Посилання на статтю

Макарова И.И. Комплексная информационная безопасность электронного документооборота / И.И. Маракова // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В.Даля, 2004. – № 3(11). – С.100-105. Режим доступу: http://www.pmdp.org.ua/

УДК 681.5.015:004.056.57

И.И. Макарова

КОМПЛЕКСНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Исследована возможность использования технологиицифровых водяных знаков (ЦВЗ)для идентификации и подтверждения целостности сообщений при электронном документообороте. В отличие от других технологий, например, цифровой подписи, ЦВЗ не увеличивают размер сообщения и являются неотделимыми от основного сообщения. Фундаментальной проблемой построения таких систем является восстановление основного сообщения после детектирования ЦВЗ. Рис. 3, ист. 4.

І.І. Макарова

КОМПЛЕКСНА ІНФОРМАЦІЙНА БЕЗПЕКА ЕЛЕКТРОННОГО ДОКУМЕНТООБОРОТУ

Розглянуто використання цифрових водяних меток (ЦВМ) обороті електронних документів, в ідентифікації та ствердження цілісності електронних документів. У відзнаки від других технології, наприклад, цифрової підписи, ЦВМ не потребують додаткового простору та є невіддільними від головного повідомлення. Фундаментальна проблема створення таких систем – відновлювання головного повідомлення без втрат після детектування ЦВМ. Рис. 3, дж. 4.

I.I. Makarova

COMPLEX INFORMATION SECURITY FOR E-DOCUMENT CIRCULATION

A watermark (WM) application to assist the integrity maintenance and verification of the e-documents is considered. The great merit of WM usage in authentication context since WM is inseparable from cover message and it does not require additional storage space for supplementary meta-data, as cryptographic signatures for instance. A fundamental problem remains: the restoration of cover message without any error after WM detection.

Общенаучная проблема. Интегрированные компьютеризированные системы на современном уровне развития Украины все шире используются в самых различных видах деятельности: торговле, производстве, оказании услуг и т.д. Широкое распространение глобальной всемирной сети Интернет практически не оставляет шансов ни у какого юридического образования рано или поздно не столкнуться с проблемой создания некоторой адаптированной системы электронного документооборота,хотя бы в ракурсе нескольких аспектов своей деятельности (связь с банком, контакты с деловыми партнерами). Одним из основных требований к системе электронного документооборота является обеспечение защиты от активных и пассивных несанкционированных действий.

С другой стороны, административная реформа, реформа государственной службы, бюджетная реформатесно связаны с внедрением новых информационных технологий в управленческие процессы. Комплексная система электронного документооборота также является существенной поддержкой реализации реформ. И даже если к информационным ресурсам предъявляется требование открытости, необходиматщательная проработка процедур, обеспечивающих прозрачность, но исключающих несанкционированные действия, разграничивающих при необходимости допуск.

В настоящее время многие организации используют новые информационные технологии, позволяющие значительно повысить эффективность деятельности в любой сфере. Однако используемые системы часто имеют изолированный, фрагментальный характер. В области документооборота это положение является наиболее тревожным. Отсутствуют технологии, отвечающие сегодняшним требованиям документационного обеспечения управления. Прежде всего необходимо подчеркнуть отсутствие комплекса нормативного обеспечения организации работы с цифровыми документами на различных уровнях государственного, общественного, экономического управления. Оставляет желать лучшего и научно-методическое обеспечение данного процесса.

Основной материал исследования. Информационная безопасность в области электронного документооборота подразумевает исключение возможности несанкционированного использования документа (рис.1).

Обеспечение конфиденциальности подразумевает исключение не только возможности несанкционированного ознакомления, но и несанкционированной отправки, т.е. связано с решением вопросов по мониторингу трафика электронного документооборота. Сохранение целостности означает исключение возможности внесения несанкционированных изменений. Персонификация подразумевает реализацию процедур идентификации и прозрачность трафика.

Рис. 1. Классификация требований, предъявляемых к процедуре электронного документооборота

Самый простой метод защиты информации в цифровом виде – криптография. Развитие компьютерной техники сделало возможнымвыполнениепроцедуршифрования и дешифрованияинформационных потоков в реальном времени. Различные криптографические протоколы также могут использоваться для обеспечения конфиденциальности или разграничения доступа [1]. Кроме реализации процедур шифрования и дешифрованиякриптографические системы находят широкое применение для выполнения других важных функций, прежде всего для подтверждения

целостности и идентификации, реализуемых на основе асимметричных криптографических стандартов (цифровая подпись) [1]. Существует также целая группа очень полезных на практике модификаций цифровой подписи (ЦП). При работе в компьютерных сетях, когда пользователи часто разделены большими расстояниями, возникает необходимость четкого соблюдения правил и порядка их взаимодействий, т.е. протоколов, как правило, криптографически защищенных и решающих задачи организации секретности открытого канала связи, доказательства обладания секретом без выдачи любой информации или подсказки к раскрытию секрета и т.д.

Однако возникает целый ряд ситуаций, когда применение криптографических методов не решает возникающих проблем. Например, ЦП может быть без труда удалена из электронного документа; шифрование документов во многих странах запрещено на законодательном уровне; к процедурам идентификации нередко предъявляется требование скрытности и т.д.

Технологии цифровых водяных знаков (ЦВЗ) являются составной частью научно-технического направления сокрытия информации,позволяющие не столькосокрыть дополнительную информацию, сколькопередатьс основной информацией некоторую дополнительную (возможно и не секретную) информацию с целью идентификации и/или верификации (подтверждения целостности), которую невозможно удалить,неухудшив значительно надежности восприятия основного документа или основного покрывающего сообщения (ОПС).

Последнее десятилетие технологии ЦВЗ активно развиваются в связи с расширяющимся практическим применением (рис. 2). Одним из основных предназначений систем с ЦВЗ является защита авторских прав при копировании, контроль за оборудованием записи и воспроизведения цифрового мультимедиа, предотвращение несанкционированного копирования, поддержка менеджмента, мониторинг вещания [2, 3].

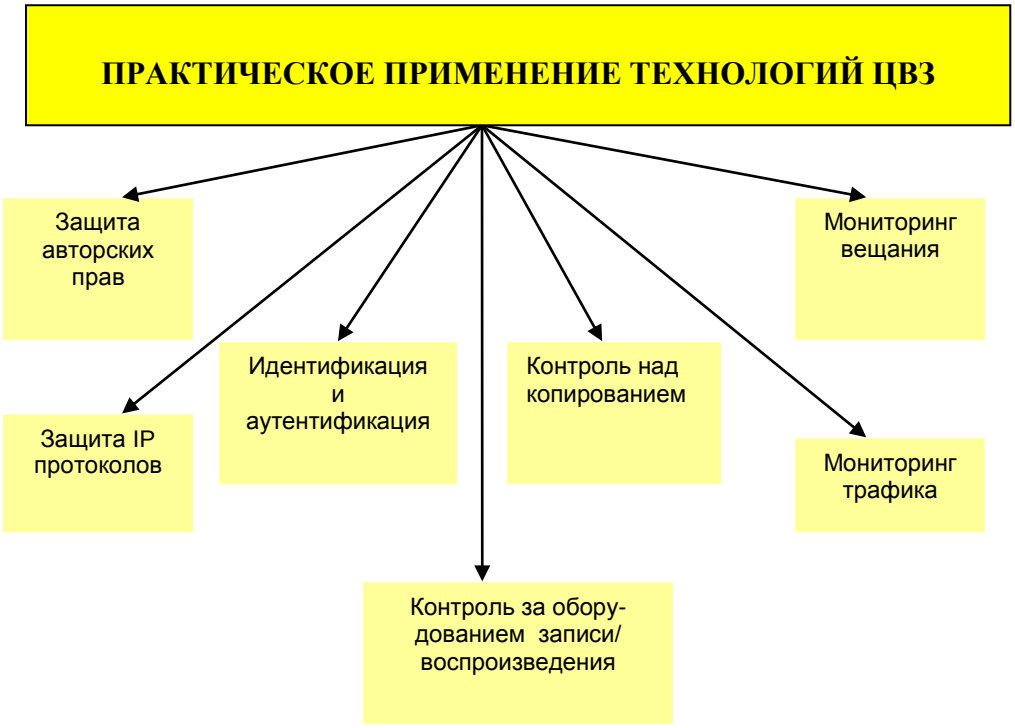

Рис. 2. Основные областипрактического применения систем с ЦВЗ

Технологиям ЦВЗ присущи свойства, которые обусловили их незаменимость относительно альтернативных методов, решающих те же задачи, а именно:

– ЦВЗ не заметные и в отличие от заграждающих кодовони не умаляют эстетики основного сообщения;

– ЦВЗ не отделимы от ОПС, в которое они погружены специальным образом и, в отличиеот применения специального заголовка, ЦП они не могут быть удалены при переформатировании, перезаписывании;

– ЦВЗ подвергаются тем же трансформациям, что и ОПС, что дает возможность исследовать эти трансформации, анализируя результирующие (выделенные) ЦВЗ или ОПС после несанкционированного удаления ЦВЗ.

Эти три отличия и обусловили незаменимость ЦВЗ для целого ряда приложений. В настоящее время на многих фирмах начинают задумываться о разработке систем документооборота с отслеживаниемтрафика в реальном времени на основе методов ЦВЗ. Однако необходим системный подходи в итоге разработка соответствующих стандартов.

Относительный рейтинг требований к системам с ЦВЗ определяется спецификой их применения. При применении технологий ЦВЗ для контроля за копированием, предотвращения несанкционированного копирования, мониторинга рекламного вещания, электронного делопроизводства и т.д.полагается, что некоторые изменения ОПС в результате погружения ЦВЗ являются допустимыми и на приемной части восстановление ОПС не требуется. Однако для подтверждения целостности, например, в медицинском менеджменте, криминалистике, требуется точное восстановление исходного ОПС. Например, если ОПС содержит *N*бити послепроцедуры сжатияостанется только *L* бит, то в *N-L* бит ОПС допустимо погружать ЦВЗ, которые, однако,

будут утрачены при сжатии (хрупкие системы с ЦВЗ). Практическое применение такого подхода ограничено. Более привлекательным является разработка теоретической базы, соответствующих алгоритмов ЦВЗ с точным восстановлением основных покрывающих сообщений, так называемых инвертируемых алгоритмов ЦВЗ [4]. В рамках такого подхода потребуется адаптация алгоритмов к типу ОПС. Данное требование не является серьезным ограничением в рамках рассматриваемого приложения. С учетом того, что объекты документооборота, как правило, являются бинарными, то кроме удовлетворения требованию инвертируемости ЦВЗвозникают сложность обеспечения надежности визуального восприятия стегаобраза, т.е. ОПС и ЦВЗ, при соблюдении правила секретности ЦВЗ для любых пользователей.

Не вдаваясь в подробности описания того или иного асимметричного стандарта для формирования ЦП, основные этапы протокола погружения ЦВЗ, сформированного как ЦП документа, таковы.

1. Формируется ЦП $SA = (T(F(h(C))^k$ для документа (ОПС), где T – функция инверсного преобразования; F – функция преобразования полученного дайджеста ОПС в бинарное; $h(C)$ – дайджест ОПС; k – секретный ключ. В качестве ЦВЗ $w(n),\ n = 1,\ldots N$ используется ЦП, причем, *N* – длина ЦП впримeняемомстандарте (RSA, DSA, ГОСТ 34.319-95 и др.).

2. Получатель стегасообщения $s(n) = c(n) + w(n) + \varepsilon(n)$, где $c(n),\ n \in A_N$ — ОПС, $\varepsilon(n),\ n \in A_N$ — аддитивная помеха (печать, сканирование и т.д.), детектирует ЦВЗи фиксирует $w'(n),\ n = 1,\ldots\ N$.

3. Инвертируемые ЦВЗ $w'(n),\ n = 1,\ldots\ N$ удаляются из стегасообщения.

4. Формируется дайджест $h(C')$ на основе хэшированиявыделенного ОПС $c'(n) = s(n) - w'(n),\ n \in A_N$, его ЦП $S\widehat{A}$ и выполняется побитное сравнение с ЦП SA.

5. При совпадении $h(C') = W'$ процедура аутентификации и идентификации успешна.

В результате анализа шагов протоколастановится очевидным, что допущенные искажения при восстановлении ОПС могут стать причиной ошибки верификации. В некоторых системах с ЦВЗтребуется учитывать неизбежное изменение сообщения в связи с компрессией, фильтрацией, редактированием и т.д. В этой связи необходимо определить группы изменений сообщения: легальные изменения, несанкционированные изменения. Система верификации на основе технологий ЦВЗ должна формировать положительное решение несмотря на наличие изменений сообщения, если эти изменения относятся к группе легальных. Необходимо выработать критерий допустимых с точки зрения процедуры верификации легальных изменений сообщения. Однако такой критерий безусловно будет изменяться в зависимости от практического приложения. Для выработки критерия необходимо ответить на вопрос, какие заключения должны быть сделаны на основесообщения (например, диагностика на основеизображения или авторские права).Если смысл этих заключений не изменен для первоначального сообщения и подверженного преобразованиям, то такие преобразования легальны и допустимы.Очевидно, что, например, вмедицинской, технической диагностике решение о допустимом уровне изменений должен делатьсоответствующий специалист. В некоторых

приложениях выбор порогового уровня допустимыхизменений является не только техническим решением, но и правовым. С правовой точки зрения требования к допустимости изменений также весьма зависят от соответствующей нормативно-правовой базы.

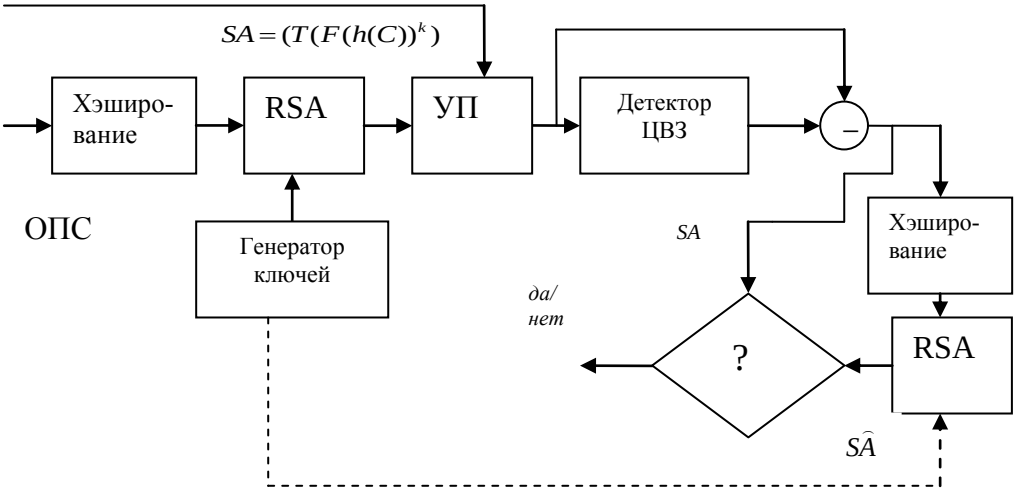

Рис. 3. Структурная схема системы подтверждения целостности электронного документа на основе технологий ЦВЗ

Выводы. Таким образом, верификация электронного документа, придание ему юридической силы возможны не только при обеспечении доказательства соответствия некоторому образцу, но и соответствию заданным стандартам применяемых информационных технологий.Следовательно, решение проблемы доверия к электронному документу возможно только при создании соответствующей инфраструктуры электронного документооборота. Основные составляющие такой инфраструктуры следующие:

– нормативно-правовая;
– управляющая и организационно-методичсекая;
– техническая (разработка комплесных аппаратно-програмных средств);
– мониторинг действия (аттестация, аудит, сертификация и т.д.).

На основе совокупности законодательных, нормативных, методических материалов, организационных решений, технических, программных, технологических объектов, разработанных методов, утвержденных стандартов возможно гарантирование эффективного электронного документооборота.

ЛИТЕРАТУРА

1. B.Schneir Applied Cryptography/ Protocols, Algorithms and Source Code in C. N.Y.:J.Wiley&Sons. – 1993. – 619p.
2. Langelaar G.C., J.C.A.Van der Lubbe, Biemond J. Copy Protectionfor MultimediaData basedon Labeling Techniques // 17th Symposium on Information Theory in the Benelux. – 1996. – P. 298-309.
3. Coatrieux G., Maitre H., Sankur B, Rolland Y., Collorec *R.* Relevance of Watermarking in Medical Imaging // Third IEEE EMBS International Technology Application in Biomedicine. – IEEE/EMBS. – 2000. – P.250-255.
4. Маракова И.И. Алгоритмы цифровых водяных знаков с точным восстановлением основных покрывающих сообщений //Правове, нормативне та метрологічне

забезпечення систем захисту інформації в Україні. – Науково-технічний збірник.– вип.7. – К.: НДЦ „Тезіс” НТУУ „КПІ”. – *в печати.*

Стаття надійшла до редакції 20.09.2004 р.