электронный научно-технический журнал
ИНЖЕНЕРНЫЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51036. ISSN 2307-0595

Особенности изучения методов стеганографии в МГТУ им. Н.Э. Баумана

 # 08, август 2015

Чичварин Н. В.[1,*]

УДК: 372.8 + 372.8

[1]Россия, МГТУ им. Н.Э. Баумана
[*]genrih.gertz@gmail.com

Введение

Настоящая статья посвящена описанию опыта, накопленного в последние восемь лет при изучении методов и алгоритмов стеганографии и стегоанализа, как раздела дисциплины «Обнаружение и распознавание сигналов» («ОиРС») на кафедре «Информационная безопасность» МГТУ им. Н.Э. Баумана. Вопросы стеганографии и стегоанализа составляют почти треть объема дисциплины «ОиРС», изучаемой студентами четвертого курса в течение двух семестров. Размещение вопросов стеганографии не случайно – при решении задач стеганографии и стегоанализа часто применяются методы, основанные на теории обнаружения и распознавания. Кроме того внимание студентов обращается на стеганографические методы защиты от НСД каналов передачи сообщений. Название публикации также сформулированно не случайно. Автор придерживается традиционного взгляда на учебный процесс в техническом ВУЗе уровня МГТУ им.Н.Э. Баумана. Напомню, что именно в Императорском Московском Техническом Училище разработан и применяется так называемый русский метод подготовки инженеров, отличающийся следующим:

- Готовятся специалисты широкого профиля, способные ставить и решать задачи, требующие сочетания разных областей знаний.
- Практическая и теоретическая подготовка тесно связаны.
- Много внимания уделяется изучению различных технологий и технологических аспектов проектирования.

Но, пожалуй, самое главное – это то, что в МВТУ не учат а учатся - и студенты, и преподаватели. Пока эта традиция сохранена и в МГТУ им. Н.Э.Баумана.

В настоящей статье на основе анализа публикаций показывается, каким образом строится учебный процесс по изучению раздела дисциплины «Обнаружение и распознавание сигналов» - «стеганография и стегоанализ». Естественно, этот опыт учтен при формировании учебно – методического комплекса дисциплины «ОиРС».

1. Анализ опыта преподавания дисциплин, связанных со стеганографией и стегоанализом

Аналитический обзор доступных публикаций, проведенный автором статьи «Современный уровень преподавания стеганографии в России» показал, что в подавляющем большинстве университетов дисциплина с точно таким названием не преподается. По данным Федерального портала «Российское образование» [2] в некоторых технических вузах дисциплина изучается параллельно с криптографией и криптоанализом. Наибольшее внимание вопросам встраивания ЦВЗ уделяется в полиграфических ВУЗах.

В свою очередь, стеганография в явном виде в законодательстве не упоминается. Не существует каких-либо официальных инструкций и государственных стандартов, регламентирующих применение стеганографических средств. Не сложился не потребительский рынок в этой области, нет четкого кадрового запроса на специалистов по стеганографии. В связи с этим стеганографии находится на вторых ролях в учебных планах вузов и рассматривается как некий раздел криптографии. Во многих ВУЗах стеганография является факультативным предметом, она может входить как раздел в различные учебные курсы. При этом вопросами стеганографии могут заниматься не только вузы, в которых студенты обучаются по направлениям подготовки и специальностям, связанным с информационной безопасностью.

Перечислим некоторые из вузов, которые реализуют обучение стеганографии в рамках отдельной учебной дисциплины:

- Национальный исследовательский ядерный университет «МИФИ» (Стеганография);
- Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Технологии стеганографии в системах инфокоммуникаций);
- Санкт-Петербургский государственный университет аэрокосмического приборостроения (Технологии стеганографии в системах инфокоммуникаций);
- Национальный исследовательский Саратовский государственный университет имени Н.Г.Чернышевского (Основы стеганографии);
- Российский государственный социальный университет (Криптография и стеганография);
- Южный федеральный университет (факультатив);
- Поволжский государственный технологический университет (Стеганография);
- Владивостокский государственный университет экономики и сервиса (Основы стеганографии и цифровые водяные знаки);
- Казанский (Приволжский) федеральный университет (Основы стеганографии);
- Дагестанский государственный институт народного хозяйства (Стеганография).

В перечисленных вузах вопросам стегоанализа отдельного внимания не уделяется. Можно полагать, что это связано с тем, что методы стегоанализа изучаются студентами –

будущими специалистами в области информационной безопасности. Пожалуй, можно согласиться и с утверждением, что стеганография и стегоанализ, строго говоря не являются самостоятельной наукой.

2. Основные аспекты методики изучения дисциплины в МГТУ им. Н.Э. Баумана

Раздел изучается на втором семестре. Объем нагрузки:
Лекции – 8 часов.
Семинары – 7 часов.
Самостоятельная работа (выполнение домашнего задания) – 30 часов.

Модуль 1. Компъютерная стеганография

- Методы использования зарезервированных для расширения полей компьютерных форматов данных.
- Методы специального форматирования текстовых файлов.
- - Методы использования известного смещения слов, предложений, абзацев.
- - Методы выбора определенных позиций букв (нулевой шифр).
- - Методы использования специальных свойств полей форматов, не отображаемых на экране.
- Методы скрытия в неиспользуемых местах гибких дисков.
- Методы использования имитирующих функций (mimic-function).
- Методы удаления идентифицирующего файл заголовка.
- Методы, основанные на разработке специальной файловой системы.

Модуль 2. Цифровая стеганография и методы стегоанализа

Направление стеганографии, основанное на скрытии данных в цифровых объектах, изначально имеющих аналоговую природу, то есть мультимедиа-объекты (изображения, видео, звуки):

- Методы использования избыточности цифровых фотографии, цифрового звука и цифрового видео.
- Методы использования младших разрядов цифровых отсчетов.

Анализ алгоритмов встраивания сообщений в изображения. Алгоритмы встраивания данных в пространственной области. Алгоритмы встраивания цифровых водяных знаков (ЦВЗ) в области преобразования. Встраивание цифровых водяных знаков (ЦВЗ) в коэффициенты ДКП. Аддитивные алгоритмы. Алгоритмы на основе линейного встраивания цифровых водяных знаков ЦВЗ. Алгоритмы на основе слияния цифровых водяных знаков ЦВЗ и контейнера. Алгоритмы на основе квантования.

Модуль 3. Комбинированные методы стеганографии.

Направление цифровой стеганографии, основанное на скрытии данных в цифровых объектах, изначально имеющих аналоговую природу, предварительно подвергнутых преперированию: фильтрация, сегментирование, формирование цифровых голограмм. Анализ методов цифровой голографии. Анализ методов конволюции и деконволюции.

Всего на дисциплину «ОиРС» отведено 170 часов. Понятно, что объем аудиторных занятий при изучении обсуждаемого раздела сравнительно мал. Причины такого размещения материалов раздела:

- Наибольшее число угроз информационной безопасности ЭВМ, системам и КПС приходится на КПС. Именно безопасность КПС изучается в дисциплине «ОиРС».
- Каких-либо трудных для осмысления теоретических аспектов методов стеганографии не существует. Они понимаются в процессе проведения численных экспериментов.
- Вопросы стегоанализа имеют ту же теоретическую основу, что и информационная безопасность КПС.
- Описание классических алгоритмов стеганографии и методов стегоанализа приведено в учебных пособиях [5, 6].

Организационные аспекты изучения раздела и уровень подготовки абитуриентов и студентов кафедры «Информационная безопасность» во многом определили и основные методические аспекты дисциплины «ОиРС» и методику изучения методов стеганографии и стегоанализа. Нелишне подчеркнуть, что абитуриенты, участвующие в олимпиаде «Шаг в будущее» разрабатывают проекты, посвященные стеганографическим методам сокрытия данных. В немалой степени это связано с тем, что для разработки какой – либо программы, реализующей алгоритм стеганогрфии не требуется серьезной математической подготовки, а программировать (писать коды), могут и школьники. Однако при разработке комбинированных, специальных методов цифровой стеганографии требуется знать теорию вероятности, математическую статистику, специальные главы физики, обладать уже значительным инженерным кругозором.

Следует отметить, что практические вопросы, связанные с компьютерной стеганографией в дисциплине «ОиРС» не рассматриваются по следующим причинам:

- Большинство методов компьютерной стеганографии реализуются в течение длительного времени. Дисциплина может оказаться перегруженной.
- Проведение семинарских занятий сопряжено с риском разрушения операционной системы. Поэтому для семинаров необходимо выделить специальный класс с числом компъютеров до 25. Кроме того непроизводительные затраты на инсталляцию операционной системы затрудняют организацию полноценных занятий.

Поэтому вопросы компъютерной безопасности рассматриваются только на лекциях. Планируется проведение демонстрации результатов курсового и дипломного проектирования. Так, например, одна из студенческих разработок позволяет делать невидимыми

файлы, размещенные на различных носителях в компьютерах и цифровых фотоаппаратах. Это достигается следующей процедурой:

- На носитель заносится специальная файловая система – FATNew, которая принимает на себя функциии базовой системы.
- Носитель сопрягается с компьютером, либо с фотоаппаратом.
- Производится запись данных на тот же носитель.

При просмотре содержимого файла ни один из записанных файлов не читается. Просмотр свойств носителя средствами штатными средствами Windows показывает, что носитель чист. Обнаружить присутствие скрытых данных позволяют программные средства AXE и WINHEX.

Интересен пример творчества студентов. Два студента выполнили проект по электронике и ДЗ по дисциплине «ОиРС», разработав и изготовив опытный образец частотного скремблера. Этот опыт изучен и учитывается при оборудовании новой лаборатории.

3. Описание аппаратно - программного обеспечения учебного процесса

Перспективой развития является постановка и внедрение в учебный процесс лабораторного практикума. Планируется дополнить класс лаборатории кафедры программно – аппаратными средствами, который позволяет студентам заниматься и самостоятельно. Ниже приводится один из вариантов.

3.1 Автоматизированный программно – аппаратный комплекс для проведения экспериментов

a. Модульная система виброакустических измерений «National Instruments cDAQ»
b. Модульная система для генерации и анализа радиосигналов «National Instruments PXI-RF 6.6»
c. Рабочее место на базе систем технического зрения NI Smart Camera.

   Состав NI Smart Camera:

   - Интеллектуальная видеокамера NI 1742 Smart Camera.
   - Универсальная плата NI, позволяющая обрабатывать и отображать мультиплицированные видеосигналы, снимаемые с видеокамеры.

d. Программные средства AXE и WINHEX.

Выбор поставщика перечисленных средств не случаен: ВУЗ имеет долгую и глубокую связь с официальным дистрибутором NI.

4. Основные результаты описанного метода

Одним из результатов обсуждаемой методики является пример самостоятельной работы студентов, традиционно участвующих в Международной научно-технической конференции «Безопасные информационные технологии». Так, например, на 3-ей Междуна-

родной научно-технической конференции «Безопасные информационные технологии – 2012» автор обобщил результаты численных экспериментов, проведенных авторами публикаций, приведенных в сборнике трудов названной конференции: Н. Гончаровым, М. Заикиным, Е. Ларионцевой, Н. Стельмашук, Я. Крохиной, Е. Ивановой, В. Карташовым, Д. Островским, К. Логиновым, А. Сиволаповым, Э. Хузиной, Р. Максимовым – студентами кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. Результаты были получены на семинарских занятиях и при выполнении домашних заданий, темы которых сами выбрали указанные студенты. Рассмотрены:

1) Алгоритмы встраивания данных в пространственной области:
   - Алгоритм Катера (Kutter).
   - Алгоритм Брундокса (Bruyndonckx).
   - Алгоритм Ленгелаара (Langelaar).
   - Алгоритм PatchWork.
   – Алгоритм LSB.
2) Алгоритмы встраивания данных в частотной области.
3) Алгоритмы встраивания данных в звуковые файлы.

Немалый интерес может вызвать проведенный студентами анализ и экспериментальные исследования комбинированных стеганографические методов, предложенных в [5]. Студенты убеждаются, что они обладают значительными преимуществами перед классическими методами. Так, моделирование, проведенное студентами показало, что применение корреляционного метода распознавания, наиболее распространенного в стеганоанализе к данным стегоалгоритмам малоэффективно. Так, студенты наглядно установили, что при дефокусировке, изменении размеров или повороте искомый объект в области анализа не обнаруживается. И, с другой стороны, применение крреляционного стегоанализа при реализации комбинированного метода стеганографии, сочетающего искуственную дефокусироку с последующим сокрытием сообщения неэффективно. Студенты убеждаются, что применение методов и критериев теории обнаружения (Байеса, Котельникова, Неймана – Пирсона) возможно как при решении задач стегоанализа, так и для оценки ИБ КПС. Понятно, что если бы эти вопросы изучались лишь на лекциях, материал бы усвоен не до конца, да и утверждения преподавтеля даже с использованием технических средств были бы неубедительны.

Оригинальные методы стеганографии, предлагаемые дипломниками ежегодно разрабатываются при подготовке дипломных проектов и дипломных работ. В год до пяти проектов защищаются по названной тематике. Характерным подтверждением широкого профиля студентов и выпускников МГТУ им. Н.Э. Баумана служит следующее: студент применил метод формирования Фурье – голограммы изображения текста, а затем записал голограмму в изображение – контейнер. С помощью численного эксперимента студент показал высокую робастность предложенного комбинированного стеганографического метода. Следует отметить, что результаты исследований опубликованы и вызвали значительный интерес. Например – [9].

Вторым примером может служить применение соревновательной методологии на семинарах. Ее суть весьма проста:

- На одном из семинаров одна группа формирует стегосообщение, применяя произвольно выбранный контейнер и произвольно выбранные данные. При этом не делается различий в выборе контейнера – звукового сэмпла, либо изображения.
- Вторая группа решает задачу стегоанализа.
- Далее группы студентов меняются ролями.

Именно такая «сревновательная игра» позволяет студентам быстрее и надежнее усвоить методы стеганографии и стегоанализа. Студенты не ограничены правилами игры – допускается применение как известных, так и придуманных стеганографических алгоритмов.

Студенты активно участвуют в формировании и коррекции электронной энциклопедии кафедры «Информационная безопасность» [4]. Участие заключается в следующем:

- Предлагается коррекция изложенных ранее материалов (при этом следует иметь ввиду то, что исходные материалы были предоставлены преподавателем, но поправлены членами редколлегии – студентами).
- Помещаются новые разделы энциклопедии, например результаты выполнения домашнего задания по выбору [4, Приложение 14].
- Студенты принимают активное участие в разработке методических и учебных пособий по дисциплине «Стеганграфия». Например – учебное пособие «Стеганография» авторов Е.Л. Зорина и Н.В. Чичварина, опубликованное среди электронных изданий кафедры и в [5].

5. Заключение

Более чем пятилетний опыт изучения дисциплины позволил сделать следующие выводы:

- Рассмотренная методика является несомненно эффективной.
- Необходимо пересмотреть учебный план кафедры «Информационная безопасность» и программу дисциплины «ОиРС». Имеется ввиду введение лабораторных работ с применением средств, поставляемых фирмой «NI», а также проведение практических занятий по компъютерной стеганографии. Это повысит долю самостоятельной работы студентов, их интерес к учебному процессу.

Список литературы

1. Галяев В.С. Современный уровень преподавания стеганографии в России. Режим доступа: http://info.fmi.shu-bg.net/skin/pfiles/13.pdf (Дата обращения 10.04.2015).
2. Российская государственная библиотека (Москва) / Официальный сайт. Режим доступа: http://www.rsl.ru/ (дата обращения 10.04.2015).

3. Российская национальная библиотека (Санкт-Петербург) / Официальный сайт. Режим доступа: http://www.nlr.ru/ (дата обращения 10.04.2015).
4. Электронная энциклопедия кафедры ИУ-8 МГТУ им. Н.Э. Баумана / Сайт кафедры ИУ-8. Режим доступа: http://gir.openrise.org/ (дата обращения 10.04.2015).
5. Зорин Е.Л., Чичварин Н.В. Стеганография и стегоанализ. М.: Изд-во МГТУ им. Н. Э. Баумана. 2013 // Блог Чичварина Н.В. Режим доступа: http://4i4.openrise.org/page/4 (дата обращения 10.04.2015).
6. Волосатова Т.М., Денисов А.В., Чичварин Н.В. Комбинированные методы защиты данных в САПР // Приложение к журналу Информационные технологии. 2012. № 5. С. 1-32.
7. Волосатова Т.М., Чичварин И.Н. Специфика информационной безопасности САПР // Известия высших учебных заведений. Сер: Машиностроение. 2012. Спец. Выпуск «Фундаментальные проблемы создания» С. 89-94.

АС	Автоматизированная система
ИБ	Информационная безопасность
КПС	Канал передачи сообщений
НСД	Несанкционированный доступ
ОЭС	Оптикоэлектронная система
РЭС	Радиоэлектронная система
АЭС	Акустоэлектронная система
ЦВЗ	Цифровой водяной знак