РАЗДЕЛ 8

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ АВТОРСКИХ ПРАВ АУДИОДАННЫХ

Информатизация общества ведет к созданию единого мирового информационного пространства, в рамках которого осуществляется накопления, обработка, хранение и обмен информацией между субъектами. Мультимедийный web-документ строго говоря представляет собой совокупность разных объектов, которые защищаются законом об авторском праве.

В то же время существует ряд технических особенностей сети, которые существенным образом усложняют защиту авторских и смежных прав. Например, легкость создания копий в неограниченном количестве, а также легкость записи на жесткий диск персонального компьютера частей Интернет-сайта (что является нарушением права на воспроизведение) делает каждого пользователя сети потенциальным нарушителем законодательства.

Проблема незаконного копирования возникла задолго до появления цифровых и даже аналоговых устройств воспроизведения и копирования произведений. Переход на цифровые методы хранения и передачи информации только усилили обеспокоенность правообладателей. Тогда как аналоговые записи неизбежно теряют свое качество не только при копировании, но даже и при нормальном использовании, цифровые записи могут быть скопированы или воспроизведены неограниченное количество раз без потери качества. В совокупности с большим распространением Интернета и файлообменных сетей это привело к увеличению объемов нелегального распространения медиапродукции в небывалых размерах.

Обычно, основываясь на особенностях языка HTML, информацию об авторстве на соответствующих страницах указывают тремя основными способами: непосредственно в тексте страницы, по обыкновению внизу; в виде комментариев в документе; с помощью тега. Однако все эти виды указаний на авторство web-документа легко подвергаются модификации и со временем достаточно проблематично доказать право на авторство того или другого документа. Поэтому кроме правовых, необходимо использовать и информационные (технические) способы защиты с учетом положений Закона Украины «Об авторском праве и смежных правах» от 23.12.1993 г. № 3792-XII.

Основные направления защиты авторских прав аудиоданных

Одним из возможных решений в борьбе с «пиратством» есть разработка технологий распознавания контрафактного контента.

На сегодняшний день можно выделить два основных направления защиты авторских прав аудио данных [37]:

Технические средства защиты авторских прав (*DRM*— Digital rights management – управление цифровыми правами, неофициально иногда Digital restrictions management). Этим термином обозначается совокупность программных либо аппаратных средств, предназначенных для ограничения, либо осуществления контроля за созданием копий информации, распространяемой в электронном виде. Эта технология используется многими производителями для защиты от незаконного и несанкционированного копирования и распространения музыкальных, видеофайлов, электронных книг и т.д;

Использование приемов **стеганографии** – внедрение в музыкальный файл определенной секретной метки или данных по аналогии с регистрационным ключом для программного обеспечения. Если ключ пользователя совпадает с секретной меткой, то этот пользователь сможет воссоздать музыку, записанную в звуковом файле. Кроме того, с помощью приемов стеганографии в звуковых файлах можно скрыто передать дополнительную информацию, например, фамилию автора.

Технические средства защиты авторских прав

Технология DRM реализует защиту информации несколькими способами:

ограничение количества раз просмотра (прослушивания) той или иной информации. Здесь имеется ввиду, что, к примеру, скачанный из Интернета музыкальный файл можно прослушать только определенное количество раз. Такой способ защиты вызывает недовольство у многих пользователей;

наложение ограничения на копирование того или иного файла на различные носители. Здесь попросту ограничиваются возможности по копированию защищаемой информации;

предотвращение перехвата видео или аудиопотока посредствам специального программного обеспечения. Этот способ основан на том, чтобы не допустить перехвата информации в процессе воспроизведения (просмотра) информации.

Довольно распространенным является ситуация, когда воспроизведение, к примеру, музыки, хранящейся на диске, возможно только при условии использования записанной на этом же диске программы. Это не что иное, как яркий пример использования технологии DRM. Однако у данного способа

имеется большое количество противников, которые в большинстве своем правы, утверждая, что такой способ способен принести вред устройству, на котором производится воспроизведение. К примеру, такие программы, при их работе, вводят в заблуждение компьютер, создавая скрытые файлы, создавая непонятные системе файлы в реестре, внося тем самым трудности в процесс функционирования ПЭВМ.

Технологии DRM достаточно хорошо освещены в литературе, поэтому более подробно остановимся на эффективности систем DRM. Большинство современных систем DRM используют криптостойкие алгоритмы защиты, однако эти методы не могут использоваться полноценно, поскольку основаны на предположении, что для получения доступа к зашифрованной информации требуется секретный ключ. Однако в случае DRM типичной является ситуация, когда ограничения обходятся правомерным обладателем копии, который для возможности просмотра (воспроизведения) должен иметь и зашифрованную информацию, и ключ к ней, что сводит к нулю всю защиту. Поэтому системы DRM пытаются скрыть от пользователя используемый ключ шифрования (в том числе используя аппаратные средства), однако это нельзя осуществить достаточно надежно, поскольку применяемые ныне устройства воспроизведения (персональные компьютеры, видеомагнитофоны, DVD-проигрыватели) являются достаточно универсальными и находятся под контролем пользователей. Следует также отметить, что разрешить воспроизведение и в то же время запретить копирование представляет собой принципиально неразрешимую задачу (так называемая «аналоговая брешь», англ. analog hole): воспроизведение – чтение информации, её обработка и запись на устройство вывода, копирование – чтение и запись информации на устройство хранения. То есть, если возможно воспроизведение (включающее промежуточный этап чтения информации), возможно и её последующее копирование.

На нынешнем этапе развития ТСЗАП сами по себе не в состоянии эффективно ограничить неправомерное использование произведений. Это обусловлено прежде всего тем, что применяемые ныне устройства для воспроизведения (персональные компьютеры, видеомагнитофоны, DVD-проигрыватели) являются достаточно универсальными устройствами и находятся под контролем пользователей. В таких условиях разрешить воспроизведение (просмотр) и в то же время запретить копирование представляет теоретически неразрешимую задачу. Эффективная техническая защита от копирования при разрешённом воспроизведении может быть

достигнута, только когда всё устройство (компьютер, проигрыватель) целиком под контролем правообладателя. Поскольку ТСЗАП малоэффективны сами по себе, для них установлена правовая защита.

Правовая поддержка технологий DRM

Поскольку технологии DRM малоэффективны сами по себе, для них установлена правовая защита. Законодатели многих стран, идя навстречу желанию крупнейших правообладателей, ввели ответственность за обход (преодоление, отключение, удаление) DRM.

На сегодняшний день практически любой человек скачивал какое-то музыкальное или аудио-визуальное произведение, фильм или телепередачу, смотрел онлайн ТВ или слушал интернет-радио. Всегда ли это делается законно? Не нарушаются ли при этом авторские и смежные права правообладателей данного контента? Законодательство в сфере авторского права и смежных прав развивается вместе с развитием науки и технологий. Основной задачей правовой регламентации отношений в данной сфере является обеспечение эффективной защиты прав интеллектуальной собственности.

В Украине правоотношения в сфере авторского права и смежных прав регламентируются Конституцией Украины, кодексами, законами, подзаконными нормативно-правовыми актами, а также международными договорами Украины.

Конституция Украины как Основной Закон Украины закрепляет право каждого владеть, пользоваться и распоряжаться своей собственностью, результатами своей интеллектуальной, творческой деятельности (ст. 41), а также гарантирует свободу литературного, художественного, научного и технического творчества, защиту интеллектуальной собственности, авторских прав, моральных и материальных интересов, возникающих в связи с разными видами интеллектуальной деятельности и запрещает использовать или распространять результаты интеллектуальной, творческой деятельности без согласия правообладателя, за исключением случаев, предусмотренных законом (ст. 54).

Правовое регулирование и охрана интеллектуальной и творческой деятельности, ее результатов, осуществляется также при помощи Книги четвертой Гражданского кодекса Украины (далее ГКУ), содержащей общие нормы авторского права и смежных прав. В частности, закрепляются перечни объектов и субъектов как авторского права так и права интеллектуальной собственности в целом, основания возникновения (приобретения) прав на объекты интеллектуальной собственности, нормы о личных неимущественных и имущественных правах, срок действия прав интеллектуальной собственности,

общие положения об использовании объектов права интеллектуальной собственности, передаче имущественных прав интеллектуальной собственности и осуществлении права интеллектуальной собственности, принадлежащего нескольким лицам, общие положения о правах интеллектуальной собственности на служебные произведения и объекты, созданные по заказу, последствиях нарушения права интеллектуальной собственности и защите права интеллектуальной собственности.

Главы 36 и 37 ГКУ посвящены авторскому праву и смежным правам. Среди имущественных прав интеллектуальной собственности на произведение ГКУ (ст. 440) указывает право на использование произведения, исключительное право разрешать использование произведения, право препятствовать неправомерному использованию произведения, в том числе запрещать такое использование. Под использованием произведения в ГКУ (ст. 441) подразумеваются такие действия как: публикация, воспроизведение любым способом и в любой форме, перевод, переработка, адаптация, аранжировка и иные подобные изменения, включение составляющей частью в сборники, базы данных, онтологии, энциклопедии и т.п., публичное исполнение, продажа, передача в найм (аренду), импорт образцов произведения, образцов его переводов, переработок и т.п. Все эти действия так или иначе взаимосвязаны с распространением произведений. В свою очередь ГКУ (ст. 445) предусматривает право автора на оплату за использование его произведения. Кроме того, использованием исполнения считаются в частности такие действия, как продажа и иное отчуждение оригинала или образца записи исполнения и обеспечения средствами связи возможности доступа любого лица к записанному исполнению с места и во время, выбранные таким лицом (ст. 453). Таким образом, ГКУ косвенно регламентирует распространение аудио- и видео- контента посредством интернета и онлайн-ТВ, радио.

Центральное место среди нормативно-правовых актов, регламентирующих распространение видео- и аудио- контента занимает Закон Украины «Об авторском праве и смежных правах» (далее - Закон). Ценность данного Закона, в целом соответствующего международным стандартам, состоит в прямом действии его норм и рыночной направленности. Закон определяет распространение объектов авторского права и (или) смежных прав как любое действие, с помощью которого объекты авторского права и (или) смежных прав непосредственно или опосредованно предлагаются публике, в том числе доведение этих объектов к сведению публики таким образом, что ее представители могут осуществить доступ к таким объектам с любого места и в

любое время по собственному выбору (ст. 1). Среди имущественных прав автора Закон, в частности называет распространение произведений путем первой продажи, отчуждения иным способом или путем сдачи в имущественный найм или в прокат и путем иной передачи до первой продажи образцов произведения, подача своих произведений к общему сведению публики таким образом, что ее представители могут осуществлять доступ к произведениям с любого места и в любое время по их собственному выбору, сдача в имущественный найм и (или) коммерческий прокат после первой продажи, отчуждение иным образом оригинала или образцов аудиовизуальных произведений, а также произведений зафиксированных в фонограмме или видеограмме или в форме, которую считывает компьютер (ст. 15).

На развитие законодательства Украины об авторском праве, направлен Закон Украины «О распространении экземпляров аудиовизуальных произведений и фонограмм» от 3.03.2000 г. № 1587-III, защищающий права и интересы лиц, занимающихся распространением экземпляров аудиовизуальных произведений и фонограмм и регламентирующий их отношения с потребителями. В данном законе приводится определение распространения образцов аудиовизуальных произведений, фонограмм, видеограмм, компьютерных программ, баз данных как их введение в оборот путем их продажи или иной передачи права собственности. Однако, данный закон не регламентирует распространение аудио- и видео- контента через интернет, поскольку предусматривает сопровождение процесса распространения произведений маркированием произведений контрольными марками.

Кроме перечисленных нормативно-правовых актов вопросам регулирования интеллектуальной собственности посвящен ряд других законов и принятых на их основе подзаконных нормативно-правовых актов.

К законодательству, регулирующему авторское право и смежные права относятся также отдельные статьи нормативно-правовых актов, устанавливающих административную и уголовную ответственность, в частности ст. 176 Уголовного кодекса Украины и ст. 51-2 Кодекса Украины про административные правонарушения.

К национальному законодательству, регламентирующему распространение аудио- и видео- контента также принадлежат международные договора Украины в сфере авторского права и смежных прав, в частности Всемирная конвенция об авторском праве, Договор Всемирной организации интеллектуальной собственности (ВОИС) об авторском праве и Договор ВОИС об исполнении и фонограммах. Также частью национального законодательства

стали Международная конвенция про охрану интересов исполнителей, изготовителей фонограмм и организаций вещания, Конвенция про охрану интересов изготовителей фонограмм от незаконного воспроизведения их фонограмм.

Право на объекты интеллектуальной собственности регулируется также договорами, которые заключаются между лицом, владеющим исключительными правами, и пользователем интеллектуального продукта (авторский, лицензионный договор). Следует отметить, что на территории Украины практика борьбы с нарушениями прав интеллектуальной собственности в Интернете на данное время очень незначительна и довольно часто ограничивается требованиями к правонарушителям прекратить незаконное использование контента без обращения к судам и правоохранительным органам. Для решения проблемы необходимо установить разумный баланс между нормативно-правовой базой и инструментами саморегулирования в сети. Практика цивилизованных стран показывает, что механизмы самоконтроля довольно действенны и вызывают доверие к тем, кто их создает (напр., британская система саморегулирования Интернета "Интернет-вотч"). Можно констатировать, что нормативно-правовая база существенным образом отстает от общественных отношений, что приводит к неурегулированности данной сферы нормами законов, применению в основном корпоративных норм или даже отсутствию любого регулирования. Поэтому на данном этапе перед специалистами и законодателями стоит задача адаптировать нормативно-правовую базу для обеспечения правового регулирования и защиты исключительных прав в сети Интернет. Кроме того, необходимо обновление механизмов реализации исключительных прав и повышение подготовки судей в сфере информационных технологий.

Недостатки концепции DRM

Главными недостатками самой концепции DRM является неминуемое ограничение возможностей использования и связанное с этим ограничение на распространение информации. Дополнительные ограничения, которые накладываются в первую очередь на честных потребителей аудиовизуальной продукции или устройств, осуществляющих запись или воспроизведение информации и поддерживающих технологии защиты авторских прав, является, по мнению экспертов, серьезным недостатком. Сами принципы DRM и множество их реализаций могут противоречить законодательству некоторых стран. Существенной проблемой является также то, что большинство систем DRM несовместимы между собой: например, музыку, купленную с помощью

Apple itunes и защищенную DRM, невозможно прослушивать на каких-нибудь других плеерах, кроме ipod. Также часто системы DRM для персональных компьютеров используют методы защиты от взлома, что делает работу системы пользователя нестабильной и представляют угрозу ее безопасности.

Некоторые из наиболее эффективных технологий DRM требуют для использования защищенной копии постоянное сетевое соединение с контролирующей системой. Когда поддержка системы контролирующим лицом прекращается, защищенные копии становятся неработающими. Некоторые компании перед отключением предлагают клиентам компенсацию или копии в незащищенном формате. Например, в апреле 2008 г. корпорация Microsoft решила закрыть до конца августа MSN Music Store, в связи с тем, что он более не работал, и отключить серверы, необходимые для получения ключей к прежде купленным в этом магазине музыкальным произведениям, после чего пользователи не смогли бы воссоздавать их после замены компьютера. Однако после многочисленных жалоб пользователей Microsoft продолжила срок работы серверов до 2011 года.

Существуют целые общественные движения, которые пропагандируют отказ от использования технологий DRM и ставят своей целью предупреждение неосведомленных о таких недостатках потребителей от приобретения подобной продукции. Наиболее известны кампания Defective by Design, запущенная Free Software Foundation против DRM, а также организация Electronic Frontier Foundation, одной из целей работы которой также является противодействие DRM.

Стеганографические методы защиты авторских прав аудио данных.

Для защиты авторских и смежных прав на мультимедийную продукцию очень хорошо подходят методы стеганографии – древней науки о средствах тайной передачи сообщений. Термин «стеганография» происходит от греческих слов steganos (секрет, тайна) и graphy (запись) и, таким образом, означает буквально «тайнопись». В отличие от криптографии, которая блокирует доступ к информации путем шифрования, стеганография имеет целью спрятать сам факт существования секретного сообщения. Этим секретным сообщением, введенным в мультимедийное произведение, может быть, например, имя его автора с другими реквизитами или изображение логотипа юридического лица, которое имеет права на это произведение. Такое секретное сообщение ни в коем случае не должно ухудшать техническое качество произведения, но с помощью специальной программы его можно определить, что может стать весомым доводом, например в суде.

В наше время под стеганографией, точнее компьютерной или цифровой стеганографией, понимают сокрытие информации в текстовых, графических,

аудио- или видеофайлах путем использования специального программного обеспечения [28]. Основываясь на базе анализа открытых информационных источников рассмотрим возможности стеганографии в отношении проблемы защиты информации путем сокрытия ее в мультимедийных файлах.

Алгоритмы встраивания скрытой информации можно разделить на несколько подгрупп [59; 116]:

• Работающие с самим цифровым сигналом, в частности изменение структуры битовых плоскостей оригинального сигнала – метод наименее значимых бит (Least Significant Bit, LSB) [131]:

• «Впаивание» скрытой информации. В данном случае происходит наложение скрытого изображения (текста, иногда звука) поверх оригинала. Часто используется для встраивания цифровых водяных знаков (ЦВЗ) [161].

• Использование особенностей форматов файлов. Сюда можно отнести запись информации в метаданные или в другие зарезервированные неиспользуемые поля файла.

Наиболее продуктивным направлением применения компьютерной стеганографии для защиты от копирования и несанкционированного использования аудио данных в настоящее время является использование избыточности аналогового аудио и видео сигнала [48]. Цифровой звук – это матрица чисел, фиксирующая интенсивность звукового сигнала в последовательно идущие моменты времени. Все эти числа не точны, поскольку не точны устройства оцифровки аналоговых сигналов, то есть присутствуют шумы квантования. Младшие разряды цифровых отсчетов содержат минимум полезной информации о текущих параметрах звука или изображения. Их заполнение ощутимо не влияет на качество восприятия, которое и дает возможность скрытия в них дополнительной информации. Например, только одна секунда оцифрованного звука в режиме стерео с частотой дискретизации 44100 Гц и разрядностью 8 бит теоретически позволяет скрыть сообщение размером около 10 Кбайт информации за счет замены наименее значимых младших отсчетов. При этом изменение значений разрядов составляет менее 1%. Такая девиация практически не ощущается при прослушивании файла большинством людей [4]. Встраивание сообщения в контейнер может производиться при помощи ключа, одного или нескольких. Ключ – псевдослучайная последовательность (ПСП) бит, порождаемая генератором, удовлетворяющим определенным требованиям (криптографически безопасный генератор). Скрываемая информация внедряется в соответствии с ключом в те отсчеты, искажение которых не приводит к существенным искажениям контейнера. Эти биты образуют стегопуть.

Таким образом, для защиты авторских прав на аудио файлы чаще всего применяются алгоритмы, использующие чрезмерность аудиовизуальной информации (LSB). Основными контейнерами при данном способе сокрытия являются форматы так называемого прямого кодирования, например, BMP для графики, или WAV для звука. Это направление – популярнейшее среди разработчиков. Следует отметить появление современных программ, поддерживающих сжатые форматы.

Однако, несмотря на преимущества этого метода, состоящие в него простоте и сравнительно большом объеме встраиваемых данных, он имеет и серьезные недостатки. Во-первых, злоумышленнику точно известно, где находится местоположение всего сообщения, то есть, не обеспечивается секретность встраивания информации. Во-вторых, зная о существовании скрытого сообщения, его теоретически можно разрушить, поскольку органы чувств человека не в состоянии внешне различить изменения в этих битах. Это означает, что данное направление требует дальнейших исследований.

Обзор программ, использующих методы стеганографии

S-Tools. Один из распространенных стеганографических программных продуктов для платформы Windows (статус – freeware). Программа S-Tools прячет информацию в графических файлах форматов bmp и gif, а также в звуковых файлах формата wav. Внешне работа с программой выглядит следующим образом. После распаковывания архива запускается файл s-tools.exe, потом Windows Explore. Последний понадобится, так как S-tools использует технологию drag and drop, соответственно окна не должны полностью перекрываться.

Соответствующий файл перетягивается мышью в окно программы S-tools. Он отображается в окне или как есть (для картинки), или в виде линии, которая изображает уровень сигнала (для звука). В правом нижнем углу окна S-tools появляется информация о размере данных, которые можно запрятать в этом файле.

Затем в окно с картинкой или уровнем сигнала перетягивается любой файл, предназначенный для сокрытия, размером не более указанного файла. После проверки размера данных программа запрашивает пароль, введя который можно будет восстановить информацию. Потом начнется процесс сокрытия, его время зависит от размера данных (наблюдать за процессом можно в окне Action). Когда все будет готово, появится окно Hidden data. Сохранить результат можно, щелкнув в окне правой кнопкой мыши и выбрав пункт «Save as ...», введя имя файла. Для восстановления сообщения необходимо перетянуть картинку или звук в окно S-tools, щелкнуть на изображении правой кнопкой и выбрать пункт «Reveal ...». После введения пароля, если скрытые данные есть, начнется их восстановление, за процессом которого можно наблюдать в окне Action Steganos for Win.

Steganos for Win. Другая распространенная стеганографическая программа – Steganos for Win, легкая в использовании, но все же мощная программа для шифрования файлов и сокрытия их внутри файлов bmp, dib, voc, wav, assii и html (Privacy Guide: Steganography – http://www .all-nettools.com/privacy/stegano.htm). Она владеет практически теми же возможностями, что и S-Tools, но использует другой криптографический алгоритм (hwy1) и, кроме того, способна прятать данные не только в файлах формата bmp, wav, а и в обычных текстовых и html-файлах, причем весьма оригинальным образом – в конце каждой строки добавляется определенное количество пропусков.

Masker 7.0 (испытательный 10-дневной период, стоимость 25 евро, http://www.softpuls.com). Позволяет скрывать сообщение среди исполняемых, видео-и аудиофайлов, а также в изображениях, причем поддерживается огромное число форматов, среди которых есть как форматы прямого кодирования, так и сжатые (JPEG, MP3, MPEG

Steganos Security Suite 2007. Наиболее известным пакетом для защиты информации, уже название которого указывает на стеганографическое "содержимое", есть Steganos Security Suite 2007 (испытательный 30-дневной период, стоимость $ 69,95, http://www.steganos.com). Как уже было сказано, это именно пакет - при запуске появляется окно для выбора конкретного приложения. Рассмотрим раздел "File Manager", с помощью которого можно скрывать файлы. На главной панели сначала активны две кнопки, первая из которых скрывает файлы, а вторая вытягивает.

После выбора пункта "New encrypted file" основная часть окна - файловый менеджер – станет активной, в нее нужно будет добавлять файлы, которые необходимо запрятать. Когда все файлы добавлены, нажатие на кнопку "Close" на той же панели запустит "Мастер сохранения".

Сначала нужно будет выбрать, что мы хотим сделать: просто зашифровать, или зашифровать и спрятать. Так как мы рассматриваем программу как средство стеганографии, выбираем второй пункт. Появится окно, где выбирается, хотим ли мы дать программе возможность самостоятельного нахождения файла-контейнера (будет избран любой файл, соответствующего типа и размера), или укажем его сами.

Программа поддерживает 3 формата: BMP, JPEG и WAV.

MSU Stegovideo, написанная студентами МГУ. (freeware, http://www.compression.ru/video/stego_video/index_en.html). Она, как понятно из названия, предназначена для сокрытия сообщений в видеофайлах, причем это может быть только текстовая информация. Но у нее есть один большой плюс - в отличие от конкурентов, здесь информация сохраняется при сжатии популярными кодеками, например, Divx. Когда другие программы упаковывают файлы и

шифруют разными алгоритмами, одного измененного бита может быть достаточно для потери всего содержания. MSU Stegovideo, конечно, не может сохранить весь переданный ей текст, но при определенных условиях потери могут не превышать 20%, что целиком приемлемо для литературного языка – содержание сообщения сохранится. Процесс упаковки секретного сообщения в целом обычный – нужно указать исходный видеофайл, текстовый файл с сообщением, пароль и путь сохранения заполненного контейнера.

Но, кроме обычных шагов, на одном из этапов нужно будет указать значение такого параметра, как "Data Redundancy" ("Чрезмерность данных"). Чем большее значение будет указано, тем меньше информации можно вместить, но тем выше будет ее стойкость при сжатии.

Особенность этой программы – сохранение большей части информации при сжатии видео – делает возможным ее применение в сфере цифровых "водяных знаков". *Imagespyer* Александра Мясникова – бесплатная отечественная разработка, известная также как плагин Stegotc для программы "Total Commader". Реализуется вариант алгоритма LSB с возможностью установки произвольного порядка бит в сочетании с 40 симметричными криптографическими алгоритмами. *Darkcrypttc* – бесплатный плагин для Total Commander с графической оболочкой Darkcrypt GUI, является продолжением разработок Imagespyer и Stegotc и реализует алгоритм LSB (от 3 до 12 бит на пиксель). Использует как контейнер для зашифрованных архивов изображения PNG, BMP, TIFF, PSD, TGA , MGA, аудиофайлы WAVE, текст, XML и HTML файлы (алгоритм замены символов).

Ограничения стеганографических методов

На протяжении последних 20-ти лет ведутся интенсивные исследования в области стеганографии. За все время исследовательской деятельности на основе обработки большого количества звуковых, графических, текстовых и других файлов удалось создать широкую базу стеганографических признаков и типов [3]. В частности, применяя технологию контрольной суммы данных, на первых этапах проверки информации удается отсеять большое количество «пустых» файлов. Существуют сайты, где содержится база данных файлов операционных систем и большого количества известного программного обеспечения. Большинство программ стегоанализа способны самостоятельно догружать информацию из сайтов, быстро отсеивая ненужные данные.

Существуют тысячи возможностей включить сообщение, звук или изображение в другой файл и несколько десятков методов обнаружить тайную интеграцию [8]. Например, простые некоммерческие (freeware) программы для стеганографии используют такой метод сокрытия информации (чаще всего в графических файлах), который довольно легко выявить. Даже использование относительно продвинутого метода LSB не дает успеха.

Простые методы дестеганографии состоят в следующем: для начала нужно найти все места возможных закладок инородной информации, которые

допускает формат файла-контейнера. Далее нужно получить данные из этих мест и проанализировать их свойства на соответствие стандартным значениям. Для решения первого задачи достаточно внимательно изучить спецификации используемых форматов файлов, а вторая, по обыкновению, решается методами статистического анализа. Например, если необходимо запрятать какой-либо текстовый фрагмент, то такое послание будет содержать только символьную информацию: 52 знака латиницы, 66 знаков кириллицы, знаки пунктуации и некоторые служебные символы. Статистические характеристики такого сообщения будут резко отличаться от характеристик случайной последовательности байтов, которую должны напоминать младшие биты, собранные вместе (для метода LSB).

Существенным недостатком ЦВЗ является то, что его достаточно легко удалить из заверенного им сообщения, после чего добавить к нему новую подпись. Удаление подписи позволит нарушителю отказаться от авторства, или, наоборот, обмануть законного получателя относительно авторства сообщения.

Все вышесказанное означает, что изучение стеганографических алгоритмов в отношении их применения для защиты авторских прав аудио данных должно и будет продолжаться, и одним из основных направлений является повышение их стойкости.

Анализ тенденций развития стеганографичских средств защиты авторских прав аудио данных

Хотя стеганография – пока еще относительно новое и необычное явление в сфере защиты информации, однако ее технологии современны и востребованы. Рядом с рядовым пользователем в ней заинтересованы и большие компании, которые работают в сфере мультимедиа и хотят защитить свой контент от незаконного использования. Если еще несколько лет тому большинство программ пользовались одинаковыми алгоритмами, а их интерфейс был чрезвычайно сложным, то современные программы обеспечивают достаточный уровень удобства в работе. Стеганография, несмотря на перечисленные недостатки, в данное время уже может успешно использоваться для защиты ценной информации.

Анализ тенденций развития компьютерной стеганографии показывает, что в ближайшие годы интерес к развитию ее методов будет усиливаться все более. Предпосылки до этого уже сформировались. В частности, общеизвестно, что актуальность проблемы информационной безопасности постоянно возрастает и стимулирует поиск новых методов защиты информации. С другой стороны, бурное развитие информационных технологий обеспечивает возможность реализации новых методов защиты. И конечно, катализатором этого процесса является бурное развитие Интернета, с одновременным ростом его нерешенных проблем таких, как защита авторского права, защита права на личную тайну, организация электронной торговли, компьютерная преступность и кибертерроризм.