Посилання на статтю

Маракова И.И. Процесс идентификации и верификации электронных сообщений на основе информационных технологий встроенных идентификаторов/И.И. Маракова, А.Н. Стасюк, А.С. Сафронов// Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В.Даля, 2005 - №3(15). С. 134-139. Режим доступу: http://www.pmdp.org.ua/

УДК 681.5.015:004.056.57

И.И. Маракова, А.Н. Стасюк, А.С. Сафронов

ПРОЦЕСС ИДЕНТИФИКАЦИИ И ВЕРИФИКАЦИИ ЭЛЕКТРОННЫХ СООБЩЕНИЙ НА ОСНОВЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ВСТРОЕННЫХ ИДЕНТИФИКАТОРОВ

Рассматриваются подходы идентификации и верификации электронных сообщений в автоматизированных информационных системах. Предложен метод идентификации и подтверждения достоверности документов для систем электронного документооборота на основе технологий встроенных идентификаторов. Рис. 4, ист. 9.

Ключевые слова: идентификация и верификация сообщений, системы электронного документооборота, технологии встроенных идентификаторов.

І.І. Маракова, А.Н. Стасюк, О.С. Сафронов

ПРОЦЕС ІДЕНТИФІКАЦІЇ ТА ВЕРИФІКАЦІЇ ЕЛЕКТРОННИХ ПОВІДОМЛЕНЬ НА ОСНОВІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ВБУДОВАНИХ ІДЕНТИФІКАТОРІВ.

Розглядаються підходи ідентифікації та верифікації електронних повідомлень в автоматизованих інформаційних системах. Запропонований метод ідентифікації та підтвердження достовірності документів для систем електронного документообігу на основі технологій вбудованих ідентифікаторів. Рис. 4, дж. 9.

I.I. Marakova, A.N. Stasuk, O.S. Safronov

PROCESS OF MESSAGES IDENTIFICATION AND VERIFICATION DEVELOPED ON THE BASE OF DIGITAL WATERMARKING TECHNOLOGIES.

Methods of messages identification and verification in the information systems are considered. Method of documents verification on the base of digital watermarking technologies is proposed.

Общенаучная проблема. На современном этапе развития Украины информационные системы (ИС) все активнее используются для повышения эффективности и автоматизации документооборота, бизнес-процессов, процессов управления в самых различных видах деятельности: образовании, производстве, медицине, торговле, сфере услуг и т.д. Однако проблемой создания в рамках структуры организации или предприятия такой

интегрированной информационной системы является своевременное обеспечение защиты системы от несанкционированных действий.

Одним из основных требований к системе электронного документооборота являются требования обнаружения и предотвращения (а в случае невозможности предотвращения – возможности доказательства) активных и пассивных несанкционированных действий.

Кроме того, области отечественного документооборота ситуация продолжает оставаться не полностью удовлетворяющей современным требованиям. Отсутствуют технологии, отвечающие условиям документационного обеспечения управленческого процесса, нередко сама система документооборота рассматривается сотрудниками не как средство облегчения их труда, а лишь как некоторая фискальная система, позволяющая руководству следить за происходящим в организации. Также следует отметить отсутствие комплекса нормативного обеспечения организации работы с электронными документами на различных уровнях государственного, экономического и социального управления.

Анализ исследований и публикаций. Безопасность любой информационной системы определяется комплексной защищенностью всех ее составляющих: человеческих ресурсов (операторы, пользователи, администраторы), технической части (сервера, рабочие станции, локальные и глобальные вычислительные сети (ЛВС)) и программных компонентов (операционные системы, программные продукты) [1].

В системах электронного документооборота можно выделить следующие возможные нарушения (рис. 1). Как правило, основная масса сообщений не содержит секретной информации, поэтому более приоритетной задачей является задача отслеживания и предотвращения нелегальной модификации сообщений.

Несанкционированное чтение информации, содержащей сведения о персонале (анкетные данные, начисления по заработной плате, состояния счетов в банках, истории болезней, данные медицинских исследований и др.), бизнесе и финансовых материалах также может нанести ущерб организации от ее разглашения, однако модификация информации более опасна.

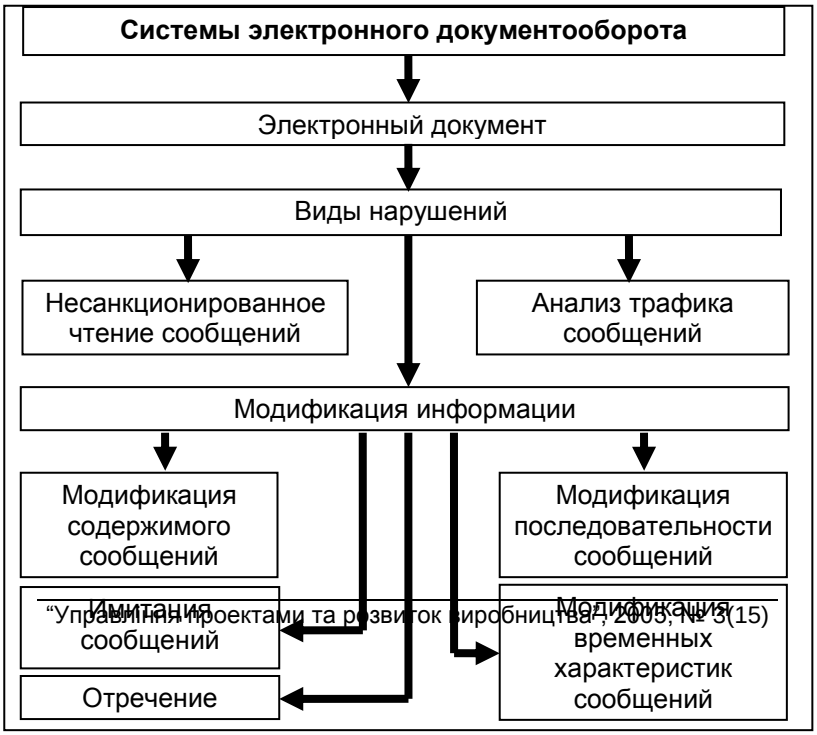


Рис.1. Основные виды нарушений в системе электронного документооборота

Если произошло раскрытие стратегической информации организации или корпорации, например, вскрыт перспективный план развития производства или анализ сегментов рынка по продаже определенных видов товаров, то потери для владельцев этой информации могут быть незаметны, но для конкурентов такие сведения будут ценными.

Предотвращение угроз, связанных с чтением информации, достаточно легко реализуется с помощью криптографических методов [2], традиционно применяемых для решения таких задач. Однако следует помнить, что в ряде стран, в том числе в Украине, применение криптографических методов, особенно в экспортируемых программных продуктах, ограничено законодательством.

Развитие компьютерной техники сделало возможным выполнение процедур шифрования и дешифрования информационных потоков в реальном времени. Различные криптографические протоколы также могут использоваться для обеспечения конфиденциальности или разграничения доступа [3]. Кроме реализации процедур шифрования и дешифрования криптографические системы находят широкое применение для выполнения других важных функций, прежде Вего, для подтверждения целостности и идентификации, реализуемых на основе асимметричных криптографических стандартов (цифровая подпись (ЦП)) Существует также целая группа очень полезных на практике модификаций ЦП.

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 часто предъявляется требование скрытности и т.д.

Альтернативой криптографическим методам для предотвращения нелегальной модификации информации выступают технологии встроенных идентификаторов, также известные как цифровые водяные знаки. Технологии встроенных идентификаторов (ВИ) являются частью научно-технического направления сокрытия информации, позволяющие не столько скрывать дополнительную информацию, сколько передавать с основной информацией некоторую дополнительную (возможно, и не секретную) информацию с целью идентификации и/или верификации, которую невозможно удалить, не ухудшив значительно надежности восприятия исходного сообщения или основного покрывающего сообщения (ОПС).

Последнее десятилетие технологии ВИ активно развиваются в связи с расширяющимся практическим применением [4]. Одним из основных предназначений систем с ВИ является защита авторских прав при копировании, контроль за оборудованием записи и воспроизведения цифрового мультимедиа, предотвращение несанкционированного копирования, контроль в медицинском менеджменте, мониторинг вещания [5,6].

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

– ВИ не заметны, и в отличие от заграждающих кодов не увеличивают размера основного сообщения;

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

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

Эти три отличия и обусловили преимущества технологий встроенных идентификаторов для целого ряда приложений, в частности, для верификации и идентификации мультимедийной информации.

Целью статьи является разработка метода идентификации и подтверждения достоверности сканированных документов либо факсов на основе технологий ВИ. Применение данной технологии позволяет работать со стандартными форматами файлов документов, что обеспечит совместимость для различных систем документооборота.

Основная часть. Общая идея метода состоит в рассмотрении изображения электронного документа как совокупности нескольких областей (фрагментов изображения): область основного текста, области печати и подписи (рис. 2). Так, область печати и подписи является практически идентичной для разных документов, что позволяет злоумышленнику перенести печать с одного документа на другой. Поэтому без применения специальных методов защиты невозможно определить, подписан ли документ легально, либо печать и подпись на нем сфальсифицированы.

Суть предлагаемого метода состоит во встраивании в область печати документа идентификатора, являющегося уникальным для данного документа.

Идентификатор формируется на основе содержания текста документа и индивидуального ключа пользователя, подписывающего документ.

Рис. 2. Схема электронного документа

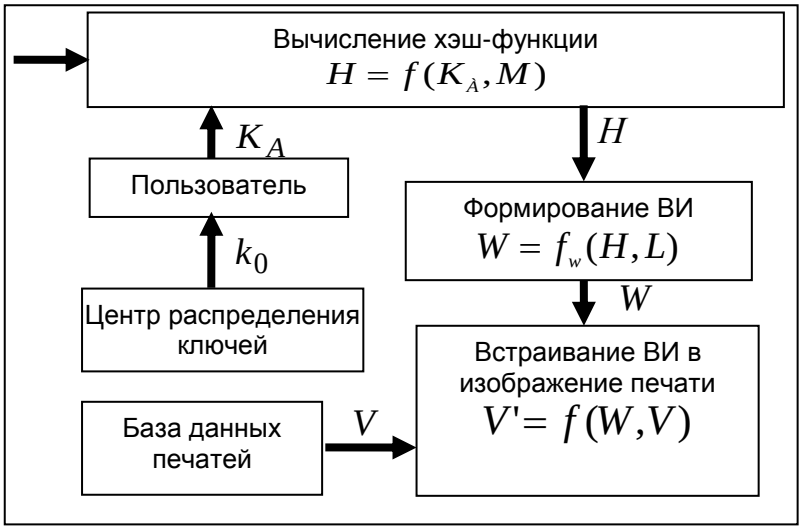
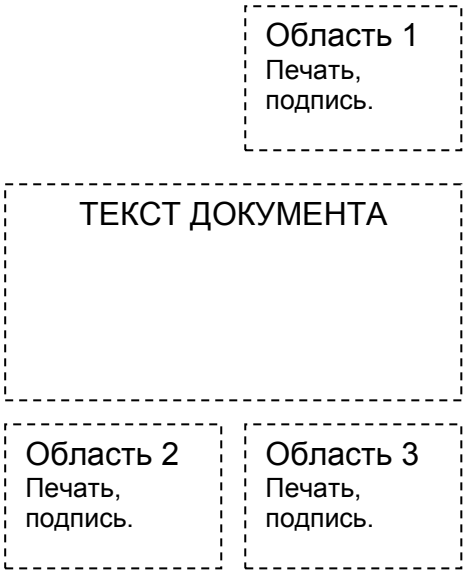


Рис. 3. Алгоритм встраивания идентификатора в электронный документ

Алгоритм встраивания идентификатора в документ (рис. 3), основан на методе, описанном в [7]:



1. Вычисляется хэш-функция $H = f(K_{\grave{A}}, M)$ на основе ключа пользователя K_A и содержимого текстовой области документа M, где f — функция хэширования, зависит от принятого в системе документооборота стандарта (RSA, DSA, ГОСТ 34.319-95 или др.).
2. Формируется идентификатор $W = f_w(H, L)$ для встраивания в область печати документа, где f_W – функция формирования встроенного идентификатора, L — маска встраивания.
3. Из базы данных печатей извлекается необходимое для данного документа изображение печати *V*. По определенному алгоритму [] в изображение печати встраивается полученный идентификатор: $V' = f_S(W, V)$, где V'— результирующее изображение печати со встроенным идентификатором.

Проверка достоверности электронного документа со встроенным идентификатором происходит следующим образом (рис. 4):

1. Из документа извлекаются изображения печати и области текста, *V'* и *M* соответственно. Из базы данных печатей извлекается оригинальное изображение печати *V*.
2. Формируется встроенный идентификатор *W* аналогично пунктам 1-2 алгоритма встраивания.
3. На основе данных печатей V' и V вычисляется идентификатор *W'*.
4. Идентичность идентификаторов *W'*. *W* свидетельствует о целостности документа, в противном случае документ был модифицирован.

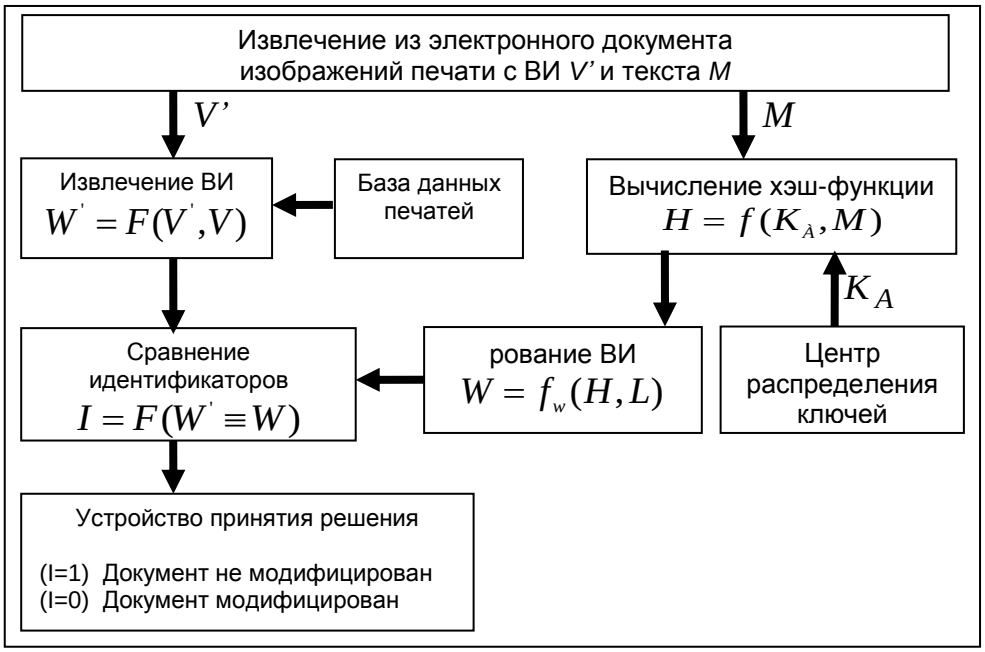


Рис. 4. Алгоритм проверки достоверности электронного документа путем сравнения встроенных идентификаторов

Для упрощения подачи материала не приводились алгоритм синхронизации встраивания и извлечения идентификаторов, детально описанный в [8], а также дополнительные меры по обеспечению помехоустойчивости [9].

Выводы. Предложенный способ проверки достоверности электронного документа является достаточно актуальным для систем электронного документооборота переходного типа, когда большая часть архивных и обрабатываемых документов является сканированными образами бумажных копий. Актуальность данного метода высока в связи с вступлением в силу закона "Об электронном документе и электронном документообороте" 01.01.2003, т.к. этот алгоритм достаточно просто реализовать на практике и в сжатые сроки интегрировать с существующими системами документооборота.

Метод пригоден для работы с монохромными и бинарными (факсовыми) изображениями документов и ограниченно пригоден для документов в формате WORD, содержащих растровые изображения.

Дальнейшие перспективы развития данного метода состоят в использовании помехоустойчивых кодов, позволяющих сохранить работоспособность системы при умышленно вносимых искажениях, а также в кодировании идентификатора некоторой дополнительной информацией на основе приема и декодирования которой могут осуществляться некоторые дополнительные операции автоматизированной обработки, например сортировка и классификация.

ЛИТЕРАТУРА

1. Маракова И.И. Комплексная информационная безопасность електронного документооборота // Управління проектами та розвиток виробництва. Збірник наукових праць. Під ред. В.А.Рач. – 2004. – № 3(11). – С.100-105.
2. Столлингс Вильям. Криптография и защита сетей: принципы и практика, 2-е изд. : Пер. с англ. – М. Издательский дом «Вильямс», 2001. – 672 с.

3. Маракова І.І., Рибак А.І., Ямпольський Ю.С. Захист інформації криптографічні методи. Кіровоград: Полімед, 2001. – 189 с.
4. Маракова И.И., Сафронов А.С. Проблематика и перспективы методов сокрытия информации // Тр. Одесск. нац. политехн. ун-та. – 2003. – Вып. 1 (19). – С. 184-188.
5. Маракова И.И., Рыбак А.И. Альтернативные способы защиты информации в условиях развивающейся экономики // Управління проектами та розвиток виробництва. Збірник наукових праць. Під ред. В.А. Рач. – 2001. – № 1(3). – С. 89-92.
6. 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.
7. Маракова И.И., Сафронов А.С. Исследование эффективности бинарных систем с цифровыми водяными знаками // Научно-технический сборник «Труды УНИИРТ». — 2003. – № 4. – С.77-82.
8. Сафронов А.С. Адаптация систем с цифровыми водяными знаками к атакам пространственной десинхронизации // Захист інформації. – збірник наукових праць НАУ. – 2005. – №1. – С. 91-97.
9. Маракова И.И., Сафронов А.С., Стасюк А.И. Оптимизация параметров систем с цифровыми водяными знаками в условиях воздействия линейной фильтрацией и аддитивным шумом // Научно-технический сборник «Труды УНИИРТ». – 2004. – № 2(38). – С.54-60.

Стаття надійшла до редакції 15.07.2005 р.