МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

подписано электронно-цифровой подписью

Программа дисциплины

Основы стеганографии М2.ДВ.6

Направление подготовки: 010300.68 - Фундаментальная информатика и информационные технологии
Профиль подготовки: Математические основы и программное обеспечение информационной безопасности и защиты информации
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Разинков Е.В.

Рецензент(ы):

Андрианова А.А.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 910414

Казань
2014

Содержание

Программу дисциплины разработал(а)(и) ассистент, к.н. Разинков Е.В. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Evgenij.Razinkov@kpfu.ru

1. Цели освоения дисциплины

В курсе рассмотрены основные понятия цифровой стеганографии, общие принципы стеганографической защиты информации, современные методы встраивания информации, эффективные стегоаналитические атаки.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " М2.ДВ.6 Профессиональный" основной образовательной программы 010300.68 Фундаментальная информатика и информационные технологии и относится к дисциплинам по выбору. Осваивается на 2 курсе, 3 семестр.

"Основы стеганографии" входит в состав профессиональных дисциплин. Читается на 2 курсе, в 3 семестре.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-1 (профессиональные компетенции)	способность применять в профессиональной деятельности современные языки программирования и языки баз данных, методологии системной инженерии, системы автоматизации проектирования, электронные библиотеки и коллекции, сетевые технологии, библиотеки и пакеты программ, современные профессиональные стандарты информационных технологий (в соответствии с профилизацией)
ПК-2 (профессиональные компетенции)	способность профессионально решать задачи производственной и технологической деятельности с учетом современных достижений науки и техники, включая: разработку алгоритмических и программных решений в области системного и прикладного программирования; разработку математических, информационных и имитационных моделей по тематике выполняемых исследований; создание информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных; разработку тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям; разработку эргономических человеко-машинных интерфейсов (в соответствии с профилизацией)
ПК-3 (профессиональные компетенции)	способность разрабатывать и реализовывать процессы жизненного цикла информационных систем, программного обеспечения, сервисов систем информационных технологий, а также методы и механизмы оценки и анализа функционирования средств и систем информационных технологий; способности разработки проектной и программной документации, удовлетворяющей нормативным требованиям

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-4 (профессиональные компетенции)	способность демонстрировать знания фундаментальных и смежных прикладных разделов специальных дисциплин магистерской программы, знания общеметодологического характера, знания истории развития информатики и информационных технологий;
ПК-5 (профессиональные компетенции)	способность использовать углубленные теоретические и практические знания в области информационных технологий и прикладной математики, фундаментальные концепции и системные методологии, международные и профессиональные стандарты в области информационных технологий, а также знания, которые находятся на передовом рубеже науки

В результате освоения дисциплины студент:

1. должен знать:

теоретические знания об основных принципах стеганографической защиты информации, стеганографической стойкости;

2. должен уметь:

ориентироваться в современных методах встраивания информации и стегоаналитических атаках;

3. должен владеть:

построениями стеганографических систем и стегоаналитических атак.

4. должен демонстрировать способность и готовность:

понимать роль цифровой стеганографии в обеспечении информационной безопасности;

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 3 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Введение в цифровую стеганографию.	3		0	0	4	домашнее задание

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. Стеганографическая стойкость.	3		0	0	4	домашнее задание
3.	Тема 3. JPEG-стеганография.	3		0	0	4	домашнее задание
4.	Тема 4. Эффективность встраивания.	3		0	0	4	домашнее задание
5.	Тема 5. Стегоанализ.	3		0	0	4	домашнее задание
6.	Тема 6. Стегоанализ алгоритма JSteg.	3		0	0	4	домашнее задание
7.	Тема 7. Стегоанализ, использующий машинное обучение.	3		0	0	4	домашнее задание
8.	Тема 8. Статистический стегоанализ.	3		0	0	4	домашнее задание
.	Тема . Итоговая форма контроля	3		0	0	0	экзамен
	Итого			0	0	32	

4.2 Содержание дисциплины

Тема 1. Введение в цифровую стеганографию.

лабораторная работа (4 часа(ов)):

Основная задача стеганографии. "Проблема заключенных". Понятие стегосистемы.

Тема 2. Стеганографическая стойкость.

лабораторная работа (4 часа(ов)):

Теоретико-информационное определение стеганографической стойкости. Практическая стойкость стегосистем. Факторы, влияющие на стойкость стегосистем.

Тема 3. JPEG-стеганография.

лабораторная работа (4 часа(ов)):

Специфика JPEG-стеганографии. Методы Jsteg и F5.

Тема 4. Эффективность встраивания.

лабораторная работа (4 часа(ов)):

Понятие эффективности встраивания. Матричное встраивание в стеганографических системах.

Тема 5. Стегоанализ.

лабораторная работа (4 часа(ов)):

Виды стегоанализа, их сравнительная характеристика.

Тема 6. Стегоанализ алгоритма JSteg.

лабораторная работа (4 часа(ов)):

Гистограммная атака на метод JSteg.

Тема 7. Стегоанализ, использующий машинное обучение.

лабораторная работа (4 часа(ов)):

Набор характеристик PEV-274. Описание характеристик набора PEV-274, предназначенного для обнаружения информации, встроенной в JPEG-изображения

Тема 8. Статистический стегоанализ.

лабораторная работа (4 часа(ов)):

Метод RS-стегоанализа.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Введение в цифровую стеганографию.	3		подготовка домашнего задания	5	домашнее задание
2.	Тема 2. Стеганографическая стойкость.	3		подготовка домашнего задания	5	домашнее задание
3.	Тема 3. JPEG-стеганография.	3		подготовка домашнего задания	5	домашнее задание
4.	Тема 4. Эффективность встраивания.	3		подготовка домашнего задания	5	домашнее задание
5.	Тема 5. Стегоанализ.	3		подготовка домашнего задания	5	домашнее задание
6.	Тема 6. Стегоанализ алгоритма JSteg.	3		подготовка домашнего задания	5	домашнее задание
7.	Тема 7. Стегоанализ, использующий машинное обучение.	3		подготовка домашнего задания	5	домашнее задание
8.	Тема 8. Статистический стегоанализ.	3		подготовка домашнего задания	5	домашнее задание
	Итого				40	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лабораторных занятий и самостоятельной работы студентов.

Список литературы разделен на две категории: необходимый для сдачи зачета минимум и дополнительная литература.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы.

Кроме того, самостоятельная работа включает подготовку к зачету. При подготовке к сдаче зачета весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к зачету, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда будет резерв времени.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Введение в цифровую стеганографию.

домашнее задание , примерные вопросы:

Программная реализация метода LSB.

Тема 2. Стеганографическая стойкость.

домашнее задание , примерные вопросы:

Программная реализация вычисление относительной энтропии между двумя дискретными распределениями.

Тема 3. JPEG-стеганография.

домашнее задание , примерные вопросы:

Программная реализация алгоритма JSteg.

Тема 4. Эффективность встраивания.

домашнее задание , примерные вопросы:

Программная реализация матричного кодирования и метода F5.

Тема 5. Стегоанализ.

домашнее задание , примерные вопросы:

Провести сравнительный анализ современных стеганографических методов с точки зрения их стойкости к стегоаналитическим атакам.

Тема 6. Стегоанализ алгоритма JSteg.

домашнее задание , примерные вопросы:

Программная реализация атаки на алгоритм JSteg.

Тема 7. Стегоанализ, использующий машинное обучение.

домашнее задание , примерные вопросы:

Программная реализация вычисления характеристик PEV-274.

Тема 8. Статистический стегоанализ.

домашнее задание , примерные вопросы:

Программная реализация метода RS-стегоанализа.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

Контрольная работа 1:

Программная реализация стеганографического встраивания с нарушением квантования.

Контрольная работа 2:

Программная реализация метода nsF5.

Вопросы к зачету:

1. Что такое стеганография?

2. Какие специфические возможности предоставляет стеганография в отличие от других средств защиты информации?

3. Какие типы нарушителей рассматриваются в стеганографии?

4. Что такое стегосистема?
5. Что такое стеганографический контейнер? Примеры.
6. Какая стеганографическая система называется стойкой?
7. Что такое теоретическая стойкость стегосистемы?
8. Что такое практическая стойкость стегосистемы?
9. Какие факторы влияют на стойкость стегосистемы?
10. Что такое матричное встраивание?
11. Что такое стегоанализ?
12. Какие виды стегоанализа Вы знаете?
13. Что такое статистический стегоанализ? Каковы его плюсы и минусы?
14. Что такое стегоанализ, основанный на контролируемом обучении? Каковы его плюсы и минусы?
15. Каковы преимущества использования адаптивного правила выбора элементов стеганографического контейнера? Какие при этом могут возникнуть проблемы?
16. Почему JPEG является предпочтительным форматом для использования в качестве стеганографического контейнера?
17. Алгоритм JSteg. Его недостатки.
18. Алгоритм F5. Его достоинства и недостатки.
19. Алгоритм матричного кодирования.
20. RS-стегоанализ.

Типовой билет:

1. Что такое стегоанализ?
2. Алгоритм матричного кодирования.

7.1. Основная литература:

Теоретическая информатика, Громкович, Юрай;Мельников, Б. Ф., 2010г.

Введение в теоретико-числовые методы криптографии, Глухов, Михаил Михайлович;Круглов, Игорь Александрович;Пичкур, Андрей Борисович;Черемушкин, Александр Васильевич, 2011г.

3. . Латыпов Р.Х. Электронный образовательный ресурс "Кодирование информации и криптография - Математические основы" - [Электронный ресурс]. 2009- Режим доступа: http://zilant.kpfu.ru/course/view.php?id=3.

4. Баранова, Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб. пособие / Е. К. Баранова. - М. : РИОР : ИНФРА-М, 2013. - 183 с. . - Режим доступа: http://www.znanium.com/bookread.php?book=415501

5. Электронная коммерция[Электронный ресурс]: Учебник / Л.А. Брагин, Г.Г. Иванов, А.Ф. Никишин, Т.В. Панкина. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2012. - 192 с. . - Режим доступа: http://www.znanium.com/bookread.php?book=304162

7.2. Дополнительная литература:

Защита информации в электронных платежных системах, Иванов, М. А.;Михайлов, Д. М.;Чугунков, И. В., 2011г.

Комплексная защита информации на предприятии. Т. 1, , 2012г.

7.3. Интернет-ресурсы:

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Интернет--портал ресурсов по математическим наукам - http://www.math.ru/

Интернет--портал ресурсов по математическим наукам - http://www.allmath.com/

Интернет-портал со статьями по алгоритмике и программированию - http://algolist.manual.ru/

Электронная библиотека по техническим наукам - http://techlibrary.ru

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Основы стеганографии" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

лабораторные занятия по дисциплине проводятся в аудитории, оснащенной доской и мелом (маркером)

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010300.68 "Фундаментальная информатика и информационные технологии" и магистерской программе Математические основы и программное обеспечение информационной безопасности и защиты информации .

Автор(ы):
Разинков Е.В. _____
"__" _____ 201 __ г.

Рецензент(ы):
Андрианова А.А. _____
"__" _____ 201 __ г.