**Abstract**: The paper reviews the basic methods of social networks analysis which are used to detect cyber threats. The main types of threats in social networks are presented and some methods for their prevention are described. Typical tasks of social networks analysis aimed at identifying cyber threats, such as community detection in networks, detection of leaders and experts in communities, stability analysis of community, clustering text information, etc. are considered. The basic classes of methods of graph theory and data mining, which are widely used in the analysis of social networks are described. **The application of fractal analysis methods to study the series of network users activity indicators is shown.**

Применение фрактального анализа для АСС

Если наблюдать во времени динамику показателей, полученных с помощью АСС, то от статических данных мы перейдем к временным рядам, к которым применимы все инструменты анализа и прогнозирования временных рядов**. В настоящее время стало общепризнанным, что многие временные ряды имеют долгосрочную зависимость и фрактальные свойства. Одними из первых реальных стохастических процессов, у которых были обнаружены самоподобные свойства, были информационные потоки данных в телекоммуникационных сетях.** Существует большое количество публикаций, посвященных анализу самоподобных и мультифрактальных свойств трафика и их влияния на функционирование и качество обслуживания телекоммукационной сети . Многочисленные исследования показали, что многие биоэлектрические сигналы обладают фрактальной структурой [Stanley, 1999**]. Другим примером фрактальных стохастических структур являются современные финансовые рынки. Анализируя динамику возникновения участков с различной фрактальной структурой, можно диагностировать и прогнозировать нестабильные состояния (кризисы) рынка** [Peters, 1996, Соловьев, 2015]. В последние годы появились исследования динамики сообществ в социальных группах, которые показывают, что соответствующие временные ряды обладают свойствами самоподобия [Cosoi, 2009, Yang, 2009, Rybski, 2012, Qingyun, 2016]. Самоподобие случайных процессов заключается в сохранении вероятностных характеристик при изменении масштаба времени. Стохастический процесс X t( ) является самоподобным с параметром H , если процесс ( ) H a X at − описывается теми же законами конечномерных распределений, что и X t( ) . Параметр H H , 0 1 < < , называемый показателем Херста, представляет собой степень самоподобия процесса. Наряду с этим свойством, показатель H > 0 5. характеризует меру долгосрочной зависимости стохастического процесса. Это означает, что если временной ряд в течении какого-то времени возрастал (убывал), то с вероятностью, близкой к показателю Херста, ряд сохранит эту тенденцию в течение аналогичного промежутка времени [Feder, 1988]. Начальные моменты самоподобного случайного процесса имеют скейлинговое соотношение E () q qH X t t ⎡ ⎤ ∝ ⎣ ⎦ , где величина t – интервал времени. International Journal "Information Technologies & Knowledge" Volume 11, Number 1, © 2017 39 Мультифрактальные объекты являются статистически неоднородными самоподобными объектами. Для мультифрактальных временных рядов статистическая неоднородность объекта выражается в неоднородности распределения данных ряда, т.е. наличии тяжелых хвостов плотности распределения вероятностей временного ряда. В сравнении с самоподобными, мультифрактальные процессы проявляют более сложное скейлинговое поведение: для моментов мультифрактальных процессов выполняется отношение ( ) E () q qh q Xt t ⎡ ⎤ ∝ ⎣ ⎦ , где h q( ) – обобщенный показатель Херста, являющийся в общем случае нелинейной функций. Значение h q( ) при q = 2 совпадает со значением степени самоподобия H . Для монофрактальных процессов обобщенный показатель Херста не зависит от параметра q : hq H ( ) = . [Reidi, 2002]. **В работе был проведен сравнительный фрактальный анализ для двух групп в социальной сети Facebook, найденным по ключевым словам, связанных с киберугрозами. Для проведения исследований в сети были выбраны две группы ThreatPost и Threat Signal, каждая численностью 13980 и 84375 пользователей соответственно. Для каждой их этих социальных групп были сняты данные за последние пять лет о количестве лайков, комментариев и уровне вовлеченности (показатель уровня вовлеченности аудитории в активности группы измеряется в процентном соотношении действий пользователей к охвату аудитории). На рис.1 слева показаны временные ряды ежедневного количества лайков для обеих групп. Фрактальный анализ показал, что временные ряды показателей этих групп обладают сильными мультифрактальными свойствами.** На рис. 1 справа представлены значения обобщенного показателя Херста для этих рядов. Оба ряда обладают фрактальными свойствами, персистентностью ( 1 2 H , 0.5 Н > ), однако ряд лайков для группы Threat Signal обладает значительно большей статистической неоднородностью, что проявляется в значительно большем диапазоне величины Δh q( ) . Исследования показали, что ряды лайков достаточно сильно коррелируют с рядами уровня вовлеченности, поэтому их соответствующие мультифрактальные характеристики очень близки**. Ряды количества комментариев (рис.2, слева), в отличие от рядов лайков, также имеют фрактальные свойства, но обладают достаточно близкой между собой мультифрактальной структурой (рис.2, справа). Можно предположить, что механизм генерации комментариев, который формирует фрактальную структуру временного ряда, достаточно сильно отличается от механизма проставления лайков**. Таким образом, проведенные в работе исследования подтвердили, что многие временные ряды показателей активности пользователей социальных сетей обладают фрактальными свойствами 40 International Journal "Information Technologies & Knowledge" Volume 11, Number 1, © 2017 и применение фрактального анализа позволяет выявить различия и обнаружить характерные черты динамики разных социальных групп.

Стеганография

**Стеганография (от греч. στεγανός — скрытый + γράφω — пишу; буквально «тайнопись») — наука, позволяющая спрятать передаваемые данные в некотором контейнере, таким образом скрыв сам факт передачи информации.**

**В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Впервые понятие стеганографии было введено в 1499, но сам метод существует очень давно. Легенды донесли до нас метод, который использовался в Римской империи: для доставки сообщения выбирали раба, голову которого брили, а затем с помощью татуировки наносили текст. После того, как волосы отрастали, раба отправляли в путь. Получатель сообщения снова обривал голову раба и читал сообщение.**

Так какие же способы спрятать информацию есть в нашем распоряжении…

Способ 1 — Банальный

**Самый простой способ — это переименовать файл. К примеру у вас есть картинка, которую надо спрятать. Вы просто переименовываете расширение файла и картинка больше не определяется системой как картинка**. Но, понятное дело, что это защита от дурака. Если вы, к примеру, переименуете файл JPG в RAR, то такой RAR архив нельзя будет открыть, WinRar поругается на то, что этот архив битый, что вызовет подозрение и более глубокое изучение данного файла.

Способ 5

Ну и напоследок хочу рассказать про один замечательный способ хранения секретных данных в MP3 файлах. Реализован он в программе [MP3Stego](http://www.petitcolas.net/fabien/steganography/mp3stego/index.html). К сожалению автор данной программы не обновлял проект с 2006 года. **Идея заключается в том, что данные сначала шифруются, а затем в сердце процесса кодирования MP3 файла (из WAV) подмешиваются в конечный результат. В итоге получается обычный MP3 файл, без заметных для слуха искажений, однако хранящий в себе закодированные данные.**

Способ 2 — Банальный, продвинутый

**Ещё один простой способ, но всё же более продвинутый — это склеивание двух разных файлов в один.** Простейший пример: добавление RAR архива в конец JPEG изображения. Такое изображение будет без проблем открываться в любой программе для просмотра/редактирования картинок, а также будет открываться и в программе WinRar. Дело в том, что почти все программы для работы с архивами рассчитаны на то, что архив начинается не с начала файла, так как возможно, что архив заключен в самораспаковывающуюся оболочку. Но недостатки данного способа в том, что такое склеивание можно легко заметить. К примеру если картинка имеет размер 200х200 и при этом весит 2 мегабайта, то тут же возникают подозрения. К тому же все форматы (контейнеры) обычно имеют четкую структуру и если вдруг в файле имеется какая то избыточная информация, то это легко обнаружить.  
  
Поэтому нам нужен способ скрытия информации, который не нарушает структуру файла выбранного формата.

На сегодня учеными разработаны и опробованы различные алгоритмы и методы стеганографии, мы отметим следующие:

//здесь будет похожая инфа с той что выше

// хотя 3 методов достаточно

* **LSB-стеганография** (сообщение скрывается в младших битах (возможно использование одного или нескольких младших бит) контейнера. Чем меньше бит задействовано, тем меньше артефактов получает оригинальный контейнер после внедрения.
* **Метод, основанный на сокрытии данных в коэффициентах дискретного косинусного преобразования** (далее ДКП) — разновидность предыдущего метода, которая активно используется, например, при внедрении сообщения в контейнер формата JPEG. При прочих равных, такой контейнер имеет несколько меньшую емкость чем в предыдущем методе, в том числе за счет того, что коэффициенты «0» и «1» остаются неизменными — внедрение сообщения в них невозможно.
* **Метод сокрытия информации при помощи младших бит палитры**— этот метод по сути является вариантом общего метода LSB, но информация встраивается не в наименее значащие биты контейнера, а в наименее значащие биты палитры, очевидный недостаток такого метода — низкая емкость контейнера.
* **Метод сокрытия информации в служебных полях формата —**довольно простой метод, основанный на использовании служебных полей заголовка контейнера для хранения сообщения. Очевидные минусы — низкая емкость контейнера и возможность обнаружения внедренных данных при помощи обычных программ для просмотра изображения (которые иногда позволяют видеть содержимое служебных полей).
* **Метод встраивания сообщения —**заключается в том, что сообщение встраивается в контейнер, затем при помощи схемы, известной обеим сторонам, извлекается. Можно встроить несколько сообщений в один контейнер, при условии, что способы их внедрения ортогональны.
* **Широкополосные методы**, которые подразделяются на:
  + метод псевдослучайной последовательности; используется секретный сигнал, который моделируется псевдослучайным сигналом.
  + метод прыгающих частот: частота несущего сигнала меняется по определенному псевдослучайному закону.
* **Метод оверлея —**по сути не является настоящей стеганографией, основан на том, что некоторые форматы содержат в заголовке размер данных, или же обработчик этих форматов будет читать файл до маркера конца данных. Примером такого метода является хорошо известный метод «rar-jpeg», который основан на конкатенации графического файла в формате JREG и RAR-архива. ПО для просмотра JPEG будет считывать информацию до границы, указанной в заголовке файла, а RAR-архиватор откинет все, что находится до сигнатуры «RAR!», которая обозначает начало архива. Таким образом, если такой файл открыть в просмотрщике графических файлов — мы увидим картинку, а если в RAR-архиваторе — содержимое RAR-архива. Очевидные минусы такого подхода заключаются в том, что оверлей, добавленный к контейнеру, легко выделяем при визуальном исследовании такого файла.

В этой статье мы рассматриваем только методы сокрытия информации в графических контейнерах и в сетевых пакетах, но область применения стеганографии значительно шире.

За недавнее время мы наблюдали использование стеганографии в следующих вредоносных программах и средствах кибершпионажа:

* **Microcin (AKA six little monkeys);**
* **NetTraveler;**
* **Zberp;**
* **Enfal (its new loader called Zero.T);**
* **Shamoon;**
* **KinS;**
* **ZeusVM;**
* **Triton (Fibbit).**

Проблемы налицо:

* Использование стеганографии сегодня — очень популярная идея среди авторов вредоносного и шпионского ПО;
* Антивирусные средства вообще и средства защиты периметра в частности мало что могут сделать с заполненными контейнерами: их очень трудно обнаружить поскольку они выглядят как обычные графические (и не только) файлы;
* Все существующие программы для детектирования стеганографии по сути являются PoC— Proof-of-Concept, и их логика не может быть имплементирована в промышленные средства защиты из-за низкой скорости работы, не слишком высокого уровня детектирования, и иногда даже иногда — из-за ошибок в математике (мы видели и такие случаи).

# **Практическое применение стеганографии**

## **1. Незаметная передача информации (СПД)**

Самое очевидное, что первое приходит на ум. В отличие от криптографических методов (которые тайны, но не скрытны), стеганография может применяться как метод незаметной передачи информации. Это составляет «классическое практическое применение» стеганографии, поэтому данная цель — на первом месте.

## **2. Скрытое хранение информации (СПД)**

## **3. Недекларированное хранения информации (СПД)**

## **4. Защита исключительного права (ЦО)**

## **5. Защита авторского права (СВЗ)**

## **6. Защита подлинности документов (СВЗ)**

## **7. Индивидуальный отпечаток в СЭДО (ЦО)**

## **8. Водяной знак в DLP системах (СВЗ)**

## **9. Скрытая передача управляющего сигнала (СПД)**

11. Подтверждение достоверности переданной информации(ЦО).