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

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Таюрский Д.А.
_____
"___"_____20___ г.

Программа дисциплины

Основы стеганографии Б1.В.ДВ.4

Направление подготовки: 02.04.02 - 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

Казань
2016

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 " Б1.В.ДВ.4 Дисциплины (модули)" основной образовательной программы 02.04.02 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
ОК-1 (общекультурные компетенции)	способность к абстрактному мышлению, анализу, синтезу
ОК-2 (общекультурные компетенции)	готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения
ОК-3 (общекультурные компетенции)	готовность к саморазвитию, самореализации, использованию творческого потенциала
ОПК-2 (профессиональные компетенции)	готовность руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия
ОПК-3 (профессиональные компетенции)	способность использовать и применять углубленные теоретические и практические знания в области фундаментальной информатики и информационных технологий
ОПК-4 (профессиональные компетенции)	способность самостоятельно приобретать и использовать в практической деятельности новые знания и умения, в том числе, в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять своё научное мировоззрение
ОПК-5 (профессиональные компетенции)	способность использовать углублённые знания правовых и этических норм при оценке последствий своей профессиональной деятельности, при разработке и осуществлении социально значимых проектов
ПК-14 (профессиональные компетенции)	способность выполнять работу экспертов в ведомственных, отраслевых или государственных экспертных группах по экспертизе проектов, тематика которых соответствует направленности (профилю) программы магистратуры

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-15 (профессиональные компетенции)	способность работать в международных проектах по разработке открытых спецификаций новых информационных технологий, реализуемых международными профессиональными организациями и консорциумами на основе принципа консенсуса
ПК-16 (профессиональные компетенции)	способность участвовать в деятельности профессиональных сетевых сообществ по конкретным направлениям
ПК-17 (профессиональные компетенции)	способность осознавать корпоративную политику в области повышения социальной ответственности бизнеса перед обществом, принимать участие в ее развитии
ПК-4 (профессиональные компетенции)	способность разрабатывать архитектурные и функциональные спецификации создаваемых систем и средств, а также разрабатывать абстрактные методы их тестирования
ПК-5 (профессиональные компетенции)	способность управлять проектами, планировать научно-исследовательскую деятельность, анализировать риски, управлять командой проекта
ПК-7 (профессиональные компетенции)	способность разрабатывать и оптимизировать бизнес-планы научно-прикладных проектов
ПК-9 (профессиональные компетенции)	способность осознавать и разрабатывать корпоративные стандарты и политику развития корпоративной инфраструктуры информационных технологий на принципах открытых систем

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.

понимать роль цифровой стеганографии в обеспечении информационной безопасности;

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 72 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	1	2	0	0	домашнее задание
2.	Тема 2. Стеганографическая стойкость.	3	2	2	0	0	домашнее задание
3.	Тема 3. JPEG-стеганография.	3	3-4	4	0	0	домашнее задание
4.	Тема 4. Эффективность встраивания.	3	5-6	2	0	0	домашнее задание
5.	Тема 5. Стегоанализ.	3	7-8	2	0	0	контрольная работа домашнее задание
6.	Тема 6. Стегоанализ алгоритма JSteg.	3	9-10	2	0	0	домашнее задание
7.	Тема 7. Стегоанализ, использующий машинное обучение.	3	11-12	2	0	0	домашнее задание
8.	Тема 8. Статистический стегоанализ.	3	13-14	2	0	0	контрольная работа домашнее задание
.	Тема . Итоговая форма контроля	3		0	0	0	экзамен
	Итого			18	0	0	

4.2 Содержание дисциплины

Тема 1. Введение в цифровую стеганографию.

лекционное занятие (2 часа(ов)):

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

Тема 2. Стеганографическая стойкость.

лекционное занятие (2 часа(ов)):

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

Тема 3. JPEG-стеганография.

лекционное занятие (4 часа(ов)):

Специфика JPEG-стеганографии. Методы Jsteg и F5.

Тема 4. Эффективность встраивания.

лекционное занятие (2 часа(ов)):

Понятие эффективности встраивания. Матричное встраивание в стеганографических системах.

Тема 5. Стегоанализ.

лекционное занятие (2 часа(ов)):

Виды стегоанализа, их сравнительная характеристика.

Тема 6. Стегоанализ алгоритма JSteg.

лекционное занятие (2 часа(ов)):

Гистограммная атака на метод JSteg.

Тема 7. Стегоанализ, использующий машинное обучение.

лекционное занятие (2 часа(ов)):

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

Тема 8. Статистический стегоанализ.

лекционное занятие (2 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	1	подготовка домашнего задания	5	домашнее задание
2.	Тема 2. Стеганографическая стойкость.	3	2	подготовка домашнего задания	5	домашнее задание
3.	Тема 3. JPEG-стеганография.	3	3-4	подготовка домашнего задания	5	домашнее задание
4.	Тема 4. Эффективность встраивания.	3	5-6	подготовка домашнего задания	5	домашнее задание
5.	Тема 5. Стегоанализ.	3	7-8	подготовка домашнего задания	2	домашнее задание
				подготовка к контрольной работе	2	контрольная работа
6.	Тема 6. Стегоанализ алгоритма JSteg.	3	9-10	подготовка домашнего задания	4	домашнее задание
7.	Тема 7. Стегоанализ, использующий машинное обучение.	3	11-12	подготовка домашнего задания	4	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
8.	Тема 8. Статистический стегоанализ.	3	13-14	подготовка домашнего задания	2	домашнее задание
				подготовка к контрольной работе	2	контрольная работа
	Итого				36	

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.

контрольная работа , примерные вопросы:

Программная реализация стеганографического встраивания с нарушением квантования.

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.

контрольная работа , примерные вопросы:

Программная реализация метода nsF5.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

Вопросы к экзамену:

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:

1. Громкович, Ю. Теоретическая информатика: Введение в теорию автоматов, теорию вычислимости, теорию сложности, теорию алгоритмов, рандомизацию, теорию связи и криптографию / Юрай Громкович; Пер. с нем.; Под ред. Б. Ф. Мельникова.?Издание 3-е.?Санкт-Петербург: БХВ-Петербург, 2010.?336 с.

2. Латыпов Р.Х., Разинков Е.В. Электронный образовательный ресурс "Теория кодирования информации и криптография", 2015. - URL: http://tulpar.kfu.ru/enrol/index.php?id=2422

3. Червяков Н.И., Евдокимов А.А., Галушкин А.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. - - М.: Физматлит, 2012. - 280 с. URL: http://e.lanbook.com/books/element.php?pl1_id=5300

4. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. URL: http://znanium.com/bookread.php?book=441493

5. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. URL: http://znanium.com/bookread.php?book=420047

6. Столов Е.Л. Генераторы случайных чисел в системах компьютерной безопасности[Электронный ресурс]. - Казань, .2014 - Режим доступа: http://shelly.kpfu.ru/e-ksu/docs/F833856100/FinalGen.pdf.

7.2. Дополнительная литература:

1. Маскаева А. М. Основы теории информации: Учебное пособие / А.М. Маскаева. - М.: Форум: НИЦ ИНФРА-М, 2014. - 96 с. - ЭБС "Знаниум": http://znanium.com/bookread.php?book=429571

2. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. - ЭБС "Знаниум": http://znanium.com/bookread.php?book=474838

3. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - ЭБС "Знаниум": http://znanium.com/bookread.php?book=503511

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 02.04.02 "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.