Содержание:

Введение

В современных условиях конкуренции организаций по производству высокотехнологичной и качественной продукции применение высокоэффективных информационных технологий (ИТ), информационных систем (ИС) и глобальной сети Internet очень важно. Благодаря таким программным разработкам увеличивается функциональность многих предприятий мира и повышается качество их работы. В то же время, люди, которые работают в этих ИС, должны быть обеспечены определёнными средствами защиты, поскольку они могут быть подвержены определённым рискам. Поэтому в Российской Федерации (РФ) возникли такие направления работ, как использования электронной подписи в Российской Федерации.

Электронной цифровой подписью (ЭЦП) называют мощное средство контроля подлинности информации в электронном виде, которое служит для того, чтобы обеспечить целостность электронных данных, подтверждать их авторство и актуальность Она также является информационным объектом, создаваемым для того, чтобы подписывать данные, позволяющие удостовериться в их целостности и аутентичности.

В связи с вышеуказанным и темой реферата, целью данной работы было описание применения электронной цифровой подписи.

Поэтому в данном реферате были поставлены следующие задачи:

- описать основные понятия, которые связаны с электронной подписью;
- привести условия признания равнозначности электронной цифровой подписи и собственноручной подписи.

Объектом исследования является электронная цифровая подпись.

Предметом исследования является особенности и технические механизмы, которые обеспечивают применение ЭЦП.

1 Основные понятия, которые связаны с электронной подписью

Электронной цифровой подписью (ЭЦП) называют особый вид реквизита документации, позволяющие произвести установку отсутствия искажений информации в электронной документации с того момента, как происходит ее формирование и выполнить подтверждение принадлежности ЭЦП владельцу. Реквизит, а точнее – его значение получается при криптографическом шифровании информации.

Для того, чтобы зашифровать ЭЦП, специалистами применяются асимметричные алгоритмы, где используются открытые ключи.

Алгоритмы такого вида для того, чтобы зашифровать и расшифровать информацию, применяют пару ключей: открытый и закрытый (рис.1).

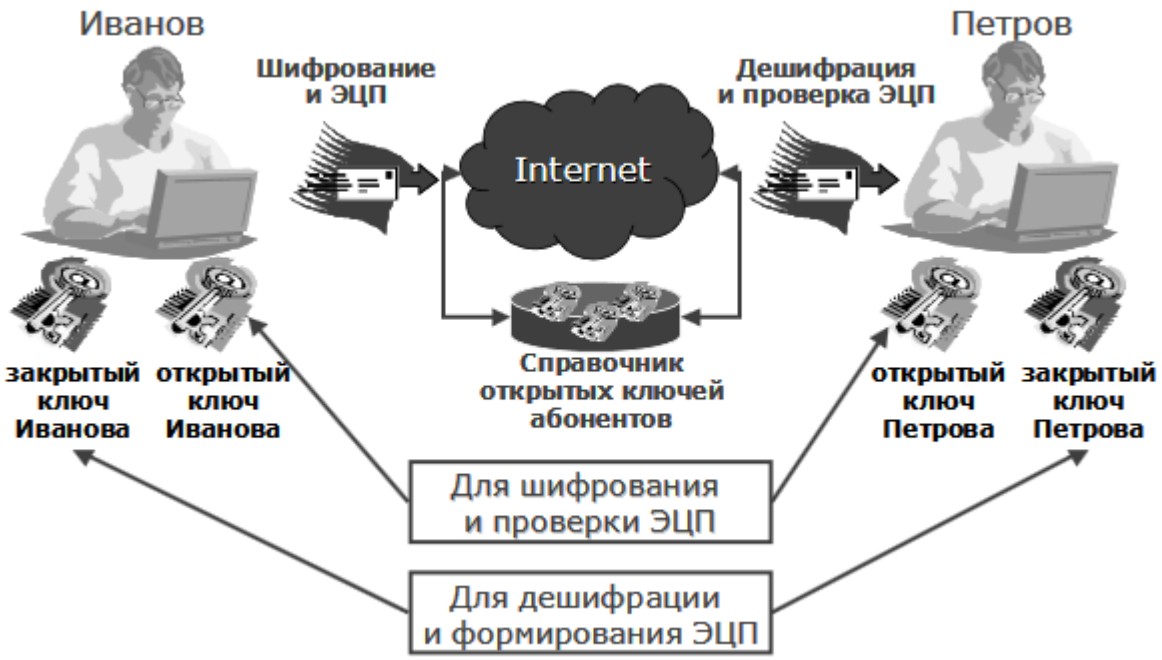

Рисунок 1 – Внешний вид схемы асимметричного шифрования ЭЦП.

В России 10 января 2002 г. принят Закон об ЭЦП, который в 2011 был модернизирован и носит называние Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электрон ной подписи» регулирует многочисленные отношения в области использования ЭЦП, когда совершаются:

- гражданско-правовые сделки;
- оказываются государственные и муниципальные услуги;
- исполняются государственные и муниципальные функции;
- совершаются иные юридически значимые действия.

Указанный выше закон определяет два основных вида ЭЦП – простую и усиленную (рис. 2). Также, согласно статье 6 Закона № 63-ФЗ, установлены условия, при которых признаются электронные документы, заверенные при помощи ЭЦП. Они признаются равнозначными бумажной документации, которая содержит собственноручную подпись оформивших их лиц.

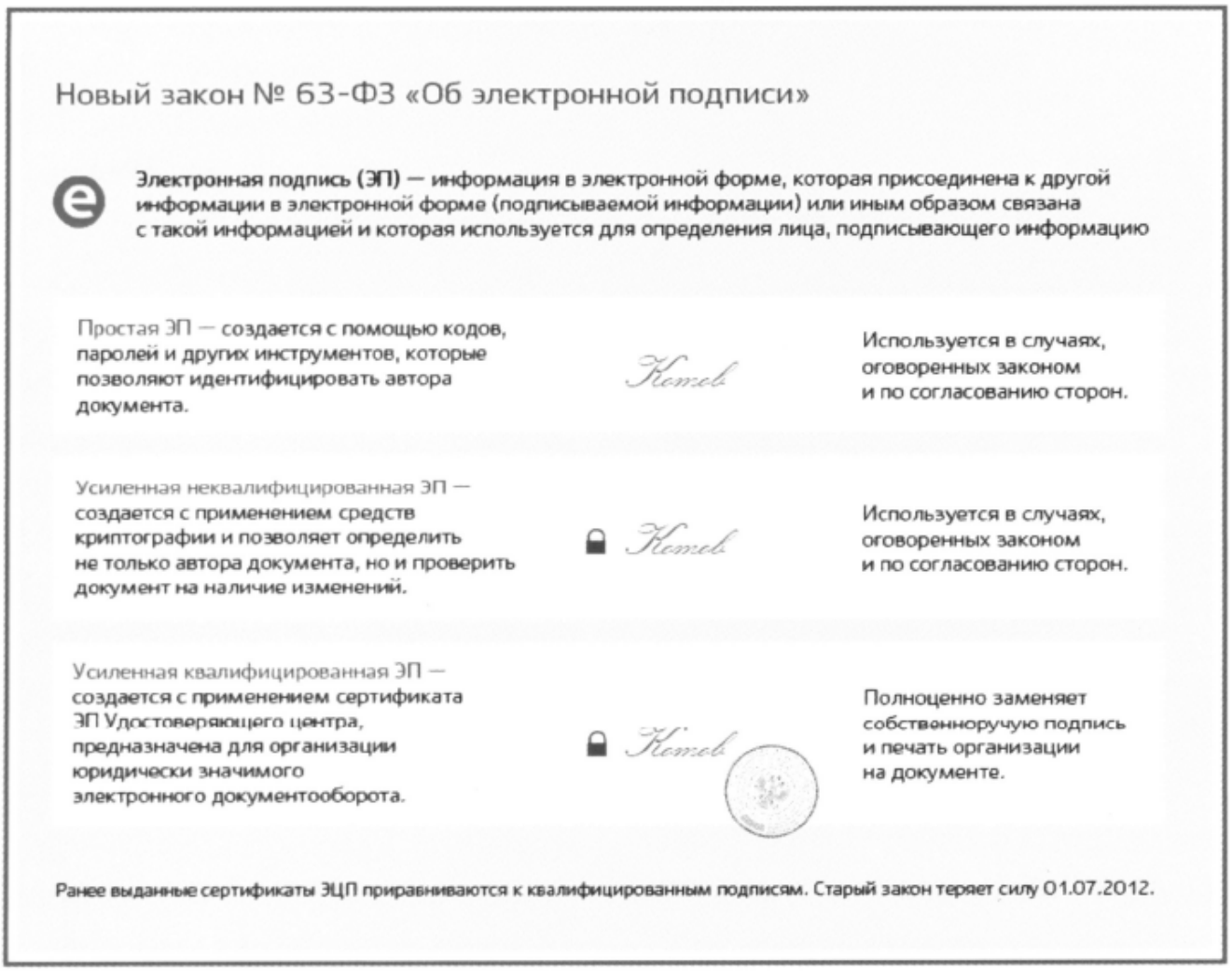

Рисунок 2 – Разновидности ЭЦП

Цель этого ФЗ – обеспечить правовыми условиями применения ЭЦП в электронных документах, при соблюдении которых она будет признана как равнозначная

собственноручной подписи на бумажном документе. Согласно статье 3 этого ФЗ дано определение электронного документа как документа, в котором информация представлена в электронно-цифровом виде и является согласно статье 4 этого же ФЗ равнозначной собственноручной подписи, поставленной владельцем на бумажном носителе.

Для того, чтобы зашифровать и дешифровать информацию, необходимо знать метод и ключ шифрования. Методом шифрования называют формальный алгоритм, который описывает порядок преобразования исходного сообщения в результирующее. Ключ шифрования – это набор параметров (данных), необходимых для применения метода. Так, например, буквы любой последовательности символов можно заменить на соответствующие комбинации цифр – это метод шифрования. А конкретное указание, какую букву заменить на какую последовательность цифр, является ключом.

Для того, чтобы был смысл в применении ЭЦП, необходимо, чтобы выполнялись два условия:

- верификации подписи при помощи открытого ключом, соответствующим именно тому закрытому ключу, который использовался при подписании;
- невозможность создания легитимной ЭЦП без обладания закрытым ключом.

Алгоритмы передачи ЭЦП показаны на рис. 3

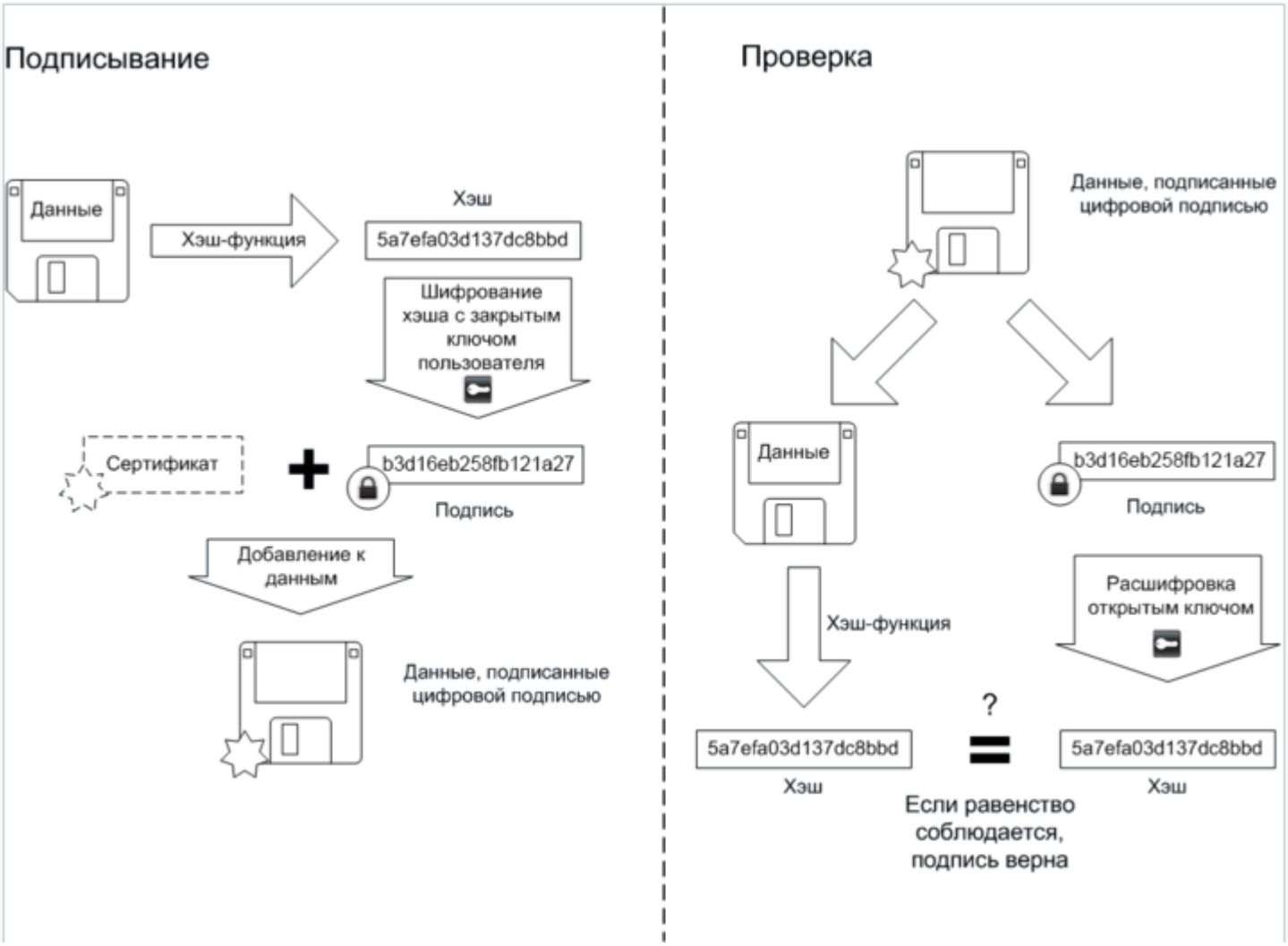

Рисунок 3 – Схема, которая поясняет алгоритмы подписи и проверки

При отправлении информации при помощи секретного ключа происходит шифрование ЭЦП, которая будет представлена в цифровом виде. При этом информация сжимается согласно определенным математическим преобразованиям. Это и есть ЭЦП. После этого отправителем информации по открытому каналу передается незашифрованная информация и ЭЦП (рис. 4).

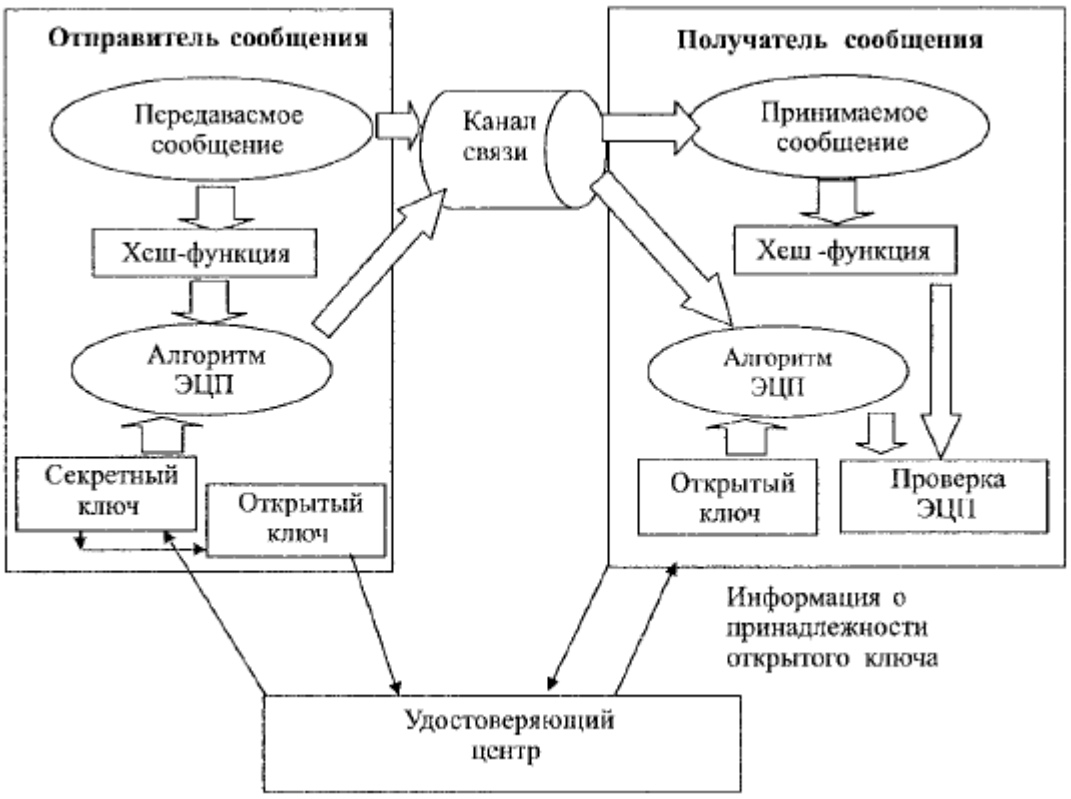

Рисунок 4 – Внешний вид блок-схемы алгоритмы формирования ЭЦП

Получатель сообщения при помощи открытого ключа и выбранного алгоритма ЭЦП осуществляет расшифровывание ЭЦП. Далее он выполняет сравнивание принятой незашифрованной информации и информации, которую он получил, когда расшифровал ЭЦП. Если она не поддельная и не происходит искажение передаваемой открытой информации, то их тексты должны полностью совпасть. Если же ЭЦП – подделка, то будут видны явные отличия в принятой открытой информации и информации, полученной при расшифровании.

2. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи

ЭЦП в электронном документе равнозначна собственноручной подписи в документе на бумажном варианте носителя, если при этом одновременно соблюдаются следующие условия:

сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

подтверждена подлинность электронной цифровой подписи в электронном документе;

- ЭЦП применяется согласно сведениям, указанным в сертификате ее ключа.

То ответственное лицо, которое участвует в информационной системе, может быть одновременно владельцем любого количества сертификатов ключей подписей.

При этом электронный документ с ЭЦП имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи. Но даже после истечения срока действия сертификата, документ не потеряет юридической силы, так как в момент подписания ставится штамп времени. Штамп времени – это аналог даты на подписываемом документе. Он подтверждает, что сертификат электронной подписи был действителен на момент подписания документа. Так, в момент подписания документа проставляется штамп времени и результат проверки сертификата.

Создание ключей электронных цифровых подписей осуществляется для использования в информационной системе общего пользования ее участником или по его обращению удостоверяющим центром, корпоративной информационной системе в порядке, установленном в этой системе.

Использование сертифицированных средств электронной цифровой подписи и созданных ими ключей электронных цифровых подписей в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления не допускается (рис. 5).

Сертификация средств ЭЦП осуществляется в соответствии с законодательством РФ о сертификации продукции и услуг.

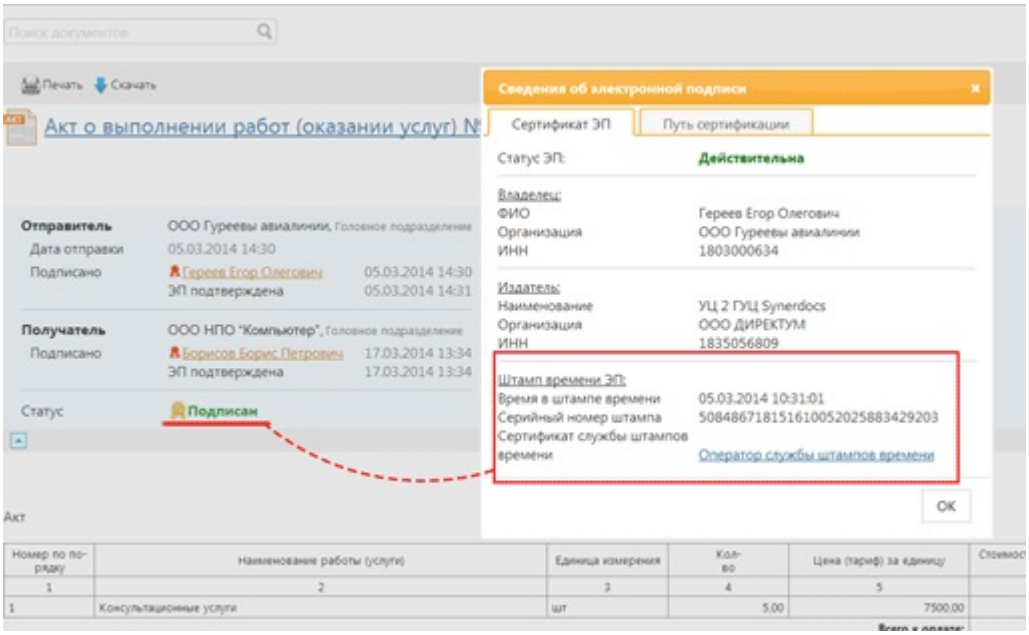

Рисунок 5 – Хранение данных об электронной подписи

Заключение

В заключении необходимо отметить, что одной из основных причин, по которой руководствам и компаниям по разработке антивирусного ПО всех государств необходимо постоянно модернизировать как законодательство по ИБ, так и сами программные разработки – это различные информационные угрозы и повышение уровня злоумышленников-нарушителей. Одной из таких угроз является получение незаконным способом персональных данных, взламывая защиту ЭЦП. Поэтому специалисты, которые борются с киберпреступностью, должны постоянно развиваться в данном направлении и уметь противостоять актуальны угрозам ИБ и применять для защиты ЭЦП все новые средства. Важно при этом постоянно модернизировать законодательную базу, поскольку применение ЭЦП позволяет значительно ускорить процесс сделок в бизнесе и в жизни граждан, одновременно избавляя их от необходимости пользоваться бумажными носителями.

В данной работе достигнута основная цель – описано применение электронной цифровой подписи.

Также при написании этой работы использовалась современная и классическая литература, а также источники, расположенные в глобальной сети Интернет.

Список использованной литературы

1. Лузянин С.Г., Васильев Л.Е. (ред.) Проблемы обеспечения безопасности на пространстве ШОС. М.: Институт Дальнего Востока РАН, 2017. — 166 с.
2. Электронная подпись документов [Электронный ресурс]. – Режим доступа: https://www.eos.ru/eos_products/eos_karma/ETSP/, свободный. – Загл. с экрана.
3. Ротков Л.Ю., Зобнев А.В. ЭЦПв электронном документообороте. Учебно-методические материалы по программе повышения квалификации «Электронный документооборот». НижнийНовгород, 2006. – 42 с.
4. Таран О.А. Электронно-цифровая подпись – актуальные вопросы. Информация как объект гражданских прав предпринимателей. Материалы конференции. - Краснодар: РГУП, 2018. – С. 111–115
5. Алискеров М.Р. (сост.) Информационные системы в налогообложении. Учебное пособие (курс лекций). — Махачкала: ДГИНХ, 2011. — 143 с.
6. Электронная подпись – Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%Электронная_подпись, свободный. – Загл. с экрана.
7. Просто об электронной подписи [Электронный ресурс]. – Режим доступа: https://ecm-journal.ru/e-sign#two, свободный. – Загл. с экрана.