серії Х.800: 10.1. Адміністрування засобів безпеки. 10.2. Класифікація моделей керування доступом. 10.3. Модель оцінювання інформаційної захищеності системи керування доступом. 11. Методи коректності реалізації функціональних критеріїв захисту інформації: 11.1. Функціональні критерії НД ТЗІ 2.5-004-99 11.2. Ранжирування вимог критеріїв конфіденційності. 11.3. Ранжирування вимог критеріїв цілісності. 11.4. Ранжирування вимог критеріїв доступності. 12. Забезпечення вимог критеріїв спостережності. 13. Класифікація та функціональні профілі захищеності інформаційно-комунікаційних систем: 13.1. Класифікація автоматизованих систем у НД ТЗІ 2ю5-005-99. 13.2. Функціон6альні профілі захищеності. Визначення та призначення. 13.3. Приклади функціонального профілю інформаційно-комунікаційних систем класу «1», «2», і «3».. 14. Основні положення «Загальних критеріїв оцінювання інформаційних технологій»: 14.1. Кваліфікування рівня безпеки. 14.2. Потенційні загрози безпеці. 14.3. Типові завдання захисту. 14.4. Політика безпеки. 14.5. Профіль захисту. 14.6. Проект захисту. 14.7. Функціональні вимоги до засобів захисту 15. Методологія оцінювання функціональних послуг безпеки у засобах захисту інформації від несанкціонованого доступу. 16. Програма і методика випробувань функціональних послуг безпеки. 17. Огляд експертних методів прийняття рішень. 18. Експертні оцінки з використанням непараметричних методів: 18.1. Особливості використання експертних методів. 18.2. Класифікація методів отримання експертних оцінок. 18.3. Процедури експертного оцінювання. 18.4. Математично-статистичні методи аналізу експертних оцінок, отриманих методом ранжирування. 19. Організація проведення експертних оцінок. 20. Оцінки і технологія оцінки ризиків експертними методами. 21. Аудит безпеки та аналіз ризиків. Актуальність аудита безпеки. Основні поняття та визначення. 22. Аудит безпеки у відповідності з BS 7799. 22.1. Організація проведення аудита. 22.2. Методика проведення аудита. 22.3. Варіанти аудита безпеки. 23. Аудит інформаційної системи: рекомендації COBIT. 24. Етапи проведення аудита.
C	**Стиль та методика навчання**
Організаційно-методичні форми вивчення	Лекційні, лабораторні та практичны заняття
Форми контролю	Поточний контроль, модульні контрольні роботи, індивідуальні завдання, залік
D	**Компетентності**
	ЗК1. Навички використання інформаційних і комунікаційних технологій

	ЗК2. Вміння виявляти, ставити та вирішувати проблеми ЗК8. Знання та розуміння предметної області та розуміння професійної діяльності ЗК9. Визначеність і наполегливість щодо поставлених завдань і взятих обов'язків ЗК10. Здатність до пошуку, оброблення та аналізу інформації з різних джерел СК15. Здатність виконувати аналіз рівня інформаційної захищеності інформаційних систем, розробляти пропозиції щодо його підвищення СК16. Здатність аналізувати та синтезувати інформацію стосовно процесів нападу на інформацію та її захисту СК17. Здатність до використання інформаційних і комп'ютерних технологій для реагування на інциденти інформаційної безпеки.
Е	**Основні результати навчання**
	РН1. Вміти використовувати методи та правила управління інформацією та роботу з документами за професійним спрямуванням. Володіти методиками та сучасними засобами інформаційних технологій. РН2. Вміти використовувати комунікаційні технології для підтримування гармонійних ділових та особистісних контактів, як передумову ділового успіху. РН3. Знати та розуміти закони та методи міжособистісних комунікацій, норми толерантності, ділових комунікацій у професійній сфері, ефективної праці в колективі, адаптивності. РН1. Вміти використовувати методи та правила управління інформацією та роботу з документами за професійним спрямуванням. Володіти методиками та сучасними засобами інформаційних технологій. РН4. Уміти складати психологічний портрет людини, підбирати робітників на визначені посади, знаходити шляхи виходу з конфліктної ситуації для ефективного управління персоналом. РН5. Знати та розуміти закономірності, методи та підходи творчої та креативної діяльності, системного мислення у професійній сфері. РН9. Вміти використовувати методи та методики проведення наукових та прикладних досліджень. РН10. Знати методологію системних досліджень, методів дослідження та аналізу складних об'єктів та процесів, розуміти їх складність, їх різноманіття, багатофункціональність для розв'язання прикладних завдань в галузі професійної діяльності. РН12. Знати методи проведення досліджень та вміти аналізувати складність технічних систем, розуміти складність задач оптимізації цих систем та їх елементів, та вдосконалювати методики їх проведення. РН14. Вміти чітко, послідовно та логічно висловлювати свої думки та переконання. РН8. Уміння застосовувати знання і розуміння для розв'язання задач, які характерні обраній спеціальності. РН10. Знати методологію системних досліджень, методів дослідження та аналізу складних об'єктів та процесів, розуміти їх складність, їх різноманіття, багатофункціональність для розв'язання прикладних завдань в галузі професійної діяльності. РН11. Систематично читати літературу за фахом (у тому числі закордонну), складати реферати, анотації, аналітичні огляди тощо. РН13. Розуміти необхідність бути наполегливим у досягненні мети та якісного виконання робіт у професійній сфері. РН1. Вміти використовувати методи та правила управління інформацією та роботу з документами за професійним спрямуванням. Володіти методиками та сучасними засобами інформаційних технологій. РН11. Систематично читати літературу за фахом (у тому числі закордонну), складати реферати, анотації, аналітичні огляди тощо. РН33. Вміти оцінювати впливи зовнішніх і внутрішніх факторів на інформаційну систему РН32. Вміти збирати, аналізувати, використовувати, упорядковувати, забезпечувати співвідношення та інтерпретувати інформацію стосовно організації

	систем захисту інформації РН34. Вміти оцінювати рівень інформаційної захищеності інформаційних систем, розробляти пропозиції щодо його підвищення РН29. Вміти удосконалювати або розробляти нові програмні методи, алгоритми і засоби забезпечення захисту інформації при її зберіганні, комп'ютерній обробці та передачі