Назва дисципліни		Програмні методи організації прихованого каналу зв'язку			
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	10	**Викладач**	Проф.Кобозєва А.А.
А	**Мета і задачі дисципліни**				
	Метою дисципліни «Програмні методи організації прихованого каналу зв'язку» є дослідження сучасних стеганографічних методів, що використовуються для прихованої передачі даних в каналах загального користування. Основними *задачами* дисципліни є: вивчення та розуміння основних концепцій та сучасних теоретичних та практичних проблем стеганографії, зокрема цифрової; оволодіння існуючими методами організації прихованого каналу зв'язку, методами рішення задач завадостійкої аутентифікації інформаційних контентів та інформації, що передається прихованим каналом зв'язку, захисту інформації від несанкціонованих дій над нею; оволодіння методами оцінки властивостей алгоритмів, що використовуються ними на основі загальної формалізації процесу стеганоперетворення, отриманої засобами матричного аналізу та теорії збурень; оволодіння методами рішення теоретичних, науково-технічних і технологічних проблем і задач з розробки та підтримки стеганосистем, їх складових, користуючись для цього сучасними математичними теоріями та підходами, зокрема загальним підходом до аналізу стану й технології функціонування інформаційних систем; оволодіння методами оцінювання впливів зовнішніх і внутрішніх факторів на інформаційну систему				
В	**Тематика дисципліни**				
	1. Загальні поняття та принципи стеганографії. Цифрова стеганографії, її особливості. 2. Стійкість стеганосистем до атак проти вбудованого повідомлення. 3. Загальний підхід до аналізу стану й технології функціонування інформаційних систем як основа підходу до оцінки властивостей довільного стеганографічного алгоритму, стеганографічної системи. 4. Формальне представлення процесу стеганоперетворення як збурення матриці контейнера. Повні набори формальних параметрів. 5. Формальні умови забезпечення певних властивостей стеганосистем, що використовуються для організації прихованого каналу зв'язку в каналі загального користування. 6. Загальний підхід до оцінки властивостей стеганографічного алгоритму. 7. Сучасний стан та актуальність проблеми забезпечення стійкості стеганосистеми до атак проти вбудованого повідомлення. 8. Метод підвищення стійкості стеганосистеми до атак проти вбудованого повідомлення. 9. Теоретичні основи забезпечення стійкості стеганоалгоритму до атак проти вбудованого повідомлення. 10. Стеганографічні перетворення, стійкі до стиску з втратами, реалізовані в області сингулярного розкладання матриці зображення: 11. Переваги просторової області зображення для організації стеганоперетворення. Стеганографічні перетворення, стійкі до атак проти вбудованого повідомлення, реалізовані в просторовій області зображення. 12. Порівняння результатів декодування додаткової інформації для стеганоалгоритмів, що працюють в різних областях контейнера. 13. Пропускна спроможність прихованого каналу зв'язку: оцінка, принципові можливості підвищення. Представлення матриці контейнера в симетричному вигляді. 14. Підвищення пропускної спроможності прихованого каналу зв'язку, створеного стеганографічними алгоритмами, стійкими до атак проти вбудованого повідомлення (область сингулярного розкладання).				

	15. Підвищення пропускної спроможності прихованого каналу зв'язку, створеного стеганографічними алгоритмами, стійкими до атак проти вбудованого повідомлення (просторова область стеганоперетворення). 16. Розробка стеганоперетворень, які забезпечують одночасну перевірку автентичності й цілісності переданої прихованої інформації. 17. Формальне представлення стеганоперетворення для контейнерів, збережених з втратами. 18. Оцінка величини пропускної спроможності прихованого каналу звязку, сформованого методом модифікації найменшого значущого біта.
C	**Стиль та методика навчання**
Організаційно-методичні форми вивчення	Лекційні та лабораторні заняття
Форми контролю	Поточний контроль, модульні контрольні роботи, індивідуальні завдання, усний екзамен
D	**Компетентності**
	ЗК1. Навички використання інформаційних і комунікаційних технологій ЗК2. Вміння виявляти, ставити та вирішувати проблеми ЗК4. Навички міжособистісної взаємодії 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 ЗК12. Здатність до аналізу та синтезу СК9. Здатність здійснювати аналіз і синтез науково-технічної, природничо-наукової та загальнонаукової інформації в сфері інформаційних, комп'ютерних технологій, інформаційної безпеки СК10. Здатність оцінювати впливи зовнішніх і внутрішніх факторів на інформаційну безпеку, розробляти програмні методи протидії СК11. Здатність до оцінки ефективності, зокрема обчислювальної складності методів і алгоритмів, що використовуються в програмному забезпеченні систем захисту інформації СК12. Здатність здійснювати протидію несанкціонованому проникненню в ІТ-системи шляхом програмного захисту СК15. Здатність виконувати аналіз рівня інформаційної захищеності інформаційних систем, розробляти пропозиції щодо його підвищення
E	**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. 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. РН8. Уміння застосовувати знання і розуміння для розв'язання задач, які характерні обраній спеціальності. 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. РН11. Систематично читати літературу за фахом (у тому числі закордонну), складати реферати, анотації, аналітичні огляди тощо. 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. РН13. Розуміти необхідність бути наполегливим у досягненні мети та якісного виконання робіт у професійній сфері. РН14. Вміти чітко, послідовно та логічно висловлювати свої думки та переконання. РН16. Застосовувати знання і розуміння для розв'язування задач синтезу та аналізу при визначенні складності досліджуваного об'єкта РН20. Вміти здійснювати науково-дослідну роботу в області комп'ютерних наук під час використання/розробки інформаційних технологій. РН28. Вміти використовувати сучасні математичні методи, моделі, інформаційні технології для розробки, аналізу та вдосконалення програмного забезпечення захисту інформації. РН29. Вміти удосконалювати або розробляти нові програмні методи, алгоритми і засоби забезпечення захисту інформації при її зберіганні, комп'ютерній обробці та передачі РН30. Вміти розробляти нові, використовувати та вдосконалювати існуючі програмні методи перевірки цілісності, автентичності інформації. РН31. Володіти навичками організації та виявлення прихованого каналу передачі інформації у межах каналу загального користування з використанням сучасних методів стеганографії та стеганоаналізу, розробляти стеганосистеми РН32. Вміти збирати, аналізувати, використовувати, упорядковувати, забезпечувати співвідношення та інтерпретувати інформацію стосовно організації систем захисту інформації РН33. Вміти оцінювати впливи зовнішніх і внутрішніх факторів на інформаційну систему. РН34. Вміти оцінювати рівень інформаційної захищеності інформаційних систем, розробляти пропозиції щодо його підвищення.