СОВРЕМЕННЫЙ УРОВЕНЬ ПРЕПОДАВАНИЯ СТЕГАНОГРАФИИ В РОССИИ*

ВЛАДИМИР С. ГАЛЯЕВ

THE MODERN LEVEL OF TEACHING OF STEGANOGRAPHY IN RUSSIA

VLADIMIR S. GALYAEV

ABSTRACT: *This paper traces the evolution of steganography as one of the areas of information security in higher education in Russia. For efficient use of these methods we need to prepare professionals in the corresponding areas.The article substantiates the necessity of training professionals versed in modern steganography techniques and practices.*

KEYWORDS: *steganography, vocational education.*

Развитие информационных технологий способствовало их проникновению во все сферы человеческой жизни. Особенно сильное влияние информационные технологии оказывают на современный бизнес, так как обрабатываются огромные объемы информации, но при этом информация должна быть актуальной и достоверной. Владение оперативной информацией является залогом успеха в современном мире. В связи с этим самым острым образом встают вопросы защиты информации. За последние 40 лет информационная безопасность получила существенное развитие и как область практических мероприятий, и как теоретическая наука. При этом информационная безопасность имеет большое количество ответвлений и направлений, в этой области уже сложились отдельные научные области. Вместе с тем есть направления, которые только недавно начали бурно развиваться.к одной из таких областей относится стеганология, которая только приобретает черты отдельной научной области, а вместе с этим и учебной дисциплины в рамках обучения в высшей школы. В данной статье дается обзор текущего положения и перспектив развития стеганографии как учебной дисциплины в вузах России.

На текущий момент в Российской Федерации действует третье поколение федеральных государственных образовательных стандартов, так называемый ФГОС-3, в рамках которого реализуется компетентностный подход и двухуровневая система обучения (бакалавриат – магистратура). Однако, по ряду направлений сохранился традиционный для советской высшей школы уровень подготовки – специалитет, который имеет статус выше бакалавра, но ниже магистра.

По данным Федерального портала "Российское образование" [1] на текущий момент в российских учреждениях высшего профессионального образования реализуется группа направлений подготовки и специальностей "Информационная безопасность", включающая в себя следующие 8 программ обучения:

1. Информационная безопасность – 109 вузов готовят бакалавров, из них 13 вузов готовит магистров по данному направлению;
2. Информационная безопасность автоматизированных систем – 41 вуз готовит специалистов;

* Работа частично финансирована проектом РД 08-238/2014 г. фонда „Научные исследования” Шуменского Университета „Епископ К. Преславски”

3. Информационная безопасность телекоммуникационных систем – 19 вузов готовит специалистов;
4. Компьютерная безопасность – 28 вузов готовит специалистов;
5. Безопасность информационных технологий в правоохранительной сфере – 13 вузов готовит специалистов;
6. Информационно-аналитические системы безопасности – 4 вуза готовит специалистов;
7. Противодействие техническим разведкам – 1 вуз готовит специалистов.

Всего более 110 вузов обучают студентов в области информационной безопасности, при этом здесь не учитываются вузы, которые в 2015 году завершают обучение специалистов, обучающихся по государственным образовательным стандартам второго поколения. Следует отметить, что за последние 5 лет идет планомерное наращивание количества вузов, реализующих направления подготовки и специальности по информационной безопасности.

Большинство вузов входит в учебно-методическое объединение вузов по информационной безопасности. На начало сентября 2014 года оно включало 74 члена.

По указанным специальностям в год выпускается более 2500 тысяч выпускников, что все еще оценивается экспертами как недостаточное количество. Трудоустройство выпускников по специальности составляет около 80%, что является одним из самых высоких показателей по России.

Для дальнейшего развития научного потенциала в области информационной безопасности возможна защита диссертаций на соискание ученых степень кандидата и доктора технических наук. Защита возможна в 14 диссертационных советах по специальности "Методы и системы защиты информации, информационная безопасность". Однако, стоит отметить, что не один из советов не является полностью профильным и совмещает указанную специальность с другими специальностями в области информационных технологий.

Что касается отдельных дисциплин, то учебный курс "Информационная безопасность" ("Основы информационной безопасности") является обязательной дисциплиной (входящей в федеральный обязательный компонент) для всех ИТ-специальностей. Такие дисциплины, как "Криптографические методы защиты" или "Криптография" входят в федеральную обязательную часть все указанных выше направлений. Кроме того, различные образовательные центры предлагают курсы различного уровня для повышения квалификации в области информационной безопасности в частности или в области применения криптографических средств в частности.

Следует отметить, следующие особенности, свойственные информационной сфере в России. В вопросах защиты информации подавляющее большинство пользователей возлагает свои надежды на криптографические методы. Криптография набрала свою популярность, получила широкое распространение и освещение. Для серьезных криптографических алгоритмов со всей математической строгостью доказывается их устойчивость ко взлому. Таким образом, мы согласны с тем, что криптография является серьезным инструментом в умелых руках в вопросах защиты конфиденциальной информации.Однако, применение криптографических средств строго регламентируется законом и отслеживается Федеральной службой безопасности.В частности, разрешается устанавливать и использовать только сертифицированные средства и только для определенного вида операций. Соответственно требуются специалисты, которые могут использовать строго определенные криптографические средства. Таким образом, можно

сказать, что в России уже сложилась относительно стабильная обстановка в области применения криптографических методов.

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. 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. В частности, большое внимание уделяется такому разделу стеганографии, как цифровые водяные знаки, на специальностях, связанных с типографским делом или юриспруденцией.

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

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

Следует отметить следующие особенности преподавания данной дисциплины в российских вузах:

1. Как видно из приведенного выше списка, существует бльшое количество вариаций названия дисциплины. Соответственно нет официальных требований и примерной программы, утвержденной хотя бы на уровне методического объединения вузов.
2. Как уже отмечалось, большое внимание уделяется использованию цифровых водяных знаков и защите авторских прав. Также такие дисциплины могут содержать большое количество (до 30%) учебного материала, посвященного законодательным методам защиты информации.
3. Практические занятия в большинстве случаев реализуются или в MathLab, или MathCad из сравнительной легкости реализации математических алгоритмов. Встречаются курсы, где предусмотрено выполнение лабораторных работ, посвященных изучению стеганографических программ и программных комплексов. Основной упор делается на освоение подобных программ и определение их эффективности. В очень малом количестве курсов предполагается разработка

собственных программных средств на одном из современных языков программирования.
4. В основном разбираются алгоритмы встраивания скрытых сообщений в мультимедийные контейнеры. Мало внимания уделяется сетевой стеганографии и современным направлениям развития стеганографических методов.
5. По данной дисциплине очень малое количество изданий, официально признанных министерством образования или учебно-методическим объединением, в том числе переводных.[2, 3, 4, 5, 6, 7, 8]

В зависимости от приоритетов конкретного вуза, а точнее приоритетов преподавателя, реализующего учебную дисциплину, ее содержание могут составлятьнекоторые (или все) из следующих тем:

1. Определения, основные задачи стеганографии и области ее применения;
2. Классификация стеганографических методов;
3. Базовые стеганографические технологии в зависимости от используемого контейнера;
4. Сетевая стеганография;
5. Водяные знаки;
6. Стеганоанализ и атаки на различные стеганографические методы.

Для повышения качества освоения дисциплины студент могут предлагаться собственные исследовательскиеработы в виде исследовательских проектов, курсовых или дипломных работ. Примерная тематика исследований приведена ниже:

1. Проблемы классификации стеганографических методов;
2. Современные методы сокрытия стеганографических сообщений в графических контейнерах;
3. Современные методы сокрытия стеганографических сообщений в аудио контейнерах;
4. Современные методы сокрытия стеганографических сообщений в видео контейнерах;
5. Сетевая стеганография – современные алгоритмы;
6. Стегоноанализ и атаки на стегонаграфические методы.

Подводя итог, можно сказать, что развитие стеганографии как научной области знаний находится в самом пике своего развития. Очевидно, что все большее распространение стеганографических методов в мировой сети, а также их использование различными криминальными, в том террористическими группировками, должно подвигнуть правительства разных стран инициировать создание основательной законодательной базы в этом вопросе. Следовательно, возникнет существенный спрос на специалистов, владеющих в достаточной степени стеганографическими и стеганоаналитическими познаниями. Поэтому уже сейчас следует в большей степени уделять внимание данному направлению при подготовке специалистов по информационной безопасности.

Также следует отметить, что наиболее перспективным направлением развития компьютерной стеганографии является применение сетевых стеганографических методов. Данное направление является очень наукоемким, на стыке множества дисциплин, и требует специальной подготовки от исследователей. Соответственно, данное направление должно в большей мере освещаться в рамках учебных дисциплин, связанных со стеганографией.

ЛИТЕРАТУРА
[1] Федеральный портал "Российское образование" http://www.edu.ru/abitur/act.6/fgos.09/index.php (31.10.2014)
[2] JesseRussell. Steganography.M.: Книга по требованию,2012. – 106 стр.
[3] LambertM. Surhone.Steganography.M.: Книга по требованию,2010. – 72 стр.
[4] Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ. М.: Вузовская книга, 2009.– 220 стр.
[5] Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2009. – 265 с.
[6] Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. М.: МК-Пресс,2006. – 288 стр.
[7] Петраков А.В.,Дворянкин С.В., Казарин О.С.Защитные информационные технологии аудиовидеоэлектросвязи. М. :Энергоатомиздат, 2010. – 616 стр.
[8] Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии. М.: Горячая Линия – Телеком, 2010. – 232 стр.

О НЕКОТОРЫХ ЭКСПЕРИМЕНТАХ ПО ПЕРЕДАЧЕ СТЕГОСООБЩЕНИЙ ЧЕРЕЗ СОЦИАЛЬНЫЕ СЕТИ*

ВЛАДИМИР С. ГАЛЯЕВ

ABOUT SOME EXPERIMENTS ON THE TRANSFER STEGOMESSAGES THROUGH SOCIAL NETWORKS

VLADIMIR S. GALYAEV

ABSTRACT: *The article discusses the possibility of using different steganographic algorithms to transmit hidden messages through the social networks services. Examined channels of communication through the social networks.The results of experiments on the transfer stegomessages in different social networks.*

KEYWORDS: *social networks, steganography, computer experiment.*

Введение. В современном информационном мире обладание актуальной и достоверной информацией становится ключевым моментом в управлении бизнесом. Вместе с тем все острее становятся вопросы информационной безопасности. Одним из аспектов информационной безопасности является предотвращение разглашения конфиденциальной информации. Согласно оценке экспертов в области защиты информации свыше 70% инцидентов с утечкой важной информации связано с деятельностью инсайдеров. Для снижения рисков в этом направлении реализуются различные организационные и технические меры безопасности. Однако, инсайдеры находят новые каналы передачи информации при преднамеренном разглашении конфиденциальной информации. Одним из таких каналов стали социальные сети. За последние несколько лет они набрали

* Работа частично финансирована проектом РД 08-238/2014 г. фонда „Научные исследования” Шуменского Университета „Епископ К.Преславски”