Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Сирота Александр Анатольевич

Кафедра технологий обработки и защиты информации

03.05.2023

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.06 Стеганография и цифровые водяные знаки

1. Код и наименование направления подготовки/специальности:

09.04.02 Информационные системы и технологии

2. Профиль подготовки/специализация:

Системы прикладного искусственного интеллекта

3. Квалификация (степень) выпускника:

Магистратура

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

6. Составители программы:

Митрофанова Елена Юрьевна, доцент, к.т.н.

7. Рекомендована:

№7 от 03.05.2023 г.

8. Учебный год:

2024-2025

9.Цели и задачи учебной дисциплины:

изучение основ стеганографического скрытия информации, вопросов выявления скрытых стеганографическим способом данных – стегоанализа, защиты информации от несанкционированного доступа, обеспечения конфиденциальности обмена информацией в информационно-вычислительных системах, вопросов защиты авторских прав с применением современных технологий создания цифровых водяных знаков; получение профессиональных компетенций в области современных технологий защиты информации.

Основные задачи дисциплины:

- обучение студентов основным теоретическим и практическим аспектам стеганографического скрытия информации, включая базовые принципы организации скрытых каналов передачи информации и принципы защиты авторских прав на цифровые объекты интеллектуальной собственности с использованием технологий создания цифровых водяных знаков;
- ознакомление студентов с современными мерами противодействия стеганографическому скрытию, принципами стегоанализа;

- овладение практическими навыками применения на практике теоретических знаний для реализации стеганографического скрытия информации в файлы распространенных форматов.

10. Место учебной дисциплины в структуре ООП:

Входит в блок дисциплин, формируемый участниками образовательных отношений Б1.В.

Для успешного освоения дисциплины необходимы входные знания в области криптографии, теории вероятностей и математической статистики, теории цифровой обработки сигналов, информатики.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников) и индикаторами их достижения:

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПКВ-8 Способен разрабатывать новые технологии проектирования информационных систем, прогнозировать развитие информационных систем и технологий	ПКВ-8.1 Знает инструменты и методы моделирования бизнес-процессов, современные подходы и стандарты автоматизации организации, отраслевую документацию, основы реинжиниринга бизнес-процессов организации	Знать базовые понятия и определения стеганографии, основы современных стеганографических средств и технологий создания цифровых водяных знаков Уметь проводить разработку и исследование теоретических и экспериментальных моделей объектов профессиональной деятельности Владеть практическими навыками применения средств и технологий создния цифровых водяных знаков

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПКВ-15 Способен разрабатывать и исследовать модели объектов профессиональной деятельности, предлагать и адаптировать методики решения научно-исследовательских задач, планировать и проводить исследования	ПКВ-15.1 Умеет обеспечивать сбор научно-технической (научной) информации, необходимой для постановки и решения задач исследования	Знать Известные в мировой практике подходы и разработки в области стеганографии Владеть анализировать адекватность известных и используемых моделей и результатов экспериментальных исследований, обобщать их для проведения сопоставительного Уметь навыками проведения компьютерного эксперимента по оценке эффективности алгоритмов

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Зачет с оценкой,Контрольная работа

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 4	Всего
Аудиторные занятия	28	28
Лекционные занятия	14	14
Практические занятия		0
Лабораторные занятия	14	14
Самостоятельная работа	80	80
Курсовая работа		0
Промежуточная аттестация	0	0
Часы на контроль		0
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Раздел 1. Современные методы цифровой стеганографии	Предметная область стеганографии. Практические области применения. Требования к проектированию стеганографических систем. Методы цифровой стеганографии. Принципы сжатия изображений, видео, аудио-данных. Принципы скрытия данных в пространственной и частотной области файлов-контейнеров. Алгоритмы стеганографического скрытия информации в текст, изображения, видео, звук, исполняемые файлы. Статистические и структурные методы стеганографического скрытия. Нейронные сети в задачах стеганографии. Программы стеганографического скрытия. Перспективные направления развития стеганографических методов.	Создан электронный онлайн - курс, размещены материалы к лекции и лабораторным работам.

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.2	Раздел 2. Цифровые водяные знаки	Криптографические и стеганографические методы в задачах идентификации и аутентификации. Виды реализации и практические области применения цифровых водяных знаков. Робастность цифровых водяных знаков. Контроль за целостностью информации с использованием технологии создания цифровых водяных знаков. Встраивание заголовков и идентификационных номеров. Голографический подход к созданию цифровых водяных знаков. Программные продукты для создания цифровых водяных знаков.	Создан электронный онлайн - курс, размещены материалы к лекции и лабораторным работам.
1.3	Раздел 3. Выявление стеганографического скрытия информации (стегоанализ)	Стеганографическая стойкость. Принципы стегоанализа. Разновидности атак на стегосистемы по аналогии с криптоанализом. Визуальный, статистический, универсальный стегоанализ. Программы стегоанализа.	Создан электронный онлайн - курс, размещены материалы к лекции и лабораторным работам.
2. Практические занятия			
2.1	нет		
3. Лабораторные работы			

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
3.1	Статистическая теория распознавания образов	Реализовать программу, реализующую метод LSB. Реализовать программу, реализующую метод Брайндокса. Провести экспериментальные исследования устойчивости алгоритмов к различного рода негативным воздействиям.	Создан электронный онлайн - курс, размещены материалы к лекции и лабораторным работам.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Лаб.					
2	Современные методы цифровой стеганографии	8		8	40	56
3	Цифровые водяные знаки	4		4	20	28
4	Выявление стеганографического скрытия информации (стегоанализ)	2		2	20	24
		14	0	14	80	108

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

1) При изучении дисциплины рекомендуется использовать следующие средства:

рекомендуемую основную и дополнительную литературу; методические указания и пособия; контрольные задания для закрепления теоретического материала; электронные версии учебников и методических указаний для выполнения лабораторно - практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала.

Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении лабораторных занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная обработка информации, излагаемых в рамках лекций.

4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций онлайн и проведения лабораторно- практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

5) При использовании дистанционных образовательных технологий и электронного обучения обучающиеся должны выполнять все указания преподавателей, вовремя подключаться к онлайн - занятиям, ответственно подходить к заданиям для самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

№ п/п	Источник
1	Источник
2	Криптографические методы защиты информации : учебное пособие для вузов / Воронеж. гос. ун-т; сост. Б.Н. Воронков .— Воронеж : ИПЦ ВГУ, 2008 .— 58 с. : ил .— Библиогр.: с.52-58 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-17.pdf>.
3	Щербаков, Андрей Юрьевич. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для студ. вузов / А.Ю. Щербаков .— М. : Кн. мир, 2009 .— 351, [1] с. : ил., табл. — (Высшая школа) .— Библиогр.: с.350-351 .— ISBN 978-5-8041-0378-2.
4	Митрофанова, Елена Юрьевна. Практикум по курсу "Стеганография и цифровые водяные знаки" [Электронный ресурс] : учебно-методическое пособие : [для студ. фак. компьютер. наук днев. формы обучения для направлений: 09.04.02 - Информационные системы и технологии, 09.03.02 - Информационные системы и технологии, 10.03.01 - Информационная безопасность; для специальности 10.05.01 - Компьютерная безопасность] / Е.Ю. Митрофанова, А.А. Сирота, М.А. Дрюченко ; Воронеж. гос. ун-т .— Электрон. текстовые дан. — Воронеж : Издательский дом ВГУ, 2018 .— Загл. с титула экрана .— Свободный доступ из интрасети ВГУ .— Текстовый файл .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m18-51.pdf>.

б) дополнительная литература:

№ п/п	Источник
1	Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2002. – 260 с.
2	Конахович Г.Ф. Компьютерная стеганография теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев: МК-Пресс, 2006. – 283 с.

№ п/п	Источник
3	Рябко Б.Я. Основы современной криптографии и стенографии / Б.Я. Рябко, А.Н. Фионов. – М.: Горячая линия-Телеком, 2010. – 232 с.
4	Харинов М.В. Запоминание и адаптивная обработка информации цифровых изображений / М.В. Харинов. – СПб.: Изд-во СПб ун-та, 2006. – 137 с.
5	Барсуков В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. – М.: Кудиц-Образ, 2001. – 489 с.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	*Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).*
2	*Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)*
3	ЭБС Лань, Лицензионный договор №3010-14/37-23 от 07.03.2023 (срок предоставления с 12.03.2023 по 11.03.2024) ЭБС «Университетская библиотека online» (Контракт №3010-06/23-22 от 30.12.2022 (срок предоставления с 12.01.2023 по 11.01.2024) ЭБС «Консультант студента» – Лицензионный договор №3010-06/22-22 от 30.12.2022 (с дополнительным соглашение №1 от 09.01.2023) (срок предоставления с 12.01.2023 по 11.01.2024)

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Криптографические методы защиты информации : учебное пособие для вузов / Воронеж. гос. ун-т; сост. Б.Н. Воронков .— Воронеж : ИПЦ ВГУ, 2008 .— 58 с. : ил .— Библиогр.: с.52-58 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-17.pdf>.
2	Щербаков, Андрей Юрьевич. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для студ. вузов / А.Ю. Щербаков .— М. : Кн. мир, 2009 .— 351, [1] с. : ил., табл. — (Высшая школа) .— Библиогр.: с.350-351 .— ISBN 978-5-8041-0378-2.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

1. ПО Microsoft в рамках подписки "Imagine/Azure Dev Tools for Teaching", договор №3010-16/96-18 от 29 декабря 2018г.
2.При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ

(https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы сети Интернет

18. Материально-техническое обеспечение дисциплины:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

1) Мультимедийная лекционная аудитория (корп.1а, ауд. № 380) - ПК-Intel-G3420, рабочее место преподавателя: проектор, видеокоммутатор, специализированная мебель: доска меловая 1 шт., столы 31 шт., стулья 64 шт.; выход в Интернет, доступ к фондам учебно-методической документации и электронным изданиям.

2) Компьютерный класс (один из корп. 1а, ауд. № 291, 293, 295, 387, 381) - ПК-Intel-Core2/i3 14 шт., специализированная мебель: доска маркерная 1 шт., столы 14 шт., стулья 28 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Современные методы цифровой стеганографии. Цифровые водяные знаки. Выявление стеганографического скрытия информации (стегоанализ).	ПКВ-8	ПКВ-8.1	Контрольная работа по соответствующим разделам или устный опрос. Лабораторные работы 1-3
2	Современные методы цифровой стеганографии. Цифровые водяные знаки. Выявление стеганографического скрытия информации (стегоанализ).	ПКВ-15	ПКВ-15.1	Контрольная работа по соответствующим разделам или устный опрос. Лабораторные работы 1-3

Промежуточная аттестация

Форма контроля - Зачет с оценкой,Контрольная работа

Оценочные средства для промежуточной аттестации

Перечень вопросов, лабораторные работы

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Устный опрос на практических занятиях

Контрольная работа по теоретической части курса

Лабораторные работы

20.1.1 Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	Устный опрос на практических занятиях	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 20.2.3
3	Лабораторная работа	Содержит 9 лабораторных заданий, предусматривающие разработку, тестирование и эксплуатацию моделей и алгоритмов анализа данных с использованием различных методов обучения.	При успешном выполнении работ в течение семестра фиксируется возможность оценивания только теоретической части дисциплины в ходе промежуточной аттестации (экзамена), в противном случае проверка задания по лабораторным работам выносится на экзамен.

20.1.2. Пример задания для выполнения лабораторной работы

Лабораторная работа №5

«Реализовать программу, реализующую метод LSB»

Цель работы:

Исследовать алгоритм LSBреализовать программную реализацию алгоритма.

Форма контроля: отчёт в электронном виде

Количество отведённых аудиторных часов: 4

20.1.3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Приведённые ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний по дисциплине

1. Перечислите способы представления изображения в частотной области
   a. дискретное косинусное преобразование
   b. дискретное преобразование Фурье
   c. вейвлет-преобразование
   d. преобразование Карунена-Лоева
   e. преобразование Лапласа

2. Какие типы статистической избыточности существуют

a. корреляция между соседними пикселами
b. корреляция между соседними частотными полосами
c. корреляция между соседними кадрами (для видео)
d. корреляция между соседними блоками (для видео)
e. корреляция между соседними

3. В схеме встраивания и извлечения ЦВЗ для реализации преобразования водяного знака к виду, пригодному для встраивания в контейнер используется

a. декодер
b. детектор
c. прекодер
d. стегокодер

4. Какие ЦВЗ характеризуются высокой устойчивостью к различным трансформациям заполненного контейнера включая компрессию с потерями, фильтрацию, яркостную коррекцию, масштабирование и т.д.

a. робастные
b. хрупкие
c. полухрупкие

5. Какие ЦВЗ разрушаются при незначительной модификации заполненного контейнера

a. робастные
b. хрупкие
c. полухрупкие

6. Какие ЦВЗ устойчивы по отношению к одному типу воздействий и неустойчивы по отношению к другим

a. робастные
b. хрупкие
c. полухрупкие

7. При реализации стеганографического встраивания в какой области контейнеров-изображений скрываемые данные внедряются в элементы преобразованного с использованием одного из известных спектральных методов растрового представления.

a. пространственной
b. частотной

8. Стегоалгоритмы данного класса предназначены для встраивания ЦВЗ в аудио- и графические контейнеры путем линейной их модификации

a. аддитивные
b. вероятностные
c. пространственные
d. частотные

9. Для чего реализуется камуфлирование защищаемого программного обеспечения

a. чтобы оно не могло быть использовано незарегистрированными пользователями
b. чтобы оно могло быть использовано зарегистрированными пользователями
c. чтобы оно не могло быть использовано всеми пользователями

10. Активный нарушитель

a. читает встроенное сообщение
b. удаляет встроенное сообщение
c. разрушает встроенное сообщение
d. создает ложное сообщение

11. Каким образом могут формироваться стеганографические ключи?

a. специально сформированные данные
b. определенная последовательность действий
c. алгоритм, задающий последовательность операций
d. зашифрованные данные объекта цифрового контента
e. проектирующая функция

12. В чем заключается камуфлирование защищаемого программного обеспечения?

a. Камуфлированное защищаемое программное обеспечение не может быть использовано незарегистрированными пользователями
b. Камуфлированное защищаемое программное обеспечение не может быть найдено незарегистрированными пользователями
c. Камуфлированное защищаемое программное обеспечение не соответствует требованиям системы
d. Камуфлированное защищаемое программное обеспечение может быть использовано незарегистрированными пользователями
e. Камуфлированное защищаемое программное обеспечение содержит встроенную последовательность ЦВЗ

13. Какие особенности встраивания данных в пространственную область исходного контейнера?

a. скрываемые данные внедряются в элементы растрового представления за счет манипуляций их яркостью
b. скрываемые данные внедряются в элементы растрового представления за счет манипуляций их цветностью
c. скрываемые данные не внедряются в неподходящие элементы контейнера
d. скрываемые данные внедряются в блоки пикселей 8*8
e. скрываемые данные внедряются в элементы растрового представления за счет манипуляций с младшими битами

14. Каким образом формируются маски, накладываемые на блоки пикселей в алгоритме Bruyndonckx

a. случайный порядок
b. зигзагом, начиная с левого верхнего элемента
c. блоками заданной размерности (2*2)
d. зигзагом, начиная с правого верхнего элемента
e. последовательно (слева направо)

15. В чем заключается основная идея атаки хи-квадрат?

a. высчитывании вероятности встраивания на основе того, как близко располагаются значения частот четных и нечетных коэффициентов DCT
b. модификации НЗБ DCT
c. оценивании статистических характеристик контейнера
d. высчитывании вероятности восстановления встроенного сообщения
e. высчитывании разности между вероятностями встраивания на основе того, как близко располагаются значения частот четных и нечетных коэффициентов DCT

16. Стеганография это

a. наука о скрытой передаче информации, путем сохранения в тайне самого факта передачи
b. наука о скрытой передаче информации, путем сохранения в тайне самой информации
c. наука о скрытой передаче информации, путем сохранения в тайне самого факта передачи и непосредственно передаваемой информации
d. наука о видимой передаче информации, путем сохранения в тайне самой информации
e. наука о скрытой передаче информации, путем сохранения в тайне исходного контейнера

17. Выберите правильное (ые) утверждения

a. Размер исходного контейнера (носителя) должен быть много больше, чем встраиваемое сообщение (информация
b. Объем встраиваемой информации напрямую зависит от объема контейнера
c. Надежность встраиваемой информации напрямую зависит от размера встраиваемого сообщения
d. Встраивание текста более незаметно, чем встраивание цифровых значений
e. Робастность контейнера определяется типом самого контейнера

18. По способу организации контейнера в методах компьютерной стеганографии различают

a. потоковые, фиксированные
b. систематические, несистематические
c. суррогатные, селективные, конструирующие

19. По способу выбора контейнера в методах компьютерной стеганографии различают

a. потоковые, фиксированные
b. систематические, несистематические
c. суррогатные, селективные, конструирующие

20. ЦВЗ могут быть:

a. робастные, хрупкие и полухрупкие
b. робастные, полухрупкие
c. текстовые, графические
d. суррогатные, селективные и конструирующие
e. робастные, хрупкие, полухрупкие, селективные, конструирующие

21. По используемому принципу скрытия методы компьютерной стеганографии делятся на

a. методы непосредственной замены и спектральные методы
b. пространственные методы и дискретные методы
c. систематические и несистематические
d. спектральные методы и дискретные методы
e. методы непосредственной замены, спектральные методы, дискретные методы

22. По способу доступа к информации в методах компьютерной стеганографии различают

d. потоковые, фиксированные
e. систематические, несистематические
f. суррогатные, селективные, конструирующие

23. Особенности человеческого восприятия изображений включают в себя

a. физиологические
b. психофизиологические
c. психологические
d. эмоциональные
e. умственные

24. Основными достоинствами метода Куттера-Джордана-Боссена являются:

a. достаточно высокая пропускная способность
b. устойчивость к разрушению младших бит контейнера
c. устойчивость к атаке сжатия
d. устойчивость к аффинным преобразованиям
e. устойчивость к масштабированию

25. Выберите правильное (ые) утверждения

a. свойства заполненного контейнера и восстанавливаемого сообщения должны искажаться минимально
b. свойства исходного контейнера и сообщения должны изменяться минимально
c. свойства заполненного контейнера и исходного сообщения должны искажаться минимально
d. свойства заполненного контейнера и восстанавливаемого сообщения должны искажаться максимально
e. свойства контейнера и сообщения не должны искажаться

26. В схеме встраивания и извлечения ЦВЗ для извлечения ЦВЗ из маркированного контейнера используется

a. декодер
b. детектор
c. прекодер
d. стегокодер

27. В схеме встраивания и извлечения ЦВЗ для определения наличия встроенного ЦВЗ в контейнере используется

a. декодер
b. детектор
c. прекодер
d. стегокодер

28. В схеме встраивания и извлечения ЦВЗ для реализации встраивания кодированного ЦВЗ в контейнер с учетом свойств контейнера и самого ЦВЗ используется

e. декодер
f. детектор
g. прекодер
h. стегокодер

29. Базовые стеганографические операторы, описывающие процедуры встраивания и извлечения данных из стегоконтейнеров, могут быть записаны в виде

a. $I^{'}=F(I,M,K)$, $M^{'}=F^{-1}(I^{'},K)$
b. $I^{'}=F(I,M,K)$, $M^{'}=F^{-1}(I^{'})$
c. $I^{'}=F(M,K)$, $M^{'}=F^{-1}(I^{'},K)$
d. $I^{'}=F(K)$, $M^{'}=F^{-1}(K)$

e. $I^{'}=F(I,K)$, $M^{'}=F^{-1}(I^{'},K)$

30. В какому направлению стеганографии относятся следующие примеры

использование стеганографических файловых систем, скрытие данных в неиспользуемых областях форматов файлов, подмена символов в названиях файлов, текстовая стеганография и т.д.

a. Компьютерная стеганография
b. Цифровая стеганография

31. Способность стегосистемы скрывать от квалифицированного нарушителя факт передачи сообщений, способность противостоять попыткам нарушителя разрушить, исказить или удалить передаваемые сообщения, а также способность подтвердить или опровергнуть подлинность скрытно передаваемой информации.

32. Вычислите элемент матрицы квантования, если соответствующий DCT коэффициент равен «405», соответствующий элемент таблицы квантования равен «16»

33. Основное отличие идентификационных номеров от ЦВЗ

34. Процедура обнаружения факта стеганографического скрытия и, если возможно, определения стегоключа и (или) выделения скрытой информации это:

35. Участки контейнера (биты, поля и т.д.), в которых стегосистема может скрыть информацию

36. Использование какого метода базируется на невосприимчивости человеческих органов чувств к малозначительным изменениям в контейнерах, обладающих психовизуальной избыточностью.

37. Потенциальный или реальный субъект (нарушитель, сторонний пользователь и пр.) осуществляющий преднамеренное (атаку) или непреднамеренное воздействие на стегоситему с целью обнаружения стегоканала, извлечения передаваемой в нем информации или ее уничтожения и искажения

38. Специальные метки, скрытно внедряемые в контейнер в целях дальнейшего контроля правомерности его использования

39. Перечислите требования к встроенному ЦВЗ.

Критерии оценивания	Шкала оценок
Обучающийся приводит все требования к встроенному ЦВЗ. Подробно описано каждое из требований.	3 балла
Обучающийся приводит все требования к встроенному ЦВЗ. Кратко описано каждое из требований. Допускаются незначительные неточности.	2 балла
Обучающийся допускает ошибку в требованиях к встроенному ЦВЗ. Кратко описано каждое из требований. Ответ не содержит грубых ошибок.	1 балл
Не перечислены требования к встроенному ЦВЗ. Присутствуют грубые ошибки или неточности.	0 баллов

40. В чем заключается основная идея метода Куттера-Джордана-Боссена.

Критерии оценивания	Шкала оценок

Обучающийся приводит основную идею, все этапы встраивания ЦВЗ. Подробно описан каждый из этапов.	3 балла
Обучающийся приводит основную идею, дает краткую характеристику методу. Допускаются незначительные неточности.	2 балла
Обучающийся допускает ошибку в основной идеи встраивания ЦВЗ, используя данный метод. Ответ не содержит грубых ошибок.	1 балл
Не представлена основная идея метода. Присутствуют грубые ошибки или неточности.	0 баллов

41. В чем заключается основная идея метода НЗБ.

Критерии оценивания	3 балла
Обучающийся приводит основную идею, все этапы встраивания ЦВЗ. Подробно описан каждый из этапов.	2 балла
Обучающийся приводит основную идею, дает краткую характеристику методу. Допускаются незначительные неточности.	1 балл
Обучающийся допускает ошибку в основной идеи встраивания ЦВЗ, используя данный метод. Ответ не содержит грубых ошибок.	0 баллов
Не представлена основная идея метода. Присутствуют грубые ошибки или неточности.	3 балла

42. Перечислите требование к проектированию стегосистем.

Критерии оценивания	Шкала оценок
Обучающийся приводит все требования к проектированию стегосистем. Подробно описано каждое из требований.	3 балла
Обучающийся приводит все требования к проектированию стегосистем. Кратко описано каждое из требований. Допускаются незначительные неточности.	2 балла
Обучающийся допускает ошибку в требованиях к проектированию стегосистем. Кратко описано каждое из требований. Ответ не содержит грубых ошибок.	1 балл
Не перечислены требования к проектированию стегосистем. Присутствуют грубые ошибки или неточности.	0 баллов

43. Нарисуйте схему извлечения ЦВЗ

Критерии оценивания	Шкала оценок
Обучающийся приводит все этапы. Подробно описано каждое из требований.	3 балла
Обучающийся приводит все этапы. Кратко описано каждое из требований. Допускаются незначительные неточности.	2 балла
Обучающийся допускает ошибку в этапах. Ответ не содержит грубых ошибок.	1 балл
Не перечислены этапы. Присутствуют грубые ошибки или неточности.	0 баллов

44. Перечислите потенциальные области практического применения современных стеганографических методов

Критерии оценивания	Шкала оценок
Обучающийся приводит все области применения. Подробно описано каждое из требований.	3 балла
Обучающийся приводит все области применения. Кратко описано каждое из требований. Допускаются незначительные неточности.	2 балла
Обучающийся допускает ошибку в областях применения. Ответ не содержит грубых ошибок.	1 балл
Не перечислены области применения. Присутствуют грубые ошибки или неточности.	0 баллов

45. В каких приложениях используются ЦВЗ

Критерии оценивания	Шкала оценок
Обучающийся приводит все приложения. Подробно описано каждое из требований.	3 балла
Обучающийся приводит все приложения. Кратко описано каждое из требований. Допускаются незначительные неточности.	2 балла
Обучающийся допускает ошибку в приложениях. Ответ не содержит грубых ошибок.	1 балл
Не перечислены приложения. Присутствуют грубые ошибки или неточности.	0 баллов

46. Нарисуйте схему встраивания ЦВЗ

Критерии оценивания	Шкала оценок
Обучающийся приводит все этапы. Подробно описано каждое из требований.	3 балла
Обучающийся приводит все этапы. Кратко описано каждое из требований. Допускаются незначительные неточности.	2 балла
Обучающийся допускает ошибку в этапах. Ответ не содержит грубых ошибок.	1 балл
Не перечислены этапы. Присутствуют грубые ошибки или неточности.	0 баллов

Номер вопроса	Ответ (буква)
1.	a,b,c,d
2.	a,b,c
3.	c
4.	a
5.	b
6.	c
7.	b
8.	a
9.	a
10.	a,b,c
11.	a,b,c
12.	a
13.	a,b
14.	a
15.	a

16.	a
17.	a,b,c
18.	b
19.	c
20.	a
21.	a
22.	a
23.	a,b
24.	a,b,c
25.	a
26.	a
27.	b
28.	d
29.	a
30.	a
31.	стеганографическая стойкость
32.	25
33.	уникальность
34.	стегоанализ
35.	Пространство сокрытия
36.	НЗБ
37.	Источник внешнего воздействия
38.	ЦВЗ

39. Требования к ЦВЗ

1. Незаметность для пользователей;
2. Индивидуальность алгоритма нанесения (достигается с помощью стеганографического алгоритма с использованием ключа);

3. Возможность для автора обнаружить несанкционированное использование файла;
4. Невозможность удаления неуполномоченными лицами;
5. Устойчивость к изменениям носителя-контейнера (к изменению его формата и размеров, к масштабированию, сжатию, повороту, фильтрации, введению спецэффектов, монтажу, аналоговым и цифровым преобразованиям).
6. Возможность добавления дополнительных ЦВЗ.

40. Основная идея метода Куттера

Метод Куттера-Джордана-Боссена (M. Kutter, F. Jordan, F. Bossen) [25] относится к группе вероятностных методов стеганографического скрытия, реализующих встраивание битов сообщения в выбранные элементы пространственной области контейнеров-изображений, представленных в цветовой модели RGB. Пространство сокрытия в данном методе формируется из значений синих цветовых компонент выбранного множества пикселей контейнера. Для встраивания данных выбирается синий цветовой канал, поскольку изменения в данном канале являются перцептивно наименее заметными.

Встраивание бита сообщения в синюю цветовую компоненту пикселя осуществляется по следующему правилу:

где – яркость пикселя с координатами , – константа, определяющая энергию встраиваемого сигнала, величина которой зависит от предназначения схемы скрытия (чем больше , тем выше робастность вложения, но тем сильнее его заметность), – измененное значение синего цвета пикселя.

После встраивания всех бит сообщения итоговый заполненный контейнер будет содержать неизменные значения красных и зеленых компонент пикселей и модифицированные значения синих компонент отдельных пикселей, выбор которых в частном случае может осуществляться в псевдослучайном порядке равномерно по всему изображению.

Извлечение бит встроенного сообщения реализуется по следующему правилу

где – оценка значения синей компоненты модифицированного при встраивании данных пикселя, полученная путем усреднения значений синих компонент немодифицированных соседних пикселей, – число пикселей сверху (снизу, слева, справа) от оцениваемого пикселя, – длина скрытого сообщения (в битах).

41. Основная идея метода НЗБ

Использование метода LSB базируется на невосприимчивости человеческих органов чувств к малозначительным изменениям в контейнерах, обладающих психовизуальной избыточностью. При встраивании данных в пространственной области графических контейнеров метод LSB реализует замену наименее значимых бит (НЗБ) значений яркости или цветности отдельных пикселей контейнера битами скрываемого сообщения:

где , – исходное и модифицированное значения яркости/цветности пикселя, – бит сообщения, – операторы битового сдвига влево и вправо, используемые для обнуления младшего двоичного разряда , – битовый оператор сложения. Обход пикселей контейнера при реализации ССИ может быть организован последовательно (например, построчно) или в псевдослучайном порядке. Второй вариант обхода является предпочтительным с точки зрения

противодействия возможному стегоанализу заполненного контейнера.

Извлечение скрытой методом LSB информации реализуется путем считывания младших двоичных разрядов значений яркости или цветности пикселей заполненного контейнера , при их обходе в том же порядке, который использовался при встраивании данных

.

На практике для обеспечения минимальной визуальной заметности результатов стеганографического скрытия модифицируется лишь один младший двоичный разряд яркости/цветности пикселя. В интересах повышения емкости встраивания при отсутствии жестких ограничений по визуальной незаметности, битами сообщения могут перезаписываться более старшие двоичные разряды элементов контейнера. Пример встраивания четырехбитного слова в пиксель полноцветного изображения в модели RGB приведении на рис. 3.

Рис. 3. Встраивание четырехбитного слова в пиксель полноцветного изображения методом LSB

Реализуемые в методе LSB принципы встраивания информации позволяют достаточно гибко управлять соотношением емкости/незаметности встраивания за счет выбора определенного количества элементов контейнера, а также определенного числа младших двоичных разрядов каждого элемента для записи в них битов сообщения. В наибольшей степени метод LSB подходит для передачи больших объемов скрываемой информации, однако он отличается слабой робастностью по отношению к искажающим воздействиям на заполненные контейнеры.

42.Требования к проектированию стегосистем

Стеганографической системой (стегосистемой) называется совокупность контейнеров, сообщений, ключей и связывающих их преобразований . Другими словами, стегосистема это совокупность средств и методов для формирования скрытого канала передачи информации (стегоканала). Для того чтобы стегосистема была надежной, при ее проектировании необходимо выполнение ряда требований.

1) Безопасность стегосистемы должна полностью определяться секретностью ключа. Это означает, что нарушитель может полностью знать все алгоритмы работы стегосистемы и статистические характеристики множеств сообщений и контейнеров, и это не даст ему никакой дополнительной информации о наличии или отсутствии сообщения в данном контейнере.

2) Знание нарушителем факта наличия сообщения в каком-либо контейнере не должно помочь ему при обнаружении сообщений в других контейнерах.

3) Заполненный контейнер должен быть визуально неотличим от незаполненного. Для удовлетворения этого требования надо, казалось бы, внедрять скрытое сообщение в визуально незначимые области сигнала. Однако, эти же области используют и алгоритмы сжатия. Поэтому, если изображение будет в дальнейшем подвергаться сжатию, то скрытое сообщение может разрушиться. Следовательно, биты должны встраиваться в визуально значимые области, а относительная незаметность может быть достигнута за счет использования специальных методов, например, модуляции с расширением спектра.

4) Стегосистема создания ЦВЗ должна иметь низкую вероятность ложного обнаружения скрытого сообщения в сигнале, его не содержащем. В некоторых приложениях такое обнаружение может привести к серьезным последствиям. Например, ложное обнаружение ЦВЗ на физическом носителе данных может вызвать отказ от его воспроизведения.

5) Должна обеспечиваться необходимая скрытая пропускная способность (актуально для систем

скрытой передачи информации).

6) Стегосистема должна иметь приемлемую вычислительную сложность реализации.

43. Схема извлечения ЦВЗ

44. Среди потенциальных областей практического применения современных стеганографических методов можно выделить следующие.

1) Защищенную связь, скрытное хранение и передачу данных.

2) Преодоление систем мониторинга и управления сетевыми ресурсами (противодействие попыткам контроля над информационным пространством при прохождении информации через серверы управления локальных и глобальных вычислительных сетей).

3) Скрытную аннотацию документов (встраивание заголовков), организацию совместного хранения гетерогенной (текстовой, графической) информации.

4) Камуфлирование защищаемого программного обеспечения под стандартные программные продукты с тем, чтобы оно не могло быть использовано незарегистрированными пользователями.

5) Создание идентификационных номеров и цифровых водяных знаков для различных приложений.

45.

В общем случае цифровые водяные знаки используются в следующих приложениях:

- скрытое маркирование объектов цифрового контента, представленных в виде графических, видео и аудио файлов для их идентификации, представления истории создания, а также внесения любой интересующей пользователя информации без существенных искажений, мешающих использовать файл-контейнер по основному назначению;

- подтверждение авторских прав на объекты цифрового контента, а также подлинности используемых копий объектов;

- создание RFID-меток повышенной скрытности и устойчивости.

46. Схема встраивания ЦВЗ

20.2 Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае невыполнения в течение семестра), проверку выполнения установленного перечня лабораторных заданий, позволяющих оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

Для оценки теоретических знаний используется перечень контрольно-измерительных материалов. Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает два задания - вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции. При оценивании используется количественная шкала. Критерии оценивания приведены выше в таблице раздела 20.2.3.

20.2.1.

Примерный перечень вопросов к зачету

1. Предметная область стеганографии (терминология, базовые отображения, области применения).
2. Алгоритмы стеганографического скрытия в видео файлы.
3. Классификация методов компьютерной стеганографии.
4. Криптографические и стеганографические методы в задачах идентификации и аутентификации.
5. Физиологические и психо-физиологические свойства человеческого зрения и слуха, используемые в интересах стеганографии.
6. Алгоритмы работы известных стеганографических утилит.
7. Методы модификации наименее значимых бит контейнера.
8. Робастные цифровые водяные знаки.
9. Скрытие данных в пространственной области контейнера.
10. Хрупкие цифровые водяные знаки.
11. Скрытие данных в частотной области контейнера.
12. Принципы использования стеганографических заголовков и идентификационных номеров.
13. Методы кодирования информации с расширением спектра сигнала.
14. Голографический подход к созданию цифровых водяных знаков.
15. Статистические и структурные методы стеганографического скрытия.
16. Принципы стегоанализа. Атаки на стегосистемы.
17. Алгоритмы стеганографического скрытия в файлы изображения.
18. Статистический стегоанализ.
19. Алгоритмы стеганографического скрытия в звуковые файлы.
20. Универсальный стегоанализ.

20.2.2. Пример контрольно-измерительного материала

УТВЕРЖДАЮ

заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота

__.__.2023

Направление подготовки / специальность 09.04.02 Информационные системы и технологии

Дисциплина Б1.В.06 Стеганография и цифровые водяные знаки

Форма обучения Очное

Вид контроля Зачёт

Вид аттестации Промежуточная

Контрольно-измерительный материал № 3

1. Физиологические и психофизиологические свойства человеческого зрения и слуха, используемые в интересах стеганографии.

2. Алгоритмы работы известных стеганографических утилит.

Преподаватель _____ Е.Ю. Митрофанова