БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Проректор по учебной работе
_____ А.Д. Толстик
(подпись)
_____
(дата утверждения)
Регистрационный № УД-2312/уч.

КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности

1-98 01 01 Компьютерная безопасность (по направлениям)
направление специальности
1-98 01 01-02 Компьютерная безопасность (радиофизические методы и программно-технические средства);

2016 г.

Учебная программа составлена на основе образовательного стандарта 1-98 01 01 – 2013 и учебного плана УВО Р98-139/уч. - 2013

СОСТАВИТЕЛИ:
В.С. Садов, профессор кафедры интеллектуальных систем Белорусского государственного университета, кандидат технических наук, доцент.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой интеллектуальных систем Белорусского государственного университета (протокол № 13 от 26 апреля 2016 г.);

Методической комиссией факультета радиофизики и компьютерных технологий Белорусского государственного университета (протокол № 9 от 24 мая 2016 г.).

Пояснительная записка

Учебная программа дисциплины «Компьютерная стеганография» разработана в соответствии с требованиями образовательного стандарта и учебного плана специальности 1-98 01 01 Компьютерная безопасность (направление: радиофизические методы и программно-технические средства).

Целью изучения данной учебной дисциплины является освоение основополагающих принципов стеганографии, состоящих в обеспечении скрытной передачи и хранения конфиденциальных данных путем незаметного встраивания их в другие данные, передаваемые по открытым каналам.

Основная задача дисциплины – научить обучаемых грамотно использовать в своей профессиональной деятельности современные методы обработки и преобразования мультимедийной информации при обеспечении ее целостности.

Для успешного освоения дисциплины необходимы знания по «Цифровой обработке сигналов», «Программированию».

Рекомендуемые формы изучения дисциплины включают лекционный курс и лабораторный практикум по принципам построения стеганографических систем, методам выполнения стеганографических модификаций и методам оценки стойкости стеганографических систем.

Целесообразно предусмотреть выполнение групповых семестровых заданий по разработке элементов стеганографических систем в рамках управляемой самостоятельной работы.

Промежуточный контроль знаний может осуществляться при защите результатов выполнения этих заданий.

В результате изучения дисциплины обучаемый должен

знать:

- основные методы и алгоритмы скрытного встраивания одних данных в другие;
- методы обнаружения встроенных сообщений;

уметь:

- применять методы стеганографии при решении задач защиты конфиденциальной информации в компьютерных системах;

владеть:

- навыками работы с современными программными средствами обработки информации;

компетенции:

- АК-3. Владеть исследовательскими навыками;
- АК-5. Быть способным вырабатывать новые идеи (креативность);
- ПК-3. Разрабатывать модели явлений, процессов или систем при организации защиты информации;

- ПК-4. Выбирать необходимые методы исследования, модифицировать существующие, разрабатывать новые методы и применять их для решения поставленных задач при организации защиты информации.

В соответствии с учебным планом на изучение дисциплины отведено всего 144 часа, из них аудиторной нагрузки – 66 часов, включая: лекции – 34 часа, лабораторные работы – 20 часов, УСР - 12 часов.

Семестр – 7, форма текущего контроля – зачет.

Содержание учебного материала:

1. Введение. Основные понятия и определения в стеганографии, область применения. Требования к стеганосистемам. Контейнеры, их основные типы и характеристики, классификация встраиваемых данных. Статистическая и психофизиологическая избыточность аудиоинформации и изображений.

2. Принципы построения стеганографических систем. Структурирование объектов стеганографического поля и классификация стеганографических систем, роль ключа в стеганографической системе. Принципы построения стеганосистем цифровых водяных знаков и стеганосистем передачи данных.

3. Форматы представления мультимедийной информации в компьютерных системах. Форматы представления аудио и графической информации в компьютерных системах.

4. Методы встраивания сообщений. Встраивание сообщений в незначащие элементы контейнера (LSB-метод). Скрытие данных в аудиопоследовательностях. Скрытие цифровых данных в пространственной области изображений. Анализ возможностей стеганографической модификации яркостной и цветовых компонент пикселей изображений.

Скрытие цифровых данных в области преобразований изображений, выбор преобразования для скрытия данных, скрытие данных в коэффициентах дискретного косинусного преобразования.

Анализ возможностей стеганографической модификации коэффициентов дискретного косинусного преобразования изображений. Скрытие данных в видеопоследовательностях.

Анализ стеганоалгоритмов встраивания информации в изображения и аудиофайлы.

5. Пропускная способность стеганографических каналов передачи информации. Понятие пропускной способности стеганосистем. Мультиплексирование пропускной способности стеганоканалов передачи информации.

5. Атаки на стеганографические системы и противодействия им. Классификация атак на стеганосистемы. Стеганографическая стойкость систем к обнаружению факта передачи скрываемых сообщений. Визуальная атака на стеганосистемы, статистические атаки на стеганосистемы с изображениями-контейнерами, статистические атаки на стеганосистемы с аудиоконтейнерами.

6. Заключение. Перспективные направления развития стеганографии. Обзор известных стеганографических программных продуктов.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ (ПРИМЕРНАЯ ФОРМА)

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1	**Введение:**	2						
2	**Принципы построения стеганографических систем:** 2.1 Структурирование объектов стеганографического поля; 2.2 Классификация стеганографических систем, роль ключа в стеганографической системе; 2.3 Принципы построения стеганосистем цифровых водяных знаков и стеганосистем передачи данных.	 2 2 2						

3	**Форматы представления мультимедийной информации в компьютерных системах:** Форматы представления аудио и графической информации в компьютерных системах.	2						
4	**Методы встраивания сообщений:** 4.1 Встраивание сообщений в незначащие элементы контейнера (LSB-метод); 4.2 Лабораторная работа № 1.Встаивание сообщений в младшие значащие элементы контейнера-изображения; 4.3 Скрытие данных в аудиопоследовательностях; 4.4 Скрытие цифровых данных в пространственной области изображений. Анализ возможностей стеганографической модификации яркостной и цветовых компонент пикселей изображений; 4.5 Лабораторная работа № 2. Исследование информативности яркостной и цветовых компонент пикселей изображений; 4.6 Скрытие цифровых данных в области преобразований изображений, выбор преобразования для скрытия данных, скрытие данных в коэффициентах дискретного косинусного	2 2 2 2			4 4			Отчет о лаб. работе № 1 Отчет о лаб. работе № 2

	преобразования; 4.7 УСР, тема № 1. 4.8 Анализ возможностей стеганографической модификации коэффициентов дискретного косинусного преобразования изображени; 4.9 Лаботаторная работа № 3. Исследование информативности коэффициентов ДКП изображений; 4.6 Анализ стеганоалгоритмов встраивания информации в изображения и аудиофайлы.	2 2			4		4	Отчет по УРС № 1 Отчет о лаб. работе № 3
5	**Пропускная способность стеганографических каналов передачи информации:** 5.1 Понятие пропускной способности стеганосистем. 5.2 Мультиплексирование пропускной способности стеганоканалов передачи информации; 5.3 УСР, тема № 2.	2 2					4	Отчет по УРС № 2
6	**Атаки на стеганографические системы и противодействия им:** 6.1 Классификация атак на стеганосистемы. Стеганографическая стойкость систем к обнаружению факта передачи скрываемых сообщений;	2						

	6.2 Лабораторная работа № 4.Стеганографическая стойкость систем; 6.3 Визуальная атака на стеганосистемы; 6.4 Лабораторная работа № 5. Организация визуальной атаки на стеганосистемы; 6.5 Статистические атаки на стеганосистемы с изображениями-контейнерами, статистические атаки на стеганосистемы с аудиоконтейнерами; 6.6 УСР, тема № 3.	2 2			4 4		4	Отчет о лаб. работе № 4 Отчет о лаб. работе № 5 Отчет по УРС № 3
7	**Заключение:** Перспективные направления развития стеганографии. Обзор известных стеганографических программных продуктов.	2						

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Список рекомендуемой литературы

Основная

1. Садов, В.С. Компьютерная стеганография : учеб. Пособие /В.С. Садов. – Минск : РИВШ, 2014. – 172 с.: ил.

2. Сейеди, С.М. Стеганографические алгоритмы на основе вейвлет-преобразований/ С.М. Сейеди, В.С. Садов.-Минск : РИВШ, 2014. – 110 с.

3. Чваркова, И.Л. Повышение пропускной способности и стойкости стеганографических систем: Основы, алгоритмы, анализ/И.Л. Чваркова, С.Г. Тихоненко, В.С. Садов. - LAP Lambert Academic Publishing, 2013.- с. 136

4. Грибунин, В. Г. Цифровая стеганография/ В.Г. Грибунин, И.Н. Окопов, И.В. Туринцев. М.: изд-во «СОЛОН-Пресс», 2002.– 272с.

5. Коханович, Г.Ф. Компьютерная стеганография/ Г.Ф. Коханович А.Ю. Пузыренко. К.: “МК-Пресс”, 2006. – 288с., ил.

6. Аграновский, А.В. Основы стеганографии/ А.В. Аграновский, П.Н. Девянин, А.В. Черемушкин, Р.А. Хади. М.: “Радио и связь”, 2003.– 152с.

7. Квач, А.Ю. Оптимизация выбора контейнеров для стеганографического скрытия данных/ А.Ю. Квач, В.С. Садов// Электроника - инфо, № 4(85), 2012, с. 114-118.

8. Селюжицкая, Ю.Н. Стеганографическое встраивание служебной информации в картографические изображения/ Ю.Н. Селюжицкая, В.С. Садов// Электроника инфо, № 1 (115), 2015, с. 45-48.

9. Чваркова, И.Л. Обнаружение стеганографического канала передачи данных путем анализа однобитного шума изображения/ И.Л. Чваркова, В.С. Садов. Известия Белорусской инженерной академии, № 1(19)/2, 2005. – с. 75-78.

10. Чваркова, И.Л. Оценка применимости критерия Хи- квадрат для обнаружения стеганографического канала в аудиоданных/ Садов В.С., И.Л. Чваркова, А.Ф. Чернявский, В.С. Садов. Вестн. Белорус. Госуд. ун-та. Сер.1: Физ. Мат. Информ. 2005, №3.– с. 92-96.

Дополнительная

1. Чваркова, И.Л. Организация стеганографического канала передачи данных модификацией частотного описания аудио-контейнера/ И.Л. Чваркова, В.С. Садов. Актуальные проблемы радиоэлектроники: научные

исследования, подготовка кадров: сб. научных статей (по итогам работы МНПК, Минск, 2-3 июня 2005 г.): в 3 ч. Ч.2/ М-во образования РБ, Учреждение образования “Минский государственный высший радиотехнический колледж”; под общ. ред. Проф. Н.А. Цырельчука.– Мн.: МГВРК, 2005.- 296 с., С. 225– 229.

2. Чернявский, А.Ф. Оценка информационных потерь при фильтрации изображений/ А.Ф. Чернявскй, С.Г. Тихоненко, В.С. Садов. Информатика, № 3(7), 2005. – с. 52-59.

3. Чваркова, И.Л. Анализ статистической атаки на стеганографические аудио системы, основанной на выравнивании частоты появления соседних отсчетов/ И.Л. Чваркова, Е.Т. Анашко, В.С. Садов. Современная радиоэлектроника: научные исследования, подготовка кадров: сб. материалов (по итогам работы МНПК, Минск, 20-21 апреля 2006 г.): в 3 ч. Ч.1/ М-во образования РБ, Учреждение образования “Минский государственный высший радиотехнический колледж”; под общ. ред. Проф. Н.А. Цырельчука. – Мн.: МГВРК, 2006. – 380 с., С. 351-354.

4. Чваркова, И.Л. Мультиплексирование пропускной способности стеганографического канала передачи данных/ И.Л. Чваркова, А.Ф. Чернявский, В.С. Садов. Известия Белорусской инженерной академии, № 1(17)/2, 2004.– с. 171-174.

Перечень заданий управляемой самостоятельной работы студентов

Управляемая самостоятельная работа студентов (УРС) осуществляется в объеме 12 учебных часов за счет времени отведенного на лабораторный практикум. Целью УРС является освоение принципов проектирования основных элементов стеганографических систем защиты информации.

Задание УСР № 1.

Тема: Методики выбора стеганографических контейнеров.

Содержание задания: Проанализировать методики выбора и возможности различных преобразований контейнеров при стеганографическом встраивании данных;

Форма отчета: групповая защита задания.

Задание УСР № 2.

Тема: Пропускная способность стеганографического канала.

Содержание задания: Мультиплексирование пропускной способности LSB – канала сокрытия данных;

Форма отчета: групповая защита задания.

Задание УСР № 3.

Тема: Атаки на стеганоконтейнеры.

Содержание задания: Статистические атаки на стеганоконтейнеры.

Форма отчета: групповая защита задания.

Перечень используемых средств диагностики результатов учебной деятельности

С целью текущего контроля знаний и умений студентов по дисциплине «Компьютерная стеганография» используются следующие диагностические средства:

- выборочный опрос на лекциях;
- отчеты по лабораторным работам;
- защита групповых заданий по УСР.