ИЗУЧЕНИЕ КРИПТОГРАФИИ И СТЕГАНОГРАФИИ В ПОВОЛЖСКОМ ГОСУДАРСТВЕННОМ УНИВЕРСИТЕТЕ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ (ПГУТИ)

АЛЕКСАНДР П. АЛЕКСЕЕВ

TEACHING CRYPTOGRAPHY AND STEGANOGRAPHY AT THE PSUTI UNIVERSITY - RUSSIA

ALEKSANDR P.ALEKSEEV

ABSTRACT: *The report examines the progress and challenges in teaching cryptography and steganography at PGUTI University – Samara, Russia. Short review of the contents of lectures and labs is done.*

KEYWORDS: *cryptography, steganography.*

В Поволжском государственном университете телекоммуникаций и информатики (Россия, Самара) обучают специалистов, работающих в области защиты информации (Информационная безопасность телекоммуникационных систем, специальность - 10.05.02 и Информационная безопасность, специальность - 10.03.01).

В докладе рассмотрены вопросы изучения криптографии и стеганографии в рамках дисциплины «Информатика», которая преподаётся студентам на первом курсе.Дисциплина «Информатика» для указанных специальностей изучаетсяв ПГУТИ в двух семестрах первого года обучения. На лекции отводится 44 часа, на лабораторные работы – 120 часов, на практику – 28 часов, во втором семестре выполняется курсовая работа. Оба семестра завершаются экзаменами.

В рамках дисциплины «Информатика» студенты изучают основные понятия информатики, арифметические и логические основы работы ЭВМ, кодирование информации (сжатие информации, помехоустойчивое кодирование, QR-коды), устройство и принцип действия ЭВМ, системное и прикладное программное обеспечение, сетевые информационные технологии, моделирование телекоммуникационных устройств, а также получают первое представление о методах защиты информации.

Перечислим лабораторные работы, посвященные защите информации:

- Моделирование криптосистемы (метод гаммирования);
- Шифрование с помощью управляемых операций;
- Скрытая передача информации в графике;
- Стеганографические программы Courier и S-Tools;
- Сокрытие информации в графике и тексте с помощью системы Mathcad;
- Сокрытие информации на HTML-страницах;
- Скрытая передача данных в субтитрах;
- Скрытая передача информации по протоколу TCP/IP;
- Стеганографическая передача данных в звуковых файлах формата WAV и MP3;
- Скрытая передача информации методом временного распыления.

В лабораторной работе «Моделирование криптосистемы» студенты с помощью программы Multisimисследуют криптосистему, состоящую из двух арифметико-логических

устройств (передающего и приемного). Результаты моделирования сопоставляются с ручными расчетами. Студенты оценивают влияние гаммы на степень криптостойкости системы.

Лабораторная работа «Шифрование с помощью управляемых операций» является развитием первой работы. В этой криптосистеме помимо операции Исключающее ИЛИ для шифрования используется логическая операция Равнозначность, а также арифметические операции сложения и вычитания [1]. Эти операции при шифровании чередуются в псевдослучайном порядке.

Лабораторная работа «Скрытая передача информации в графике» дает студентам первое представление о стеганографии. Студенты извлекают информацию из рисунков, на которых информация в двоичном виде скрыта в различных местах (рамка рисунка, цвет лампочек на новогодней ёлке, псевдослучайно расположенные точки).

Следующая работа дает первое представление о профессиональной стеганографической программе S-Tools и стеганоанализе. Программа S-Tools перед сокрытием информации выполняет её шифрование. При извлечении информации, скрытой с помощью программы Courier, студенты анализируют дамп памяти рисунка и, выделяя два последних бита, получают скрытое сообщение. В качестве вспомогательного инструмента используется редактор памяти.

Очередные лабораторные работы показывают принципы срытой передачи информации с помощью различных контейнеров (HTML-страниц, субтитров в фильмах, звуковых файлов).

Лабораторная работа «Скрытая передача информации по протоколу TCP/IP» основывается на преднамеренном изменении длины передаваемых пакетов [2]. Идея лабораторной работы «Скрытая передача информации методом временного распыления» заключается в кратковременной замене рисунка, размещенном на Web-странице, другим рисунком, содержащим вложение [3]. Основная цель этих лабораторных работ была показать студентам возможность скрытой передачи информации практически в любом электронном контейнере.

Кроме лабораторных работ вопросы защиты информации изучаются студентами на практических занятиях. Студенты выполняют дешифрацию криптограмм, составленных с помощью классических шифров (Цезаря, атбаш, квадрат Полибия, таблица Виженера, метод перестановок, шифр Плейфейра, аффинные преобразования, метод гаммирования).

На лекциях и практике кроме перечисленных вопросов рассматриваются шифры с открытым ключом.

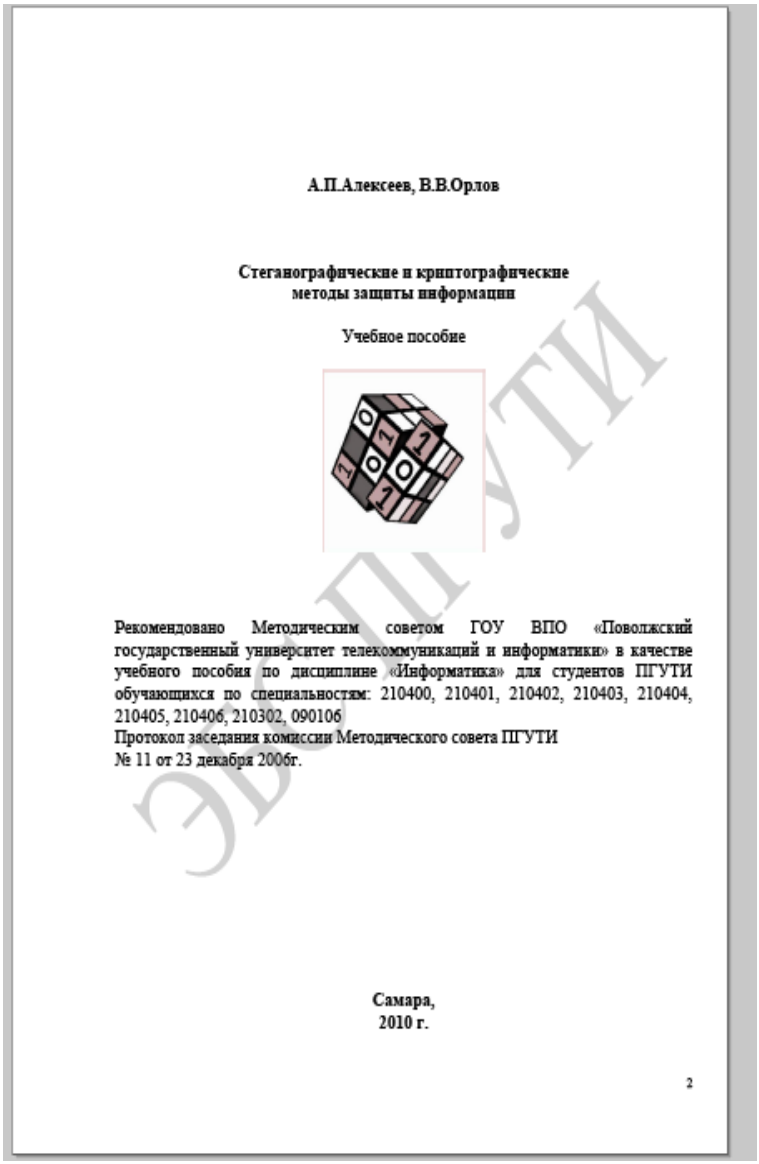
При выполнении курсовой работы студенты извлекают информацию из HTML-контейнеров. Причем передаваемая информация распылена по нескольким контейнерам, а перед распылением сообщение, преобразованное в двоичный код, шифруется путем выполнения перестановок битов с помощью матриц. В некоторых вариантах курсовой работы ведется моделирование шифра RSA с помощью математической системы Mathcad.

Проблемам защиты информации посвящено достаточно большое число дипломных работ. Перечислим темы некоторых дипломных работ:

- Разработка шифра с большим числом математических преобразований;
- Разработка и исследование методов обнаружение вложений в графических контейнерах путем проверки статистических гипотез;
- Исследование Midi-файлов на предмет скрытой передачи информации;
- Разработка атаки на шифр «Графические матрицы» с помощью нейронных сетей;
- Пространственно-временное сокрытие информации на HTML-страницах;
- Адаптивный шифр со скрытым ключом.

По результатам исследований, проведенных преподавателями совместно со студентами, было опубликованы монографиии учебники [7, 8, 9] (фиг.1), сделано свыше 70 докладов на научно-технических конференциях, получены патенты и опубликованы статьи в научно-технических журналах России, защищена магистерская диссертация. За последние пять лет в ПГУТИ защищено три диссертации на соискание степени кандидата технических наук, тематика которых связана с крптографией и стеганографией.

Наиболее способные студенты продолжили заниматься наукой и преподавательской деятельностью после окончания ВУЗа. Между ПГУТИ и Шуменском Университете заключен договор о творческом сотрудничестве (фиг. 2).



А.П.Алексеев, В.В.Орлов

Стеганографические и криптографические
методы защиты информации

Учебное пособие

Рекомендовано Методическим советом ГОУ ВПО «Поволжский государственный университет телекоммуникаций и информатики» в качестве учебного пособия по дисциплине «Информатика» для студентов ПГУТИ обучающихся по специальностям: 210400, 210401, 210402, 210403, 210404, 210405, 210406, 210302, 090106
Протокол заседания комиссии Методического совета ПГУТИ
№ 11 от 23 декабря 2006г.

Самара,
2010 г.

2

Фиг.1

KONSTANTIN PRESLAVSKY UNIVERSITY SHUMEN

ШУМЕНСКИ УНИВЕРСИТЕТ "ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ"

9712 SHUMEN tel. (+359 54) 830 350 telex 73421
fax (+359 54) 830 371
www.shu-bg.net

RECTOR tel. (+359 54) 830 350
e-mail: rector@shu-bg.net

ШУМЕНСКИ УНИВЕРСИТЕТ "ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ"
Изх. No РД-09-1696
09.09.2013 г.
п.код 9712 Шумен

„Утверждаю"

Проректор Шуменского университета
им. Епископа Константина Преславского

проф. дин ...../Г. Колев/
2013 г.

АКТ

использования результатов исследовательской работы

Настоящим актом подтверждается использование результатов разработки и исследования методов защиты информации, изложенных в книге Алексеева А.П. и Орлова В.В. „Стеганографические и криптографические методы защиты информации" в учебном процессе при изучении дисциплин „Компьютерная и сетевая безопасность" и „Компьютерная сеганография" и в научно-исследовательской работе преподавателей, докторантов и студентов лаборатории "Компютерная безопасность" Факультета математики и информатики.

Декан
Факультета математики и информатики:
Проф. д-р Р. Петрова

Заведующий кафедрой
Компьютерных систем и технологий:
Доц. д-р инж. Ст. Станев

09 Сентября 2013 г.
г. Шумен, Болгария

Фиг.2

ЛИТЕРАТУРА

1. Алексеев А.П., Жеренов Ю.В., Орлов В.В. Моделирование криптосистемы с управляемыми операциями с помощью MULTISIM// Инфокоммуникационные технологии, том 7, № 4, 2009. Стр. 78-82.
2. Орлов В.В., Алексеев А.П. Способ стеганографической передачи информации в сети TCP/IP. Патент 2463670. Заявка 2010125304/08(035921). Дата подачи заявки 18.06.2010. МПК G09C 1/00, H04L 9/00.
3. Алексеев А.П., Макаров М.И. Адаптивный шифр с пространственно-временным распылением информации// Инфокоммуникационные технологии, том 9, № 1, 2011. Стр. 62-66.
4. Аленин А.А. Разработка и исследование методов скрытой передачи информации в аудиофайлах. Специальность 05.13.15 – «Вычислительные машины, комплексы и компьютерные сети». Автореферат. 2012 г.
5. Орлов В.В. Методы скрытой передачи информации в телекоммуникационных сетях. Специальность 05.12.13 – «Системы, сети и устройства телекоммуникаций». Автореферат. 2012 г.
6. Макаров М.И. Разработка и исследование методов скрытой распределённой передачи сеансовых данных в телекоммуникационных сетях. Специальность 05.12.13 – «Системы, сети и устройства телекоммуникаций».Автореферат. 2013 г.
7. Алексеев А.П. Информатика 2001. – М.: Солон-Р, 2001. – 364 с.
8. Алексеев А.П. Информатика 2007. – М.: СОЛОН-ПРЕСС, 2007. - 608 с.
9. Алексеев А.П., Орлов В.В. Стеганографические и криптографические методы защиты информации: учебное пособие. - Самара: ИУНЛ ПГУТИ, 2010. – 330 с.