Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и образовательным инновациям

_____ О.И. Чуприс
(подпись) (И.О.Фамилия)

27.06.2018
(дата утверждения)

Регистрационный № УД-5235 /уч.

ПРИКЛАДНАЯ СТЕГАНОГРАФИЯ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности:

1-31 80 07 Радиофизика

2018 г.

Учебная программа составлена на основе образовательного стандарта ОСВО 1-31 80 07-2012 «Радиофизика», учебного плана УВО № G31-284/уч. от 26.05.2017 г.

СОСТАВИТЕЛИ:

Василий Сергеевич САДОВ, профессор кафедры интеллектуальных систем Белорусского государственного университета, кандидат технических наук, доцент

Александр Васильевич КУРОЧКИН, ассистент кафедры интеллектуальных систем Белорусского государственного университета

Екатерина Александровна ГОЛОВАТАЯ, ассистент кафедры интеллектуальных систем Белорусского государственного университета

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой интеллектуальных систем

(протокол № 12 от 06.06.2018 г.);

Учебно-методической комиссией факультета радиофизики и компьютерных технологий Белорусского государственного университета

(протокол № 10 от 19.06.2018 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа дисциплины по выбору специальной подготовки «Прикладная стеганография» разработана в соответствии с требованиями образовательного стандарта по специальности 1-31 80 07 «Радиофизика». Программа предназначена для магистрантов дневной формы получения высшего образования.

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

Основная задача дисциплины – сформировать представление о стеганографических системах, а также об основных областях применения; представить основные понятия, связанные со скрытой передачей сообщений по открытым каналам, а также подходы и методы для встраивания и обнаружения передаваемой информации; представить и научить применять подходы и методы для обнаружения несанкционированной передачи данных и защиты конфиденциальной информации.

Для успешного усвоения данной учебной дисциплины необходимы знания по дисциплинам «Основы радиоэлектроники», «Цифровая обработка сигналов», «Программирование» в объеме программы высшей школы.

В результате изучения дисциплины обучаемый должен

знать:

- основные методы и алгоритмы скрытного встраивания одних данных в другие;
- методы обнаружения встроенных сообщений;
- методы повышения пропускной способности стеганографических каналов передачи данных и обеспечения их стойкости;

уметь:

- применять подходы стеганографического анализа каналов передачи информации для обнаружения несанкцианированной передачи данных и противодействия ей;
- применять полученные знания при решении задач защиты конфиденциальной информации в компьютерных системах;

владеть:

- основными методами прикладной стеганографии, в том числе методами встраивания, извлечения, анализа открытых каналов передачи информации.

Формируемые компетенции:

- ПК-7. Работать с научно-технической информацией с использованием современных информационных технологий.
- ПК-11. Разрабатывать численные алгоритмы и программы
- ПК-12. Обосновывать достоверность полученных результатов.
- ПК-13. Формулировать выводы и рекомендации по применению

результатов научно-исследовательской работы.

- ПК-19. Осуществлять поиск, систематизацию и анализ информации по перспективным направлениям информационной безопасности, инновационным технологиям, проектам и решениям.

В соответствии с учебным планом на изучение дисциплины в 3 семестре отведено всего 122 часа, в том числе 48 аудиторных часов, из них лекции – 22 часа, лабораторные работы – 20 часов, управляемая самостоятельная работа – 6 часов. Форма текущей аттестации – зачет в 3 семестре.

Зачетные единицы – 3,5.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

1. **Введение.** Основные понятия и определения в стеганографии, область применения. Понятие открытого канала передачи информации. Общая модель стеганографических систем и требования, предъявляемые к ним.
2. **Стеганографические контейнеры.** Стеганографические контейнеры, их основные типы и характеристики. Способы представления информации. Графические, аудио и видео форматы и контейнеры. Сжатие информации.
3. **Методы встраивания.** Методы встраивания в пространственную область. Встраивание в наименее значащие биты. Метод распределения сообщения по контейнеру. Ключевые и псевдослучайные последовательности. Метод блочного скрытия и метод Куттера-Джордана-Боссена. Методы встраивания в частотную область. Спектральное представление. Дискретное косинусное преобразование. Дискретное вейвлет-преобразование и сингулярное разложение. Метод Коха и Жао и метод Бенгама-Мемона-Эо-Юнга. Особенности алгоритмов встраивания информации в изображения и аудиофайлы. Скрытие данных в видеопоследовательностях.
4. **Цифровой водяной знак.** Особенности и основные свойства цифровых водяных знаков. Цифровые водяные знаки и электронные цифровые подписи. Методы нанесения, извлечения и верификации ЦВЗ.
5. **Атаки на стегосистемы и противодействия им.** Классификация атак на стегосистемы. Визуальная атака на стегосистемы. Статистические атаки на стегосистемы. Особенности атак на графические, аудио и видеоконтейнеры. Понятие стеганографической стойкости. Оценки стойкости стеганографических систем и условия их достижения.
6. **Пропускная способность стеганографических каналов.** Понятие скрытой пропускной способности стегоканалов. Мультиплексирование пропускной способности стегоканалов передачи информации.
7. **Перспективные направления развития стеганографии.**

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

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	**Стеганографические контейнеры**	**2**			4			Выборочный опрос на лекции, отчет по лабораторной работе.
3	**Методы встраивания**	**6**						
	3.1 Методы встраивания в пространственную область.	2			4			Выборочный опрос на лекции, отчет по лабораторной работе.
	3.2 Методы встраивания в частотную область. Спектральное представление.	2						Выборочный опрос на лекции.
	3.3 Особенности алгоритмов встраивания информации в изображения и аудиофайлы. Скрытие данных в видеопоследовательностях.	2			4		2	Выборочный опрос на лекции, отчет по лабораторной работе, реферат.
4	**Цифровой водяной знак**	**2**			4			Выборочный опрос на лекции,

								отчет по лабораторной работе.
5	**Атаки на стегосистемы и противодействия им**	**6**						
	5.1 Классификация атак на стегосистемы. Визуальная атака на стегосистемы. Статистические атаки на стегосистемы.	2						Выборочный опрос на лекции.
	5.2 Особенности атак на графические, аудио и видеоконтейнеры.	2			4			Выборочный опрос на лекции, отчет по лабораторной работе.
	5.3 Оценки стойкости стеганографических систем и условия их достижения. Понятие стеганографической стойкости.	2					2	Выборочный опрос на лекции, реферат.
6	**Пропускная способность каналов передачи скрываемой информации**	**2**						Выборочный опрос на лекции. .
7	**Перспективные направления развития стеганографии.**	**2**					2	Выборочный опрос на лекции, реферат.
	Всего:	22			20		6	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень рекомендуемой литературы

Основная

1. Садов, В.С. Компьютерная стеганография/ В.С. Садов. М.: *изд-во,* 2014.
2. Грибунин, В.Г. Цифровая стеганография/ В.Г. Грибунин, И.Н. Окопов, И.В. Туринцев. М.: изд-во «СОЛОН-Пресс», 2002. - 272 с.
3. Коханович, Г.Ф. Компьютеная стеганография/ Г.Ф. Коханович, А.Ю. Пузыренко. К.: «МК-Пресс», 2006. – 288с., ил.
4. Аграновский, А.В. Основы стеганографии/ А.В, Аграновский, П.Н. Девянин, А.В. Черемущкин, Р.А. Хади. М.: «Радио и связь», 2003. – 152с.
5. Малюк, А.А. Введние в защиту информации в автоматизированных системах. Учебное пособие для вузов. – 3-е издание, стереотипное/ А.А. Малюк, С.В. Пазини, Н.С. Погожин. М.: Горячая линия-Телеком, 2005. – 147с.; ил.
6. Wayner, P. Disappearing Cryptography, Third Edition: Information Hiding: Steganography and Watermarking/ P. Wayner. The Morgan Kaufmann Series in Software Engineering and Programming, 2008. – 456p.
7. Raggo, M. Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols/ M. Raggo, C. Hosmer. Syngress, 2012. – 350p.

Дополнительная

1. Cole, E. Hiding in Plain Sight: Steganography and the Art of Covert Communication/ E. Cole. Wiley, 2003 – 360p.
2. Cox, I.J. Digital Watermarking and Steganography/ I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, T. Kalker. The Morgan Kaufmann Series in Software Engineering and Programming, 2008. – 593p.
3. 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.
4. Чернявский, А.Ф. Оценка информационных потерь при фильтрации изображений/ А.Ф. Чернявский, С.Г. Тихоненко, В.С. Садов. Информатика, №3(7), 2005. – с. 52-59.
5. 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.: 2006. – 380 с., С. 351-254.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ЗАДАНИЙ УСР

1. Анализ существующих стеганографических систем (Xiao Steganography, Image Steganography, Steghide, Crypture и др.)
2. Системы эталонного тестирования: Stirmark, Checkmark, Optimark, RK Benchmark и др.
3. Реализация стеганографической системы с использованием языка javascript.
4. Стеганография на базе стека протоколов TCP/IP.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ РЕФЕРАТОВ

1. Возможности межсетевых экранов для защиты локальных сетей от стеганографической передачи.
2. Возможности стеганографического встраивания в текстовые документы для защиты авторских прав.
3. Машинное обучение в стеганографических системах.
4. Online-системы стеганографического встраивания.
5. Возможности отслеживания факта передачи сообщения при потоковой передаче в режиме реального времени.
6. Передача вредоносных программ посредством стеганографических каналов и подходов.
7. Стеганографическая передача данных посредством голосовых помощников.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ЛАБОРАТОРНЫХ РАБОТ

1. Анализ структуры данных, представленных в различных форматах, преобразование информации, получение служебной информации.
2. Встраивание стеганографических данных в графические файлы.
3. Анализ алгоритмов встраивания скрытого сообщения в частотную область на основе предложенных аудиофайлов.
4. Нанесение, верификация и удаление цифрового водяного знака.
5. Обнаружение и извлечение стеганографических данных.

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СРЕДСТВ ДИАГНОСТИКИ

С целью текущего контроля знаний и умений студентов по учебной дисциплине используются следующие диагностические средства:

- Выборочный опрос на лекциях;
- Отчеты по лабораторным работам;
- Обсуждение рефератов, презентаций и докладов студента, подготовленных по результатам выполнения лабораторных работ и выполняемых в их рамках УСР, самостоятельной работе по индивидуальным заданиям в рамках тематики учебной дисциплины.

Оценивание результатов выполнения лабораторных работ, заданий УСР и выполнения рефератов проводится в соответствии с критериями оценки знаний и компетенций студентов по 10-балльной шкале, изложенными в письме Министерства образования Республики Беларусь №21-04-1/105 от 22.12.2003 г.

Оценка текущей успеваемости определяется как средняя по оценкам лабораторных работ, управляемой самостоятельной работе и рефератам.

МЕТОДИКА ФОРМИРОВАНИЯ ИТОГОВОЙ ОЦЕНКИ

Итоговая оценка формируется на основе:

1. Правил проведения аттестации студентов (Постановление Министерства образования Республики Беларусь № 53 от 29.05.2012 г.);
2. Положения о рейтинговой системе оценки знаний по дисциплине в БГУ (Приказ ректора БГУ от 18.08.2015 г. № 382-ОД);

Критериев оценки знаний студентов (письмо Министерства образования от 22.12.2003 г.)

Итоговый контроль усвоения дисциплины проводится в форме устного собеседования.

Итоговая оценка «зачтено» по дисциплине может быть выставлена студентам, получившим среднюю оценку по результатам итогового собеседования, лабораторным работам, рефератам и управляемой самостоятельной работе не ниже, чем «четыре».

Изложение лекционных материалов рекомендуется сопровождать примерами, иллюстрационным материалом и тестовыми заданиями с контрольными вопросами для закрепления понятий и терминов, устными фронтальными опросами на лекциях. Для успешного выполнения лабораторных работ студентам предлагается предварительно ознакомиться с описанием заданий, соответствующей теоретической частью курса, содержанием рекомендованной литературы. В целях формирования и развития у студентов навыков самоуправления, коммуникативных и

организационно-управленческих умений, а также приобретения опыта командного решения поставленных задач, предлагается организовывать группы студентов численностью до 3 человек для выполнения лабораторных работ. Лабораторные работы выполняются на компьютерах с использованием ресурсов сети Интернет, в средах математических пакетов, отчет подготавливается также на бумажном носителе. Управляемая самостоятельная работа студентов организуется в рамках выполнения лабораторных работ. Формой отчетности по итогам выполнения заданий УСР является реферат (на бумажном носителе).