УДК 070.41

# ЗАЩИТА АВТОРСКИХ ПРАВ КАК ЗАДАЧА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

© 2011 В.А. Голуб

Воронежский государственный университет

Поступила в редакцию 5 апреля 2010 года

**Аннотация:** *В статье рассматриваются различные подходы к защите авторских прав на материалы, используемые в средствах массовой коммуникации. Показано, что наиболее действенными методами защиты прав авторов на материалы, представленные в цифровом виде, следует признать программно-аппаратные методы, базирующиеся на принципах защиты информации от несанкционированного копирования и использования.*

**Ключевые слова:** *авторское право, информационная безопасность, средства массовой коммуникации.*

**Abstract:** *The different methods of copyright protection, using by communication media is considered. It is shown, that the most effective methods of copyright protection are the hardware-software solutions, based on principles of defence of information from unauthorized coping and using.*

**Key words:** *copyright, information security, communication media.*

Проблема защиты авторских прав приобрела особую актуальность с развитием цифровых технологий и Интернета. Несмотря на постоянное совершенствование законодательства, в том числе международного, в сфере авторского права, а также, несмотря на непрерывное совершенствование и усложнение технических и программных средств, направленных на предотвращение нарушений в этой области, пиратское использование интеллектуальной собственности стало массовым явлением, ущерб от которого в глобальном масштабе превышает многие миллиарды долларов. Крайне актуальной задача защиты авторских прав является для тех, чья работа связана со СМИ, как печатными, так и электронными, а также рекламной деятельностью. Как только текст, фотография или видеозапись представлены публично, автор или правообладатель практически теряет контроль над возможным несанкционированным использованием материала. Для всех очевидна острота этой проблемы, когда речь идет о размещении тех или иных работ в Интернете, однако на практике очень часто грубые нарушения авторского права имеют место и тогда, когда представленный в виде цифрового файла материал предоставляется, например, в издательство или напрямую в типографию. В случае, когда помимо законной публикации, появляются и несанкционированные, естественно, без заключения договора с автором или правообладателем, без выплаты соответствующего вознаграждения за использование работы, а зачастую, даже без указания авторства, у законного владельца прав на пиратски использованный материал остается, практически, только один путь – путь судебного разбирательства. Судебное разрешение такой ситуации, как правило, требует немалых усилий истца и занимает много времени, в связи с чем, нередко законные владельцы авторских прав предпочитают игнорировать имевшие место нарушения, несмотря на материальные, а возможно, и репутационные потери. Кроме того, для того, чтобы подать иск в суд, прежде всего, необходимо выявить сам факт нарушения авторского права, что далеко не всегда возможно, так

как уследить за всеми публикуемыми материалами, включая Интернет-публикации, совершенно не реально. В этой связи наиболее надежным путем защиты авторских прав следует признать использование специальных технических и программных средств.

Целью данной работы является анализ возможностей существующих технических и программных методов и средств, предназначенных для защиты от нарушений прав авторов.

Технические и программные методы защиты авторских прав можно разделить на три группы:

1) методы, предусматривающие наличие явной подписи, указывающей на автора или владельца прав на материал;

2) методы, предусматривающие наличие скрытой авторской «подписи», внедряемой в цифровой файл, как правило, с использованием стеганографических технологий;

3) методы защиты от несанкционированного копирования, распространения и использования авторского материала, например, путем защиты от копирования CD или DVD, содержащих защищаемые цифровые файлы.

Рассмотрим первую группу методов – методов «подписывания» авторских материалов. Явное наличие подписи под текстом, фотографией, рисунком или иным изображением, а также указание авторства в титрах видеозаписи никоим образом не защищает материал от незаконного использования. Некоторым исключением можно считать ситуацию, когда прямо по фотографии наносится надпись, указывающая на автора работы, причем такая надпись, что ее незаметное удаление практически невозможно. Очевидно, что в этом случае мы имеем дело с приемом, который портит фотографию настолько, что ее пиратское воспроизведение становится бессмысленным. Такой метод часто применяется при размещении фотоизображений в Интернете, наряду с другим методом, предполагающим размещение изображения столь малого размера и плохого качества, что его использование иначе, кроме как в качестве «превьюшки» для предварительного просмотра невозможно. Понятно, что методы «подписывания» авторских материалов не способны обеспечить защиту прав авторов.

Вторая группа методов предусматривает скрытное внедрение в графический аудио- или видеофайл специальной информации, включая информацию о правообладателе, его почтовом и электронном адресе, телефоне и других данных (скрытное внедрение данных в текстовые файлы также возможно, но с целью защиты авторских прав не используется, так как присутствие «явной» подписи не портит текст). Наличие информации об авторе материала дает возможность лицам, заинтересованным в его использовании связаться с автором с целью заключения с ним соглашения о законном использовании его работы. С другой стороны, наличие стеганографически внедренных данных, в принципе, позволяет «отследить» размещение материала в Интернете, а значит, выявить факты возможного его несанкционированного использования. Рассмотрим эту группу методов более подробно.

Стеганография (в переводе с греческого – тайнопись) – техника скрытой передачи или скрытого хранения информации. Основной принцип компьютерной стеганографии предполагает использование двух типов файлов – файл-сообщение, которое должно быть скрыто, и файл-контейнер, в котором должно быть скрыто сообщение. Контейнер – любой файл или поток данных, в который может быть скрыто встроена информация. Если контейнер не содержит встроенное сообщение, то он называется пустым. Контейнер, содержащий встроенную информацию, называется заполненным или стегоконтейнером. В нашем случае в роли файла-контейнера выступает цифровой файл, в который необходимо внедрить информацию о владельце авторских прав. Важнейшим требованием к стегоконтейнеру является внешняя неотличимость пустого и заполненного контейнеров, чтобы наличие скрытой информации для стороннего наблюдателя никак внешне не проявлялось.

Одним из основных и наиболее перспективных направлений использования стеганографии является встраивание цифровых водяных знаков (ЦВЗ) (watermarking), способствующих защите авторских прав на графические и аудио- или видеофайлы от пиратства и обеспечивающих возможность контроля за распространением защищенной информации.

Цифровой водяной знак (ЦВЗ) – специальная метка, незаметно внедряемая в графический, аудио-, видео- или иной файл с целью контроля его использования. Для внедрения и распознавания цифровых водяных знаков разработано специальное программное обеспечение. Программы распознавания ЦВЗ позволяют извлекать информацию о владельце авторских прав и о том, как вступить с ним в контакт. Программы обнаружения ЦВЗ позволяют контролировать распространение защищенной информации. Таким образом, основной областью применения ЦВЗ является защита интеллектуальной собственности от копирования и несанкционированного использования.

Основным недостатком методов, предусматривающих внедрение в цифровых водяных знаков, является их неспособность предотвратить незаконное использование авторских материалов.

Третья группа методов защиты авторских прав направлена на блокирование несанкционированного копирования и использования авторского материала. Следует отметить, что такая задача является типичной задачей защиты информации, решение которой часто является обязательной для обеспечения информационной безопасности. Очевидно, что если тем или иным методом обеспечить защиту от несанкционированного копирования графических, аудио- или видеофайлов, то их пиратское использование становится невозможным и задача защиты авторских прав решается наиболее успешно. Таким образом, можно считать, что наилучшим способом защиты прав авторов на материалы, представленные в цифровом виде, является обеспечение информационной безопасности носителей этих данных или защита соответствующих файлов от копирования.

На сегодняшний день самыми распространенными являются методы, обеспечивающие защиту от копирования информации, записанной на CD или DVD. Несмотря на то, что такие методы широко используются, почти все они обладают существенным недостатком – недоступностью для «простого» пользователя, не являющегося профессионалом-компьютерщиком и не обладающего определенными аппаратными средствами. Кроме того, не все существующие методы достаточно надежны и зачастую легко обходятся с помощью специальных «хакерских» программ. В работе [1; 2] предложена свободная от указанных недостатков система защиты информации, записанной на компакт-диск, от несанкционированного копирования. Алгоритм и реализующая его программа предусматривают несколько степеней защиты данных с использованием криптографии, физических характеристик диска и контроля реестра.

Программа состоит из двух подпрограмм, первая из которых хранится в компьютере, на котором осуществляется запись информации на компакт-диск, и обеспечивает постановку защиты на диск, а вторая подпрограмма записывается на компакт-диск вместе с защищаемой информацией и предназначена для проверки диска на оригинальность. При успешном завершении проверки диска на оригинальность вторая подпрограмма обеспечивает работу с защищенным диском.

Предложенный алгоритм защиты от копирования данных, записанных на CD, включает несколько уровней защиты.

Первый уровень защиты предполагает шифрацию данных. Для шифрации используется быстро работающий криптографический алгоритм симметричного шифрования Blowfish. Ключ шифрования составляется путем умножения фиксированного коэффициента, запрограммированного в программе защиты диска, и случайного числа, автоматически генерируемого и записываемого в специальный файл, записываемый на жесткий диск в папку с проектом записи. Использование в качестве ключа только случайного числа не обеспечивает необходимой защиты, так как файл, в котором это число хранится, может быть легко взломан, а определение хранящегося в программе защиты дополнительного множителя усложняет в этом случае задачу определения ключа только по случайному числу.

Второй уровень защиты – это «плавающий» серийный номер используемой для записи «болванки» компакт-диска. «Плавающим» он является потому, что на чистых компакт-дисках серийный номер не является постоянным и генерируется программами записи при каждой записи или дозаписи диска, т.е. только при окончании записи диска. Использование этого номера программой защиты осуществляется следующим образом. После записи проекта на компакт-диск программа защиты считывает с компакт-диска сгенерированный «плавающий» номер и количество занятого проектом на диске места в байтах. С помощью этих данных, являющихся уникальными для каждого диска, генерируется специальный серийный номер защищенного проекта. Этот номер сообщается пользователю по окончании записи компакт-диска, для чего на экран монитора выводится окно с предложением записать номер защищенного проекта на поверхность компакт-диска или его упаковку. Необходимость записи номера проекта связана с тем, что в дальнейшем этот номер будет использоваться для проверки диска на оригинальность, т.е., для проверки является ли диск копией или оригиналом.

Третий уровень защиты – запись в реестр в специально создаваемую ветвь HKEY_LOCAL_MACHINE\SOFTWARE\SYSDBA набора данных, используемых в дальнейшем для проверки диска на оригинальность. Этими данными являются буква, обозначающая диск, соответствующий приводу CD-ROM, в который вставлен защищенный диск, и номер защищенного проекта. Запись этой информации в реестр происходит при первом запуске защищенного диска, а при последующих запусках автоматически осуществляется проверка защищенного диска на оригинальность. Такая запись обеспечивает защиту от эмуляторов диска, так как эмулятору соответствует другая буква диска, а запись в реестр номера защищенного проекта при первом запуске CD делает возможным не вводить этот номер при последующих запусках. Это достигается благодаря тому, что записанная на защищенный компакт-диск подпрограмма проверяет записи в реестре и при

обнаружении указанных выше данных сверяет номер, записанный в реестре защищенного проекта, с аналогичным номером, записанным на CD, также сверяется буква привода CD-ROM, распознанная программой, с буквой, записанной в реестре. Более подробно порядок работы с программой описан в [1; 2].

Методы противодействия несанкционированному копированию компакт-дисков позволяют защитить от пиратского использования любые цифровые файлы: графические, видео-, аудио- и др. Но если авторские материалы представлены на ином носителе, например, USB-флеш накопителе или флеш-карте (USB Flash Drive, Flash-Card), то защита данных должна организовываться иначе. Для того, чтобы не было зависимости от того, на каком носителе записаны авторские материалы, необходима разработка специальных методов. Более простыми и надежными такие методы защиты оказываются тогда, когда разрабатываются под конкретный вид авторского материала.

Рассмотрим, как может быть решена проблема защиты авторских прав на представленные в цифровом виде фотографии и иные изображения. С точки зрения информационной безопасности такая задача может трактоваться как задача защиты файлов графических форматов от несанкционированного копирования.

Как указывалось выше, самый простой путь предотвращения незаконного использования графических материалов заключается в том, что изображения представляются в сильно уменьшенном размере и/или намеренно ухудшенном качестве. Такой подход далеко не всегда допустим. Так, в сфере рекламы весьма распространенной является ситуация, когда заказчик просит фотографа или дизайнера предоставить подборку фотографий или графических работ для возможного отбора с целью использования в рекламных изданиях или наружной рекламе. Важнейшим условием, предъявляемым к отбираемым изображениям, является их высокий технический и художественный уровень. Разумеется, никакие приемы защиты авторских прав, основанные на ухудшении качества изображения в таком случае неприменимы. В то же время, предъявив потенциальному заказчику крупноформатные высококачественные изображения, автор рискует, что его работа может быть пиратски использована, т.е. его права будут нарушены. Выход из этой ситуации возможен, если сделать высококачественные цифровые изображения защищенными от копирования. В работах [3; 4; 5] предложен новый подход к решению такой задачи. Сложность противодействия пиратскому использованию изображений заключается в том, что необходимо не только обеспечить защиту от несанкционированного копирования файла, но и защиту от сохранения изображения, выведенного на экран, для чего обычно используется функция Print Screen.

На первый взгляд, размер изображения на экране в пикселах, а именно такое изображение может быть скопировано с помощью Print Screen, не столь велик, чтобы автору следовало беспокоиться по поводу его возможного, например, полиграфического воспроизведения. На самом деле это не так. Например, при размере цифрового файла, равного размеру экрана 2560 x 1600 пикселов (такое разрешение имеют многие мониторы, например, Dell 3007WFP-HC, Apple Cinema Display 30 (Alu) и др.) возможна качественная типографская печать изображения формата 21,7 x 13,5 см, что близко к формату A5 (расчеты проведены для печати с линиатурой типографского растра 150 lpi и коэффициентом качества 2, чему соответствует разрешение цифрового файла 300 dpi). Если принять коэффициент качества равным 1,5 (разрешение цифрового файла 225 dpi), то размер печати составит 28,9 x 18 см. Понятно, что изображение такого размера может использоваться не только для печати открыток, но и календарей, буклетов и другой рекламной продукции, а также в наружной рекламе. В том случае, когда размер цифрового файла составляет 3840 x 2400 пикселов (такое разрешение – более 9 мегапикселов – имеет, например, монитор IBM T221 с размером диагонали 22,2 дюйма) размер качественного полиграфического отпечатка может достигать 43,3 x 27,1 см, что можно отнести к крупноформатной печати. Таким образом, как показывают приведенные расчеты, требование представления размера графического файла всего лишь равного разрешению хорошего монитора, создает предпосылки для самого разнообразного пиратского использования изображения, включая не только размещение в Интернет-галереях, но и качественное полиграфическое воспроизведение.

Программное обеспечение, предназначенное для защиты авторских прав на изображения путем блокирования их несанкционированного копирования, в том числе на стадии просмотра, должно решать следующие задачи.

Во-первых, необходимо осуществить противодействие копированию изображения с использованием функции Print Screen, представляющей самый простой способ копирования информации, выведенной на экран. Для защиты от такого способа копирования необходимо обеспечить перехват нажатий клавиши <Print Screen> и после этого подменить изображение, размещенное в буфере обмена на некоторое изображение, подготовленное заранее.

Во-вторых, необходимо решить задачу защиты цифрового изображения от копирования, осуществляемого при помощи сторонних приложений, делающих скриншоты в автоматическом режиме. Наиболее эффективной защитой от программ, делающих скрин-шоты при помощи API-функций, является контроль вызовов WinApi функций, т.е. при вызове функций, копирующих изображение, запрещать это действие системными средствами. Для решения такой задачи необходимо обеспечить получение всего списка запущенных в системе процессов или потоков с целью последующего контроля вызовов со стороны этих процессов WinApi функций, копирующих изображение, выведенное на экран.

В предложенном в работах [1; 2; 3] методе решения задачи защиты цифровых изображений от копирования при запуске специально разработанной программы формируется список всех процессов и к каждому из них прикрепляется dll библиотека, которая заменяет перехватываемую WinApi функцию в таблице импорта на некую заранее написанную функцию, код которой реализован в данной библиотеке. Далее, при обнаружении нового процесса к нему также прикрепляется dll библиотека, что обеспечивает контроль над всеми выполняющимися в системе потоками. Основной сложностью при этом является проблема обмена данными с dll библиотекой, так как наличие всех входных данных для получения контроля над вызываемыми процессом WinApi-функциями требуется на момент запуска библиотеки, что обусловливает необходимость получения данных в dll Entry Point. Для этого используется технология File Mapping.

Описанные принципы защиты цифровых изображений от несанкционированного копирования были реализованы в специальном программном обеспечении, тестирование которого показало его корректную и стабильную работу. В частности, как это и должно быть, оказалось заблокировано копирование с использованием функции Print Screen, а также копирование при помощи стороннего программного обеспечения.

Таким образом, наиболее действенными методами защиты авторских прав на материалы, представленные в цифровом виде, в том числе материалы, предназначенные для размещения в средствах массовой коммуникации, следует признать программно-аппаратные методы, базирующиеся на принципах защиты информации от несанкционированного копирования и использования. В этом смысле защита прав автора может рассматриваться как специальный случай обеспечения информационной безопасности его работ.

**ЛИТЕРАТУРА**

1. Голуб В.А. Система защиты информации, записанной на компакт-диск / В.А. Голуб, А.Н. Нечипоренко // Материалы Международной конференции и Российской научной школы «Системные проблемы надежности, качества, информационных и электронных технологий в инновационных проектах (Инноватика - 2005)». – М. : «Радио и связь», 2005. – С. 121-122.

2. Голуб В.А. Защита информации на компакт-дисках / В.А. Голуб, А.Н. Нечипоренко // Безопасность. Бизнес. Наука. – 2006. – № 4. – С. 9-10.

3. Голуб В.А. Защита информации, представленной в виде графических файлов / В.А. Голуб, Ю.А. Дергачев, Д.В. Сурнин // Материалы Международной конференции и Российской научной школы «Системные проблемы надежности, качества, информационных и электронных технологий в инновационных проектах (Инноватика - 2006)». – М. : «Радио и связь2, 2006. – Ч. 5. – Т. 1. – С. 98-100.

4. Голуб В.А. Защита цифровых изображений от несанкционированного копирования / В.А. Голуб, И.В. Цветков // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. – 2009. – № 2. – С. 30-33.

5. Голуб В.А. Защита цифровых изображений от несанкционированного копирования / В.А. Голуб, И.В. Цветков // Материалы X Международной научно-методической конференции Информатика : проблемы, методология, технологии. – Воронеж, 2010. – С. 205-209.

*Голуб В.А.*
*Воронежский государственный университет.*
*Доцент кафедры рекламы и дизайна,*
*кандидат технических наук.*
*e-mail: v.a.golub@yandex.ru, vgol@list.ru.*

*Golub V.A.*
*Voronezh State University.*
*Candidate of Technical Sciences, Associate Professor,*
*Department of Advertisement and Design.*