**Abasov Nizam Dzhavidovich**
Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University".
E-mail: and@radiansb.ru.
22, Chekhova Street, Taganrog, 347928, Russia.
Phone: +79528169696.
Postgraduate Student.

УДК 004.91

**Н.И. Елисеев, Д.А. Ржевский**

## ОБЕСПЕЧЕНИЕ ПОДЛИННОСТИ ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИИ

*Предложены в общем виде решения, позволяющие обеспечить подлинность документированной информации на всех этапах ее обработки, независимо от формы (электронная или бумажная (аналоговая)) и формата (xml, txt, tiff, pdf и пр.) ее представления.*

*Предложено конкретное решение обеспечения подлинности документированной информации на материальном носителе средствами электронной подписи со всеми вытекающими преимуществами, прежде всего, обеспечением криптографической стойкости.*

*Предложена структура системы, позволяющей обеспечить возможность проверки подлинности информации при отсутствии реквизитов.*

*Проверка подлинности; электронная подпись; система электронного документооборота; электронный документ; аналоговый документ; гибридный документ.*

**N.I. Eliseev, D.A. Rzhevskij**

## DOCUMENTED INFORMATION FOR THE EFFECTIVE

*Are offered decisions of the supporting authenticities at all Information processing stages independently of the form (electronic or paper) and format (xml, txt, tiff, pdf etc.).*

*Offered concrete decisions of supporting authenticities documentary information on the material carrier with using electronic signature for cryptography resistance supporting.*

*Offered the structure of system allowing allow the authentication information in the absence of details.*

*Authentication; electronic signature; electronic document management system; electronic document; an analog document; a hybrid document.*

**Введение.** В настоящее время существуют две основные формы представления документированной информации: аналоговая и электронная [1]. *Аналоговый документ (АнД)* – форма представления информации в среде физических объектов (явлений) [7]. *Электронный документ (ЭД)* – документ, в котором информация представлена в электронно-цифровой форме [8]. Одним из основных требований, предъявляемых в настоящее время к системам документооборота является возможность обработки различных форматов и форм представления документированной информации. Таким образом, можно утверждать, что процесс обработки документов в современных системах документооборота имеет смешанный характер (электронный и аналоговый) [2, 3]. Определим такой вид систем как *системы смешанного документооборота.*

В процессе обработки документов формат ЭД (способ представления данных в электронной среде) и внешние признаки АнД (размер, носитель и т.д.) могут подвергаться различным преобразованиям. Одна и та же документированная информация может преобразовываться. Например, при обработке входящего АнД

типичным преобразованием является оцифровка АнД путем сканирования его оригинала. Тогда результатом оцифровки может быть как электронный образ АнД, т.е. файл графического формата, так и файл текстового формата, полученный путем распознавания электронного образа (OCR преобразования) [4].

Одним из основных требований, предъявляемым к документу в процессе его жизненного цикла, является требование к подлинности документа. Под *подлинностью* документированной информации в общем виде понимается свойство документа сохранять неизменным (целостным) свое содержание относительно исходного состояния, а также обеспечивать возможность однозначной идентификации источника сообщения, даты, времени и места создания сообщения. Поэтому важной задачей системы юридически значимого документооборота является обеспечение подлинности документированной информации на всех этапах ее обработки независимо от текущей формы и носителя документированной информации. В электронной среде необходимый уровень достоверности результата проверки подлинности обеспечивается применением электронной подписи (ЭП) [8, 9]. В аналоговой среде основным элементом, обеспечивающим возможность проверки подлинности документа, является собственноручная подпись. Однако способы обеспечения подлинности документа в одной среде, как правило, перестают выполнять свои функции при преобразовании документа в другую форму.

*Целью статьи* является обеспечение достоверности результата проверки подлинности документа на уровне не ниже уровня, обеспечиваемого ЭП в условиях изменения формы и внешних признаков документа. Ограничением представленного решения является рассмотрение документированной информации только текстового формата.

**1. Системные основы представления документа.** В соответствии с [6] *документ (документированная информация)* представляет собой информацию, зафиксированную на материальном носителе с реквизитами, позволяющими ее идентифицировать. При рассмотрении технических систем информация условно приравнивается к своей материальной форме представления – *сообщению*. Соответственно процесс фиксации (документирования) информации в материальной среде неразрывно связан с триединством понятий: *сообщения, реквизита и материального носителя*. Пояснение к понятию документ, с учетом формы его представления, представлено на рис. 1.

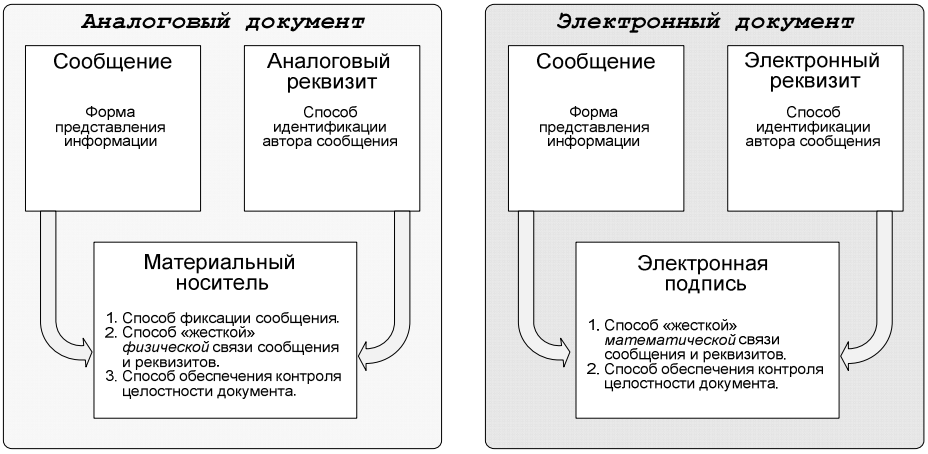


*Рис. 1. Пояснение к понятию документ*

Системной особенностью АнД является «жесткая» физическая связь содержания сообщения и реквизитов, идентифицирующих автора сообщения. Функцию элемента, связывающего информационное сообщение и автора в АнД, выполняет конкретный носитель информации.

Смена носителя в процессе обработки АнД (оцифровка, тиражирование, форматирование) приводит к нарушению связи между содержанием сообщения и его автором, а как следствие – теряет *свойство подлинности*. Для АнД носителем является бумага, пластик и любые другие «твердые» носители.

**2. Существующий способ проверки подлинности документированной информации.** Проверка подлинности АнД условно включает в себя два основных цикла:

1) первый цикл основан на визуальной проверке АнД, при которой основные реквизиты, отображенные на проверяемом АнД, сравниваются с эталоном, хранящимся в памяти человека в виде нечетких образов. В редких случаях сравнение производится с эталонными образцами, зафиксированными на материальном носителе;

2) второй цикл основан на технической проверке подлинности АнД (технической экспертизе), при которой реквизиты исследуемого АнД сравниваются с предоставленными эталонными образцами с помощью технических средств. Недостатками технической проверки подлинности АнД являются временные и материальные затраты, а также необходимость наличия эталонных реквизитов для более точного результата, что может быть проблематично при отсутствии автора документа (например при экспертизе архивных документов).

Проверка подлинности ЭД определяется ГОСТ Р 34.10-2001 и Законом «Об электронной подписи». Достоинством проверки подлинности в электронной среде является более высокий (криптографический) уровень стойкости ЭД при незначительных временных и относительно низких материальных затратах. Недостатками являются: энергозависимость (необходимость в постоянном источнике питания) всех процессов проверки подлинности, отсутствие контроля экземплярности ЭД, а также избыточная чувствительность результата проверки подлинности ЭД к любым, в том числе и не влияющим на содержание сообщения погрешностям, возникающим в процессе обработки ЭД [1].

**3. Предлагаемый способ формирования и проверки подлинности документированной информации.** Учитывая достоинства и недостатки существующих процессов формирования и проверки подлинности документов, можно сделать вывод о необходимости применения ЭП как наиболее эффективного способа обеспечения подлинности документированной информации. При представлении документа в электронной форме его подлинность должна обеспечиваться в соответствии с ГОСТ Р 34.10-2001 и возможным использованием квалифицированных сертификатов ключа подписи. При этом вопрос экземплярности электронной формы документированной информации остается открытым.

Отличием предлагаемого способа обеспечения подлинности документа является формирование значения ЭП в составе аналоговой формы документа. Тем самым аналоговая форма документа будет носить гибридный характер, т.е. одновременно обладать свойствами и ЭД, и АнД. Пояснение к понятию *«гибридной»* формы АнД представлено на рис. 2.

Особенность проверки «*гибридной»* формы АнД будет заключаться в преобразовании документа в электронную форму промежуточного графического формата (сканирование, фотографирование и т.п.) с последующим распознаванием элементов документа. После чего проверка подлинности документа будет осуществляться в соответствии с традиционным алгоритмом проверки ЭД.

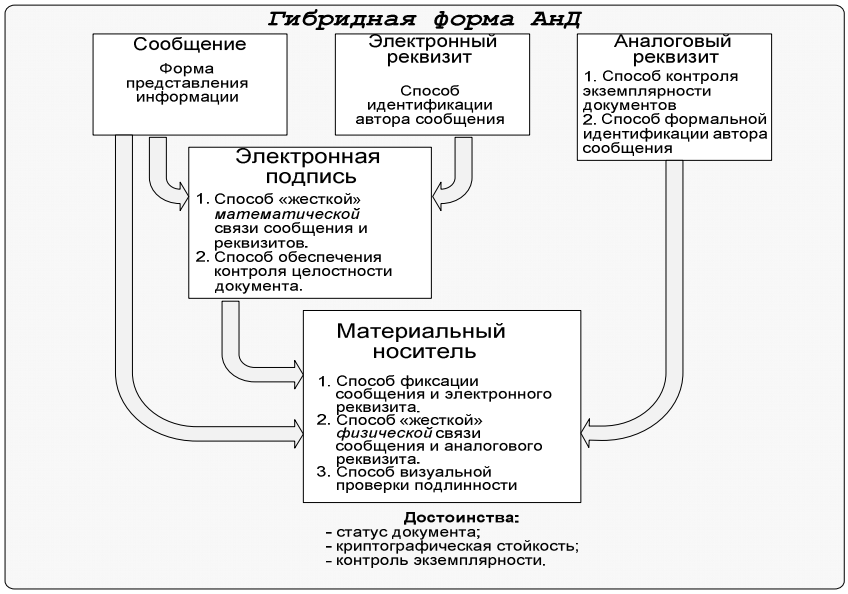


*Рис. 2. Гибридная форма АнД*

Однако в прямой постановке данный способ не реализуем, так как в соответствии с существующим законодательством ЭД – это файл, представляющий собой совокупность сообщения и служебной информации, характеризующей порядок поиска, форму представления сообщения и других атрибутов, определяемых особенностями применяемой системы обработки информации. Процесс преобразования «гибридной» формы АнД в электронную форму характеризуется сопутствующими погрешностями, как влияющими на смысл сообщения (ошибки в тексте), так и не влияющими (искажение формата файла, формата текста). Как следствие – отрицательный результат проверки подлинности документа (с помощью проверки ЭП). Для устранения данного недостатка необходимо решить следующие частные задачи:

- разработать унифицированную (эталонную) форму исходного электронного сообщения, инвариантную искажениям, не влияющим на смысловую составляющую документа (формат файла, формат текста);
- обеспечить положительный результат проверки ЭП при наличии допустимого количества устраняемых искажений в тексте документа.

*Первая* задача может быть решена путем формирования ЭП отунифицированной (эталонной) формы исходного электронного сообщения, инвариантной к изменениям формата файла и формата текста. Способ формирования и проверки гибридной формы АнД представлен на рис. 3.

*Вторая* задача может быть решена посредством введения в состав гибридной формы АнД информации о сообщении, которая может быть размещена в составе информационного поля сертификата ЭП и которая предназначается для восстановления исходного состояния эталонной формы документа при возникновении допустимого количества ошибок в тексте.

Особенностью решения второй задачи является использование метода помехоустойчивого кодирования информации, например, основанного на применении гибридной семантико-кодовой избыточности (естественной языковой избыточности и искусственной кодовой) [5]. Дополнения к способу, представленному на рис. 4 с учетом требований к помехоустойчивости документированной информации, представлены на рис. 4.

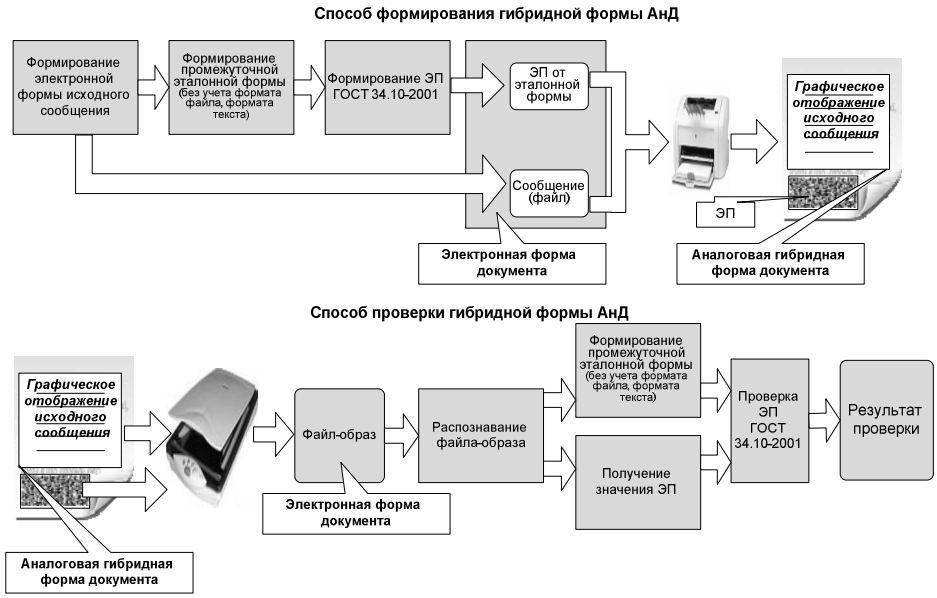


*Рис. 3. Способ формирования и проверки гибридной формы АнД*

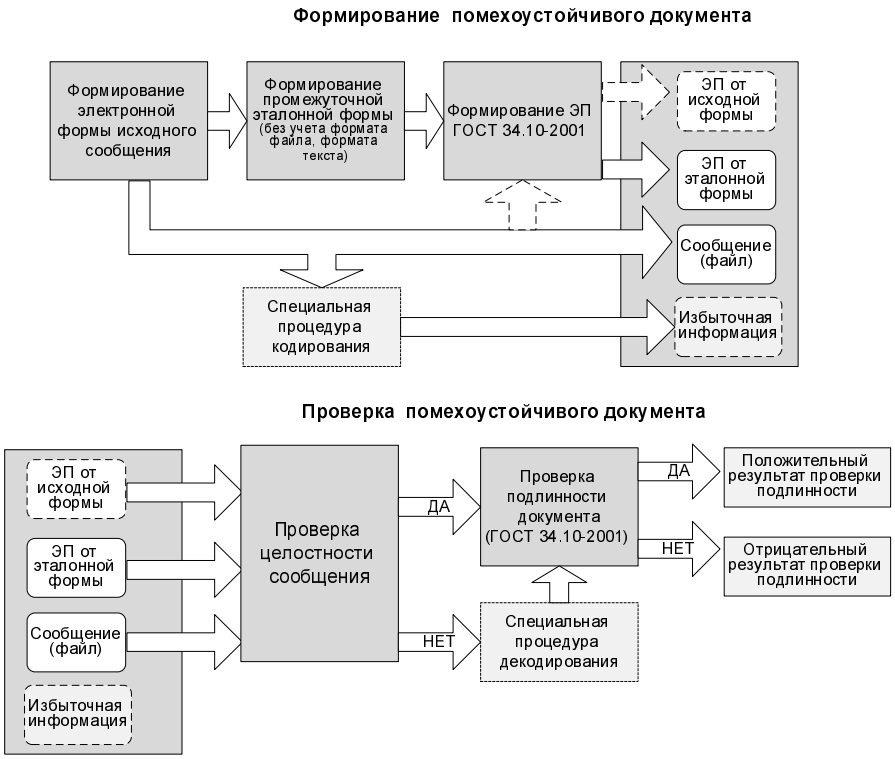


*Рис. 4. Усовершенствованный способ формирования и проверки гибридной формы АнД с учетом требований помехоустойчивости*

Рассмотрим другой практический аспект гибридного документооборота [2]. В процессе использования информационных ресурсов возникает необходимость проверки их подлинности при отсутствии реквизитов (обезличенной информации). Решение данной задачи возможно посредством реализации системы проверки подлинности документированной информации (СППД), включающей взаимосвязанные подсистемы эталонных баз данных, средств доступа к ним и технические средства проверки подлинности документов. Структурная схема предлагаемой СППД представлена на рис. 5.

Эталонные базы данных в составе СППД должны представлять упорядоченные по определенным классам массивы значений ЭП, полученных определенным способом (не противоречащим ГОСТ 34.10-2001) от исходных (эталонных) документов, а также уникальных значений (классификаторов), связанных с конкретными документами. Процесс определения подлинности документа независимо от источника формата и формы представления документа с использованием СППД должен проводиться в несколько этапов.

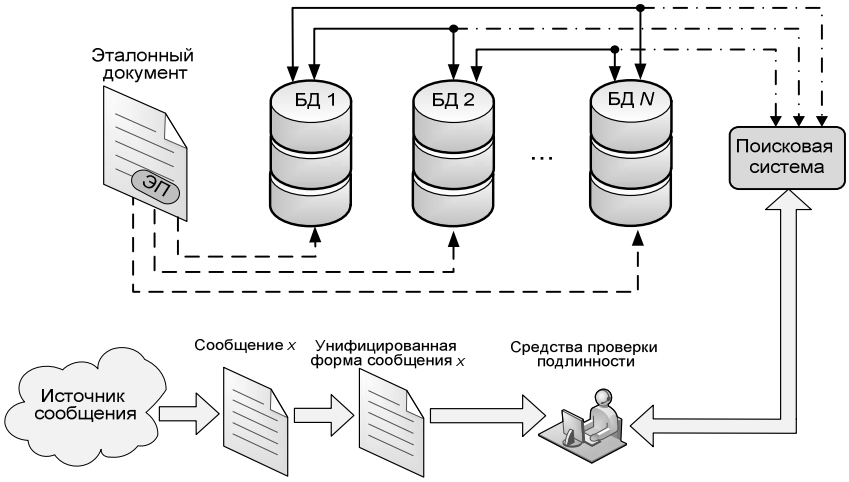


*Рис. 5. Структурная схема системы проверки подлинности обезличенной информации*

На первом этапе проверяемый документ необходимо преобразовать в унифицированный (эталонный) формат, соответствующий формату эталонных баз данных. На втором этапе с помощью специальных программных средств из состава проверяемого сообщения выделяется уникальный классификатор, соответствующий определенному эталонному документу. На третьем этапе выполняется проверка соответствия значения ЭП, полученной от унифицированной формы проверяемого документа, и значения ЭП, хранящейся в эталонной базе данных.

Достоинством предлагаемой СППД является возможность автоматизированной проверки подлинности документированной информации независимо от источника, текущей формы и формата представления документа.

**Выводы.** Предложен в общем виде способ, обеспечивающий проверку подлинности содержания документированной информации независимо от текущей формы документа. Предложено решение, позволяющее обеспечить защиту аналоговой формы представления документированной информации криптографическими методами. Показан возможный подход к решению задачи обеспечения помехоустойчивости документа. Предложена структура системы проверки подлинности документов при отсутствии реквизитов в составе проверяемого сообщения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Финько О.А., Елисеев Н.И.* Повышение функциональной гибкости и оперативности системы электронного документооборота посредством переопределения понятия «электронный документ» // Информационная безопасность 2010: Материалы 11-й международной научно-практической конференции (Таганрог, 22-25 июня 2010 г.). Ч. III. – Таганрог: Изд-во ТТИ ЮФУ, 2010.
2. *Елисеев Н.И., Финько О.А.* Многоуровневая электронная цифровая подпись и алгоритм ее реализации // Инфофорум-2011: Материалы Юбилейного Национального форума информационной безопасности (Москва, 7–8 февраля 2011 г.). – URL: http://www.infoforum.ru/news (дата обращения: 22.03.2011).
3. *Елисеев Н.И., Финько О.А.* Системные основы защищенного гибридного документооборота // Управление развитием крупномасштабных систем (MLSD`2011): Труды V Международной конференции (Москва, Россия, ИПУ РАН им. Трапезникова 3-5 октября 2011 г.).
4. *Елисеев Н.И., Финько О.А.* Проблемы обеспечения подлинности документированной информации // Документация в информационном обществе: проблемы оптимизации документооборота: Труды XIII Международной научно-практической конференции (Москва, Россия, ВНИИДАД, 26-27 октября 2011 г.).
5. *Минаков С.В., Финько О.А.* Повышение достоверности обработки данных на основе избирательного избыточного кодирования семантических единиц текста // Электронные библиотеки: перспективные методы и технологии, электронные коллекции: Труды XI Всероссийской научной конференции RCDL'2009 (Петрозаводск, Россия, 17-21 сентября 2009 г.). – Петрозаводск: КарНЦ РАН, 2009. – С. 439-443.
6. ГОСТ Р 51141 – 98. Делопроизводство и архивное дело. Термины и определения. – М.: Госстандарт России, 1998.
7. ГОСТ Р 52292-2004. Информационная технология. Электронный обмен информацией. Термины и определения. – М.: Госстандарт России, 2004.
8. Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 г. // Собрание законодательства РФ 2002. № 2. ст. 127.
9. Федеральный закон «Об электронной подписи» от 6 апреля 2011 г. // Российская газета, № 5451 (75) от 8.04.2011 г.

Статью рекомендовал к опубликованию д.т.н., профессор В.Н. Марков.

**Ржевский Дмитрий Александрович**
Филиал Военной академии связи (г. Краснодар).
E-mail: ofinko@yandex.ru.
350035, г. Краснодар, ул. Красина, 4.
Тел.: +79615874848.
Старший специалист отдела.

**Елисеев Николай Иванович**
E-mail: eliseev_81_09@mail.ru.
Тел.: +79094476289.
Доцент.

**Rzhevskij Dmitriy Alexsandrovich**
Branch of the Military Academy of Communications (Krasnodar).
E-mail: ofinko@yandex.ru.
4, Krasina, Krasnodar, 350035, Russia.
Phone: +79615874848.
Senior Specialist of the Department.

**Eliseev Nikolay Ivanovich**
E-mail: eliseev_81_09@mail.ru.
Phone: +79094476289.
Associate Professor.