

ИСПОЛЬЗОВАНИЕ DRM В ЗАЩИТЕ АВТОРСКИХ ПРАВ В ЭКОНОМИЧЕСКИХ СИСТЕМАХ

Левитасова В.Б., студент; Кайдановский К.А., студент; Губенко Н.Е., к.т.н., доц.
(Донецкий национальный технический университет, г. Донецк, Украина)

По мере развития общества и повышения значимости информации интеллектуальная собственность постепенно стала утверждаться как один из наиболее важных нематериальных активов экономики. В субъективном смысле авторское право (АП) – те имущественные и личные неимущественные права, которые принадлежат лицам, создавшим произведения науки, литературы и искусства. Изначально идея защиты АП развивалась преимущественно как социальная и правовая система, поэтому долгое время она не имела того же значения для экономистов, как и патентная система в результате чего произошла недооценка экономической значимости защиты объектов АП [1].

Однако в настоящее время АП стало основой для развития многих отраслей промышленности, обеспечивая рост добавленной стоимости, рабочих мест и внешней торговли. Согласно некоторым оценкам, доля отраслей промышленности, основанных на АП, в мировой экономике составила порядка 7,3% (2,2 триллиона долларов) в начале нового тысячелетия, при этом рост в этих отраслях составил в среднем на 5% в год, что быстрее, чем средний рост экономики всей планеты [2].

В экономических системах используются общепринятые технические средства защиты АП (DRM – Digital rights management) – программные или программно-аппаратные средства, которые затрудняют создание копий защищаемых произведений (в электронной форме), либо позволяют отследить создание таких копий. Кроме DRM-схемы, существуют также две распространенных технологии защиты – Watermarking (наложение цифровых "водяных меток") и Fingerprinting (нанесение, считывание и сравнение цифровых отпечатков файла) [3].

Из-за невозможности техническими средствами автоматически отличить «законное» копирование от «незаконного» DRM не допускают любое копирование, что вызывает их критику со стороны правозащитников. Поскольку DRM малоэффективны сами по себе, для них устанавливается правовая защита – законодатели многих стран ввели ответственность за обход 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, однако это нельзя осуществить достаточно надежно, поскольку применяемые ныне устройства воспроизведения (персональные компьютеры, видеомэгафоны, DVD-проигрыватели) являются достаточно универсальными и находятся под контролем пользователей.

В DRM-схеме, в основном, применяется принцип блочного симметричного шифрования AES (Advanced Encryption Standard) – расширенный стандарт

шифрования, в основе, которого лежит алгоритм Rijndael. Данный алгоритм преобразует блок данных длиной 128 бит в другой с помощью секретного ключа шифрования, который может быть длины 128 (AES-128), 192 (AES-192) или 256 бит (AES-256). Для шифрования в алгоритме AES (рис.1) применяются следующие процедуры преобразования данных:

- ExpandKey – вычисление раундных ключей для всех раундов;
- SubBytes – подстановка байтов с помощью таблицы подстановок;
- ShiftRows – циклический сдвиг строк в форме на различные величины;
- MixColumns – смешивание данных внутри каждого столбца формы;
- AddRoundKey – сложение ключа раунда с формой [4].

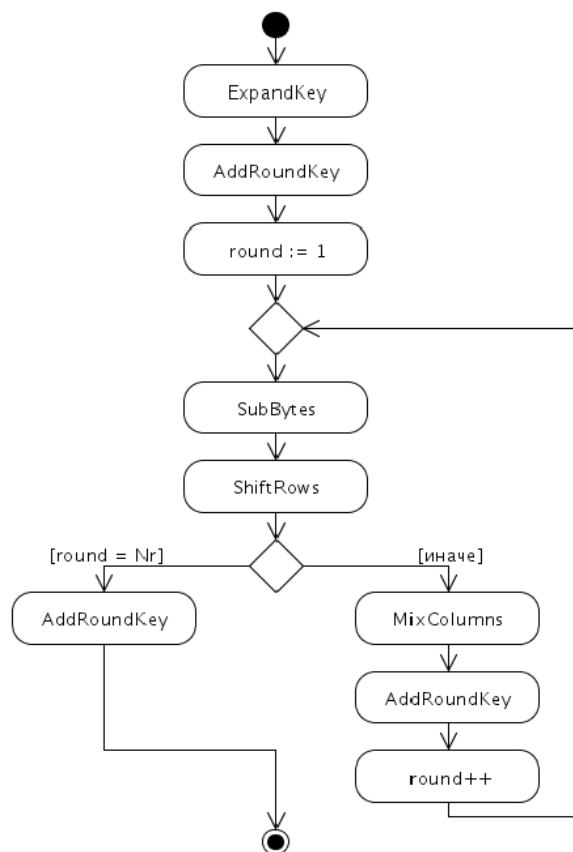


Рисунок 1 – Схема шифрования по алгоритму AES

Специфика DRM технологий защиты зависит от защищаемого объекта – электронного документа, книги, видео- и аудиоматериалов и т.д.

Для защиты текста и электронных книг используют формат Adobe PDF, который поддерживает следующие методы защиты содержимого:

- полное криптостойкое шифрование документа, требующее ввод пароля для любых операций с документом;
- защита документа, определяющая, возможно ли копирование, извлечение текста, печать или изменение документа.

Adobe DRM – технология защиты, используемая в Adobe Reader версии 6.0 и выше. Используется в различных книжных Интернет-магазинах, поддерживает привязку возможности просмотра к компьютеру пользователя или другому устройству (КПК, электронной книге), позволяет ограниченное количество раз копировать документ, позволяет запретить извлечение текста и печать документа, а также ограничить срок, в течение которого возможен доступ к документу.

Для защиты видеоматериалов от копирования используется система Advanced Access Content System – система DRM, используемая для защиты HD DVD и BluRay дисков, опубликованная в апреле 2005 г. и окончательно принятая 5 июня 2009 г. консорциумом AACSLA (AACSLicensing Administrator), включающим Disney, Intel, Microsoft, Panasonic, Warner Bros., IBM, Toshiba и Sony. Система использует цифровые водяные знаки для отслеживания взломанных ключей, водяные знаки компании Verance для звуковых дорожек к фильмам, позволяющие обнаруживать звук, записанный в кинотеатре («экранка»), и блокировать его воспроизведение [5].

Для защиты компьютерных игр от копирования DRM технологии применяются следующим образом: при запуске диск с игрой необходимо вставить в оптический привод, при этом проверяются низкоуровневые особенности лицензионных CD и DVD-дисков (топология диска), которые невозможно воспроизвести при копировании в домашних условиях, однако возможно эмулировать в специальных программах. Также подобные системы DRM часто устанавливаются в систему драйвера для защиты от эмуляторов дисководов (например, DAEMON Tools и Alcohol 120%), а иногда требуют ввода ключа или регистрации через Интернет. Игровые приставки (Xbox 360 и PlayStation 3), также содержат систему проверки диска на наличие лицензии [6].

На данный момент ни один из используемых в системах DRM алгоритмов не является универсальным и надежным. В условиях все более обостряющегося противостояния в сфере распространения цифрового содержимого невозможно появление системы DRM, одновременно удовлетворяющей как правообладателей, так и потребителей. В случае принятия системы DRM в качестве стандарта в целой отрасли, ее методы будут обеспечивать защиту цифрового содержимого на каждом этапе его продвижения. В таком случае компьютеры автоматически определяют, что разрешено пользователю делать с данным цифровым содержимым. С точки зрения пользователей, наилучший компромисс может быть достигнут тогда, когда программисты каким-то образом смогут выразить количественно «принцип правомерного использования» для практического применения в компьютерах.

Таким образом, можно сделать вывод о том, что, исходя из мировой практики, одним из наиболее применяемых подходов для защиты авторских прав в экономических системах являются DRM технологии. Они обеспечивают достаточно высокий уровень защиты, но имеют ряд недостатков. Таким образом, использование одних DRM технологий для защиты АП недостаточно, необходимо совмещать несколько алгоритмов (DRM, Watermarking, Fingerprinting) для более надежной защиты информации или пересмотреть подход к защите авторских прав в целом.

Перечень ссылок

- 1 Авторское право_Свечникова И.В_Уч пос_2009 -206с.
- 2.Димитр Гантчев, главный советник ВОИС по авторским и смежным правам
- 3.Википедия— свободная энциклопедия. <http://ru.wikipedia.org/>Технические средства защиты АП.
- 4.Пан К.С., Цымблер М.Л. Алгоритм блочного симметричного шифрования Advanced Encryption Standard (AES).
- 5.Летюка И.А., Терещенко Т.М. Анализ технических средств защиты авторских прав. www.nbuv.gov.ua. Режим доступа: Анализ технических средств защиты АП
- 6.Луцкер А. П. Авторское право в цифровых технологиях и СМИ — М.: КУДИЦ-ОБРАЗ, 2005. — С. 100-109. — 416 с.