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”

популярность, проникли в различные сферы деятельности, но, вместе с тем, стали одним из каналов утечки информации. И чтобы несанкционированные действия были более незаметными, злоумышленники стали использовать стеганографические средства для передачи информации.

Данная статья посвящена обзору возможностей скрытой передачи информации с использованием сервисов социальных сетей, а также содержит результаты экспериментов по передачи файлов различных форматов со скрытыми сообщениями через различные инструменты, доступные в социальных сетях.

1. Социальные сети как канал передачи сообщений. Социальные сети уже перестали быть только развлекательным ресурсом или средством индивидуального общения. На текущий момент социальные сети являются одним из лучших маркетинговых инструментов с многомиллиардным оборотом. Также социальные сети активно используются в корпоративном секторе для подбора персонала, поиска клиентов, получения репутационной информации о людях и организациях. В связи с этим многие фирмы отказались от жесткого ограничения на использование социальных сетей с рабочих мест. Появился спрос на менеджеров по работе с социальными сетями (SocialMediaManager). Таким образом, для сотрудников компании социальные сети остаются доступным каналом связи с людьми вне фирмы, в том числе, с потенциальными конкурентами и другими противниками компании.

Ранее утечки информации были связаны с передачей данных в открытом виде, и основную опасность представляла миграция данных из одной социальной сети в другую. Однако, такие факты передачи можно было отследить (непосредственно с аккаунта пользователя или через сервер социальной сети). Сейчас передачу конфиденциальной информации стараются защитить различными методами, например, с применением криптографических или стеганографических средств. Однако, следует заметить, что в большинстве стран, в том числе России, применение криптографических средств регламентируется законодательными актами различного уровня и отслеживается соответствующими органами (в России - Федеральной службой безопасности). Поэтому применение криптографии для передачи коммерческой конфиденциальной информации нарушает не только интересы фирмы, но и законы государства. Применение стеганографии никак не регламентируется современным законодательством. Компьютерная стеганографии вообще очень молодая отрасль науки, но она активно развивается, и ее методы быстро набирают популярность.

2. Методика применения стеганографии в социальных сетях и проведенный эксперимент. Сначала дадим несколько необходимых определений.

Стеганограмма – сообщение, полученное после применения стеганографического преобразования к исходному сообщению и контейнеру

Сообщением (message) называют файл произвольного типа, существование и содержание которого необходимо скрыть.

Файл или пакет данных, в который скрываемая информация встраивается, называют контейнером (container).

В настоящее время уже известны и еще разрабатываются стеганографические методы, которые в качестве контейнера используют не только файлы, но и особенности сетевых протоколов (сетевая стеганография). Однако, в исследовании мы прежде всего ориентировались на злоумышленника с средним уровнем знаний (опытный пользователь), который не в состоянии разработать собственные методы, а пользуется готовыми программными продуктами. В связи с этим нами были рассмотрены лишь наиболее популярные методы сокрытия информации:

А. Встраивание в графические файлы:

– сокрытие в пространственной области (например, использование младших битов, замена палитры);
– сокрытие в частной области (например, модификация дискретного косинусного преобразования);

В. Встраивание в аудиофайлы

– сокрытие во временной области (например, замена младших битов, расширение спектра);
– сокрытие в частотной области (например, фазовое кодирование);
– использованиеэхо-сигнала.

Соответственно были рассмотрены следующие сервисы социальных сетей, которые позволяют передавать графическую или аудиоинформацию:

– Изображение – аватар;
– Фотоальбомы;
– Изображения в сообщениях;
– Аудиоальбомы;
– Аудиофрагменты, размещенные в сообщениях;
– Внешние файлы и размещение ссылок на них в переписке или личной странице.

Для проведения эксперимента были отобраны наиболее популярные социальные сети:

– Одноклассники
– Вконтакте
– Мой Мир
– Facebook
– Instagram
– Google+
– Linkedin

А в качестве программных средств – наиболее доступные, которые легко найти в глобальной сети:

– Red JPEG XT (freeware)
– Masker 7.5 (demo)
– Free File Camouflage 1.12 (freeware)
– MP3Stego 1.1.18 (freeware)
– Собственная программа, разработанная совместно со студентами, работающая с изображениями.

В эксперименте принимала участие группа студентов Дагестанского государственного института народного хозяйства, таким образом, для каждой из сетей было задействовано минимум 16 аккаунтов. Использовались различные аппаратные платформы для взаимодействия с социальными сетями: персональные компьютеры, ноутбуки, планшеты, смартфоны под управлением различных операционных систем. В результате эксперимента было выявлены следующие закономерности:

– Аватарнепригоден для передачи данных (сильное сжатие изображения);
– Большинство социальных сетей конвертируют формат изображений в переписке, поэтому стегосообщение не удается извлечь;
– Фотоальбомы и аудиоальбомы передают скрытое изображение без искажений;
– Любые ссылки на внешние файлы передают сообщения без искажений и не фиксируются социальной сетью;
– Мобильные приложения вносят искажения и в изображения из фотоальбомов, т.к. данные сжимаются для передачи по мобильным сетям.

Выводы. Социальные сети по-прежнему остаются одним из самых уязвимых каналов утечки информации. Социальные сети очень популярны, передают большие объемы информации в различных форматах, что затрудняет выявление нарушений конфиденциальности информации. Ситуация ухудшается еще и потому, что контроль за передаваемой информацией не может быть эффективен из-за применения средств маскировки.

Данная проблема является не только частной, затрагивающей интересы коммерческого сектора, но и более глобальной, на государственном и международном уровне. Описанной технологией передачи скрытых сообщений могут пользоваться члены различных террористических организаций, передавать важную информацию и координировать свои действия.

Поэтому на текущий момент важно разработать механизм противодействия наиболее популярным методам передачи стеганографических сообщений. Одним из вариантов может стать принудительная обработка передаваемых изображений и аудиофайлов – дополнительное сжатие или изменение формата в процессе передачи. Однако, это решение может быть реализовано только на международном уровне.

ЛИТЕРАТУРА

[1] Aimie Chee. Steganographic techniques on social media: Investigation guidelines. // Auckland. NewZealand. 2013. 255p.

[2] Аграновский А.В., Балакин А.В., Грибунин В.Г. Стеганография, цифровые водяные знаки и стеганоанализ // М: Вузовская книга, 2009. 220 стр.

[3] Галяев В.С. Социальныесетииаспектыинформационнойбезопасности. //InternationalScientificConference "Contemporarymethodsandtechnologiesinscientificresearch", October 12-13, 2012, Varna, Bulgaria.стр. 218-224.

[4] Станев С., Галяев В. Семантична еквивалентност на основните термини на компютърната стеганология в българските, английските и рускитенаучни публикации. // В: Сборник научни трудовена научна конференция с международно участие МАТТЕХ2012, Шумен 2012. стр.119-126.