Московский Государственный Физико-Технический институт.
Факультет Радиотехники и Кибернетики.

Защита авторских прав для мультимедийной информации.

Исп. Куликов А.Н.
гр. 916

Москва
2003г.

Введение.

В цифровую эру проблема защиты авторского права становится особенно актуальной. Сеть уже насыщена всевозможной графической, видео-, звуковой информацией. Растет пропускная способность каналов, совершенствуются потоковые технологии. Все аналоговое переводится в цифровое, либо сразу в цифровом виде и производится.

Естественно, что у каждого произведения-творения есть свой автор-правообладатель. Среди них немало альтруистов. Но большинство все-таки без особого восторга относятся к заимствованию плодов его бессонных ночей и полетов мысли. Имеется в виду отчисления в пользу автора или правообладателя. Именно на решении этой проблемы строят свой бизнес компании, столь своевременно разрабатывающие и внедряющие системы, призванные положить конец пиратскому беспределу в Интернете.

В настоящем эссе будут рассмотрены наиболее распространенные технологии защиты информации, не затрагивая ее правовых аспектов.

Технологии.

Сегодня существуют технологии, программное и аппаратное обеспечение, позволяющие сравнительно легко и с небольшими затратами производить копирование и тиражирование оригинальных авторских произведений (программ, компьютерных игр, цифровых аудио- и видеофайлов, компьютерной графики, электронных книг). В силу экономических факторов и пренебрежительного отношения к закону массовым тиражом расходятся именно пиратские копии. В сложившейся ситуации для защиты авторских прав законодательных мер явно недостаточно, поэтому авторам, разработчикам и издателям необходимо иметь представление о методах защиты своих разработок и произведений.

Вопрос о применении и выборе методов защиты требуется рассматривать еще на начальной стадии разработки и создания программ или цифровых произведений. Обычно методы защиты используются с целью:

- предотвратить пиратское копирование и тиражирование программ и цифровых произведений;
- обеспечить целостность программ и цифровых произведений, т.е. предотвратить внесение неавторизованных изменений;
- обеспечить соблюдение пользователем условий лицензионного соглашения.

Для защиты программного обеспечения и баз данных обычно применяются следующие технологии:

- шифрование данных и аутентификация пользователей;
- защита носителей (дискеты, компакт-диски);
- электронные ключи.

Для защиты цифрового контента применяются:

- шифрование контента и связанной с ним информации;
- защита носителей (дискеты, компакт-диски);
- маркирование информации с помощью цифрового водяного знака, цифровых меток и меток времени;
- трастовые аппаратные устройства.

Следует отметить, что надежно защитить интеллектуальную собственность может только комплексное применение различных технологий защиты на различных этапах распространения и использования продукта. Так как разработка собственной технологии защиты - дело сложное и дорогостоящее, лучше воспользоваться готовыми коммерческими решениями или обратиться за советом к специалистам, которые помогут выбрать оптимальный по стоимости и надежности вариант защиты вашего продукта.

Шифрование.

Защита цифровых произведений, программ и данных на основе методов шифрования широко используется разработчиками программного обеспечения и издателями цифрового контента для предотвращения незаконного копирования и пиратского тиражирования интеллектуальной цифровой собственности.

Шифрование представляет собой основанный на криптографических алгоритмах способ защиты информации. Под шифрованием понимается процесс преобразования открытых данных в последовательность данных, недоступных для понимания, с помощью некоторого алгоритма (алгоритма шифрования).

При защите цифровых произведений, программ и данных методы шифрования применяются для решения следующих задач:

- обеспечение *секретности* и *конфиденциальности* передаваемой информации для предотвращения их незаконного использования
- обеспечение *целостности* данных для предотвращения их изменения в процессе передачи
- *идентификация* участников финансовых транзакций и пользователей электронного контента
- применение *цифровой подписи* для подтверждения подлинности источника информации
- *совместное распространение* цифрового контента и информации о способах его использования (цифровых прав)
- *подтверждение* передачи информации или предоставления услуг.

Существует множество криптографических алгоритмов, которые предоставляют такие возможности. Наиболее известными являются DES, RSA, IDEA, ГОСТ, алгоритм Эль-Гамаля.

Защита носителей.

Защита носителей производится двумя способами, которые различаются применяемыми технологиями.

Первый способ заключается в том, что на дискете или компакт-диске участок некоторого файла повреждается аппаратным способом. В процессе работы программа проверяет наличие поврежденного файла и его параметры, после чего делается вывод о легальности копии исполняемой программы. В основном, этот способ применяется для защиты программ и баз данных. Однако этот способ защиты имеет свои недостатки. Существуют средства, которые могут копировать файлы без поврежденного участка и заменять его некоторой "вставкой". Поэтому иногда используют вариант этого метода, в котором кроме проверки поврежденного файла анализируется также и поверхность носителя на наличие физического дефекта в заданной области.

Второй способ основан на применении одного из вариантов технологии цифрового водяного знака и используется в основном для защиты компакт-дисков. В этом случае на каждый диск записывается некоторая уникальная информация, т.н. электронный отпечаток. В случае обнаружения пиратской копии компакт-диска электронный отпечаток используется для определения авторизованного диска, с которого производилось копирование.

Обычно каждый из этих способов применяется в комплексе с другими методами (шифрование, цифровая подпись и т.п.), что повышает степень защищенности программного обеспечения и цифрового контента.

Электронные ключи.

Наряду с программными средствами защиты программ и данных от пиратского копирования и нелегального тиражирования применяются и средства аппаратной защиты. Наиболее широкое применение среди разработчиков находят электронные ключи.

Электронный ключ представляет собой небольшое микроэлектронное устройство, которое подключается к одному из портов компьютера, и является аппаратным элементом системы защиты приложения.

Электронный ключ имеет два разъема, при этом один разъем служит для подключения ключа к параллельному или последовательному порту компьютера, а другой - для подключения периферийных устройств (принтера, модема и т.п.). С точки зрения этих устройств электронные ключи обычно являются "прозрачными" и, как правило, не создают проблем для их работы. Электронные ключи могут работать в каскадном режиме, то есть к одному порту компьютера могут подключаться несколько ключей одновременно.

Электронные ключи собираются на базе специально разрабатываемых для этого микросхем. В настоящее время существуют ключи двух типов:

- на базе микросхем с EEPROM-памятью (EEPROM - Electrically Erasable Programmable Read-Only Memory)
- на основе ASIC-чипов с памятью или без памяти, которые изготавливаются "под заказ" для каждого разработчика (ASIC - Application Specific Integrated Circuit).

Более совершенные модели ключей имеют энергонезависимую память, в которой храниться служебная информация, необходимая для идентификации самого ключа, разработчика, приложения и его версии. Часть памяти электронного ключа доступна только для чтения, остальная часть доступна для чтения/записи из защищаемого приложения.

В настоящее время возможности технологии электронных ключей настолько широки, что охватывают практически весь спектр способов защиты программного обеспечения. Используя электронные ключи, разработчики программ и баз данных могут разрабатывать надежные системы защиты своей интеллектуальной собственности. Электронный ключ является аппаратным элементом системы защиты приложения и используется для генерации отклика после обращения к нему из программного кода приложения. Обычно применяются два варианта защиты:

- создание защитной оболочки приложения, или так называемого "конверта" (Envelope)
- создание схемы защиты с использованием вызова функций обращения к ключу.

В первом случае защищаются исполняемые файлы уже готового приложения без изменения исходного кода программы. Модуль защиты внедряется в тело программы и при запуске приложения перехватывает управление на себя. При этом он проверяет наличие электронного ключа и соответствие параметров требуемым значениям. В случае положительного ответа защищенная программа загружается, расшифровывается и ей передается управление. В противном случае загрузка и расшифровка программы не производится, и приложение заканчивает выполнение. Недостатком этого варианта защиты является однократная проверка наличия ключа только в момент запуска программы.

Во втором случае для создания системы защиты в исходном коде программы используются вызовы функций обращения к ключу. Эти функции могут не только проверять наличие ключа, но и осуществлять операции чтения/записи в памяти ключа. При встраивании функций обращения к ключу в код программы степень защиты приложения значительно возрастает. Однако, чем сложнее проектируемая схема защиты

приложения на основе функций обращения к ключу, тем больше усилий и времени придется потратить на разработку и сопровождение программы.

Следует отметить, что проектирование схемы защиты приложения с использованием функций обращения к ключу является самостоятельной сложной задачей и зависит от многих факторов. В частности, значительное влияние оказывает функциональность и вид приложения - "облегченная" или профессиональная версия, версия с ограничением количества запусков или с ограничением по времени и т.п. Как правило, более подробно процесс разработки системы защиты с учетом особенностей конкретного типа электронного ключа описывается в руководстве разработчика, поставляемого в комплекте с ключом.

Цифровые водяные знаки

Цифровой водяной знак представляет собой некоторую информацию, которая добавляется к цифровому контенту и может быть позднее обнаружена или извлечена для предъявления прав на этот контент. Чаще всего в качестве охраняемого контента выступают музыкальные произведения, цифровое видео и компьютерная графика.

Теоретическим фундаментом технологии цифрового водяного знака является стеганография - раздел математики, разрабатывающий методы скрытия данных. Как самостоятельное научное направление стеганография сформировалась два-три года назад.

Обычно цифровой водяной знак используется в следующих случаях.

- Для того чтобы *подтвердить право собственности* на цифровое произведение
- Для внедрения в каждую копию произведения *электронного отпечатка*
- Для *защиты* цифрового контента
- Для *идентификации* цифрового водяного знака и проверки *целостности* контента
- Для *маркировки* цифрового произведения, когда цифровой водяной знак содержит дополнительную информацию о самом произведении

Существуют различные способы формирования цифрового водяного знака. Они различаются в зависимости от вида контента, маркетинговой политики и каналов распространения. В современных системах формирования цифровых водяных знаков используется принцип встраивания метки, являющейся узкополосным сигналом, в широком диапазоне частот маркируемого изображения. Указанный метод реализуется при помощи двух различных алгоритмов и их возможных модификаций. В первом случае информация скрывается путем фазовой модуляции информационного сигнала (несущей) с псевдослучайной последовательностью чисел. Во втором - имеющийся диапазон частот делится на несколько каналов, и передача производится между этими каналами. Относительно исходного изображения метка является некоторым дополнительным шумом, но так как шум в сигнале присутствует всегда, его незначительное возрастание за счет внедрения метки не дает заметных на глаз искажений. Кроме того, метка рассеивается по всему исходному изображению, в результате чего становится более устойчивой к вырезанию.

Рассмотрим для примера мультикастинговую MPEG-трансляцию. Основная сложность заключается в том, что каждый пользователь должен получать различные копии помеченных данных, с другой стороны задача данной схемы – избежать ретрансляции многочисленных копий.

Основная идея обеспечения защиты для такой трансляции состоит в том, чтобы создать два отмеченных водяными знаками потока, приписать произвольную уникальную последовательность бит каждому пользователю и использовать ее, чтобы разрешить конфликт между двумя помеченными потоками. Перед изложением алгоритма следует подчеркнуть следующие моменты:

- Следует использовать необратимую схему добавления цифрового водяного знака. Иначе, такая отметка видеопотока может быть легко дискредитирована.

- Различные водяные знаки можно применять для каждого кадра трансляции или один и тот же знак для каждого кадра отдельного потока. Для простоты рассмотрим второй случай.

Детальная схема представлена ниже:

1. Создаются два потока W_1 и W_2.
2. К каждому потоку по необратимой схеме добавляется собственный водяной знак.
3. Помечается каждый кадр синфазного канала I_1, I_2,…, I_n.

Помечается весь видеопоток, используя по отдельности W1 и W2. Соответственно на выходе получая результирующие потоки $I_1 + W_0$; $I_2 + W_0$;…; $I_n + W_0$, и $I_1 + W_1$; $I_2 + W_1$; …; $I_n + W_1$.

4. Создается случайная последовательность бит для каждого пользователя. Длина последовательности равна количеству кадров в потоке. При живой трансляции длина такой последовательности может быть бесконечной.
5. Для i-го (i = 1,…, количество кадров) помеченного кадра в потоке о (в случае двух потоков j = 0 или 1) используется ключ K_{ij} для его кодирования. Потом мы передаем ключ K_{i0} или K_{i1} пользователю n, основываясь на последовательности бит, сгенерированной для этого пользователя. Другими словами, если i-й бит последовательности 0 передаем пользователю n ключ K_{i0}, иначе K_{i1}.
6. Измененный ключевой заголовок для i-го кадра выглядит следующим образом:
   $$K_{i0k1}K_{i1k2}K_{i1k3}\ldots K_{i0kn}$$
   Предполагая, что в i-ом бите последовательности стоит 0 для пользователя 1, 1 для пользователя 2, 1 для пользователя 3,…, 0 для пользователя n.
7. Таким образом, i-й кадр синфазного потока, который подлежит трансляции, имеет следующую структуру:
   $$K_{i0k1}K_{i1k2}K_{i1k3}\ldots K_{i0kn}\, I_i+W_{oKi0I}i+W_{1Ki1}$$

Дадим несколько комментариев к такой схеме. Во-первых, поскольку для каждого кадра используется новый ключ, то к потоку легко присоединяться и отсоединяться. Эта схема также позволяет легко приостанавливать трансляцию отдельным пользователям и возобновлять ее без перерегистрирования (чтобы исключить пользователя n достаточно не передавать ему новый ключ). Во-вторых, хотя схема не выглядит масштабируемой в соответствии с распределением ключей, она предоставляет оптимизированное решение, благодаря часто меняющимся ключам. С другой стороны, в связи с необходимостью ретранслировать ключи, она оправдана в использовании для трансляций среднего размера (не больше 1000 пользователей). Предположим, каждый ключ состоит из 128 бит или 16 байт, тогда длина ключевого заголовка составляет 16000 байт и сравнима с размером одного кадра синфазного потока.

Технология цифрового водяного знака используется обычно совместно с другими методами защиты цифровых произведений. В последнее время она завоевывает все более широкий рынок благодаря своей гибкости и возможности использования новых бизнес-моделей тиражирования и распространения электронного контента.

Заключение.

Средства защиты авторских прав среди цифровых источников информации активно развиваются. Совершенствуется и законодательство в этой области. Рынок программных средств защиты интеллектуальной собственности, распространяемой в Интернете и на других цифровых носителях, только складывается. Высоки и рыночные ожидания, хотя в настоящее время определить их трудно. На мой взгляд, основная причина в том, что представители индустрии цифровых изображений до сих пор не сформулировали четких критериев оценки существующих коммерческих продуктов и предлагаемых решений по защите авторского права. Очевидно одно - будущее за комплексными решениями.

Источники.

1. Сайт Digital Intellect (http://www.intellect.vsu.ru).
2. Lintian Qiao “Multimedia security and copyright protection”.
3. Журнал «Мир Internet».
4. Сайт Citforum (http://www.citforum.ru).
5. Сайт Иероглиф (http://www.hiero.ru)