РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 543 928**(13) **C1**

(51) МПК
H04L 9/32 (2006.01)
G06F 21/64 (2013.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2013151257/08, 18.11.2013**

(24) Дата начала отсчета срока действия патента:
18.11.2013

Приоритет(ы):
(22) Дата подачи заявки: **18.11.2013**

(45) Опубликовано: **10.03.2015** Бюл. № **7**

(56) Список документов, цитированных в отчете о поиске: **RU 2365047 C2, 20.08.2009. RU 2325768 C1, 27.05.2008. RU 2380838 C1, 27.01.2010. RU 2452013 C2, 27.05.2012. US 7039805 B1, 02.05.2006. US 2011/0238999 A1, 29.09.2011 . KR 1149695 B1, 23.05.2012**

Адрес для переписки:
644119, г.Омск, ул. Бульвар Зеленый, 8, кв. 7, Ложникову Павлу Сергеевичу

(72) Автор(ы):
Ложников Павел Сергеевич (RU),
Иванов Александр Иванович (RU)

(73) Патентообладатель(и):
Ложников Павел Сергеевич (RU),
Иванов Александр Иванович (RU)

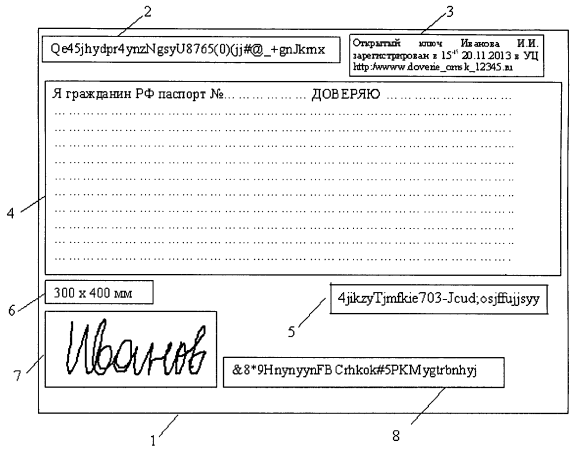
(54) СПОСОБ ФОРМИРОВАНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТА И ЕГО КОПИЙ

(57) Реферат:

Изобретение относится к области электросвязи, а именно к области электронного документооборота. Технический результат - повышенная защита электронных документов. Способ формирования электронного документа и его копий, состоящий в том, что создают пару из открытого и личного ключа, регистрируют открытый ключ в удостоверяющем центре, формируют первую электронную цифровую подпись под информацией электронного документа с помощью личного ключа, проводят сравнение первой электронной цифровой подписи, отличающийся тем, что в электронном документе с помощью автора электронного документа формируют его автограф, воспроизводя этот автограф на экране компьютера и охватывая его ограничивающей рамкой, далее автограф в ограничивающей рамке преобразуют в бинарный файл с толщиной линии в один пиксел и этот бинарный файл объединяют с подписанным электронным документом, также вносят в документ данные о размере рамки графического бинарного файла с автографом, далее созданную комбинацию данных подписывают второй электронной цифровой подписью. 2 н. и 1 з.п. ф-лы, 1 ил.

RU 2543928 C1

RU 2543928 C1



RU 2543928 C1

RU 2543928 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 543 928** (13) **C1**

(51) Int. Cl.
H04L 9/32 (2006.01)
G06F 21/64 (2013.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2013151257/08, 18.11.2013**

(24) Effective date for property rights:
18.11.2013

Priority:
(22) Date of filing: **18.11.2013**

(45) Date of publication: **10.03.2015** Bull. № **7**

Mail address:
644119, g.Omsk, ul. Bul'var Zelenyj, 8, kv. 7, Lozhnikovu Pavlu Sergeevichu

(72) Inventor(s):
Lozhnikov Pavel Sergeevich (RU),
Ivanov Aleksandr Ivanovich (RU)

(73) Proprietor(s):
Lozhnikov Pavel Sergeevich (RU),
Ivanov Aleksandr Ivanovich (RU)

(54) METHOD FOR GENERATION OF ELECTRONIC DOCUMENT AND ITS COPIES

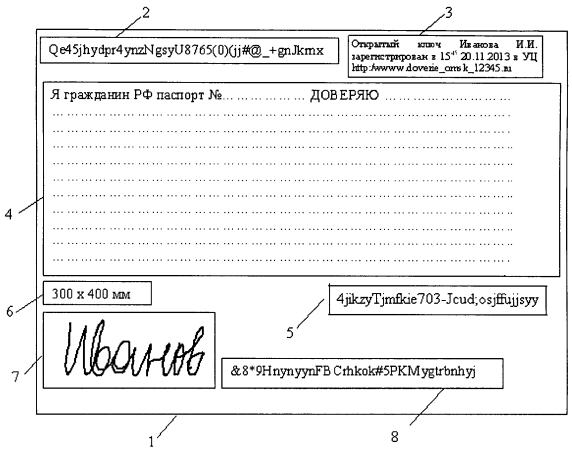
(57) Abstract:

FIELD: electricity.

SUBSTANCE: method for generation of electronic document and its copies consists in generating a pair of public and private keys, registering of public key at certification authority, forming the first electronic digital signature under data in electronic document by means of the private key, comparing of the first electronic digital signature featured by the fact that in electronic document the originator of this electronic documents generates own autograph, reproduces this autograph at PC display and captures it by the limiting frame; then autograph in the limiting frame is converted to a binary file with line thickness of one pixel and this binary file is united with the signed electronic file, data on size of the graphic binary file with autograph are also introduced to it, then generated data combination is signed by the second electronic digital signature.

EFFECT: enhanced protection of electronic documents.

3 cl, 1 dwg



RU 2543928 C1

RU 2543928 C1

Изобретение относится к области электросвязи, точнее к области электронного документооборота, позволяющего оперативно и с высокой достоверностью авторизовать каждый созданный (полученный или используемый) документ. Изобретение также относится к области создания и проверки подлинности обычных документов на бумажном носителе.

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. В частности подобные средства изготовления электронных документов производятся рядом фирм, к которым относятся:

- фирма США SignNow [1] выпускает одноименный продукт;
- фирма США HelloSign [2] выпускает одноименный продукт;
- фирма США Smile [3] выпускает продукт «PDFpenPro 6»;
- фирма Словакии APIS [4] выпускает продукт «Signosign/2».

Положительным свойством всех перечисленных выше технических решений является то, что они привычны для людей. В частности документ с подписью в формате «PDF» легко превращается в его бумажную копию путем распечатывания на принтере.

Основным недостатком этого способа формирования электронных и бумажных документов является то, что он строится на полном доверии к источнику документа (лицу его создающему). Этот способ вообще не защищает от подделок электронных документов и их бумажных копий. Из подлинного документа в формате «PDF» легко изымается подпись под ним и далее этот атрибут документа может быть встроен в любой фальшивый документ.

Еще одним недостатком способа встраивания рисунка подлинной подписи в электронный документ или его бумажную копию является то, что оценить подлинность рукописной подписи (подлинность электронного документа и целесообразность изготовления его бумажных копий) может только человек, хорошо знающий особенности подписи хозяина документа.

Последний недостаток пытаются устранить путем запоминания автоматического контроля биометрических параметров рукописного автографа в документе. Так, японская фирма Cyber-SIGN [5] продает продукты «Cyber-SIGN Acrobat» и «Cyber-SIGN MSWords». Также американская фирма CIC [6] продает продукт «Sign-it», российская фирма НТЦ «КАСИБ» выпускает продукт «SignToLogin» [7]. Эти продукты контролируют 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 может оценить достоверность автографа человека, которого он не знает, если он доверяет программному продукту.

Основной недостаток автоматической биометрической проверки подписи в электронном документе состоит в том, что вероятности ошибок первого и второго рода биометрической проверки высоки и составляют от 5% до 15%. Кроме того, результат проверки может быть легко фальсифицирован, достаточно 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 не 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 проверить, только если есть исправная

электронная вычислительная машина с доверенной вычислительной средой и доверенными средствами отображения электронного документа. В случае когда может отключиться электричество (возможны вирусные атаки и иные форс-мажорные обстоятельства), прибегают к распечатыванию электронного документа на бумажном носителе с последующим заверением этой распечатки дополнительной печатью отдела кадров и дополнительной подписью лица, поставившего печать.

К сожалению, этот способ так же не надежен, так как злоумышленник способен 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. Известен способ защиты документа [8]. По этому способу на бумажную копию может быть наклеена голограмма, что является серьезной защитой от подделок.

Недостатком способа является то, что им 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 учетности, находящихся в обороте голограмм.

На сегодняшний день наиболее эффективным способом защиты целостности и авторизации электронных документов является криптография. Известны несколько схем асимметричной криптографии, позволяющих защитить электронной цифровой подписью содержание электронного документа [9, 10].

Наиболее близким к предлагаемому техническому решению является способ формирования и проверки подлинности электронной цифровой подписи [10], заверяющей электронный документ, заключающийся в том, что генерируют секретный ключ в виде, по крайней мере, одной битовой строки, по секретному ключу формируют открытый ключ Y в виде более чем одной битовой строки, принимают электронный документ, представленный битовыми строками $H_1, H_2, \ldots, H_z$, где $z \geq 1$, в зависимости от принятого электронного документа и от значения секретного ключа формируют электронную цифровую подпись Q в виде совокупности многоразрядных двоичных чисел e, $S_1, S_2, \ldots, S_u$, где $1 \leq u \leq 8$, в зависимости от открытого ключа, принятого электронного документа и электронной цифровой подписи формируют первую A и вторую B проверочные битовые строки, сравнивают их и при совпадении их параметров делают вывод о подлинности электронной цифровой подписи.

Основным недостатком ВСЕХ существующих способов криптографической защиты электронных документов является то, что они работоспособны только в доверенной вычислительной среде с доверенным средством отображения информации. Если доверенная вычислительная среда не работает (отключено электропитание, прошла вирусная атака, нарушена целостность исполняемых программных модулей проверки электронной цифровой подписи), убедиться в достоверности электронного документа нельзя.

Задача изобретения - расширение функциональных возможностей существующих систем электронного документооборота за счет обеспечения создания неограниченного числа бумажных копий электронного документа, каждая из которых обладает юридической значимостью своего электронного оригинала, при этом каждая бумажная копия может использоваться людьми в обычном документообороте обычных бумажных

носителей достоверной информации. По предложенному способу фактически осуществляется надежная связь электронного документооборота с обычным бумажным документооборотом без дополнительных затрат на услуги нотариусов, заверяющих копии бумажных документов.

Поставленная задача достигается тем, что в способе формирования электронного документа и его копий, состоящем в том, что создают пару из открытого и личного ключа, регистрируют открытый ключ в удостоверяющем центре, формируют первую электронную цифровую подпись под информацией электронного документа с помощью личного ключа, проводят сравнение цифровой подписи, согласно изобретению в электронном документе с помощью автора электронного документа формируют его автограф, воспроизводя этот автограф на экране компьютера и охватывая его ограничивающей рамкой, далее автограф в ограничивающей рамке преобразуют в бинарный файл с толщиной линии в один пиксел и этот бинарный файл объединяют с подписанным электронным документом, также вносят в документ данные о размере рамки графического бинарного файла с автографом, далее созданную комбинацию данных подписывают второй электронной цифровой подписью. Задача достигается тем, что в способе формируют копии электронного документа на бумажном носителе путем распечатывания на бумажном носителе открытого ключа автора документа и данных удостоверяющего центра, где открытый ключ зарегистрирован, текста самого документа, графического файла первой электронной цифровой подписи под документом, данные о размере графического файла с автографом автора электронного документа, данные об образе автографа автора электронного документа, второй электронной цифровой подписи под документом, одновременно охватывающей весь текстовый документ и графический файл с автографом автора электронного документа.

Поставленная задача достигается также тем, что в способе формирования электронного документа и его копий, состоящем в том, что каждый из нескольких авторов электронного документа создает пару из открытого и личного ключа, регистрирует открытый ключ в удостоверяющем центре, формирует первую электронную цифровую подпись под информацией электронного документа с помощью личного ключа, проводит сравнение цифровой подписи, согласно изобретению в электронном документе с помощью нескольких авторов электронного документа формируют их автографы, воспроизводя эти автографы на экране компьютера и охватывая их ограничивающей рамкой, далее автографы в ограничивающей рамке преобразуют в бинарный файл с толщиной линии в один пиксел и этот бинарный файл объединяют с подписанным электронным документом, также вносят в документ данные о размере рамки графического бинарного файла с каждым автографом, далее каждый из авторов созданную комбинацию данных подписывает второй электронной цифровой подписью.

Достигаемым техническим результатом является то, что в электронном документе появляется бинарное изображение автографа автора его сформировавшего. То есть люди, знающие автограф автора документа, могут проверять документ по знакомому автографу даже в том случае, когда документ распечатан на бумажном носителе. При этом достоверность содержания документа, как и по способу-прототипу, является высокой, так как под текстом документа сохраняется электронная цифровая подпись (в полном соответствии с традиционной технологией формирования электронной цифровой подписи). Сохраняется юридическая значимость содержания документа.

Важным преимуществом предложенного способа в сравнении с прототипом является то, что пользователь электронного документа, знающий подпись автора, может быть

уверен в том, что подписывал документ именно сам автор (нет факта компрометации его личного ключа). Эта уверенность появляется в случае, если доверенное программное обеспечение, формирующее электронную цифровую подпись, проверяет свою целостность и вставляет в документ не любые изображения, а только изображения автографа, лично воспроизведенные автором на экране компьютера.

Таким образом, реализация предложенного способа по п.1 формулы изобретения позволяет надеяться пользователю электронного документа на то, что подписавший документ автор 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 подчеркнуть, что использованная в предложенном способе процедура бинаризации изображения подписи (удаляются все градации яркости и шумы вне линии подписи) гарантируют защиту контроля целостности графического файла, встроенного в электронный документ. Если производятся попытки атаки на вторую цифровую подпись путем подмешивания шума или иного искажения графического файла при поисках коллизий хэш-функций второй цифровой подписи, то эти манипуляции будут видны глазом на изображении графического файла. Пользователь, проверяющий электронный документ на похожесть автографа в нем на подпись его автора, должен контролировать отсутствие каких-либо дополнительных графических включений в графический файл. Автограф должен быть похож на оригинал 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 (в соответствии с отечественным стандартом на хэширование) вероятность коллизий будет близка к величине 2^{-256}.

Достигаемым техническим результатом является также то, что на бумажную копию наносится информация, достаточная для проверки бумажного документа органолептически (глядя на графический файл) и криптографически путем проверки двух электронных цифровых подписей, внесенных в бумажный документ. Первый эффект возможности органолептической проверки очевиден, проверяющий смотрит на графику автографа в документе и, если он знаком с подписью, то 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 в нем размерам. Также следует распознать символы кода второй электронной цифровой подписи. Далее следует 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 проверяет и содержание документа, и содержание восстановленного графического файла. При этом проверяющий получает код, совпадающий с кодом второй цифровой подписи. При совпадении кодов первой

и второй цифровой подписи проверяющий может быть уверен в том, что имеет на руках достоверную бумажную копию электронного документа. Если проверяющий заранее не знает код открытого ключа автора документа, то он должен обратиться в удостоверяющий центр, где этот ключ зарегистрирован, и скачать с сайта этого удостоверяющего центра его сертификат.

Таким образом, любой проверяющий может убедиться в достоверности информации, содержащейся в имеющейся у него бумажной копии. При этом осуществляется двухуровневая проверка документа. Проверяющий оценивает похожесть подписи на известную ему и дополнительно проверяет криптографически содержание документа на бумажном носителе. Очевидно, что криптографическая проверка является более надежной, чем проверка по наличию на документе голографической наклейки. Очевидно, что органолептическая проверка достоверности информации по очертаниям знакомого автографа много удобнее криптографической проверки содержания документа.

Технический положительный результат состоит также в том, что документ формируют несколько человек, и его пользователи убеждаются в достоверности документа, проверяя только автографы тех людей, которые хорошо знают. Вся информация, необходимая для проверки, в созданных документах уже имеется.

В случае если человек, формирующий коллективный документ, не согласен с его информационным содержанием, несогласный вносит коррективы в информационную часть, далее сам первый подписывает документ своей электронной цифровой подписью, далее вставляет в документ свой автограф и повторно подписывает эту комбинацию своей второй электронной цифровой подписью. Далее инициатор правки в документ отсылает его 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 п.2 формулы изобретения. Комбинация п.2 и п.3 формулы изобретения вытекает из их сущности и не подлежит защите.

На фигуре представлен вариант реализации предложенного способа по п.1 и п.2 формулы изобретения при реализации электронного документа в формате «PDF» и его достоверной копии на бумажном носителе, где: 1 - полное информационное поле всего достоверного документа; 2 - поле для размещения кода открытого ключа автора документа в виде штрихкода или в виде любой иной кодировки; 3 - поле, где размещается информация 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, где размещается первая электронная цифровая подпись, охватывающая текстовый файл документа в поле - 4; 6 - поле, где размещен текст о размере графического файла с автографом автора электронного документа; 7 - поле, где размещен образ автографа автора электронного документа; 8 - вторая электронная цифровая подпись под документом одновременно охватывающая весь текстовый документ и графический файл с автографом автора электронного документа.

Следует отметить, что при реализации предложенного способа формирования достоверных электронных документов и их достоверных копий на бумаге взаимное размещение информационных полей документа может быть любым. Где и какие размещены поля документа, задается программным обеспечением, реализующим предложенный способ. Критичным является наличие в документе соответствующей информации и рамок, ограничивающих поля с информацией. Рамки необходимы для того, чтобы информация из разных полей не перепутывалась при ее извлечении из

документа в формате «PDF» или из отсканированного электронного образа достоверного документа на бумажном носителе.

Необходимость в двух электронных цифровых подписях 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 неверного распознавания нескольких букв в документе или знаков (точка, запятая, двоеточие). Если произошла ошибка при сканировании, то первая электронная цифровая подпись не совпадет с данными поля - 5. То есть содержание отсканированного бумажного документа оказывается искажено (не правильное).

Корректировку небольшого числа ошибок в содержании документа проводят обычными способами. Первый способ состоит в правке документа читающим (устраняются грубые грамматические ошибки путем привлечения любого из существующих редакторов текста). Второй более надежный способ состоит в полном переборе возможных 1, 2, 3, 4, 7 ошибок в тексте. При малом числе ошибок распознанных символов букв текста операция перебора от 1 до 7 возможных ошибок вполне технически осуществима и занимает несколько минут машинного времени. Если исправить ошибки не удалось за малый интервал времени, то документ следует повторно сканировать и повторно распознавать в его полях символы.

После подтверждения достоверности содержания документа производят проверку автографа под ним. Для этой цели восстанавливают линия (линии) автографа так, что бы толщина линии была фиксированной и составляла один пиксел. После этого проверяют вторую электронную цифровую подпись (поле - 8), охватывающую текст достоверного документа, первую электронную цифровую подпись (поле - 5) и графический бинарный файл автографа. Если вторая электронная цифровая подпись оказывается неверна, то осуществляют корректировку положения линий автографа путем их сдвига на один или два пиксела вверх, вниз, вправо, влево. Кроме того, осуществляют перестановку 1, 2, 3, 4, …16 пикселов линий в местах скачков линий подписи на один бит. Фактически производят малые деформации линии подписи до момента, пока не совпадут ЭЦП графического файла и документа с ЭЦП в поле - 8. Если за небольшое время перестановок не удается добиться нужного значения второй электронной цифровой подписи, то подпись под достоверным документом считается недостоверной. При корректировке возможных ошибок в бинарном графическом файле допустимо привлекать классические коды с обнаружением и исправлением ошибок. При этом в документ следует вводить дополнительное поле с синдромами ошибок использованного классического кода.

В целом предложенный способ обладает новыми полезными качествами, при его реализации удается осуществить надежную связь достоверных электронных документов 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. По предложенному способу преодолевается разрыв между высокой достоверностью электронных документов и относительно низкой достоверностью обычных копий документов на бумажном носителе.

Источники информации

1. Сайт фирмы SignNow [Электронный ресурс] - Режим доступа: http://www.signnow.com

2. Сайт фирмы HelloSign [Электронный ресурс] - Режим доступа: http:///

www.hellosign.com
3. Сайт фирмы Smile [Электронный ресурс] - Режим доступа: http://smilesoftware.com
4. Сайт фирмы APIS [Электронный ресурс] - Режим доступа: http://www.biometria.sk
5. Сайт фирмы Cyber-SIGN [Электронный ресурс] - Режим доступа: http://www.cybersign.com
6. Сайт фирмы CIC [Электронный ресурс] - Режим доступа: http://www.cic.com
7. Сайт фирмы НТЦ «КАСИБ» [Электронный ресурс] - Режим доступа: http://signtologin.com
8. Патент №2461882 RU, G07D 7/00, опубликован 20.09.2012
9. Патент №2409903 RU, H04L 9/14, опубликован 10.02.2009
10. Патент №2401513 RU, H04L 9/32, опубликован 10.10.2010

Формула изобретения

1. Способ формирования электронного документа и его копий, состоящий в том, что создают пару из открытого и личного ключа, регистрируют открытый ключ в удостоверяющем центре, формируют первую электронную цифровую подпись под информацией электронного документа с помощью личного ключа, проводят сравнение первой электронной цифровой подписи, отличающийся тем, что в электронном документе с помощью автора электронного документа формируют его автограф, воспроизводя этот автограф на экране компьютера и охватывая его ограничивающей рамкой, далее автограф в ограничивающей рамке преобразуют в бинарный файл с толщиной линии в один пиксел и этот бинарный файл объединяют с подписанным электронным документом, также вносят в документ данные о размере рамки графического бинарного файла с автографом, далее созданную комбинацию данных подписывают второй электронной цифровой подписью.

2. Способ по п.1, отличающийся тем, что формируют копии электронного документа на бумажном носителе путем распечатывания на бумажном носителе открытого ключа автора документа и данных удостоверяющего центра, где открытый ключ зарегистрирован, текста самого документа, графического файла первой электронной цифровой подписи под документом, данные о размере графического файла с автографом автора электронного документа, данные об образе автографа автора электронного документа, второй электронной цифровой подписи под документом, одновременно охватывающей весь текстовый документ и графический файл с автографом автора электронного документа.

3. Способ формирования электронного документа и его копий, состоящий в том, что создают пару из открытого и личного ключа, регистрируют открытый ключ в удостоверяющем центре, формируют первую электронную цифровую подпись под информацией электронного документа с помощью личного ключа, проводят сравнение первой электронной цифровой подписи, отличающийся тем, что несколько авторов электронного документа создают несколько пар из открытого и личного ключа, регистрируют несколько открытых ключей в удостоверяющем центре, формируют несколько первых электронных цифровых подписей под информацией электронного документа с помощью нескольких личных ключей, проводят сравнение цифровых подписей, с помощью нескольких авторов электронного документа формируют их автографы, воспроизводя эти автографы на экране компьютера и охватывая их ограничивающей рамкой, далее автографы в ограничивающей рамке преобразуют в бинарный файл с толщиной линии в один пиксел и этот бинарный файл объединяют с подписанным электронным документом, также вносят в документ данные о размере

рамки графического бинарного файла с каждым автографом, далее каждый из авторов созданную комбинацию данных подписывает второй электронной цифровой подписью.