СПИСОК ЛИТЕРАТУРЫ:

1. *Александрович Г. Я., Нестеров С. А., Петренко С. А.* Автоматизация оценки информационных рисков компании // Защита информации. Конфидент. 2003. № 2. С. 78–81.
2. *Малюк А. А.* Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. М.: Горячая линия–Телеком, 2004.
3. *Симонов С.* Современные технологии анализа рисков в информационных системах // PCWEEK. 2001. № 37.
4. *Симонов С.* Технологии и инструментарий для управления рисками // JetInfo. 2003. № 2.
5. The logic behind CRAMM's assessment of measures of risk and determination of appropriate countermeasures. URL: http://www.cramm.com/downloads/techpapers.htm.
6. *Taylor L.* Risk analysis tools & how they work. URL: http://www.riskwatch.com.

*М. В. Гончаренко, В. Г. Иваненко, И. А. Кириллов*
Московский инженерно-физический институт (государственный университет)

## ПРОБЛЕМА ЗАЩИТЫ АВТОРСКИХ ПРАВ НА АУДИО- И ВИДЕОДАННЫЕ С ПОМОЩЬЮ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

Рассматриваются вопросы защиты авторских прав на цифровые аудиоданные (звукозаписи) и видеоданные и способы их решения с помощью цифровых водяных знаков (ЦВЗ). Отмечаются основные методы встраивания ЦВЗ в аудио- и видеосигналы, позволяющие решать рассматриваемую проблему.

Проблема защиты авторского права на представленную в электронном цифровом виде информацию включает с себя, помимо защиты права собственности и доказательства этого права, проблему защиты от несанкционированного копирования [1]. Решение подобной задачи — процесс сложный и пока еще весьма далекий от полного завершения, а достижение удовлетворительных результатов возможно лишь с помощью целого комплекса мер и средств, правовых и технических. Среди технических средств защиты авторских прав на аудио- и видеоданные особый интерес как наиболее перспективные представляют технологии применения цифровых водяных знаков.

Цифровой водяной знак — это данные о владельце или авторе цифровой информации, встроенные в цифровые аудиоданные, видеоизображение или текст, которые могут быть обнаружены и извлечены специальными способами для выявления своей подлинности либо для предъявления претензий владельцу самой информации. ЦВЗ встраивается в несущие данные таким образом, что он неотделим от них. Сами же данные со встроенным в них ЦВЗ оказываются общедоступными, но перманентно помеченными [2].

В отличие от криптографических средств защиты, целью которых является ограничение доступа к данным неавторизованных пользователей, цифровые водяные знаки позволяют иметь доступ к информации всем желающим, при этом в случае необходимости встроенный ЦВЗ позволяет определить ее владельца.

Методы встраивания ЦВЗ в аудиосигналы основываются на использовании особенностей слуховой системы человека, которая различает изменение фазы сигнала слабее, чем изменение его амплитуды и частоты, а также является чувствительной к аддитивному белому шуму [3]. Большинство существующих к настоящему времени методов встраиваемых ЦВЗ в аудиосигналы является развитием следующих методов встраивания информации: кодирование наименьших

значений бит, фазовое кодирование, расширение спектра за счет изменения времени задержки эхо-сигнала, маскирования ЦВЗ.

Из различных возможных методов встраивания информации в видеопоследовательности наибольшее распространение получили следующие три группы методов: встраивание информации на уровне коэффициентов дискретных преобразований, встраивание информации на уровне битовой плоскости и методы дифференциального энергетического встраивания [4]. Следует отдельно отметить последний из них, отличающийся от других лучшей устойчивостью к различным последующим преобразованиям самих видеоданных, таких как сжатие, фильтрование и т. п.

Круг задач защиты авторского права, решаемых с помощью ЦВЗ, постоянно расширяется. Так, появились алгоритмы встраивания ЦВЗ в интернет-радиовещании. Крупнейшие производители программного обеспечения начинают предоставлять свои продукты с возможностями встраивания в аудиофайлы ЦВЗ для решения проблем, связанных с пиратством [5].

При наличии достаточной правовой поддержки цифровые водяные знаки могут стать наиболее эффективным инструментом для защиты авторских прав на аудио- и видеопродукцию.

## СПИСОК ЛИТЕРАТУРЫ:

1. *Ларичев В. Д., Трунцевский Ю. В.* Защита авторского права в аудиовизуальной сфере. Уголовно-правовой и криминалистический аспекты. М.: Дело, 2004. — 352 с.
2. *Chun-Shien Lu.* Steganography and digital watermarking techniques for protection of intellectual property. Idea Group Publishing, 2005.
3. *Грибунин В. Г., Оков И. М., Турищев И. В.* Цифровая стеганография. М.: Салон-Пресс, 2002. — 272 с.
4. *Cassuto Y., Lustig M., Mizrachyy S.* Real-time digital watermarking system for audio signals using perceptual masking. Signal and Image Processing Lab, Faculty of EE. URL: http://www-sipl.technion.ac.il/.
5. Digital Audio Watermarking. Technical Pre-release / Prototype Product Overview. Microsoft Corporation, 2006. URL: http://download.microsoft.com/download/d/6/b/d6bde980-5568-4926/_audio_watermark.

*М. Н. Даннави*
Московский технический университет связи и информатики

## АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ DOS В СЕТЯХ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

Рассматриваются угрозы DoS в ОКС-7, вызванные фальсификацией сообщений обновления маршрутизации, реализация которых может нанести серьезный урон функционированию сетей связи общего пользования.

Вопросы информационной безопасности (ИБ) в сетях связи общего пользования обладают высокой важностью [1]. Фальсификация злоумышленником некоторых сообщений обновления маршрутизации в системе общеканальной сигнализации ОКС-7 может вызвать нарушение функционирования сетей связи общего пользования вплоть до вывода из строя части сети ТфОП, GSM и интеллектуальной сети (IN) [2, 3]. Возможность отсутствия механизмов защиты от таких угроз или несовместимость этих механизмов в ОКС-7 разных производителей показывают