УДК 004.056 DOI: 10.32362/2500-316X-2018-6-5-5-14

ОБ ЭЛЕКТРОННОЙ ПОДПИСИ И ЕЕ ПЕРСПЕКТИВАХ В ЦИФРОВОЙ ЭКОНОМИКЕ

С.С. Дубов,
Я.Я. Месенгисер@

Московский государственный университет геодезии и картографии, Москва 105064, Россия
@Автор для переписки, e-mail: Dubovss@gmail.com

В условиях цифровой экономики, когда информация в цифровой форме является ключевым фактором производства во всех сферах социально-экономической деятельности, бумажные документы будут активно заменяться на электронные, а собственноручная подпись – на ее цифровые аналоги. Однако переход к данным в цифровом виде требует переработки и обновления существующих технологий и концепций. В статье описаны основные аспекты и некоторые особенности применения электронной подписи в Российской Федерации. 28 июля 2017 года Правительство Российской Федерации утвердило программу «Цифровая экономика Российской Федерации». В программе уделяется серьезное внимание вопросу создания доверенного контура, в рамках которого будет возможно производить обмен различными данными в цифровой форме, их хранение и обработку, а также обеспечение необходимого и достаточного уровня доверия к этим данным. В отличие от знакомого всем бумажного документа, для которого однозначно установить подлинность информации, заверенной собственноручной подписью автора, может специальная почерковедческая экспертиза, ответ на вопрос, как убедиться в подлинности информации в цифровой форме в электронном виде – не очевиден. Как определять автора – создателя информации? Каким образом следует присваивать информации уникальную метку автора? Необходимо иметь специальный инструмент, который позволит однозначно выполнить проверку и определить подлинность информации в электронной форме, определить создателя или создателей информации. Основным атрибутом обеспечения достаточного уровня доверия к данным в электронной форме является в настоящее время электронная подпись. В этом вопросе существуют свои тонкости, особенности и правила работы с данной технологией, которые необходимо знать для того, чтобы электронная подпись прочно вошла в нашу жизнь.

Ключевые слова: цифровая экономика, информационные системы, электронная подпись, виды электронных подписей, объектные идентификаторы электронных подписей.

ABOUT ELECTRONIC SIGNATURE AND ITS PROSPECTS IN THE DIGITAL ECONOMY

S.S. Dubov,
Y.Y. Mesengiser@

Moscow State University of Geodesy and Cartography, Moscow 105064, Russia
@Corresponding author e-mail: Dubovss@gmail.com

On July 28, 2017, the Government of the Russian Federation approved the program "Digital Economy of the Russian Federation". In the conditions of digital economy, when information in digital form is a key factor in the production of all spheres of socioeconomic activity, paper documents will be actively replaced by electronic ones, and handwritten signature – by its digital counterparts. However, the transition to digital data requires the updating of existing technologies and concepts. Special attention in the program "Digital Economy of the Russian Federation" is given to the issue of creating a trusted circuit, within the framework of which it will be possible to exchange various data in digital form, store and process data, and provide the necessary and sufficient level of confidence in this data. Unlike a paper document signed by analog signatures, the authenticity of which can be verified by handwriting examination, the authentication of the document raises a number of questions. How is it possible to confirm the authenticity of information in digital (electronic) form? How to identify the information creator? How should the author's unique label be assigned to information? And so on. It is necessary to have some tool that uniquely confirms the authorship in electronic form. One of the fastest-growing areas and, to date, the main attribute of ensuring a sufficient level of trust in the data in electronic form is the electronic signature. However, there are subtleties, specific features and rules for working with this technology, which you need to know in order for the electronic signature to become more tightly integrated into our life. This article describes the main aspects and some features of using electronic signatures in the Russian Federation.

Keywords: digital economy, information systems, electronic signature, types of electronic signatures, OIDs.

Введение

В настоящее время мы все чаще используем различные виды электронных подписей в повседневной жизни: одни для совершения банковских операций, другие при входе в информационные системы, в том числе и государственные, третьи – при взаимодействии с операторами связи. Количество систем, использующих электронную подпись, велико, и оно продолжает активно расти [1, 2]. Интенсивное внедрение электронной подписи для обеспечения юридической значимости электронных документов породило термин «юридически значимый электронный документооборот». В принятой в 2017 г. программе «Цифровая экономика» указано [3], что данная тенденция сохранится. Ведь одной из основных целей, выделенных в этой программе, является переход на данные в цифровой форме во всех сферах социально-экономической деятельности: развитие сетей связи, создание доверенного контура, оказание услуг в электронном виде, переход на электронный документооборот. Отсюда следует, что электронная подпись имеет большие перспективы развития.

Однако согласно исследованию, проведенному по предложению Всемирного экономического форума для оценки готовности стран к цифровой экономике, Российская Федерация занимает 41-е место со значительным отрывом от десятки лидирующих стран, таких, как Сингапур, Финляндия, Швеция, Норвегия, Соединенные Штаты Америки, Нидерланды, Швейцария, Великобритания, Люксембург и Япония. Значительное отставание в развитии цифровой экономики от мировых лидеров объясняется пробелами нормативной базы, недостаточно благоприятной средой для ведения бизнеса и инноваций. Более того, хотя все большее число граждан Российской Федерации признает необходимость обладания цифровыми компетенциями, уровень использования персональных

компьютеров и информационно-телекоммуникационной сети «Интернет» в России все еще ниже, чем в Европе. Существует серьезный разрыв в цифровых навыках между отдельными группами населения. Поэтому одним из основных направлений, выделенных в данной программе, является создание условий для развития общества знаний и повышения степени информированности и цифровой грамотности граждан Российской Федерации [3]. В направлении «Кадры и образование» выделены следующие основные цели:

- создание ключевых условий для подготовки кадров цифровой экономики;
- совершенствование системы образования, которая должна обеспечивать цифровую экономику компетентными кадрами;
- рынок труда, который должен опираться на требования цифровой экономики;
- создание системы мотивации по освоению необходимых компетенций и участию кадров в развитии цифровой экономики России.

Для успешного внедрения электронной подписи во все сферы деятельности общества гражданам необходимо:

– понимать, что такое электронная подпись;

– различать виды электронных подписей;

– разбираться в том, какие документы нужно предоставить в удостоверяющий центр для изготовления ключа электронной подписи и сертификата ключа проверки электронной подписи;

– понимать, как ими пользоваться;

– разбираться в том, почему сертификаты ключей проверки электронных подписей покупаются для определенных целей;

– понимать условия и требования, при которых электронная подпись признается юридически значимой;

– владеть юридическими аспектами применения электронной подписи.

Классификация электронных подписей

В соответствии с ФЗ № 149 «Об информации, информационных технологиях и о защите информации», электронный документ (далее ЭД) – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком, с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах [4]. Однако под этим определением может пониматься и скан-копия аналогового документа, и электронный документ с его электронной подписью.

Основное назначение электронной подписи (далее ЭП) – подтверждение авторства и подлинности электронного документа, а, значит, и придания ему юридической силы. Электронная подпись может быть использована также для входа в различные системы.

Основным нормативно-правовым актом, регулирующим использование ЭП, является ФЗ № 63 «Об электронной подписи». Данный акт определяет основные понятия и устанавливает требования для признания электронного документа с электронной подписью аналогом документа с собственноручной подписью. В Федеральном законе дается определение электронной подписи: электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации)

или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию [5]. В цитируемом документе определены виды электронных подписей: простая, неквалифицированная и квалифицированная.

Простая ЭП (далее ПЭП) – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом [5]. Примером может служить использование одноразовых СМС-кодов. Для формирования таких кодов может быть использована хеш-цепочка – последовательность, каждый элемент которой является значением хеш-функции от предыдущего элемента. Одноразовые СМС-коды являются развитием карт переменных кодов. Основное назначение ПЭП – подтверждение намерения человека на выполнение той или иной операции. Для признания электронного документа с ПЭП аналогом бумажного документа с собственноручной подписью требуется регламент или соглашение об использовании ПЭП, в котором должны быть указаны:

- правила, по которым подписанта определяют по его простой электронной подписи;
- права и обязанности каждой из сторон.

Неквалифицированная электронная подпись (далее НЭП) – подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи [5].

Ключевым отличием ПЭП и НЭП является получение подписи путем криптографического преобразования информации с использованием ключа электронной подписи. Происходит это так. У подписанта имеется пара «ключ ЭП – ключ проверки ЭП». Ключ проверки ЭП находится по ключу ЭП с помощью специальных криптографических алгоритмов, а восстановление ключа ЭП по ключу проверки ЭП является довольно трудным занятием. Ключ ЭП доступен только подписанту, а ключ проверки ЭП – всем заинтересованным сторонам:

1. Подписант находит значение хеш-функции от подписываемого ЭД.
2. Подписант зашифровывает полученное значение ключом ЭП.
3. Полученное зашифрованное значение хеш-функции от электронного документа является НЭП ЭД.
4. Подписант отправляет получателю НЭП вместе с ЭД.

Проверка НЭП происходит следующим образом:

1. Получатель использует ключ проверки ЭП для расшифровки зашифрованного значения хеш-суммы от ЭД.
2. Получатель находит значение хеш-функции от полученного ЭД.
3. Если расшифрованное значение хеш-функции совпадает с найденным, то документ признается подлинным.

Неквалифицированная электронная подпись применима для внутреннего и внешнего юридически значимого электронного документооборота при условии, что стороны заключили соглашение об использовании НЭП, в котором должны быть указаны:

- правила выработки ключей ЭП;
- порядок использования ключей и их хранение;
- правила, по которым подписанта определяют по его неквалифицированной электронной подписи;
- порядок признания неквалифицированной электронной подписи;
- права и обязанности сторон соглашения.

Квалифицированная электронная подпись (далее КЭП) – электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в Федеральном законе [5].

Сертификат ключа проверки ЭП – документ в бумажном или электронном виде, в котором в соответствии с приказом ФСБ от 27.12.2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи» [6] заполнены необходимые поля, позволяющие однозначно идентифицировать подписанта. Содержание полей определено в ФЗ № 63 и продублировано в приказе ФСБ № 795. Ключ ЭП хранится на специальном носителе. Самым распространенным видом носителя является токен – устройство, похожее на USB. На токене может храниться и сертификат ключа проверки ЭП.

Средства ЭП – криптографические средства, которые используются для реализации хотя бы одной из следующих функций: создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП. Требования к средствам ЭП определены в приказе ФСБ от 27.12.2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра» [7]. В отличие от НЭП, документы с КЭП признаются юридически значимыми без каких-либо дополнительных соглашений или регламентов. Квалифицированный сертификат ключа проверки ЭП также может выдать только удостоверяющий центр, который прошел аккредитацию Минкомсвязи. Требования к квалифицированному удостоверяющему центру определены в ФЗ № 63.

Область применения КЭП довольно обширна. Это и использование КЭП в юридически значимом электронном документообороте, при отправке электронной отчетности в контролирующие органы, для оказания государственных услуг в электронном виде, для электронных торгов и т.п. Однако существуют требования, при несоблюдении которых электронная подпись не будет признана юридически значимой. При использовании ПЭП или НЭП такие требования устанавливаются в соглашении; в случае КЭП требования определены Федеральным законом № 63 «Об электронной подписи»:

1) квалифицированный сертификат создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата;

2) квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;

3) имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания. При этом проверка осуществляется с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным Федеральным законом № 63, и с использованием квалифицированного сертификата лица, подписавшего электронный документ;

4) квалифицированная электронная подпись используется с учетом ограничений, содержащихся в квалифицированном сертификате лица, подписывающего электронный документ (если такие ограничения установлены) [5]. Более того, при получении информации о нарушении конфиденциальности ключа электронной подписи требуется в течение не более чем одного рабочего дня со дня получения информации о таком нарушении уведомить удостоверяющий центр (УЦ), который выдал сертификат и ключ [5].

Таким образом, электронная подпись – результат определенного преобразования исходной информации, который логически связан с ней. Электронная подпись не используется для подписания электронного документа, а прикрепляется к нему. Поэтому приобрести электронную подпись нельзя. Можно приобрести пару «ключ ЭП – ключ проверки ЭП», хотя для удобства, чтобы не вводить потенциального клиента в замешательство, многие УЦ в своих предложениях указывают именно покупку ЭП, что неправильно.

Процесс изготовления квалифицированного сертификата ключа проверки ЭП и ключа ЭП состоит из нескольких этапов:

1) формирование необходимого пакета документов (заявление, доверенности, заверенные копии документов);
2) подача документов в УЦ;
3) оплата;
4) получение сертификата ключа проверки ЭП и ключа ЭП;
5) проверка работоспособности;
6) составление акта о приеме работ.

Объектные идентификаторы

Сегодня аккредитованные удостоверяющие центры выдают сертификаты и ключи электронной подписи по различным тарифам: тариф «Ключ директора», тариф «ЕГАИС ФСРАР», тариф «Торги Банкротов максимальный», тариф «Росреестр» и т.д. Каждый из тарифов предполагает использование электронной подписи в определенных системах, которые указаны на сайте продавца. Тариф «Росреестр» включает ЭП, которой можно пользоваться только при взаимодействии с Росреестром, а тариф «ЕГАИС ФСРАР» позволяет работать только с системой Росалкогольрегулирования. На рис. 1 приведена круговая диаграмма, отражающая долевое участие систем, в которых клиент может работать, приобретая сертификаты и ключи электронной подписи по тому или иному тарифу.

Очевидно, что приобретя сертификат и ключ ЭП по тарифу «Росреестр», невозможно будет их использование в других системах. Отечественная система сертификации не предлагает возможности самостоятельного формирования содержимого сертификата, отсутствует и эффективная система его изменения. Нельзя добавить полномочия в серти-

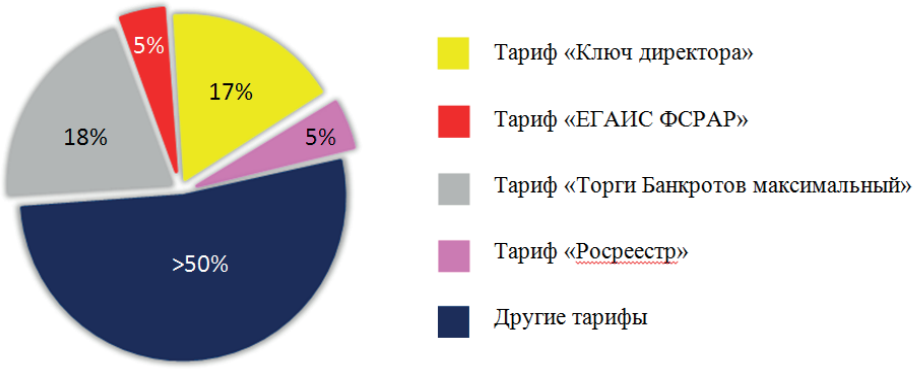

Рис. 1. Тарифы для приобретения сертификатов и ключей электронной подписи, доступные клиенту в РФ.

фикат. В настоящее время отсутствует механизм самостоятельного формирования списка площадок и порталов, на которых нужно работать; нет механизма оперативного изменения сертификата: можно его либо перевыпустить, либо купить новый. Хотя на рынке и присутствуют подписи, которые предназначены для многих систем, но стоят они значительно дороже. Поэтому часто у сотрудника имеется несколько подписей, в которых он порой путается. Более того, регулярно появляются новые системы, а, соответственно, и новые полномочия для работы в них. Может сложиться ситуация, при которой требуется работа в новой системе, а полномочий для работы с ней нет. Это обусловлено тем, что в сертификате ключа проверки ЭП УЦ, помимо сведений, которые позволяют однозначно идентифицировать владельца сертификата, указывают определенные коды – последовательности чисел, разделенных точками, которые можно найти в пункте «Сведения о сертификате».

Рассмотрим произвольный сертификат ключа проверки электронной подписи (рис. 2).

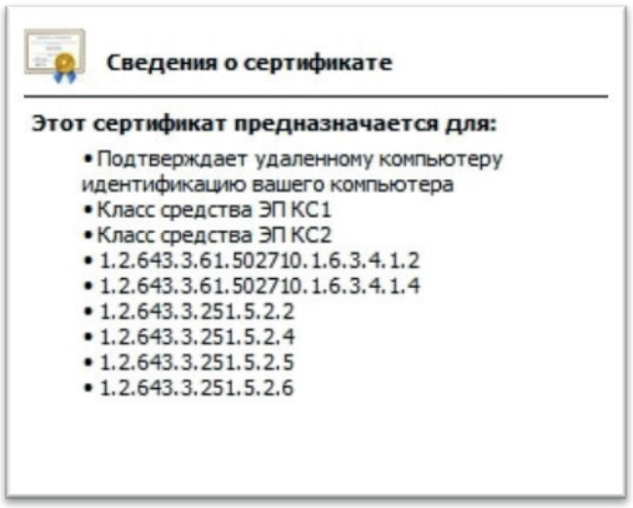

Рис. 2. Сведения о квалифицированном сертификате ключа проверки электронной подписи.

Приведенные в сертификате последовательности являются кодами и называются объектными идентификаторами (OID). Существует целое дерево таких идентификаторов с множеством ответвлений. Каждый идентификатор определяет уникальную функцию, полномочие, стандарт. Расположение корня и верхних дуг дерева регламентирует международный стандарт ISO 9834-1. В каждой стране существует уполномоченный орган по ведению данного дерева. В нашей стране таким органом является организация ОАО «ИнфоТеКС Интернет траст» [8]. Дерево объектных идентификаторов РФ опубликовано на сайте *oid.iitrust.ru*. Дерево, однако, не поможет при поиске отдельного идентификатора. В РФ нет нормативно-правового акта, который бы описывал правила ведения данного дерева, поэтому организации вправе не предоставлять компании ОАО «ИнфоТеКС Интернет траст» информацию об объектных идентификаторах, используемых в их системах. Поэтому дерево в РФ включает в себя только организации, которые получили свой идентификатор. Ознакомиться с идентификаторами, которые используются в определенной системе, можно либо на ее сайте, либо в приказе, который выпустила организация (к примеру, «Росреестр» [9]).

Все УЦ задают приобретающим КЭП вопросы: «Для чего Вам нужна электронная подпись? В каких системах Вы будете с ней работать?» На рынке присутствуют электронные подписи самых разных видов: для директора организации, для доверенных лиц, для работы с порталом закупок в качестве поставщика или закупщика и т.д. В зависимости от выбора «начинки» ЭП ее использование возможно только в этих системах. Полномочия записываются в сертификате в виде объектных идентификаторов.

Изначально права администратора системы выдаются директору организации, а он уже должен сделать администратором одного из сотрудников. Руководитель организации должен быть специально обучен работе с системами и распределением ролей между сотрудниками и работе по формированию электронных подписей. На текущий момент программное обеспечение (ПО), которое используется для формирования подписей и ее проверки, одного производителя может конфликтовать с ПО другого производителя. При формировании подписи или аутентификации в системе в окне выбора сертификата отображается их список с Ф.И.О. владельца сертификата и датами его действия. Руководитель может различать сертификаты только по дате их выпуска. Если же сертификаты выпущены в один день, то отличить их удастся, только перепробовав все варианты. Не все руководители организаций являются IT-специалистами, поэтому они передают или копируют свои сертификаты другим членам организации [10].

Заключение

Чтобы электронная подпись более прочно вошла в нашу жизнь, необходимо:

– совершенствовать нормативно-правовую базу;

– освещать тему электронной подписи в рамках основного учебного процесса образовательных учреждений среднего профессионального и высшего образования;

– формировать более гибкую и оперативную систему выдачи сертификатов и их замены;

– сделать возможным добавление объектных идентификаторов без процедуры перевыпуска сертификата;

– создать сертификат с необходимыми объектными идентификаторами;

– усовершенствовать интерфейсы программ, которые позволяют осуществлять подпись, проверку подписи и их аутентификацию.

Литература:

1. Майоров А.А., Дубов С.С., Левина Н.И. Об архитектуре системы автоматизированного мониторинга реализации мероприятий схемы территориального планирования Российской Федерации в области высшего образования // Известия высших учебных заведений. Геодезия и аэрофотосъемка. 2016. № 6. С. 111–115.

2. Дубов С.С., Левина Н.И. Методика мониторинга данных об организации летнего отдыха // Известия Тульского государственного университета. Технические науки. 2017. № 10. С. 151–155.

3. Программа «Цифровая экономика Российской Федерации». URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

4. Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации» с поправками на 19.07.2018, статья 2, пункт 11.1. URL: http://docs.cntd.ru/document/901990051

5. Федеральный закон № 63 «Об электронной подписи» с поправками на 23.06.2016. URL: http://docs.cntd.ru/document/902271495

6. Приказ ФСБ № 795 от 27.12.2011 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи». URL: http://base.garant.ru/70133464/

7. Приказ ФСБ № 796 от 27.12.2011 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра». URL: http://www.garant.ru/products/ipo/prime/doc/70039150/

8. Соглашение о регистрирующем уполномоченном органе в соответствии со стандартом ГОСТ Р ИСО/МЭК 9834-1-2009 между Открытым акционерным обществом «ИнфоТеКС Интернет Траст» и Федеральным агентством по техническому регулированию и метрологии. URL: https://oid.iitrust.ru/downloads/soglashenie_o_registrirushem_organe.pdf

9. Приказ Федеральной Службы Государственной Регистрации, Кадастра и Картографии от 14 января 2011 г. № П/1 «О требованиях к совместимости, сертификату ключа подписи, обеспечению возможности подтверждения подлинности электронно цифровой подписи при оказании Федеральной Службой Государственной Регистрации, Кадастра и Картографии государственных услуг в электронном виде». URL: https://rosreestr.ru/upload/Doc/prikaz_p_1.doc

10. Худкина Е.А., Долгова Т.Г. Проблемы использования электронно-цифровой подписи на электронных торгах // Актуальные проблемы авиации и космонавтики. 2014. № 10. С. 397–398.

References:

1. Majorov A.A., Dubov S.S., Levina N.I. About the architecture of the automated monitoring system for the implementation of the activities of the territorial planning scheme of the Russian Federation in the field of higher education. *Izvestiya vysshikh uchebnykh zavedenij. Geodesiya i aerofotos'yemka* (Proceedings of the Higher Educational Institutions. Geodesy and Aerophotosurveying). 2016; (6): 111-115. (in Russ.)

2. Dubov S.S., Levina N.I. Methods of monitoring data for the organization of summer holidays. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki* (Proceedings of the Tula State University. Technical Sciences). 2017; (10): 151-155. (in Russ.)

3. The program “Digital Economy of the Russian Federation”. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf. (in Russ.)

4. The Federal Law No. 149 “About Information, Information Technologies and Information Protection” as amended on 07/19/2018, Article 2, paragraph 11.11. URL: http://docs.cntd.ru/document/901990051. (in Russ.)

5. The Federal Law No. 63 “About electronic signature” as amended on 06/23/2016. URL: http://docs.cntd.ru/document/902271495. (in Russ.)

6. The Order of the FSS No. 795 “About approval of the Requirements to the form of the qualified certificate of the electronic signature verification key”. 12/27/2011. URL: http://base.garant.ru/70133464/. (in Russ.)

7. The Order of the FSS No. 796 “About approval of the Requirements for electronic signature tools, and tool requirements of the certification center”. 12/27/2011. URL: http://www.garant.ru/products/ipo/prime/doc/70039150/. (in Russ.)

8. The agreement on the registering authorized body in accordance with the standard GOST R ISO/IEC 9834-1-2009 between the Company “InfoTech Internet Trust” and the Federal Agency for Technical Regulation and Metrology. URL: https://oid.iitrust.ru/downloads/soglashenie_o_registrirushem_organe.pdf . (in Russ.)

9. The Order of the Federal State Registration Service, Cadastre and Cartography No. П/1 “On compatibility requirements, certificate key certificate, ensuring the possibility of confirming the authenticity of digital signatures in the provision of state services by the Federal State Registration Service, Cadastre and Cartography in electronic form”. URL: rosreestr.ru/upload/Doc/prikaz_p_1.doc. (in Russ.)

10. Khudkina E.A., Dolgova T.G. The problems of using electronic digital signature in electronic trading. *Aktualnye problemy aviatsii i kosmonavtiki* (Actual Problems of Aviation and Cosmonautics). 2014; (10): 397-398. (in Russ.)

Об авторах:

Дубов Сергей Сергеевич, кандидат технических наук, доцент, кафедра информационно-измерительных систем ФГБОУ ВО «Московский государственный университет геодезии и картографии», директор Центра отраслевых мониторинговых систем и информационной безопасности ФГБОУ ВО «Московский государственный университет геодезии и картографии» (105064, Россия, Москва, Гороховский пер., д. 4).

Месенгисер Якоб Якобович, студент кафедры информационно-измерительных систем ФГБОУ ВО «Московский государственный университет геодезии и картографии», сотрудник Центра отраслевых мониторинговых систем и информационной безопасности ФГБОУ ВО «Московский государственный университет геодезии и картографии» (105064, Россия, Москва, Гороховский пер., д. 4).

About the authors:

Sergey S. Dubov, Ph.D. (Eng.), Associated Professor, Chair of Information-Measuring Systems, Director of the Center for Sectoral Monitoring Systems and Information Security, Moscow State University of Geodesy and Cartography (4, Gorokhovskiy per., Moscow 105064, Russia).

Yakob Y. Mesengiser, Student, Chair of Information-Measuring Systems, Employee of the Center for Sectoral Monitoring Systems and Information Security, Moscow State University of Geodesy and Cartography (4, Gorokhovskiy per., Moscow 105064, Russia).

Для цитирования: Дубов С.С., Месенгисер Я.Я. Об электронной подписи и ее перспективах в цифровой экономике // Российский технологический журнал. 2018. Т. 6. № 5. С. 5–14. DOI: 10.32362/2500-316X-2018-6-5-5-14.

For citation: Dubov S.S., Mesengiser Y.Y. About electronic signature and its prospects in the digital economy. *Rossiyskiy tekhnologicheskiy zhurnal* (Russian Technological Journal). 2018; 6(5): 5-14. (in Russ.). DOI: 10.32362/2500-316X-2018-6-5-5-14.