УДК 004.91

А.И. ИВАНОВ, П.С. ЛОЖНИКОВ, А.Е. САМОТУГА

ТЕХНОЛОГИЯ ФОРМИРОВАНИЯ ГИБРИДНЫХ ДОКУМЕНТОВ

Аннотация. Предлагается технология, позволяющая расширить функциональные возможности существующих систем электронного документооборота за счет обеспечения создания неограниченного числа бумажных копий электронного документа. Каждая бумажная копия может использоваться в обычном документообороте на обычных бумажных носителях с достоверной информацией. Предлагаемая технология осуществляет надежную связь электронного документооборота с обычным бумажным документооборотом без дополнительных затрат на различные услуги. Рассматривается процесс проверки достоверности гибридного документа. Описаны достоинства данной технологии и дано изображение гибридного документа.

Ключевые слова: гибридный документооборот, электронно-цифровая подпись, динамическая подпись.

В настоящее время широко распространен способ создания электронных документов в формате PDF, куда наряду с текстом встраивается графический образ подписи (автографа) лица, создавшего этот документ. Так, в AppStore доступны следующие программные продукты: SignNow, HelloSign, PDFpenPro, Signosign/2, QuickSign. Положительным свойством этих продуктов является то, что они общеприняты. В частности, документ с подписью в формате PDF легко преобразуется в его бумажную копию путем распечатывания на принтере. Основной недостаток такого документа — он строится на полном доверии к автору и уязвим к подделкам. Из подлинного документа в формате PDF легко изымается подпись под ним в виде изображения, и далее этот атрибут документа может быть встроен в любой фальшивый документ.

Недостаток способа встраивания рисунка подлинной подписи в электронный документ или его бумажную копию заключается также в том, что оценить подлинность рукописной подписи может только человек, хорошо знающий нюансы подписи хозяина документа. Этот недостаток пытаются устранить путем автоматического запоминания биометрических параметров рукописного автографа в документе. Так, российское предприятие НТЦ «КАСИБ» выпускает продукт SignToLogin [1], который контролирует качество подписи на рисунке в электронном документе, сравнивая его параметры с эталонными. В результате пользователь может судить о подлинности электронного документа с рисунком автографа, опираясь на данные программного продукта. Пользователь, доверяя программному продукту, может оценить достоверность автографа человека, которого он не знает.

Основной недостаток автоматической биометрической проверки подписи в электронном документе состоит в том, что вероятности ошибок первого и второго рода биометрической проверки могут быть высоки и составлять до 15%. Кроме того, результат проверки может быть легко фальсифицирован, достаточно лишь подменить биометрический шаблон, находящийся в программе проверки электронного документа.

Еще одним недостатком электронных документов и средств апостериорной проверки статической подписи на рисунке является то, что они пригодны для проверки подлинности бумажных копий электронного документа с незнакомой подписью.

Проблема перевода электронных документов в параллельно существующие бумажные документы является актуальной для ряда корпоративных технологических приложений. Электронные документы можно видеть и проверять только в случае, если доступна соответствующая инфраструктура открытых ключей (PKI). Поэтому многие юридически значимые документы более предпочтительно хранить в бумажном виде. К сожалению, этот способ также ненадежен, поскольку

можно нелегально отсканировать документ на бумажном носителе в цвете, внести в него дезинформацию и вновь распечатать. В связи с актуальностью этой угрозы используют способ, усиливающий стойкость бумажного носителя к копированию. Известны способы защиты документов [2] с помощью голограммы, которую наклеивают на бумажную копию. Однако этими методами нельзя осуществлять защиту копий электронных документов при массовом их использовании. Применение большого числа голограмм затрудняет их учет; кроме того, снятие подлинной голограммы с достоверного документа и ее переклейка на фальшивый документ позволяет злоумышленнику обойти защиту. Чем больше будет использоваться защищенных голограммой бумажных документов, тем сложнее осуществить эффективную политику учета находящихся в обороте голограмм.

В настоящее время наиболее эффективным способом защиты целостности и авторизации электронных документов является криптография. Известны традиционные технологии асимметричной криптографии, позволяющие защитить электронной цифровой подписью содержание электронного документа [3, 4]. Но их основной недостаток — работоспособность только в доверенной вычислительной среде с доверенным средством отображения информации. Если доверенная вычислительная среда недоступна, то убедиться в достоверности электронного документа нельзя.

В данной статье предлагается технология, позволяющая расширить функциональные возможности существующих систем электронного документооборота за счет обеспечения создания неограниченного числа бумажных копий электронного документа. При этом каждая бумажная копия может использоваться в обычном документообороте на обычных бумажных носителях с достоверной информацией. Предлагаемая технология осуществляет надежную связь электронного документооборота с обычным бумажным документооборотом без дополнительных затрат на услуги нотариусов, заверяющих копии бумажных документов.

Поэтапно выполняются следующие действия.

1. Создается пара из открытого и личного ключа автора.

2. Регистрируется открытый ключ автора в удостоверяющем центре (Certificate Authority).

3. Формируется первая электронная цифровая подпись под информацией электронного документа с помощью личного ключа автора.

4. Автор электронного документа формирует свой автограф, воспроизводя его на экране компьютера и заключая его в рамку.

5. Автограф в ограничивающей рамке преобразуют в бинарный файл; при его создании используются биометрические данные подписи автора, считанные при воспроизведении автографа автором документа, который объединяют с подписанным электронным документом. При этом в документ вносятся данные о размере рамки графического бинарного файла с автографом.

6. Созданная комбинация данных заверяется второй электронной цифровой подписью.

На рис. 1 представлен вариант гибридного документа, который может быть электронным в формате PDF и распечатан на бумажном носителе.

Следует отметить, что при реализации предложенного способа формирования гибридных документов взаимное размещение информационных полей документа может быть любым. Определение и место размещения поля документа задается программным обеспечением, реализующим предложенный способ. Критичным является наличие в документе соответствующей информации и рамок, ограничивающих поля с информацией. Рамки необходимы для предотвращения проникновения информации из разных полей при ее извлечении из документа в формате PDF или из отсканированного электронного образа достоверного документа на бумажном носителе.

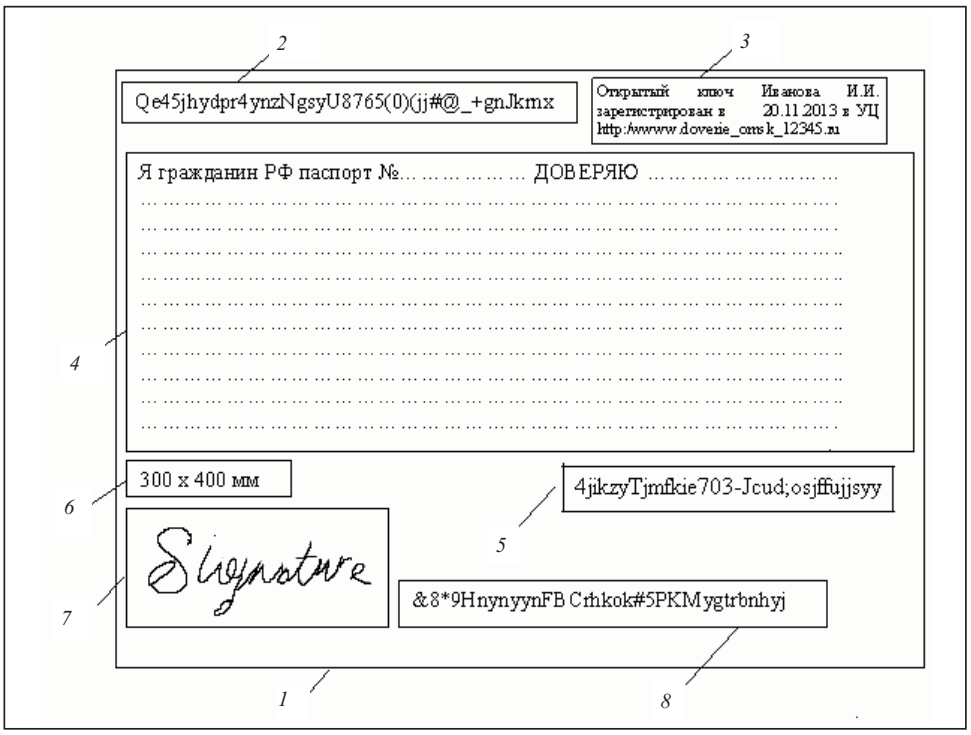

Рис. 1. Формат гибридного документа: *1* — полное информационное поле всего достоверного документа; *2* — поле для размещения кода открытого ключа автора документа в виде штрих-кода или в виде любой иной кодировки; *3* — поле для размещения информации об удостоверяющем центре, где зарегистрирован открытый ключ подписавшего документ и откуда можно скачать сертификат открытого ключа; *4* — поле достоверного содержания документа в виде текста; *5* — поле для размещения первой электронной цифровой подписи, охватывающей текстовый файл документа в поле *4*; *6* — поле для размещения текста о размере графического файла с автографом автора электронного документа; *7* — поле для размещения образа автографа автора электронного документа; *8* — вторая электронная цифровая подпись под документом, одновременно охватывающая весь текстовый документ и графический файл с автографом автора электронного документа

Необходимость двух электронных цифровых подписей в документе (поле *5* и поле *8*) обусловлена различной природой защищаемой ими информации. Первая электронная подпись (поле *5*) охватывает текст документа в виде обычных букв на языке документа. При сканировании этого документа возможны ошибки сканирования и неправильного распознавания в документе нескольких букв или знаков (точка, запятая, двоеточие). Если произошла ошибка при сканировании, то первая электронная цифровая подпись не совпадет с данными поля *5*, т.е. содержание отсканированного бумажного документа будет искаженным.

Таким образом, данная технология позволяет пользователю гибридного документа рассчитывать на то, что автор, подписавший документ, одновременно обладал и личным ключом, и умением воспроизводить автограф. Гарантией того, что автограф не подменен (не подставлен графический файл из другого документа), является поставленная под автографом вторая электронная цифровая подпись, одновременно охватывающая и содержание самого документа, и первую электронную цифровую подпись под ним, и графический бинарный файл автографа, включенный в электронный документ.

Следует отметить, что использованная в предложенной технологии процедура бинаризации изображения подписи (удаляются все градации яркости и шумы вне линии подписи) гарантирует защиту контроля целостности графического файла, встроенного в электронный документ. При попытках атаки на вторую цифровую подпись путем зашумливания или иного искажения графического

файла при поисках коллизий хэш-функций второй цифровой подписи эти манипуляции будут зрительно зафиксированы на изображении графического файла. Пользователь, проверяющий электронный документ на сходство автографа в нем и подписи его автора, должен контролировать моменты отсутствия каких-либо дополнительных графических включений в графический файл. Автограф должен быть схож с оригиналом по числу возможных отрывов и иметь чистое поле, на котором он воспроизведен. Тогда вероятность атаки подмены через поиск коллизий вычисляемой хэш-функции при формировании второй электронной цифровой подписи ничтожно мала. При длине хэш-функции 256 бит вероятность коллизий будет близка к величине 2^{-256}.

Важным преимуществом технологии является также то, что на бумажную копию наносится информация, достаточная для проверки бумажного документа визуально (глядя на графический файл) и криптографически путем проверки двух электронных цифровых подписей, внесенных в бумажный документ. Первый эффект возможности визуальной проверки очевиден: проверяющий сверяет начертание автографа в документе с подписью, с которой он ознакомлен, и признает документ как достоверный.

Для криптографической проверки достоверности бумажного документа сам документ необходимо отсканировать и распознать в нем открытый ключ и адрес удостоверяющего центра. Также необходимо распознать текст документа и восстановить графический файл подписи в документе по указанным его размерам. Кроме того, следует распознать символы кода первой электронной цифровой подписи. Далее необходимо использовать открытый ключ электронной цифровой подписи документа для проверки первой цифровой подписи под информационной частью документа. Если содержание документа не изменено, то по открытому ключу проверяющий получает ту же последовательность, что и в первой цифровой подписи.

Далее для криптографической проверки подлинности графического файла автографа проверяющий с использованием открытого ключа контролирует содержание документа и содержание восстановленного графического файла. При этом он получает код, совпадающий с кодом второй цифровой подписи. При совпадении кодов первой и второй цифровых подписей проверяющий с уверенностью может констатировать достоверность бумажной копии электронного документа. Если проверяющему заранее не известен код открытого ключа автора документа, то он должен обратиться в удостоверяющий центр, где этот ключ зарегистрирован, и загрузить с сайта этого центра его сертификат.

Таким образом, любой проверяющий может убедиться в достоверности информации, содержащейся в бумажной копии. При этом осуществляется двухуровневая проверка документа. Проверяющий оценивает сходство подписи с известной ему и дополнительно проверяет криптографически содержание документа на бумажном носителе. Очевидно, что криптографическая проверка является более надежной, чем проверка на наличие в документе голографической наклейки, и визуальная проверка достоверности информации по очертаниям знакомого автографа намного удобнее криптографической проверки содержания документа.

Для восстановления электронного документа с бумажной копии необходимо отсканировать документ, распознать в нем расположение полей, данные, находящиеся в этих полях, и внести их в соответствующие поля восстанавливаемого электронного документа. Получение бинарных версий первой и второй электронных цифровых подписей также происходит при сканировании документа и распознавании символов данных подписей.

Преимущество технологии также состоит в том, что она может применяться для коллективного подписания документов. Документ формируют несколько человек, и его пользователи убеждаются в достоверности документа, проверяя только автографы тех людей, которых хорошо знают. Вся информация, необходимая для проверки, в созданных документах уже имеется.

Если человек, формирующий коллективный документ, не согласен с его информационным содержанием, то он вносит коррективы в информационную часть и первым подписывает документ своей электронной цифровой подписью. Далее он вставляет в документ свой автограф и повторно подписывает эту комбинацию своей второй электронной цифровой подписью. Затем инициатор правки отсылает документ другим лицам, формирующим этот документ. Фактически предложена технология коллективного формирования электронных документов, при этом коллективный электронный документ может быть распечатан на обычной бумаге и проверен по описанному выше алгоритму.

Предложенная технология формирования гибридных документов обладает новыми полезными качествами. При ее реализации удается осуществить надежную связь между достоверными электронными документами в формате PDF и двумя электронными цифровыми подписями с достоверными копиями этих документов на бумажных носителях. Копии электронных документов на бумажных носителях не утрачивают основного свойства электронных документов — высокой достоверности, оперативно проверяемой криптографическими процедурами. С помощью предложенного способа преодолевается разрыв между высокой достоверностью электронных документов и относительно низкой достоверностью обычных копий документов на бумажном носителе.

СПИСОК ЛИТЕРАТУРЫ

1. Л о ж н и к о в П . С . Облачная система идентификации пользователей по рукописным паролям «SIGNTOLOGIN» // Электроника инфо. — 2013. — № 6 (96). — С. 74–76.
2. Пат. 2461882 RU, G07D 7/00. Способ защиты документов / А.Н. Адамчук (MD), А.Н. Бойко (RU), В.А. Моложен (MD), В.А. Редченко (MD), И.Н. Слепнев (MD), В.Д. Шкилев (MD). — Опубл. 20.09.2012.
3. Пат. 2409903 RU, H04L9/14. Способ формирования и проверки подлинности электронной цифровой подписи, заверяющей электронный документ / Н.А. Молдовян (RU), А.А. Молдовян (RU). — Опубл. 10.02.2009.
4. Пат. 2401513 RU, H04L 9/32. Способ формирования и проверки подлинности электронной цифровой подписи, заверяющей электронный документ / Д.Н. Молдовян (RU), Н.А. Молдовян (RU). — Опубл. 10.10.2010.

Поступила 30.01.2014