2. *Бабаш А. В.* Решение автоматных уравнений с искажениями в функции переходов автомата // Проблемы передачи информации. М., 2002. Том 38. Вып. 3.
3. *Бабаш А. В.* Isoperiods of output sequences of automata // Probabilistic Methods in Discrete Mathematics. VCP. Utrecht, 2002.
4. *Бабаш А. В.* Приближенные модели конечных автоматов // Обозрение прикладной и промышленной математики. 2005. Том. 12. № 2. С. 209–248.
5. *Бабаш А. В.* О восстановлении информации о входном слове перестановочного автомата Медведева по начальным и заключительным состояниям // Проблемы передачи информации. М., 2007. Том 43. Вып. 2. С. 74–84.

Е. К. Баранова
Российский государственный социальный университет (Москва)

АНАЛИЗ И УПРАВЛЕНИЕ РИСКАМИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматриваются два подхода к обоснованию проекта подсистемы обеспечения информационной безопасности (ИБ). *Первый подход* основан на проверке соответствия уровня защищенности информационной системы (ИС) требованиям одного из стандартов в области информационной безопасности. *Второй подход* к построению системы обеспечения ИБ связан с оценкой и управлением рисками, изначально он исходит из принципа «разумной достаточности», примененного к сфере обеспечения ИБ.

На основе идентификации риска по трем параметрам:

— *угроза*, возможной реализацией которой вызван данный риск,

— *ресурс*, в отношении которого может быть реализована данная угроза,

— *уязвимость*, через которую может быть реализована данная угроза в отношении данного ресурса,

оценивается ожидаемый ущерб и сравнивается с затратами на меры и средства защиты, после чего принимается решение в отношении данного риска, который может быть *снижен*, *устранен*, *перенесен* или *принят*.

Рассматривается графовая модель системы безопасности с полным перекрытием, описываемая соотношением:

$S=\{O,Y,M,V,B\}$,

где O — набор защищаемых объектов; Y — набор угроз; M — набор средств обеспечения безопасности; V — набор уязвимых мест; B — набор барьеров, упорядоченных троек $bi=(yi, oj, mk)$, представляющих собой точки, в которых требуется осуществлять защиту в системе.

В модели определяется каждый объект, требующий защиты, оцениваются средства обеспечения безопасности с точки зрения их эффективности и их вклад в обеспечение безопасности всей ИС.

Отмечается, что рассмотренная модель безопасности с полным перекрытием применима в основном как инструментарий при разработке определенных политик безопасности либо в случае построения комплексной системы защиты информации для малого предприятия.

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