

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт  
Политехнический

Кафедра ИнОУП

Направление подготовки

46.04.02 "Документоведение и  
архивоведение"

Магистерская программа

"Документационное  
обеспечение управления электронного  
правительства"

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему

Нормативное регулирование внедрения и использования ЭП  
в делопроизводстве

Автор работы

\_\_\_\_\_  
(подпись, дата)

А.В. Щепеткова  
(инициалы, фамилия)

Научный руководитель

\_\_\_\_\_  
(подпись, дата)

Н.Н. Шокорова  
(инициалы, фамилия)

Нормоконтролёр

\_\_\_\_\_  
(должность, место работы)

\_\_\_\_\_  
(подпись, дата)

Ю.Г. Кирюхин  
(инициалы, фамилия)

Рецензент

\_\_\_\_\_  
(должность, место работы)

\_\_\_\_\_  
(подпись, дата)

\_\_\_\_\_  
(инициалы, фамилия)

Магистерская диссертация по содержанию и объему соответствует заданию, профилю направления подготовки и может быть допущена к защите на заседании Государственной аттестационной комиссии "\_\_\_" \_\_\_\_\_ 20\_\_\_ г.

Проверяющий преподаватель

\_\_\_\_\_  
(подпись, дата)

\_\_\_\_\_  
(инициалы, фамилия)

Работа допущена к защите (протокол заседания кафедры от \_\_\_\_\_ № \_\_\_\_\_)

Заведующий кафедрой

\_\_\_\_\_  
(подпись)

Л.Р. Фионова  
(инициалы, фамилия)

Диссертация защищена с оценкой \_\_\_\_\_ (протокол заседания ГЭК от \_\_\_\_\_ № \_\_\_\_\_)

Секретарь ГЭК

\_\_\_\_\_  
(подпись)

Л.В.Коровина  
(инициалы, фамилия)

г. Пенза 2021

## Реферат

Пояснительная записка содержит 70 страниц текста, 4 рисунка, 1 таблицу, 48 источников, 1 приложение.

ЭЛЕКТРОННАЯ ПОДПИСЬ, НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ, ЭЛЕКТРОННЫЙ ДОКУМЕНТ, ТЕХНОЛОГИИ ПРИМЕНЕНИЯ ЭЛЕКТРОННЫХ ПОДПИСЕЙ, СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА, МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

**Цель магистерской диссертации:** анализ действующей нормативной законодательной и методической базы по внедрению и использованию электронной подписи при работе с электронными документами и разработка рекомендаций по усовершенствованию использования электронной подписи в делопроизводстве конкретной организации.

Цель позволила поставить следующие **задачи исследования:**

- проанализировать действующую нормативную законодательную базу по использованию электронной подписи при работе с электронными документами в России и за рубежом;
- проанализировать современный опыт использования электронной подписи в России и за рубежом;
- на основании анализа, выявить проблемы, сдерживающие полноценное использование электронной подписи в документообороте организаций и дать методические рекомендации по оптимизации использования электронной подписи на примере исследуемой организации - ГАСУСОССЗН ПО «Сердобский дом ветеранов труда».

**Актуальность исследования:** анализ нормативного регулирования внедрения и использования электронной подписи в делопроизводстве позволит определить существующие проблемы в применении электронной подписи, дать рекомендации по улучшению использования электронной

подписи в исследуемой организации и тем самым повысить качество электронного взаимодействия.

**Объект исследования:** существующие технологии, нормативные акты, стандарты и подходы по реализации процессов создания и использования электронной подписи.

**Предмет исследования:** система электронного документооборота ГАСУСОССЗН ПО «Сердобский дом ветеранов труда».

**Методы исследования:** анализ, синтез информации; сопоставительный и сравнительный методы.

**Характер НИР:** прикладной характер.

**Приоритетные направления развития науки:** нет.

**Код ГРНТИ:** 82.13.13 Документационное обеспечение управления. Делопроизводство. Документоведение.

**Критические технологии:** нет.

**Область науки:** технические.

Магистерская диссертация состоит из введения, трех глав, заключения, списка используемых источников и литературы, приложения.

В первой главе рассмотрены действующие нормативные законодательные и методические акты Российской Федерации, зарубежные нормативные акты в области применения электронной подписи.

Во втором разделе исследован опыт использования электронной подписи в России и за рубежом, рассмотрены технологии их применения, а так же приведены критерии выбора вида электронной подписи для электронного делопроизводства.

В третьем разделе рассмотрены вопросы получения и применения электронной подписи для ведения делопроизводства в ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» и предложено разработанное руководство по обеспечению информационной безопасности при работе с электронной подписью в ГАСУСОССЗН ПО «Сердобский дом ветеранов труда».

## Содержание

|                                                                                                                                                                    |    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Введение.....                                                                                                                                                      | 6  |
| 1 Анализ нормативной базы, регламентирующей использование<br>электронной подписи .....                                                                             | 7  |
| 1.1 Понятие «электронная подпись». Понятия «электронный<br>документ и электронный документооборот». Понятие «межведомственное<br>электронное взаимодействие» ..... | 7  |
| 1.2 Нормативно-законодательные и методические акты,<br>регламентирующие создание и применение электронной подписи<br>в России .....                                | 11 |
| 1.3 Анализ зарубежных нормативных актов в сфере<br>использования электронной подписи .....                                                                         | 29 |
| 2 Исследование опыта использования электронной подписи в России<br>и за рубежом .....                                                                              | 34 |
| 2.1 Технологии создания и использования электронной подписи<br>в России .....                                                                                      | 34 |
| 2.2 Зарубежный опыт использования электронной подписи .....                                                                                                        | 37 |
| 2.3 Критерии выбора вида электронной подписи для электронного<br>делопроизводства .....                                                                            | 39 |
| 3 Методические рекомендации по оптимизации использования<br>электронной подписи на примере ГАСУСОССЗН ПО «Сердобский дом<br>ветеранов труда» .....                 | 45 |
| 3.1 Получение электронной подписи ГАСУСОССЗН ПО<br>«Сердобский дом ветеранов труда» .....                                                                          | 45 |

|     |                                                                                                                                                                  |    |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 3.2 | Применение электронной подписи в ГАСУСОССЗН ПО<br>«Сердобский дом ветеранов труда» .....                                                                         | 49 |
| 3.3 | Разработка Руководства по обеспечению информационной<br>безопасности при работе с электронной подписью в ГАСУСОССЗН ПО<br>«Сердобский дом ветеранов труда» ..... | 52 |
|     | Заключение .....                                                                                                                                                 | 61 |
|     | Список использованных источников и литературы.....                                                                                                               | 65 |
|     | Приложение А. Комплект документов при получении электронной<br>подписи и сертификата ключа .....                                                                 | 72 |

## Введение

Электронный документооборот давно и прочно вошел в нашу жизнь. Развитие информационных технологий привело к цифровизации в различных сферах деятельности.

Федеральный закон №476-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи»<sup>1</sup>, по мнению участников форума РКІ – Форум 2020<sup>2</sup> приведет к масштабным преобразованиям в сфере использования электронной подписи. С января 2021 года появятся права и возможности использования облачной квалифицированной электронной подписи (ЭП), также появится возможность аккредитоваться операторам доверенной третьей стороны.

В настоящее время электронная подпись используется и при обращении на портал государственных услуг за предоставлением конкретной услуги, и при формировании налоговой и прочей отчетности индивидуальными предпринимателями и организациями. Однако до сих пор, многие вопросы, связанные с использованием электронной подписи в делопроизводстве находятся в стадии проработки.

Следовательно, анализ нормативного регулирования внедрения и использования электронной подписи в делопроизводстве является актуальной темой исследования магистерской диссертации.

---

<sup>1</sup> Федеральный закон от 27.12.2019 № 476-ФЗ (ред. от 23.06.2020) "О внесении изменений в Федеральный закон "Об электронной подписи" и статью 1 Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля". [Электронный ресурс] URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_341757/](http://www.consultant.ru/document/cons_doc_LAW_341757/) (дата обращения 16.11.2020).

<sup>2</sup> РКІ – Форум 2020. XVIII международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи //URL: <http://pki-forum.ru> (дата обращения 16.11.2020).

# **1 Анализ нормативной базы, регламентирующей использование электронной подписи**

Развитие современного общества невозможно представить без использования, обработки, хранения информации. Современные информационные технологии повышают эффективность труда в сфере делопроизводства, в деятельности, которая обеспечивает работу с документами, как в электронной, так и в бумажной форме.

## **1.1 Понятие «электронная подпись». Понятия «электронный документ и электронный документооборот». Понятие «межведомственное электронное взаимодействие»**

Электронная подпись (ЭП) неразрывно связана с понятием электронного документа, так как позволяет подтвердить авторство этого документа. Причем автором электронного документа может быть реальное лицо, аккаунт в криптовалютной системе.

Существует несколько определений электронной подписи, встречающихся в нормативных актах, стандартах. В России понятие электронной *цифровой* подписи впервые было прописано в 1994 году в ГОСТе 34 группы «Информационные технологии».

Прежде всего, рассмотрим определение Федерального закона «Об электронной подписи» (далее ФЗ-63): «*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»<sup>1</sup>.

Государственный стандарт ГОСТ Р. 7.0.8-2013<sup>2</sup> также трактует понятие *электронной подписи* как информации в электронной форме, связанной с электронным документом, которая позволяет определять лицо, подписавшее электронный документ.

На сегодняшний день определение из ФЗ-63 считается устоявшимся определением электронной подписи, но нельзя не отметить, что оно конкретизировалось в результате развития правовых отношений в сфере электронного взаимодействия и развития информационных технологий. Первый федеральный закон об электронной цифровой подписи от 10.01.2002 (ФЗ-1) определял *электронную цифровую подпись* (ЭЦП) как реквизит электронного документа, который получен в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи. Это преобразование позволяло идентифицировать владельца сертификата ключа подписи и отслеживать искажения информации в электронном документе.

Исторически сложилось несколько понятий в области работы с электронной информацией. Кроме электронной подписи (ЭП), электронной цифровой подписи (ЭЦП) существует и такое равнозначное понятие, как *цифровая подпись* (ЦП). В любом случае, такая подпись связана как с автором, так и с самим электронным документом с помощью криптографических методов и не может быть подделана с помощью обычного копирования.

Говоря об электронной подписи, необходимо отметить, что это понятие появилось еще в 1976 году, когда Уитфилдом Диффи и Мартином

---

<sup>1</sup> Федеральный закон от 06.04.2011 № 63 – ФЗ (ред. от 08.06.2020) «Об электронной подписи» (с изм. и доп. от 01.07.2020), статья 2, пункт 1. [Электронный ресурс] URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_112701/](http://www.consultant.ru/document/cons_doc_LAW_112701/) (дата обращения 16.10.2020).

<sup>2</sup> ГОСТ Р.7.0.8-2013 СИБИД. Делопроизводство и архивное дело. Термины и определения. [Электронный ресурс] URL: <http://docs.cntd.ru/document/1200108447> (дата обращения 16.10.2020).

Хеллманом было впервые предложено понятие «электронная цифровая подпись»<sup>1</sup> в связи с разработкой схем электронного шифрования [48].

В России понятие электронной цифровой подписи впервые было прописано в 1994 году в ГОСТе 34.10-94<sup>2</sup> Федеральным агентством правительственной связи и информации при президенте Российской Федерации (ФАПСИ – существовал с 24.12.1991 по 11.03.2003). В данном и последующих стандартах этой группы «электронная цифровая подпись (signature) – строка бит, полученная в результате процесса формирования подписи....Строка бит, являющаяся подписью, может иметь внутреннюю структуру, зависящую от конкретного механизма формирования подписи»<sup>3</sup>

Федеральный закон об электронной подписи от 2011 года (ФЗ-63) разграничил электронную подпись на простую и усиленную, что дало возможность использовать ее и физическим лицам. Расширилась и сфера применения электронной подписи. Исследователи, эксперты в области использования электронной подписи, специалисты IT-компаний, преподаватели учебных центров и высших учебных заведений приводят характерные особенности для простой и усиленной подписи, условия ее применения [29, 32, 36, 38, 40].

Во-первых, простая электронная подпись (ПЭП) образуется как логин плюс пароль пользователя. ПЭП может выступать как СМС-код. Также этот код может быть записан на банковской карте.

Во-вторых, ПЭП может формировать сама система электронного взаимодействия, где эта подпись будет использоваться.

---

<sup>1</sup> Электронная подпись. История возникновения. [Электронный ресурс] URL: <https://ru.wikipedia.org/> (дата обращения 16.10.2020).

<sup>2</sup> ГОСТ 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма». [Электронный ресурс] URL: <https://intuit.ru/> (дата обращения 16.10.2020).

<sup>3</sup> ГОСТ 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». [Электронный ресурс] URL: <https://internet-law.ru/gosts/gost/70512/> (дата обращения 16.10.2020).

В третьих, получить простую электронную подпись может как физическое, так и юридическое лицо и срок действия такой подписи законодательно не ограничен.

Усиленная электронная подпись (УЭП) образуется путем шифрования данных. Криптографическое преобразование создает уникальную последовательность символов, защищающих УЭП от взлома.

УЭП подтверждает не только факт формирования подписи определенным лицом, но также позволяет обнаружить факт внесения изменений в документ после его подписания. УЭП в свою очередь подразделяется на неквалифицированную (УНЭП) и квалифицированную электронную подпись (УКЭП).

УКЭП выдается удостоверяющим центром, имеющим аккредитацию в Минкомсвязи России (с 11 сентября 2020 г. – Министерство цифрового развития, связи и массовых коммуникаций России) и использующем программное обеспечение, одобренное Федеральной службой безопасности России.

Электронной подписью подписываются *электронные сообщения* или *электронные документы*, подтверждая тем самым авторство лица, отправляющего это сообщение или электронный документ.

Понятие *электронного документа* прописано в Федеральном законе №149-ФЗ «Об информации, информационных технологиях и о защите информации»<sup>1</sup>. Выделено, что это «документированная информация, представленная в электронной форме, с использованием электронных вычислительных машин и пригодная для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах».

---

<sup>1</sup> Федеральный закон №149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», статья 2, пункт 11.1. [Электронный ресурс] URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](http://www.consultant.ru/document/cons_doc_LAW_61798/) (дата обращения 16.10.2020).

Более короткую и конкретную формулировку понятию электронного документа дает ГОСТ Р.7.08-2013. Под электронным документом понимается «документ, информация которого представлена в электронной форме».

Часто в зарубежных источниках под электронным документом (electronic document) понимается любой электронный контент, который предназначен для использования в электронном виде.

Чтобы документ был легитимен, имел юридическую значимость, он должен быть подписан. Для электронного документа это будет электронная подпись. Работа с электронными документами имеет свою специфику.

Движение электронных документов в организации с момента их создания или получения до завершения работы с ними составляет *электронный документооборот*. Электронный документооборот обеспечивается использованием автоматизированных информационных систем документооборота. Важным в этой сфере является применение электронного документооборота в органах государственной власти.

Информационная система, позволяющая федеральным, региональным, муниципальным органам власти обмениваться электронными документами и информацией, необходимыми для оказания государственных услуг гражданам и организациям, относится к *системам межведомственного электронного взаимодействия*.

## **1.2 Нормативно-законодательные и методические акты, регламентирующие создание и применение электронной подписи в России**

Предпосылки для развития такого правового понятия как, электронная подпись, заложил **Гражданский кодекс Российской Федерации**<sup>1</sup>. В *статье 160* сказано, что письменная форма сделки считается правомочной,

---

<sup>1</sup> Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред от 08.12.2020). [Электронный ресурс] URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_5142/](http://www.consultant.ru/document/cons_doc_LAW_5142/) (дата обращения 10.01.2021).

если сделка совершается лицом, использующим при этом электронные средства. Требование о наличии подписи считается выполненным, если можно достоверно определить лицо, подписавшее этот документ.

В **Налоговом кодексе Российской Федерации**<sup>1</sup> в *статье 11.2* прописывается, что для получения от налогового органа информации по налогам и сборам, налогоплательщики могут через личный кабинет получать эту информацию и отсылать в налоговый орган документы в электронной форме по оплате соответствующих налогов. Личный кабинет налогоплательщика позволяет распечатать электронные документы (уведомления о налогах), оплатить налоги непосредственно из личного кабинета или через терминал (если для оплаты используется распечатанный бумажный документ). При электронном взаимодействии физических лиц с налоговыми органами используется усиленная неквалифицированная электронная подпись. Эта подпись служит для идентификации лица, входящего в личный кабинет налогоплательщика. При электронном взаимодействии с налоговыми органами юридических лиц – используется усиленная квалифицированная подпись, которую можно приобрести в аккредитованном удостоверяющем центре. Перечень аккредитованных удостоверяющих центров приведен на портале Минцифры России.

В России первым документом, регламентирующим применение электронной подписи, был Федеральный закон «Об электронной цифровой подписи» от 2002 года, который затем был заменен **Федеральным законом «Об электронной подписи»**<sup>2</sup>. Развитие телекоммуникационных технологий, методов криптографической защиты информации способствовало разработке Федерального закона «Об электронной подписи» (далее – ФЗ-63) с

---

<sup>1</sup> Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 №146-ФЗ (ред. от 23.11.2020). [Электронный ресурс] URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_19671/](http://www.consultant.ru/document/cons_doc_LAW_19671/) (дата обращения 10.01.2021).

<sup>2</sup> Федеральный закон от 06.04.2011 № 63 – ФЗ (ред. от 08.06.2020) «Об электронной подписи» (с изм. 08.06.2020). [Электронный ресурс] URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_112701/](http://www.consultant.ru/document/cons_doc_LAW_112701/) (дата обращения 16.10.2020).

последующими редакциями и изменениями, а также постановлений, распоряжений Правительства РФ, приказов соответствующих министерств РФ, государственных стандартов РФ для применения электронной подписи.

Прежде всего, рассмотрим изменения в ФЗ-63, вступающие в силу с 1 января 2021 года.

Как было сказано ранее, усиленную электронную подпись формируют аккредитованные удостоверяющие центры. В новой редакции ФЗ-63 добавился *пункт 8.1* о введении доверенных третьих сторон (организаций). Одной из функций доверенных третьих сторон - проверка электронной подписи подписанта в определенный момент времени (*статья 1, п.17*). В этой же статье ФЗ-63 далее прописывается, что программные и аппаратные средства для проверки электронной подписи доверенной третьей стороной должны пройти процедуру подтверждения требованиям данного федерального закона. Аккредитацию как удостоверяющих центров, так и доверенных третьих сторон осуществляет уполномоченный федеральный орган. В настоящее время таким уполномоченным федеральным органом вместо Минкомсвязи РФ является Минцифры РФ.

Кроме того усилились требования и к удостоверяющим центрам: добавился пункт о соответствии требованиям деловой репутации руководителей и учредителей удостоверяющих центров; уставной фонд организации, выполняющей функции удостоверяющего центра должен быть не менее 1 млрд рублей.

Новым в ФЗ-63 является также то, что получить усиленную квалифицированную электронную подпись теперь можно с помощью биометрических данных, путем предоставления таких сведений из единой системы идентификации и аутентификации и единой системы персональных данных (*статья 4, пункт 7*). Квалифицированный сертификат в таком случае может быть выдан без личного присутствия гражданина. Собственно и на основе данных гражданина, полученных из единой системы персональных данных, также можно получить усиленную электронную подпись без

личного присутствия гражданина. Т.е. с 1 июля 2020 года получить усиленную электронную подпись можно тремя способами:

- посетить удостоверяющий центр лично;
- на основании действующей электронной подписи, срок действия которой заканчивается;
- на основании биометрических данных, содержащихся в единой системе идентификации и аутентификации и единой системе персональных данных.

В новой редакции ФЗ-63 усилились требования к защите информации (*статья 5*). Это касается требований:

- по хранению ключей квалифицированной электронной подписи;
- аутентификации владельцев квалифицированных сертификатов;
- защите информации, передаваемой по каналу взаимодействия;
- доказательству невозможности отказа владельца квалифицированного сертификата от поручения на создание усиленной квалифицированной электронной подписи.

Вопросы защиты информации и направления развития в формировании электронной подписи рассматривались на конференции РКІ – Форум 2020. Представитель ФСБ А. Бондаренко по теме облачной ЭП (законодательно это понятие не закреплено) предлагает взять на вооружение термин «удаленная ЭП» или «дистанционная ЭП» [28].

Создание и применение дистанционной электронной подписи и дистанционной идентификации пользователей в первую очередь затронет удостоверяющие центры. По мнению специалистов-аналитиков в сфере IT- технологии создания и использования электронной подписи технология дистанционной идентификации пользователей позволит не ездить за сертификатом в удостоверяющий центр, время получения сертификата сократится до нескольких минут. Но остается множество спорных моментов – доставка ключевых носителей, доставка криптографических средств, вопрос удержания удостоверяющими центрами своих клиентов и т.д. Кроме

того, носители электронной подписи как мобильное приложение, SIM- карта, токены, облачные решения также имеют недостатки. Возникает вопрос доверия к устройству, а значит к безопасности самих ключей, надежности идентификации пользователя [29, 35].

По мнению специалистов в сфере использования электронной подписи, введение изменений в ФЗ-63, может привести к ряду рисков [37]:

- риск нарушения правовых норм;
- риск нормативных коллизий с другими актами в рамках закона;
- риск коррупциогенности и др.

О документированной информации, представленной в электронной форме и пригодной для обработки в информационных системах, говорится и в **Федеральном законе №149-ФЗ «Об информации, информационных технологиях и о защите информации»**<sup>1</sup> (статья 2, пункт 11.1).

Документы в электронной форме, электронный документооборот используются практически во всех сферах деятельности. В финансовой деятельности первичные учетные документы могут составляться как на бумажном носителе информации, так и в виде электронного документа, подписанного электронной подписью, что прописано в **Федеральном законе «О бухгалтерском учете»**<sup>2</sup>, статье 9, пункте 5.

Регламентация вопросов в сфере предоставления государственных и муниципальных услуг, разъяснения по работе с порталом предоставления государственных и муниципальных услуг отражены в **Федеральном законе №210-ФЗ «Об организации предоставления государственных и**

---

<sup>1</sup> Федеральный закон №149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации». [Электронный ресурс] URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](http://www.consultant.ru/document/cons_doc_LAW_61798/) (дата обращения 16.10.2020).

<sup>2</sup> Федеральный закон от 06.12.2011 №402-ФЗ «О бухгалтерском учете» (ред. от 26.07.2019). [Электронный ресурс] URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_122855/](http://www.consultant.ru/document/cons_doc_LAW_122855/) (дата обращения 17.11.2020).

муниципальных услуг»<sup>1</sup> (далее ФЗ-210). В данном законе прописано, что для обращения по вопросу предоставления государственных или муниципальных услуг можно воспользоваться единым порталом, который осуществляет электронное взаимодействие между государственными органами, органами местного самоуправления и заявителем, предоставляя государственные и муниципальные услуги в электронной форме. В *статье 2 пунктах 9, 10* подчеркивается, что межведомственное информационное взаимодействие осуществляется документами и информацией также и в электронной форме. И далее, в *статье 6* данного закона сказано, что органы, предоставляющие государственные или муниципальные услуги обязаны обеспечивать возможность получения заявителем требуемой услуги в электронной форме (если это не запрещено законодательством России).

**Постановление Правительства РФ от 25.06.2012 № 634 «О видах электронной подписи, использование которых допускается при обращении за получением государственных или муниципальных услуг»<sup>2</sup>** было принято во исполнение ФЗ-210. В этом Постановлении прописано, что при обращении за получением государственных и муниципальных услуг допускается использование простой электронной подписи и усиленной квалифицированной электронной подписи. Постановление утвердило и **Правила определения видов электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг**. В соответствии с Правилами<sup>3</sup> пакет электронных

---

<sup>1</sup> Федеральный закон от 27.07.2010 №210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (ред. от 30.12.2020). [Электронный ресурс] URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_103023/01fbae25b3040955277cbd70aa1b907cceda878e/](http://www.consultant.ru/document/cons_doc_LAW_103023/01fbae25b3040955277cbd70aa1b907cceda878e/) (дата обращения 13.01.2021).

<sup>2</sup> Постановление Правительства РФ от 25.06.2012 № 634 «О видах электронной подписи, использование которых допускается при обращении за получением государственных или муниципальных услуг». [Электронный ресурс] URL: <https://www.consultant.ru/cons/cgi/> / (дата обращения 17.11.2020).

<sup>3</sup> Правила определения видов электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг. Утверждены Постановлением

документов, прилагаемых к заявлению за получением государственной или муниципальной услуги, подписывается тем видом электронной подписи, допустимость использования которой установлена федеральными законами, которые регламентируют вопросы использования электронной подписи. В данных Правилах имеется ссылка на приложение (таблица 1), в котором приводятся критерии определения видов электронной подписи при обращении гражданином или юридическим лицом за получением государственных или муниципальных услуг.

Таблица 1. Критерии для определения вида электронной подписи при обращении за получением государственных или муниципальных услуг

| Виды электронных документов, представляемых заявителем при обращении за предоставлением государственной или муниципальной услуги                       | Виды используемой электронной подписи                                                                                                             |                                                                                                                                                                                                                              |                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|                                                                                                                                                        | Если содержание государственной, муниципальной услуги не предусматривает выдачу документов и (или) состоит в предоставлении справочной информации | Если процедура предоставления государственной, муниципальной услуги предусматривает необходимость обязательного личного присутствия заявителя (его представителя, с предъявлением документа, подтверждающего его полномочие) | В остальных случаях |
| 1                                                                                                                                                      | 2                                                                                                                                                 | 3                                                                                                                                                                                                                            | 4                   |
| 1. Документы, формируемые заявителем:                                                                                                                  |                                                                                                                                                   |                                                                                                                                                                                                                              |                     |
| 1.1. Запрос заявителя                                                                                                                                  | ПЭП                                                                                                                                               | ПЭП                                                                                                                                                                                                                          | УКЭП                |
| 1.2. Согласие заявителя на обработку информации, которая связана с его законными правами и интересами и доступ которой ограничен федеральными законами | ПЭП                                                                                                                                               | ПЭП                                                                                                                                                                                                                          | УКЭП                |

| 1                                                                                                                     | 2    | 3    | 4    |
|-----------------------------------------------------------------------------------------------------------------------|------|------|------|
| 1.3. Документы, указанные в части 3 статьи 7 ФЗ «Об организации предоставления государственных и муниципальных услуг» | УКЭП | УКЭП | УКЭП |
| 1.4. Документы в электронной форме, информация о которых необходима для предоставления услуги                         | УКЭП | УКЭП | УКЭП |

В Правилах также прописано, что если установлена возможность подачи документов, подписанных простой электронной подписью, то для получения государственной или муниципальной услуги можно воспользоваться и усиленной электронной подписью.

Анализ Правил определения видов электронной подписи показывает сложность толкования и неопределенность отнесения использования вида электронной подписи для получения государственной или муниципальной услуги, если нужно не просто сделать запрос, а получить конкретный комплект документов, затрагивающих права заявителя. Даже после редакции в 2018 году Постановления, утвердившего Правила определения видов электронной подписи, в новой редакции Правил добавляется отсылка к Административному регламенту по предоставлению услуги, из которого нужно еще понять, какой вид подписи использовать заявителю для получения необходимой услуги.

**Постановление Правительства РФ от 25.01.2013 № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг»<sup>1</sup>** внесло изменения в требования к регистрации в федеральной государственной информационной

<sup>1</sup> Постановление Правительства РФ от 25.01.2013 № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг». [Электронный ресурс] URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=373175&dst=1000000001%2C0#05568395865159432> (дата обращения 12.01.2021).

системе «Единый портал государственных и муниципальных услуг». Гражданам, зарегистрировавшимся в системе идентификации и аутентификации для предоставления государственных и муниципальных услуг в электронной форме, в качестве ключа простой электронной подписи можно использовать страховой номер индивидуального лицевого счета (ИНН) и пароль, сформированный при регистрации. В Правилах использования простой электронной подписи при оказании государственных и муниципальных услуг, утвержденных вышеназванным Постановлением, сказано, что «*простой электронной подписью* является электронная подпись, которая посредством использования ключа простой электронной подписи (далее – ключ) подтверждает факт формирования электронной подписи конкретным заявителем» (*статья 2*). Ключом ЭП является объединение (ИНН) и пароля. Создание или замена ключа осуществляется сервисом системы ЕСИИА (Единая система идентификации и аутентификации).

**Правила обмена документами в электронном виде при организации информационного взаимодействия, утвержденных постановлением Правительства Российской Федерации от 25 декабря 2014 г. N 1494<sup>1</sup>** установили порядок информационного взаимодействия органов исполнительной власти различного уровня и государственных внебюджетных фондов посредством обмена документами в электронном виде. В этих Правилах обмена говорится, что единицами передачи информации является *транспортный контейнер документа в электронном виде* или *технологическое электронное сообщение*. Приводится состав транспортного контейнера, состоящий из нескольких файлов (рисунок 1).

---

<sup>1</sup> Правила обмена документами в электронном виде при организации информационного взаимодействия. Утверждены Постановлением Правительства Российской Федерации от 25 декабря 2014 г. N 1494. [Электронный ресурс] URL: <https://base.garant.ru/70832680/#friends> (дата обращения 17.11.2020).

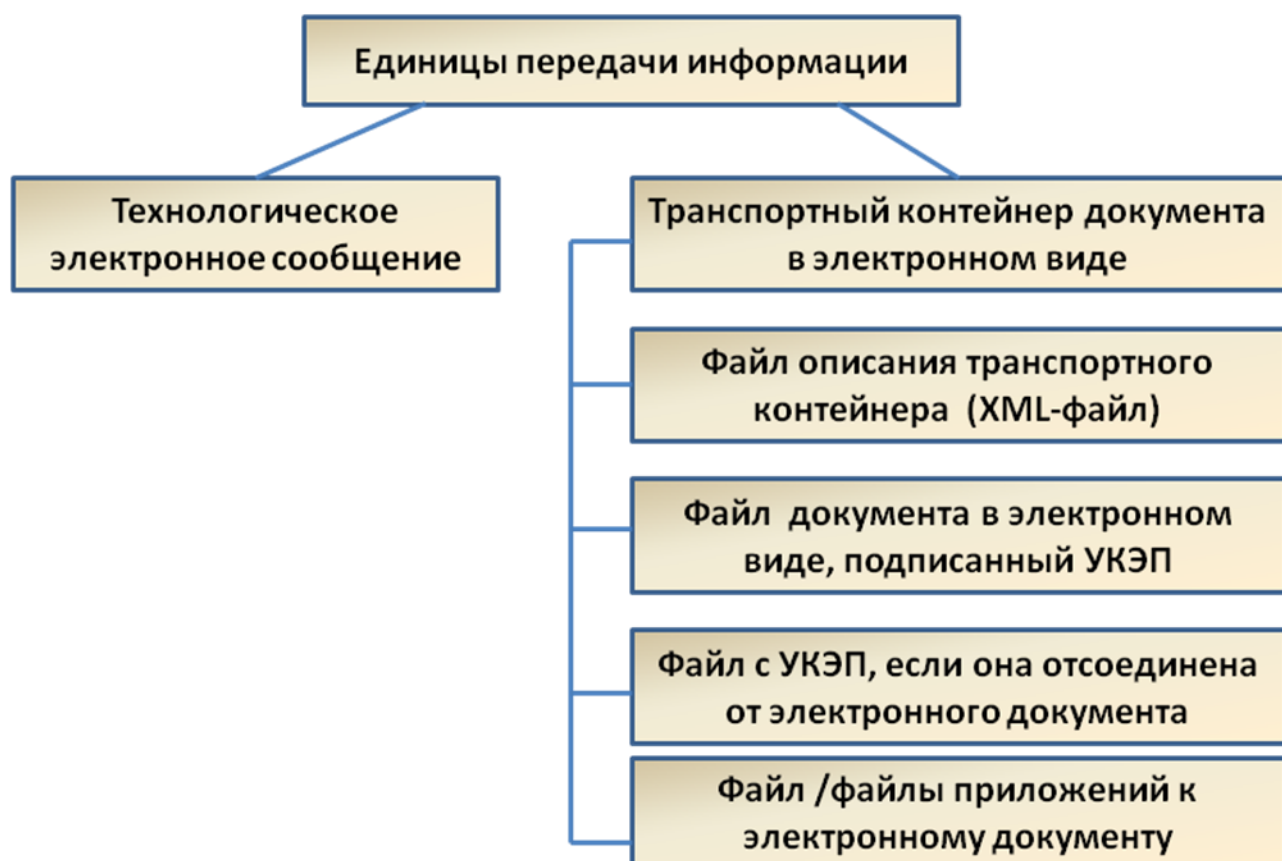


**Рисунок 1 – Единицы передачи информации при электронном обмене**

В транспортный контейнер обязательно входит xml- файл с его описанием, также файл электронного документа, подписанный УКЭП. Если УКЭП сформирована на отдельном файле, то в транспортном контейнере загружаются отдельно два файла: с УКЭП и с документом.

Если к электронному документу есть приложения, то они также входят в контейнер отдельными файлами.

В Правилах обмена сказано, что состав и структура файла описания транспортного контейнера определяется в соответствии с положениями и регламентами эксплуатации транспортной шины. Транспортной шиной может быть или специализированная защищенная информационно-коммуникационная магистраль, или совокупность взаимосвязанных сегментов информационно-телекоммуникационных сетей общего назначения, если они соответствуют требованиям законодательства Российской Федерации в области информационной безопасности.

Для государственных органов и государственных учреждений формат документа в электронном виде определяется Министерством цифрового развития, связи и массовых коммуникаций РФ, а также Федеральной службой охраны РФ.

В Правилах обмена документами в электронном виде также регламентированы процедуры обмена документами в СЭД. Прежде всего это процедура формирования отправителя документа в виде транспортного контейнера. Также прописывается процесс переноса транспортного контейнера от отправителя к получателю при различных вариантах информационного взаимодействия отправителя и получателя (защищенная шина, сеть общего пользования). В системе обмена важной является процедура проверки транспортного контейнера на целостность и отсутствие вирусов. Последней процедурой является извлечение из транспортного контейнера необходимых файлов и формирование для отправителя уведомления о приеме документов, либо об отказе в их регистрации.

Порядок взаимодействия в системах межведомственного взаимодействия был еще заложен в 2009 году, когда было принято **Положение о системе межведомственного электронного документооборота**<sup>1</sup>. В данном Положении определено взаимодействие информационных систем электронного документооборота органов государственной власти на федеральном, региональном уровнях, государственных организаций Российской Федерации. Следует заметить, что в этом документе сказано, что взаимодействие информационных систем осуществляется за счет обмена *электронными сообщениями*. Для своего времени это был важный документ, определивший основные принципы межведомственного электронного документооборота (*статья 6*),

---

<sup>1</sup> Положение о системе межведомственного электронного документооборота. Утверждено Постановлением Правительства Российской Федерации от 22.09.2009 №754 (ред. от 16.03.2019). [Электронный ресурс] URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=320535&dst=1000000001%2C0#030227832722794856/> (дата обращения 17.11.2020).

технологическую инфраструктуру (*статья 7*), технические средства и основные функции головного узла - организатора межведомственного электронного документооборота (*статьи 8, 9*). Также в этом Положении указаны основные функции и технические средства узла участника межведомственного электронного взаимодействия (*статьи 10, 11*).

Настройку технических средств, средств защиты, установку специального программного обеспечения осуществляет организатор межведомственного электронного документооборота. И здесь нужно отметить, что если нет единого стандарта по техническим средствам межведомственного взаимодействия, то могут быть разногласия в оценке правомочности подписания электронного документа УКЭП.

Электронный документооборот может быть реализован на различных уровнях: межведомственный, корпоративный, внутренний.

По мнению многих авторов (Ермолаева А.В., Ульяновца С.Э., М.П. Бобылева, С.Л. Кузнецов и др.) системы электронного документооборота прочно вошли в документационное обеспечение управления организаций различного уровня: от коммерческой организации до государственной структуры [27, 30, 31, 32, 34, 38].

В целях совершенствования делопроизводства в государственных органах власти, повышения эффективности работы с электронными документами, однозначности толкования процедур организации работы с документами, взамен Правил от 2009 года были разработаны и утверждены приказом Росархива № 71 в 2019 году **Правила делопроизводства в государственных органах, органах местного самоуправления**<sup>1</sup>. Действие этих правил распространяется не только на организационно-распорядительную документацию, но и на бухгалтерскую, кадровую и

---

<sup>1</sup> Правила делопроизводства в государственных органах, органах местного самоуправления, утвержденных приказом Росархива от 22 мая 2019 г. № 71. [Электронный ресурс] URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_342093/](http://www.consultant.ru/document/cons_doc_LAW_342093/) (дата обращения 11.01.2021).

другую документацию в части общих принципов работы с документами и подготовки документов к архивному хранению.

Анализ этого документа в сравнении со старыми Правилами от 2009 года показывает, что в Правилах от 22 мая 2019 г. указываются ссылки на другие нормативные законодательные или методические документы, регламентирующих организацию работы с документами; требования к их оформлению. Также указываются ссылки на нормативный документ, статью или пункт этого документа, на основании чего был введен тот или иной пункт в разделы Правил. В Правилах от 2019 года в разделе «Документирование управленческой деятельности» (*пункт 2.10*) подчеркнуто обязательность подписания усиленной квалифицированной подписью руководителем электронных документов, направляемых в государственные органы и органы местного самоуправления.

В сфере архивного дела и делопроизводства главенствующая роль принадлежит Росархиву. Росархив осуществляет функции по выработке и реализации государственной политики и по нормативно-правовому регулированию в сфере делопроизводства и архивного дела.

Росархив разрабатывает, утверждает правила делопроизводства для государственных органов и органах местного самоуправления. В его компетенцию входит разработка типовых требований к обеспечению хранения электронных документов в архивах государственных органов, к изданию и утверждению соответствующих нормативных и методических документов.

**Приказ Росархива от 15.06.2020 №69 «Об утверждении Типовых функциональных требований к системам электронного документооборота и системам хранения электронных документов в архивах государственных органов»<sup>1</sup>** утвердил типовые функциональные

---

<sup>1</sup> Приказ Росархива от 15.06.2020 №69 «Об утверждении Типовых функциональных требований к системам электронного документооборота и системам хранения электронных документов в архивах

требования к системам электронного документооборота (СЭД) и системам архивного хранения документов (СХЭД) в государственных органах. Эти требования не касаются процессов создания СЭД или СХЭД, не регламентируют требования к интерфейсу автоматизированных рабочих мест пользователей СЭД, СХЭД. Естественно, Типовые функциональные требования к СЭД и СХЭД не распространяются на работу с документами, содержащими государственную тайну. Анализируя приведенные в третьем разделе функциональные требования к управлению документами в СЭД государственного органа, делаем вывод, что в соответствии с требованиями СЭД должна обеспечивать возможность управления электронными документами и электронными копиями документов. Система должна иметь возможность создавать, хранить, передавать документы в электронном виде. При работе с электронным документом, система должна осуществлять проверку подлинности электронной подписи и формировать уведомление отправителю документа об отказе в регистрации, в случае отрицательных результатов проверки электронной подписи.

Также анализ Типовых требований показал, что в этом документе также имеются ссылки на нормативные акты, на основании которых готовился текст этих требований.

Перечень причин отказа в регистрации документа определены **Требованиями к организационно-техническому взаимодействию государственных органов и государственных организаций посредством обмена документами в электронном виде<sup>1</sup>**. Это может быть:

- нарушение комплектности;
- недействительность электронной подписи;

---

государственных органов». [Электронный ресурс] URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_365612/](http://www.consultant.ru/document/cons_doc_LAW_365612/) (дата обращения 11.01.2021).

<sup>1</sup> Требования к организационно-техническому взаимодействию государственных органов и государственных организаций посредством обмена документами в электронном виде. Утвержден приказом Минкомсвязи РФ и Федеральной службы охраны РФ от 27 мая 2015 г. № 186/158. [Электронный ресурс] URL: [https://base.garant.ru/71199902/#block\\_1132](https://base.garant.ru/71199902/#block_1132) (дата обращения 17.12.2020).

- неверные данные подписанта документа, не совпадающие с данными в сертификате электронной подписи документа;
- неверное наименование организации – отправителя транспортного контейнера, не совпадающие с данными, указанными в сертификате электронной подписи документа;
- несоответствие формата файла документа формату PDF/A-1.

В данных Требованиях приведены и требования к электронной подписи. Сказано, что при создании усиленной квалифицированной подписи должен использоваться формат RKCS#7 (Public-Key Cryptography Standard #7), указан [http](#) адрес общего описания стандарта RKCS#7. Также приведено такое требование, что электронные подписи должностных лиц, при обмене документами в электронном виде, должны формироваться в отдельных файлах.

В Требованиях указано о формате передачи документов. В контейнере документы могут быть представлен в формате ZIP-папки, куда входит один, или несколько файлов. Пояснено, что возможно преобразование содержимого транспортного контейнера из одного вида представления в другой в процессе его создания, обработки и хранения. Однозначно определено только имя файла описания транспортного контейнера и вариант его кодировки. Файл должен иметь имя – `Passport.xml`, кодировка восьмибитная - UTF-8.

Если используется межведомственное электронное взаимодействие, в данном случае рекомендуется отправителем формировать один файл для транспортного контейнера.

Необходимо отметить, что все три документа: Правила обмена документами в электронном виде при организации информационного взаимодействия, Требования к организационно-техническому взаимодействию государственных органов и государственных организаций посредством обмена документами в электронном виде, Типовые функциональные требования к системам электронного документооборота и

системам хранения электронных документов в архивах государственных органов разрабатывались с учетом национальных и зарубежных стандартов в сфере криптографической защиты информации.

Помимо рассмотренных выше нормативных актов в сфере использования электронной подписи, нужно сказать о государственных стандартах, на основании чего электронная подпись создается, проверяется и оформляется при выводе электронного документа в бумажную форму.

В связи с повышением уровня развития средств вычислительной техники взамен ГОСТа Р 34.10-94 был разработан **ГОСТ Р 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»<sup>1</sup>**. На тот момент времени применяемые алгоритмы шифрования не обеспечивали в полной мере криптографическую защиту передаваемой информации. Создаваемые ключи не обеспечивали требуемый уровень защиты. Поэтому необходимо было описать новые методы и алгоритмы шифрования для создания и проверки цифровой подписи. Утвержденный в 2018 году стандарт регламентировал процессы по созданию и проверке цифровой подписи и ключа подписи.

**ГОСТ 34.11-2018. Информационная технология. Криптографическая защита информации. Функция хэширования<sup>2</sup>** прописывает методы и алгоритм криптографической защиты информации, подробно рассматривая современные подходы по реализации шифрования данных.

---

<sup>1</sup> ГОСТ Р 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». [Электронный ресурс] URL: <https://internet-law.ru/gosts/gost/70512/> (дата обращения 17.11.2020).

<sup>2</sup> ГОСТ Р 34.11-2018 «Информационная технология. Криптографическая защита информации. Функция хэширования». [Электронный ресурс] URL: <https://internet-law.ru/gosts/gost/70512/> (дата обращения 17.11.2020).

Эти и другие стандарты 34 группы по криптографической защите информации были разработаны с учетом терминологии и концепций международных стандартов ИСО 2382, ИСО/МЭК 14888 и ИСО/МЭК 10118.

Правила оформления электронной подписи в делопроизводстве регламентирует ГОСТ Р 7.0.97-2016. **Национальный стандарт Российской Федерации. СИБИД. Организационно-распорядительная документация. Требования к оформлению документов**<sup>1</sup>. Для оформления электронной подписи на бумажном документе ГОСТом был установлен реквизит *отметка об электронной подписи*. В схеме размещения реквизитов на документе определено место размещения отметки об электронной подписи на документе и отображение элементов электронной подписи при предварительном просмотре или печати электронного документа.

В реквизите отметка об электронной подписи обязательно должны быть приведены:

- фраза «Документ подписан электронной подписью»;
- номер сертификата ключа электронной подписи;
- фамилия, имя, отчество владельца сертификата;
- срок действия сертификата ключа электронной подписи.

В реквизит отметка об электронной подписи может быть включено изображение герба, эмблемы или товарного знака организации в соответствии с действующим законодательством.

При выводе электронного документа на печать реквизит отметка об электронной подписи печатается на месте рукописной подписи. Информация реквизита выводится на бумажный документ в виде штампа.

Элементы отметки об электронной подписи должны быть видимыми и читаемыми при отображении документа в натуральном размере, не должны

---

<sup>1</sup> ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов (утв. Приказом Росстандарта от 08.12.2016 N 2004-ст) (с изм. от 14.05.2018).

перекрываться или накладываться друг на друга, а также не должны перекрывать элементы текста документа.

### **1.3 Анализ зарубежных нормативных актов в сфере использования электронной подписи**

Электронная подпись прочно укрепилась за рубежом с конца 20 века. Этому способствовало, прежде всего, развитие электронной торговли. Генеральная Ассамблея ООН, ссылаясь на правовое значение записей на ЭВМ, принятую Комиссией ООН еще в 1985 году, приняла решение о разработке Типового закона об электронной торговле.

В 1996 году был разработан **Типовой закон ЮНСИТРАЛ «Об электронной торговле»<sup>1</sup>**, сферой применения которого стал любой вид информации в форме *сообщения данных*, используемых в контексте торговой деятельности. Здесь, под сообщением данных понимается информация, подготовленная, полученная или хранимая с помощью «электронных, оптических или аналогичных средств, включая электронный обмен данными (ЭДИ), электронную почту, телеграмму, телекс или телефакс, но не ограничиваясь ими» (*статья 2, пункт а*).

Под электронным обменом данными в этом Типовом законе понимается электронная передача информации с одного компьютера на другой, с использованием «согласованного стандарта структуризации информации» (*статья 2, пункт b*).

В данном Типовом законе в *статье 5* прописано признание юридической силы сообщений данных. Сказано, что информация не может быть лишена юридической силы на том лишь основании, что она составлена в форме сообщения данных.

---

<sup>1</sup> Типовой закон ЮНСИТРАЛ «Об электронной торговле». Принят в г. Нью-Йорке 28.05.1996. [Электронный ресурс] URL: [https://www.uncitral.org/pdf/russian/texts/electcom/05-89452\\_Ebook.pdf](https://www.uncitral.org/pdf/russian/texts/electcom/05-89452_Ebook.pdf) (дата обращения 11.01.2021).

В *статье 7* Типового закона говорится, что требование наличия подписи лица в отношении сообщения данных выполняется, если:

«а) использован какой-либо способ для идентификации этого лица и указания на то, что это лицо согласно с информацией, содержащейся в сообщении данных;

б) этот способ является как надежным, так и соответствующим цели, для которой сообщение данных было подготовлено или передано с учетом всех обстоятельств, включая любые соответствующие договоренности».

Анализ данного Типового закона позволяет сделать вывод, что он рекомендует признавать доказательственную силу сообщений данных. Информация не может быть лишена юридической силы только на том основании, что она составлена в форме сообщения данных. Кроме того допускается использование любого способа для идентификации составителя сообщения данных, при условии, что этот способ надежен и соответствует цели, для которой это сообщение было подготовлено.

**Типовой закон ЮНСИТРАЛ «Об электронных подписях и Руководство по применению»<sup>1</sup>** был разработан для использования в контексте торговой деятельности. *Статьей 2* данного Типового закона понятие *электронная подпись* трактуется как данные в электронной форме, содержащиеся в сообщении данных, приложены к этому сообщению или логически ассоциируются с ним и которые могут быть использованы для идентификации подписавшего «в связи с сообщением данных и указания на то, что подписавший согласен с информацией, содержащейся в сообщении данных».

В этом Типовом законе *статьей 2* вводится понятие *сертификат*: «сообщение данных или иную запись, подтверждающую наличие связи между подписавшим и данными для создания подписи».

---

<sup>1</sup> Типовой закон ЮНСИТРАЛ «Об электронных подписях и Руководство по применению». Принят в г. Нью-Йорке 12.12.2001. [Электронный ресурс] URL: <https://www.uncitral.org/pdf/russian/texts/electcom/ml-elecsig-r.pdf> (дата обращения 11.01.2021).

Надежность электронной подписи согласно *статьи 6* данного Типового закона подтверждается, если выполняются следующие требования:

«а) данные для создания электронной подписи в том контексте, в котором они используются, связаны с подписавшим и ни с каким другим лицом;

б) данные для создания электронной подписи в момент подписания находились под контролем подписавшего и никакого другого лица;

с) любое изменение, внесенное в электронную подпись после момента подписания, поддается обнаружению».

Услуги для подкрепления электронной подписи предоставляет поставщик сертификационных услуг.

Положения этих Типовых законов об электронной торговле и об электронных подписях были использованы для разработки единообразных законодательных актов в ряде стран: Австралии, Италии, Франции, Дании и других [44, 48].

Алгоритмы построения цифровой подписи, методы и способы шифрования и криптографической защиты информации регламентируются стандартами [25, 26].

В США законом, регулирующим электронную подпись, стал Единый закон об электронных транзакциях (UETA). Этот закон ориентирован на электронную коммерцию, с электронными подписями связаны только юридические лица. В 2000 году в США был принят федеральный Закон об электронных подписях в международной и внутригосударственной торговле (ESIGN)<sup>1</sup>. Статьи этого закона распространяются на физических и юридических лиц. Электронная подпись в США, подтвержденная щелчком мыши, имеет одинаковый правовой статус с рукописной подписью.

В Канаде с 2004 года использование электронной подписи регламентируется федеральным Законом о защите личных сведений и

---

<sup>1</sup> The Electronic Signatures in Global and National Commerce Act (E-Sign Act)]. *Federal Deposit Insurance Corporation*.

электронных документов (PIPEDA)<sup>1</sup>. Отдельный город, как Квебек использует в сфере применения электронной подписи Закон о создании правовой основы для информационных технологий, который не приравнивает в полной мере в правовом отношении электронную и рукописную подпись.

С 1 июля 2016 года в странах Евросоюза начал работать регламент eIDAS (electronic IDentification, Authentication and trust Services)<sup>2</sup> в соответствии с европейским законом eIDAS – законом «Об электронной идентификации и услугах доверия для электронных транзакций на внутреннем рынке». Закон eIDAS заменил европейскую Директиву от 1999 года об электронных подписях. Этот закон регламентирует обязательное использование высокозащищенного устройства для создания подписи [40, 42]. Закон регламентирует и деятельность удостоверяющих центров. Усиленные электронные подписи на основе квалифицированных сертификатов (в соответствии с законом eIDAS), будут использоваться в банковских и финансовых операциях, использующих электронную подпись. eIDAS устанавливает единый стандарт, которому должно соответствовать аппаратное и программное обеспечение для генерации цифровых подписей. С сентября 2018 года взаимное признание электронных идентификаторов стало обязательным для стран Евросоюза.

Развертывание международной электронной коммерции способствует прогрессу в развитии экономики стран, заставляет конкретизировать положения в нормативных законодательных актах в сфере использования электронной подписи.

#### **Выводы по результатам исследования:**

1. В нормативных актах Российской Федерации используется различные определения для электронного документа (электронное сообщение, документ в электронном виде, электронный документ).

---

<sup>1</sup> Personal Information Protection and Electronic Documents Act . *Justice Laws Website*.

<sup>2</sup> Регламент Евросоюза №910/2014 URL: <http://rusrim.blogspot.com/2018/02/eidas-etsi.html>

2. Эксперты РКІ-Форума 2020 считают, что не хватает системности, работа по нормативно-правовому и нормативно-техническому регулированию в сфере применения электронной подписи должна быть синхронизирована и не должна дублироваться. До сих пор в российском законодательстве остаются проблемой вопросы идентификации и аутентификации..

3. Нет нормативного документа, регламентирующего технологии проверки архивных ЭП.

4. Необходима доработка ряда подзаконных актов, касающихся сферы применения электронной подписи, например, корректировку *статьи 189* Гражданского кодекса РФ «Последствия прекращения доверенности», поскольку по доверенности можно получать сертификат ключа электронной подписи в удостоверяющем центре.

5. Различия в законодательствах разных стран в сфере электронного документооборота служат причиной юридической неопределенности в отношениях сторон. В частности, согласно *статье 1209* Гражданского кодекса РФ форма сделки подчиняется праву места ее совершения. Однако при заключении сделки путем обмена электронными документами бывает проблематично установить место ее совершения.

## **2 Исследование опыта использования электронной подписи в России и за рубежом**

В первоначальном своем понимании цифровая подпись была связана с понятием «электронное сообщение». В результате развития информационных технологий и средств вычислительной техники, были введены понятия «электронная подпись» и «электронный документ». Тем не менее, в современных государственных и международных стандартах осталась предыдущая терминология, поэтому в дальнейшем исследовании также будем использовать термины «цифровая подпись», «электронное сообщение».

### **2.1 Технологии создания и использования электронной подписи в России**

Электронная подпись предназначена для аутентификации лица, подписывающее электронное сообщение.

Согласно Положению о межведомственном электронном документообороте электронное сообщение состоит из сопроводительной и содержательной частей. Сопроводительная часть сообщения служит для адресации сообщения, а содержательная – для текста сообщения. К тексту сообщения могут быть присоединены файлы, содержащие электронный образ документа, или электронный документ и их реквизиты, описанные с помощью языка XML. По требованиям этого Положения формат файлов должен соответствовать национальным или международным стандартам, либо иметь открытый исходный код и открытую структуру.

По российским и международным стандартам общепризнанная модель цифровой подписи охватывает следующие процессы [18]:

- генерация ключей подписи;
- формирование подписи;

– проверка подписи.

Способы реализации процесса генерации ключей определяются вовлеченными в процесс электронного взаимодействия субъектами, которые устанавливают соответствующие параметры взаимодействия по взаимному согласованию.

Сообщение пользователя, подписываемое цифровой подписью, будет состоять из сообщения и дополнения, являющегося частью сообщения. Подписание сообщение можно представить в виде рисунка 2 [18]:



Рисунок 2 – Схема подписания сообщения

Под сообщением (message) понимается строка бит произвольной конечной длины. Подписанное сообщение (signed message) понимается как набор элементов данных, состоящий из сообщения и дополнения, являющегося частью сообщения. Дополнение (appendix) – это строка бит, формируемая из цифровой подписи и произвольного текстового поля.

Сообщение пользователя  $M$  принадлежит множеству всех двоичных векторов произвольной конечной длины  $V^*$ :

$$M \in V^* \quad (1)$$

На рисунке 2 цифровая подпись под сообщением  $M$  обозначается как  $\xi$ .

Поле «Текст» и дополняющее поле «Цифровая подпись  $\xi$ » может содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени.

Для рисунка 2 схема цифровой подписи будет реализована с использованием операций группы точек эллиптической кривой, определенной над конечным простым полем, а также хэш-функции [18, 19].

В стандартах 34 группы приведено обоснование криптографической стойкости подобной схемы подписания, описаны базовые математические объекты, используемые в процессе формирования подписания и проверки цифровой подписи. Также приведены параметры цифровой подписи, требования к этим параметрам. Приведен алгоритм вычисления хэш-функции, обеспечивающей криптографическое преобразование данных.

Механизм цифровой подписи под сообщением пользователя определяется посредством реализации следующих основных процессов:

- формирование подписи;
- проверка подписи.

Для реализации данных процессов необходимо, чтобы всем пользователям электронного взаимодействия были известны параметры схемы цифровой подписи (модуль эллиптической кривой, функция этой кривой, хэш-функция, ключ подписи и другие показатели) [18].

Исходными данными для процесса формирования цифровой подписи являются ключ подписи  $d$  и подписываемое сообщение  $M$ . Выходным результатом – цифровая подпись  $\xi$ .

Исходными данными для процесса проверки цифровой подписи являются подписываемое сообщение  $M$ , цифровая подпись  $\xi$  и ключ проверки подписи  $Q$ . Выходным результатом – свидетельство о достоверности или ошибочности данной подписи.

Конкретный алгоритм генерации параметров схемы цифровой подписи определяется субъектами схемы, исходя из требований к аппаратно-программным средствам, реализующим электронный документооборот.

## **2.2 Зарубежный опыт использования электронной подписи**

Почти весь документооборот за рубежом строится с использованием электронной подписи.

Предложенный в 1991 году стандарт цифровой подписи (digital signature standard), был ориентирован на использование электронной подписи преимущественно в документообороте государственных органов власти США. Создание электронной подписи по данному стандарту осуществлялось с помощью симметричного шифрования. Этот подход предполагает наличие единого зашифрованного ключа электронной подписи, которым владеют как отправитель, так и получатель документов. По мнению специалистов в области применения электронной подписи, симметричная система шифрования увеличивает вероятность утраты ключа, поэтому на государственном уровне этот стандарт закреплён не был [39].

Развитие технологий применения электронных подписей в США позволило использовать другую модель, когда к электронной подписи прилагается отдельный файл – сертификат. В сертификат занесена информация о владельце электронной подписи, об организации, выдавшей сертификат и открытый ключ. В системе обмена электронными документами получателем сначала проверяется сертификат, потом с помощью открытого ключа проверяется электронная подпись на электронном документе. Инфраструктура открытых ключей, по мнению многих разработчиков технологии использования электронной подписи, гарантирует достоверность, целостность и конфиденциальность электронных сообщений. Представление сертификата электронной подписи в электронном виде увеличивает скорость документооборота, снижает ряд затрат технического характера.

Кроме того, в США есть практика простого уравнивания собственноручной и электронной подписей, полагаясь на судей [39,48].

В Китае на данный момент времени для каждой провинции может действовать своя система применения электронной подписи. Из-за отсутствия в стране единой нормативной базы имеются проблемы по информационному взаимодействию. Кроме того, нет единой системы удостоверяющих центров для всей страны.

Если в США есть практика простого уравнивания собственноручных и электронных подписей, полагаясь на судей, то в Китае судьи не обладают такими правами. При формировании электронной подписи в Китае используются как симметричная, так и асимметричная системы. Чаще используется инфраструктура открытых ключей, служащая для функционирования асимметричной системы.

В Австралии электронная подпись, как и в Китае, является одной из составляющих бизнеса. Аналитики в области использования электронной подписи в Австралии выделяют открытую, закрытую модели документооборота, а также открытую, но ограниченную. По мнению аналитиков (Гомалеев А., Фураков А, Храмцовская Н.) в открытой модели документооборота достаточно простого обмена ключами, в закрытой модели необходимо предварительное соглашение сторон. В третьей модели (открытой, но ограниченной), между участниками электронного взаимодействия, находится посредник – удостоверяющий центр.

В Тунисе, в отличие от Австралии, по законодательству необходима обязательная аккредитация всех удостоверяющих центров страны. Удоверяющие центры в Тунисе подчиняются Национальному Агентству по Электронной Сертификации (NAES), которое в свою очередь, подчинено Министерству телекоммуникаций [39]. Таким образом, в Тунисе высокая степень защиты электронной подписи уже определена на государственном уровне. Также предусматриваются разграничения ответственности удостоверяющего центра и владельца электронной подписи, предусматриваются финансовые гарантии и защиту от несанкционированного доступа.

Европа считается регионом, где наиболее развит электронный документооборот, использующий модель открытую, но ограниченную. Такая модель предполагает наличие удостоверяющего центра.

Наиболее развит подход к использованию электронной подписи и межведомственному электронному взаимодействию, по мнению участников форума PKI-2020 в Сингапуре [28]. В частности, в Сингапуре создается открытая цифровая платформа для участников внешнеэкономической деятельности, позволяющая сервис-провайдерам размещать и продвигать сервисы по логистике, перевозке, страхованию, таможенным операциям, взаимодействию с государственными органами, предоставлению отчетности. Цифровая платформа электронного взаимодействия в этой стране строится с использованием инфраструктуры открытых ключей (PKI) и на основе международных стандартов.

В Южной Корее уже давно ведутся работы по упрощению трансграничного безбумажного документооборота. В частности, чтобы реализовать трансграничные безбумажные сервисы, группа компаний по безбумажной торговле (KTNET) сотрудничает с Паназиатским альянсом электронной коммерции (Pan Asian E-Commerce Alliance, PAA) – объединением сервис-провайдеров в сфере трансграничной безбумажной торговли. В настоящее время их 12 участников.

Однако при трансграничном электронном обмене данными установление доверия может быть затруднено из-за различий в законодательстве стран, в стандартах электронного обмена и хранения данных, а использование облачных вычислений приводит к получению данных, находящихся в нескольких юрисдикциях. Новые технологии, такие как блокчейн или искусственный интеллект, приводят к увеличению типов и источников данных.

## **2.3 Критерии выбора вида электронной подписи для электронного делопроизводства**

Документооборот как внутренний, так и внешний на подавляющем большинстве организаций осуществляется в электронном виде. Почти вся отчетность, предоставляемая организациями в налоговые органы, Пенсионный фонд России, проверяющие и другие органы формируется в электронном виде.

Принятая в 2020 году Концепция<sup>1</sup> сформулировала требования для перехода к безбумажному документообороту. Прежде всего, для предприятия, в котором предполагается ввести электронный документооборот, согласно Концепции, необходимо:

- определить видовой состав документов предприятия;
- составить перечень документов, которые будут обрабатываться в СЭД;
- выбрать СЭД для организации работы с электронными документами;
- определить для документов виды электронных подписей;
- сформировать требования к процессу передачи электронных документов из СЭД на долговременное хранение в специализированную архивную систему.

От вида документа и от функционала СЭД зависит, какая электронная подпись – простая или усиленная будет использоваться, поэтому прежде чем перейти непосредственно к критериям выбора электронной подписи, рассмотрим с какими документами можно работать в электронном формате, а также основные функции систем электронного документооборота.

---

<sup>1</sup> Концепция безбумажного документооборота и электронного архива. [Электронный ресурс]. UML: <https://upr.ru/upload/adminFiles/2020/koncepciia-bezbumazhnogo-dokumentoooborota-i-elektronnogo-arhiva.pdf> (дата обращения 15.01.2021).

Законодательно не запрещено работать в электронном формате с документами длительного и постоянного сроков хранения, исключением на данный момент времени являются только документы по личному составу, где предусматривается личная подпись работника. Минтруд разрабатывает поправки в Трудовой кодекс РФ, которые будут регулировать электронный кадровый документооборот. Сейчас для кадрового делопроизводства, даже если документы есть в электронном виде, их нужно дублировать на бумаге.

В настоящее время есть поправки в Трудовом кодексе РФ (*статьи 312.1 - 312.9*) в части регулирования удаленной занятости<sup>1</sup>. Работодатель может обмениваться кадровыми документами с дистанционными работниками в электронном формате. В отношении сотрудников, работающих удаленно, они имеют такую же юридическую силу, как и документы на бумажном носителе.

Системы автоматизации документооборота, предлагаемые в настоящее время в России: DIRECTUM, Lotus Notes, Optima-Workflow, Евфрат-Документооборот, Дело и другие обеспечивают как внутренний, так и внешний документооборот. Для обеспечения электронного делопроизводства наиболее востребованы такие функции СЭД, как [30]:

- хранение и поиск документов;
- работа с входящими, исходящими и внутренними документами;
- поддержка маршрутов движения документов;
- контроль исполнения документов;
- аналитические отчеты (о поручениях, о выполнении работ, текущей занятости и другие);
- информационная безопасность.

---

<sup>1</sup> Федеральный закон от 08.12.2020. № 407-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации в части регулирования дистанционной (удаленной) работы и временного перевода работника на дистанционную (удаленную) работу по инициативе работодателя в исключительных случаях». URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=370070&dst=1000000001%2C0#035399689463296635> (дата обращения 15.01.2021).

Работа с входящими, исходящими, внутренними документами – важный функционал СЭД, используемый как в государственных органах, так и в любых организациях.

Электронная подпись обеспечивает криптографическую защиту передаваемой по незащищенным сетям информации. Реализация и поддержка электронной подписи документов является одной из важных функций такого компонента СЭД, как информационная безопасность. Основными функциями модуля Информационная безопасность являются [30, 39, 46]:

- аутентификация и распределение прав доступа для пользователей СЭД;
- возможность работы с электронной подписью документов;
- шифрование и дешифрование электронной подписи документов;
- ведение истории и статистики работы с документами.

При выборе системы электронного документооборота прежде всего руководствуются ее функционалом, стоимостью и возможностью дальнейшего сопровождения. Если предполагается, что системой будет формироваться усиленная квалифицированная подпись, то провайдеры электронной подписи должны быть сертифицированы органами ФСБ.

Выбор вида применяемой электронной подписи определяется структурой предприятия и задачами, которые необходимо решить с помощью электронной подписи. В СЭД может использоваться и простая и усиленная электронные подписи. Руководство организации, подписывающие финансовые документы, обладают усиленной квалифицированной подписью (УКЭП). Руководители структурных подразделений государственных организаций визировать и подписывать электронные документы правомочны усиленной неквалифицированной электронной подписью (УНЭП). Простой электронной подписью (ПЭП), которая может создаваться самой СЭД, подписываются, визируются внутренние документы организации [41, 43].

Если для исследования рассмотреть Концепцию перехода от бумажного к электронному документообороту, то в этом документе предусматривается такой подход к выбору и использованию электронных подписей: значительная часть операций по созданию и обработке электронных документов в СЭД защищаются ПЭП пользователя информационной системы (вводится логин и пароль). Действия по визированию (согласованию) документа, его подписанию или утверждению в государственных структурах защищаются УНЭП.

Для нормативного регулирования использования различных видов электронной подписи в организации должны быть разработаны и утверждены соответствующие локальные нормативные акты. Таким нормативным актом должен быть утвержден перечень документов, которые будут подписываться и использоваться с применением УКЭП.

При подготовке такого перечня документов нужно учесть: во-первых положения федеральных законов, устанавливающих условия представления электронных документов, а во-вторых вероятность использования конкретного документа в судебном разбирательстве в качестве прямого доказательства.

Налоговый кодекс РФ признает только те электронные документы, которые подписаны УКЭП. Исключением является только передача налогоплательщиками – физическими лицами документов в электронной форме через личный кабинет. В данном случае допускается УНЭП.

Нотариус, на основании закона о нотариате<sup>1</sup> принимает электронные документы, подписанные УКЭП.

Исследования показывают, что в настоящее время ни Гражданский кодекс РФ, ни Федеральный закон «О бухгалтерском учете» не уточняют, какой вид электронной подписи необходимо использовать в бухгалтерских документах, чтобы эти документы были юридически значимы.

---

<sup>1</sup> Основы законодательства Российской Федерации о нотариате (утв. ВС РФ 11.02.1993 №4462-1) (ред. от 27.12.2019, от 01.01.2020).

Выбор вида электронной подписи зависит также от срока хранения данного документа. Если в дальнейшем из СЭД предполагается выгрузка электронных документов постоянного, длительного срока хранения свыше 10 лет, для передачи на архивное хранение, то эти документы должны быть подписаны УКЭП.

**Выводы по результатам исследования:**

Требуется принятие подзаконных актов, уточняющих вид электронной подписи, используемой в гражданских правоотношениях. Необходимо создать общеевропейское правовое и экономическое пространство, в котором будут признаваемы всеми сертификаты электронной подписи. Удостоверяющие центры должны проходить обязательную аккредитацию. Требуется признание электронных подписей, полученных за рубежом.

### **3 Методические рекомендации по оптимизации использования электронной подписи на примере ГАСУСОССЗН ПО «Сердобский дом ветеранов труда»**

С развитием информационных технологий, развитие современного общества невозможно представить без использования, обработки, хранения информации. Современные информационные технологии повышают эффективность труда работников.

#### **3.1 Получение электронной подписи ГАСУСОССЗН ПО «Сердобский дом ветеранов труда»**

Электронная подпись (ЭП) позволяет установить факт отсутствия искажений информации в электронном документе с момента ее создания. Кроме того она подтверждает принадлежность ЭП владельцу. Электронная подпись получается в результате криптографического преобразования информации.

Чтобы получить электронную подпись заявителю, подготовив необходимые документы, нужно обратиться в любой аккредитованный удостоверяющий центр (АУЦ). Правовой статус АУЦ, выдающих усиленные электронные подписи, определен федеральным законом ФЗ-63. В нем описываются их функции и обязанности. В частности, АУЦ обязан вести реестр выданных сертификатов ключей подписей.

В выдаваемом квалифицированном сертификате для физического лица указывается фамилия, имя, отчество владельца квалифицированного сертификата. Для индивидуального предпринимателя указывается фамилия, имя, отчество, основной государственный регистрационный номер индивидуального предпринимателя. В квалифицированном сертификате юридического лица (организации) указывается фамилия, имя, отчество

владельца квалифицированного сертификата, наименование, место нахождения организации, а также идентификационный номер владельца сертификата.

Наличие УКЭП является обязательным условием для работы с порталами госуслуг, системами межведомственного электронного взаимодействия, сдачи отчетности в налоговые органы, отправки финансовых и иных документов через интернет, исполнении государственных, муниципальных функций, а также других юридически значимых действий.

Для получения УКЭП необходимо:

1. Обратится в удостоверяющий центр, который имеет лицензию на выдачу электронной подписи.
2. Подать заявку на получение УКЭП.
3. Подать все необходимые документы.
4. Дождаться срока изготовления УКЭП (5-7 рабочих дней).
5. Получить УКЭП.

Чтобы оформить электронную подпись, необходимо:

6. Иметь персональный компьютер.
7. Иметь лицензионное программное обеспечение для работы на компьютере.
8. Выбрать лицо, на которое будет оформляться электронная подпись.
9. Определить способ получения подписи и заключить договор с удостоверяющим центром.
10. Оплатить услуги и получить ключ.

Чтобы получить квалифицированную электронную подпись, необходимы различные документы. Чаще всего требуется:

1. Заявка установленного образца, где будет минимальная необходимая информация о заявителе (компания вправе запрашивать расширенные анкетные данные).

2. Паспорт заявителя.
3. ИНН и СНИЛС заявителя.
4. Квитанция об оплате услуг удостоверяющего центра.

Если необходим квалифицированный сертификат, то потребуются:

1. Учредительные документы организации.
2. Выписка из ЕГРЮЛ.
3. ИНН.

Ключ действует в течение одного года, а при его оформлении обязательно личное присутствие заявителя. Далее требуется продление путем написания соответствующего заявления в удостоверяющий центр. При этом не обязательно личное присутствие в центре, достаточно отправить заявление по электронной почте или заказным письмом. Какие именно условия продления действуют в конкретно взятом центре необходимо уточнять у его специалистов. Чаще всего требуется только произвести оплату за следующий год и предоставить заявление.

Для получения усиленной квалифицированной электронной подписи и сертификата ключа руководство Государственного автономного стационарного учреждения социального обслуживания системы социальной защиты населения Пензенской области «Сердобский дом ветеранов труда» (ГАСУСОССЗН ПО «Сердобский дом ветеранов труда») заключила договор с ООО РГЦ «Партнер», выполняющего функции удостоверяющего центра, а также оператора по обслуживанию системы электронного документооборота «Контур-Экстерн».

На основании договора и предоставленных документов от ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» удостоверяющий центр в лице доверенного представителя ООО РГЦ «Партнер» сформировал усиленную квалифицированную подпись и сертификат ключа (рисунок 3).

Владельцем сертификата электронной подписи является руководитель организации – Щетинин А.В.

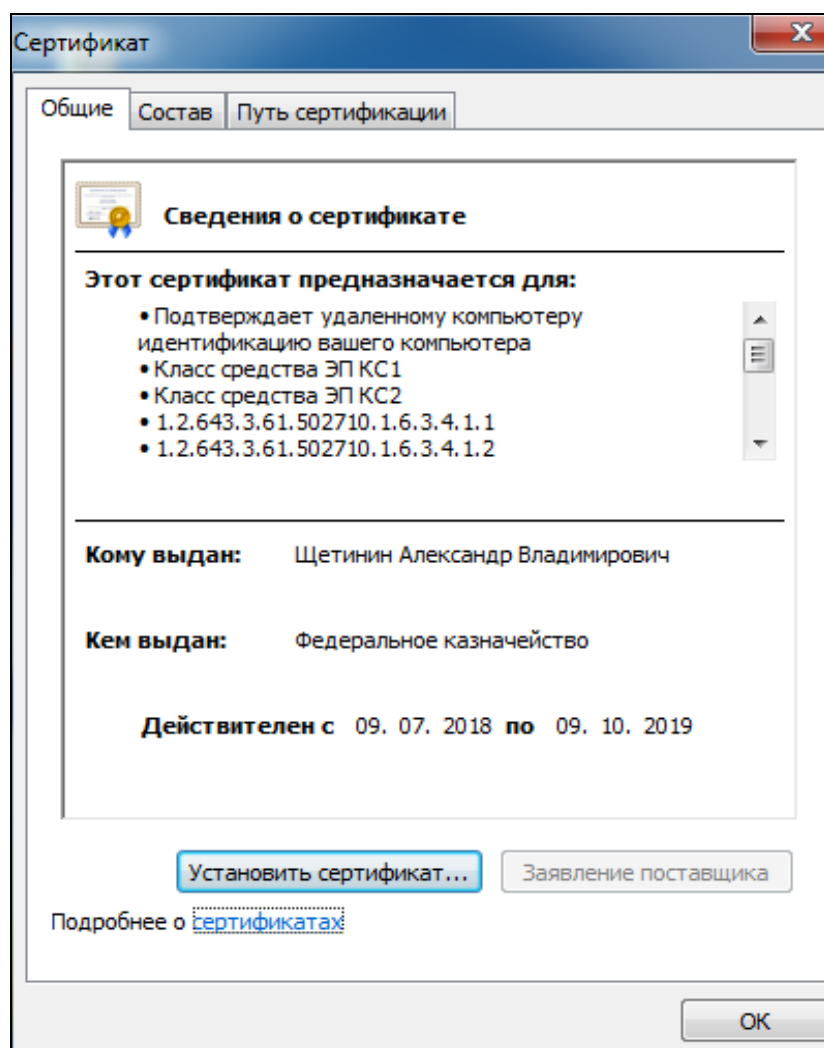


Рисунок 3 – Окно системы

По договору между ООО РПЦ «Партнер» и ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» срок действия сертификата ключа подписи действителен один год.

Помимо сертификата ключа для усиленной квалифицированной электронной подписи ООО РПЦ «Партнер» предоставило ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» квалифицированный сертификат для системы электронного документооборота «Контур-Экстерн» и право пользоваться этой системой электронного документооборота.

ООО РПЦ «Партнер» является оператором связи по электронному взаимодействию, а ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» – абонентом этой связи.

Копии документов: Договор, Акт согласования стоимости услуг и прав, Регистрационная карта абонента приведены в приложении А.

### **3.2 Применение электронной подписи в ГАСУСОССЗН ПО «Сердобский дом ветеранов труда»**

После получения сертификата ключа, в ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» на персональный компьютер было установлено лицензионное программное обеспечение, полученное из удостоверяющего центра (ООО РПЦ «Партнер»). Затем на персональный компьютер были установлены библиотеки «Cadescom» и «Сapicom».

Теперь у руководства ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» есть возможность проставлять электронную подпись, работая с электронными документами.

В ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» для подписания документов используется УКЭП. Применение УКЭП позволяет подписывать документы, используя механизм криптопреобразования, и уникальная комбинация исходных данных и ключа на выходе дает уникальный массив данных (подпись). Проверка подписи предполагает повторное ее вычисление и сравнение с имеющимися данными на стороне проверяющего. Таким образом, авторство документа подтверждается только при условии, что ключ однозначно принадлежит только лицу, подписывающему документ.

Схематично этот процесс приведен на рисунке 4 [36].

При проставлении электронной подписи руководством ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» автоматически прописывается дата, таким образом, становится понятно, что штамп с электронной подписью действителен на момент его проставления.

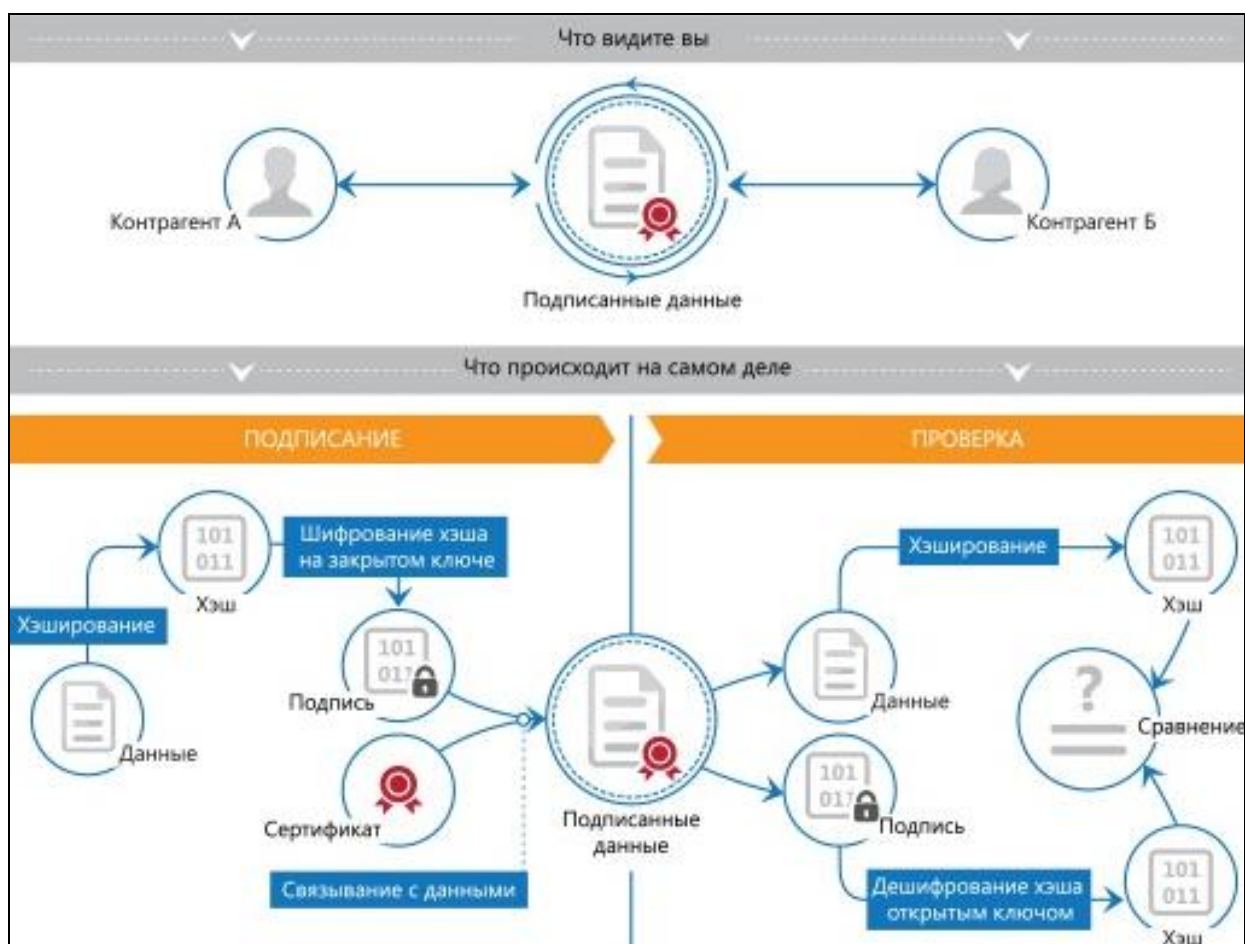


**Рисунок 4 – Схема подписания и проверки электронного документа**

Электронный документооборот ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» решает следующие задачи:

1. Подписание документов электронной подписью и их отправка.
2. Прием электронных документов и проверка электронной подписи на документах.
3. Обработка электронных документов.

Задачи подписания документов электронной подписью, отправка их адресатам, а также прием электронных документов и проверка в них электронной подписи решают сервисы обмена электронных документов под управлением операторов электронного документооборота. Таким оператором ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» является, согласно договору - ООО РПЦ «Партнер». При выборе оператора обращалось внимание на то, чтобы у оператора электронного документооборота была лицензия на осуществление подобной деятельности.

Для решения двух последних задач подходят такие системы документооборота, в которых уже имеется необходимый функционал. Примерами таких систем являются система DIRECTUM, система «Контур-Экстерн».

В ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» в системе электронного документооборота используются следующие виды документов:

- отчетность по использованию средств;
- налоговая отчетность;
- сведения в Управление Пенсионного фонда по Пензенской области.

Для подписания документов УКЭП используется программный продукт «Контур-Экстерн».

Поскольку на компьютере руководителя уже установлено программное обеспечение «Контур Отчет ПФ», система «Контур-Экстерн», то не нужно с каждым из контрагентов (Управление ПФР по Пензенской области, Управление Федерального казначейства по Пензенской области, налоговыми органами), заключать отдельные соглашения об электронном взаимодействии. Это учтено при установке средств электронной подписи и средств криптографической защиты, при установке общесистемного и специального программного обеспечения.

Также необходимо решить вопрос хранения электронных документов. Кроме того при организации электронного обмена документами останутся открытыми вопросы безопасности и конфиденциальности передаваемых данных. Поэтому в качестве методических рекомендаций по оптимизации использования электронной подписи можно назвать следующие:

- для небольших организаций, не имеющих квалифицированных сотрудников – специалистов в сфере IT-технологий, целесообразно подключаться к услугам оператора электронного документооборота;

- разработать меры, обеспечивающие защиту от несанкционированного доступа к информации;
- выполнять требования по обеспечению информационной безопасности при работе с СЭД.

Для исследуемой организации ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» оператором электронного документооборота для обмена электронными документами с контрагентами является ООО РПЦ «Партнер», осуществляющий установку специального программного обеспечения для работы в системе. ООО РПЦ «Партнер» осуществляет настройку всей системы и ее дальнейшее сопровождение.

Первая рекомендация по оптимизации использования электронной подписи реализована за счет привлечения специалистов – операторов электронного документооборота. Основные положения для выполнения второй и третьей рекомендации должны быть прописаны локальным нормативным актом.

Анализ локальных нормативных актов, регламентирующих организацию работы с применением электронной подписи в ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» показал их отсутствие.

### **3.3 Разработка Руководства по обеспечению информационной безопасности при работе с электронной подписью в ГАСУСОССЗН ПО «Сердобский дом ветеранов труда»**

Исследование практики применения электронной подписи в ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» позволило сделать вывод об отсутствии мер по обеспечению защиты от несанкционированного доступа и требований по обеспечению информационной безопасности при работе в системе обмена электронными документами.

Руководство по обеспечению информационной безопасности при работе с электронной подписью в организации (далее – Руководство) должно

содержать следующие разделы, отвечающие целям создания данного документа:

1. Общие положения.
2. Рекомендации по установке средств электронной подписи и средств криптографической защиты.
3. Меры по обеспечению защиты от несанкционированного доступа.
4. Рекомендации по обеспечению информационной безопасности при работе в системах обмена электронными документами.

В разделе Общие положения должны приводиться нормативные акты, на основании которых создается данный документ. Указываются цели разработки этого документа.

В разделе Рекомендации по установке средств электронной подписи и средств криптографической защиты (далее – Рекомендации) указывается, что нужно для приобретения и установки УКЭП.

УКЭП формируется с помощью криптографических средств, записывается на специальный носитель – *токен*, который внешне похож на обычную флэшку, но в отличие от флешки имеет сложную систему защиты. При покупке УКЭП приобретается:

- сертификат электронной подписи;
- средства криптографической защиты информации (например, СКЗИ КристоПро);
- токен.

Стоимость УКЭП напрямую зависит от ее возможностей.

В настоящее время ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» использует электронную подпись на одном компьютере, поэтому организация покупает лицензию СКЗИ КристоПро для одного компьютера на один год.

Для того чтобы пользоваться ключом электронной подписи, необходимо настроить компьютер. Поэтому в Рекомендациях нужно указать:

- драйверы токена;

- ПО в виде дистрибутива СКЗИ (например, КриптоПро CSP);
- браузер-плагин для работы с сертификатом УКЭП на конкретном портале или сервисе.

В разделе Меры по обеспечению защиты от несанкционированного доступа необходимо указать все возможные средства доступа к информации и риски от несанкционированного доступа. Привести меры защиты информации от злоумышленников и недобросовестных пользователей системы обмена электронными документами. *Статьей 10* ФЗ-63 установлена обязанность участников электронного взаимодействия обеспечивать конфиденциальность ключей электронных подписей. Токен с действующим сертификатом УКЭП нельзя передавать посторонним лицам, в случае его утери – сразу сообщить об этом в удостоверяющий центр для прекращения действия сертификата.

В разделе Рекомендации по обеспечению информационной безопасности при работе в системах обмена электронными документами (далее – Рекомендации) нужно привести рекомендуемые средства по защите ключей электронной подписи, меры безопасности при работе с системой обмена электронными документами, а также привести рекомендации при обращении с ключевыми носителями.

С учетом вышесказанного было разработано Руководство по обеспечению информационной безопасности при работе с электронной подписью в ГАСУСОССЗН ПО «Сердобский дом ветеранов труда», представленное ниже.

Для введения данного Руководства в действие должен быть издан приказ директора ГАСУСОССЗН ПО «Сердобский дом ветеранов труда».

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ СТАЦИОНАРНОЕ УЧРЕЖДЕНИЕ  
СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ СИСТЕМЫ СОЦИАЛЬНОЙ  
ЗАЩИТЫ НАСЕЛЕНИЯ ПЕНЗЕНСКОЙ ОБЛАСТИ «СЕРДОБСКИЙ ДОМ  
ВETERАНОВ ТРУДА»  
(ГАСУСОССЗН ПО «Сердобский дом ветеранов труда»)

УТВЕРЖДЕНО  
приказом директора  
ГАСУСОССЗН ПО  
«Сердобский дом ветеранов труда»  
от \_\_\_\_\_ № \_\_\_\_\_

РУКОВОДСТВО ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ  
ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОДПИСЬЮ

2021

## **1. Общие положения**

Настоящее руководство составлено в соответствии с требованиями Федерального закона от 06.04.2011 №63-ФЗ (с изменениями) «Об электронной подписи».

Электронная подпись (ЭП) необходима для идентификации лица, подписавшего электронный документ, и является полноценной заменой собственноручной подписи.

Получение юридически значимого квалифицированного сертификата усиленной квалифицированной электронной подписи (УКЭП) осуществляется в аккредитованном удостоверяющем центре.

Подробная информация об электронной подписи, способах ее получения и использования содержится на сайте Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры РФ) по ссылке: <https://digital.gov.ru/ru/>.

## **2. Рекомендации по установке средств электронной подписи и средств криптографической защиты**

Для корректной работы с электронной подписью необходимо установить специализированное программное обеспечение КриптоПро или САРИСОМ.

В состав КриптоПро должны входить следующие компоненты:

1. Криптопровайдер КриптоПро CSP. Данный компонент позволяет:

- осуществлять авторизацию, подтверждать юридическую значимость электронных документов при обмене электронными документами между пользователями;
- обеспечивать работоспособность системы;
- осуществлять контроль целостности программного обеспечения, обеспечивая тем самым его защиту от несанкционированных изменений и нарушений правильности функционирования.

2. CryptoPro Browser Plug-in. Данный компонент необходим для создания и проверки электронной подписи на веб-страницах (используется вместе с программой КриптоПро CSP). Может использоваться в современных браузерах: Internet Explorer, Google Chrome, Opera, ЯндексБраузер, Mozilla Firefox.

3. КриптоАРМ. Данная программа предназначена для шифрования и дешифрования данных; для создания и проверки электронной подписи с использованием сертификатов открытых ключей; для работы с сертификатами и криптопровайдерами.

Компонент CAPICOM предназначен для работы только с Internet Explorer.

Установка общесистемного и специального программного обеспечения, средств электронной подписи (ЭП) и средств криптографической защиты информации (СКЗИ) возможна только специально подготовленными лицами.

Устанавливаемое программное обеспечение должно отвечать следующим требованиям:

- на компьютере, где устанавливаются средства ЭП и СКЗИ, необходимо использовать только лицензионное программное обеспечение;
- загрузка программного обеспечения средств ЭП и СКЗИ должна производиться только с дистрибутива, полученного в аккредитованном удостоверяющем центре (АУЦ).

На компьютере с установленными средствами ЭП и СКЗИ не должно быть программ-отладчиков, других программ, позволяющих изменять настройки операционной системы.

Необходимо предусмотреть меры исключающие возможность несанкционированного изменения аппаратной части компьютера, на котором установлены средства ЭП и СКЗИ.

Для подключения носителя ключевой информации (токена) к компьютеру использовать драйвер, выдаваемый удостоверяющим центром при покупке УКЭП.

### **3. Меры по обеспечению защиты от несанкционированного доступа**

Защита от несанкционированного доступа обеспечивается грамотной работой на компьютере, используя пароли.

Назначение и смена паролей должны удовлетворять следующим правилам:

- длина пароля берется не менее 6 символов;
- в символах пароля обязательно должны присутствовать любые символы клавиатуры верхнего и нижнего регистров, а также цифры и специальные символы (&, #, @, \$, ?, %, \_ и т.п.);
- в пароле не должно быть легко вычисляемых сочетаний символов (имен, фамилий, дат рождения и т.д.), обще употребительных сокращений слов (User, Admin и т.д.);
- при смене пароля новый пароль должен отличаться от предыдущего не менее чем в 4-х позициях;
- пользователь никому не должен сообщать личный пароль;
- пароль нужно периодически изменять.

При работе с компьютером, работая с электронными документами, запрещается:

- оставлять компьютер с установленными средствами ЭП и СКЗИ без контроля;
- разглашать содержимое сертификата ключа или передавать носители ключевой информации (токены), лицам, к ним не допущенным;
- выводить ключевую информацию на принтер, монитор, другие средства отображения информации;

- записывать на токены постороннюю информацию;
- осуществлять несанкционированное копирование ключевой информации с токенов.

В случае подключения компьютера с установленными средствами ЭП и СКЗИ к общедоступным сетям передачи данных необходимо исключить возможность попадания из сети исполняемых и загрузочных файлов, а также вредоносных программ. На компьютере необходимо иметь лицензионную антивирусную программу с периодически обновляемой антивирусной базой.

#### **4. Рекомендации по обеспечению информационной безопасности при работе в системах обмена электронными документами**

При работе в системе с электронными документами используются ключи электронной подписи. Роль ключевого носителя выполняет специальная флешка – токен.

Ключ ЭП на токене защищается паролем (ПИН-кодом). ПИН-код формируется при генерации кода ключа. Генерацией ключей занимается сотрудник АУЦ, который сообщает сгенерированный пароль владельцу ключа ЭП. Надежность ключа ЭП от взлома возлагается на АУЦ, выдавшего ключ электронной подписи.

Дальнейшую ответственность за конфиденциальность сохранения пароля (ПИН-кода) несет владелец ключа ЭП.

Ключ ЭП должен размещаться только на сменном носителе информации - токене (e-Token, ru-Token, USB-flash накопитель и др.). При размещении ключа ЭП на локальном или сетевом диске возможен несанкционированный доступ к ключевой информации и использование ключа ЭП в корыстных целях.

Токены должны использоваться только их владельцами либо уполномоченным лицом на использование данного носителя. Храниться токены должны в месте, недоступном третьим лицам.

В считывающее устройство токен вставляется только на время выполнения средствами ЭП и СКЗИ операций формирования и проверки электронной подписи, шифрования и дешифрования. На токене недопустимо хранить рабочие или личные файлы.

На компьютере, используемом для работы в системах обмена электронными документами должна быть:

- установлена лицензионная операционная система и лицензионная антивирусная программа;
- включена автоматическая блокировка экрана после ухода ответственного работника с рабочего места.

Дополнительные требования по обеспечению информационной безопасности при работе в системах обмена электронными документами могут устанавливаться правилами системы электронного документооборота, требованиями по эксплуатации и безопасности средств ЭП и СКЗИ.

## Заключение

Электронный документооборот давно вошел в нашу жизнь. Это современное и эффективное решение обмена электронными документами в любой сфере деятельности.

Анализ нормативных актов, регламентирующих создание и использование электронной подписи в России, позволил сделать следующие выводы:

1. В нормативных актах Российской Федерации используется различные толкования электронного документа, подписанного электронной подписью (электронное сообщение, документ в электронном виде, электронный документ).

2. Работа по нормативно-правовому и нормативно-техническому регулированию в сфере применения электронной подписи должна быть синхронизирована и не должна дублироваться.

3. Необходима доработка ряда подзаконных актов, касающихся сферы применения электронной подписи, например корректировку статьи 189 Гражданского кодекса РФ «Последствия прекращения доверенности» (по доверенности можно получать сертификат ключа в удостоверяющем центре), корректировку статьи 1209 Гражданского кодекса РФ о праве места совершения сделки.

4. Необходима разработка нормативных актов в сфере технологии проверки архивных ЭП.

Анализ зарубежного законодательства в сфере использования электронной подписи показал:

1. Развитие технологий применения электронной подписи в России шло с некоторым отставанием от развитых зарубежных стран, что связано,

прежде всего, с отставанием в развитии информационных технологий, а также с назначением использования электронной подписи (в России большее внимание уделялось электронному документообороту в органах власти, в крупных корпорациях, а за рубежом электронный документооборот в большей степени связан с электронной коммерцией).

2. Различия в законодательствах разных стран в сфере электронного документооборота служат причиной юридической неопределенности в отношениях сторон.

Анализ опыта использования электронной подписи в России и за рубежом позволил сделать следующие выводы:

1. Необходимо создать общеевропейское правовое и экономическое пространство, в котором будут признаваемы всеми сертификаты электронной подписи.

2. Удостоверяющие центры во всех странах должны проходить обязательную аккредитацию.

3. Необходимо признание электронных подписей, полученных за рубежом.

Обобщая цели и задачи внедрения электронного документооборота, систем межведомственного взаимодействия можно выделить следующее:

1. Делопроизводство с использованием электронного документооборота повышает эффективность работы с документами, улучшает исполнительскую дисциплину, минимизирует затраты времени.

2. Межведомственное электронное взаимодействие оптимизирует работу государственных учреждений.

3. Использование электронной подписи на портале государственных услуг при получении конкретной услуги приводит к дальнейшей цифровизации общества, повышению компьютерной грамотности практически всех слоев населения РФ.

4. Несложное получение усиленной электронной подписи индивидуальными предпринимателями и организациями позволяет организовывать обмен электронными документами при формировании налоговой и прочей отчетности.

Выбор вида электронной подписи зависит от целей и задач, решаемых с помощью применения электронной подписи.

**В ходе выполнения магистерской диссертации были выполнены следующие задачи:**

- рассмотрены понятия «электронная подпись», «электронный документ», «электронный документооборот», «межведомственное электронное взаимодействие»;
- проведен анализ нормативной базы, регламентирующей использование электронной подписи в России и за рубежом;
- проведен анализ зарубежных нормативных актов в сфере использования электронной подписи;
- исследован опыт использования электронной подписи в России и за рубежом; описаны технологии создания и применения электронной подписи в России и ряде зарубежных стран;
- выделены критерии выбора вида электронной подписи для электронного делопроизводства;
- рассмотрен процесс получения и применения электронной подписи в Государственном автономном стационарном учреждении социального обслуживания системы социальной защиты населения Пензенской области «Сердобский дом ветеранов труда» (ГАСУСОССЗН ПО «Сердобский дом ветеранов труда»);
- на основании анализа нормативного регулирования применения электронной подписи в делопроизводстве ГАСУСОССЗН ПО

«Сердобский дом ветеранов труда» были разработаны методические рекомендации по улучшению использования электронной подписи для ГАСУСОССЗН ПО «Сердобский дом ветеранов труда».

Разработанное Руководство по обеспечению информационной безопасности при работе с электронной подписью позволит в ГАСУСОССЗН ПО «Сердобский дом ветеранов труда» обеспечить необходимые меры защиты при обмене электронными документами.

## **Список использованных источников и литературы**

### **I. Источники**

#### **Кодексы Российской Федерации**

1. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред от 08.12.2020).
2. Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 №146-ФЗ (ред. от 23.11.2020).

#### **Федеральные законы Российской Федерации**

3. Федеральный закон от 06.04.2011 № 63 – ФЗ «Об электронной подписи» (с изм. от 08.06.2020).
4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. от 29.12.2020).
5. Федеральный закон от 06.12.2011 №402-ФЗ «О бухгалтерском учете» (ред. от 26.07.2019).
6. Федеральный закон от 27.07.2010 №210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (ред. от 30.12.2020).

#### **Постановления Российской Федерации**

7. Постановление Правительства РФ от 25.06.2012 № 634 «О видах электронной подписи, использование которых допускается при обращении за получением государственных или муниципальных услуг» (ред. от 27.08.2018).

8. Правила определения видов электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг. Утверждены Постановлением Правительства РФ от 25.06.2012 № 634.

9. Постановление Правительства РФ от 25 декабря 2014 г. № 1494 «Об утверждении Правил обмена документами в электронном виде при организации информационного взаимодействия» (ред. от 24.01.2017 №63).

10. Постановление Правительства РФ от 22.09.2009 № 754 «Об утверждении Положения о системе межведомственного электронного документооборота» (ред. от 16.03.2019).

11. Постановление Правительства РФ от 25.01.2013 № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг» (ред. от 23.12.2020).

### **Распоряжение Правительства Российской Федерации**

12. Перечень видов документов, передаваемых при взаимодействии федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, государственных внебюджетных фондов в электронном виде. Утверждено распоряжением Правительства РФ от 2 апреля 2015 г. №583-р.

### **Приказы Министерств Российской Федерации**

13. Правила делопроизводства в государственных органах, органах местного самоуправления, утвержденных приказом Росархива от 22 мая 2019 г. № 71 (зарегистрировано в Минюсте России 27.12.2019 № 57023).

14. Приказ Росархива от 15.06.2020 №69 «Об утверждении Типовых функциональных требований к системам электронного документооборота и системам хранения электронных документов в архивах государственных органов» (зарегистрировано в Минюсте России 20.10.2020 №60484).

15. Требования к организационно-техническому взаимодействию государственных органов и государственных организаций посредством обмена документами в электронном виде. Утвержден приказом Минкомсвязи РФ и Федеральной службы охраны РФ от 27 мая 2015 г. № 186/158.

### **Государственные стандарты Российской Федерации**

16. ГОСТ Р 7.08-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения.

17. ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. СИБИД. Организационно-распорядительная документация. Требования к оформлению документов.

18. ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

19. ГОСТ 34.11-2018. Информационная технология. Криптографическая защита информации. Функция хэширования.

20. ГОСТ Р 54989-2012 (ISO/TR 18492:2005). Обеспечение долговременной сохранности электронных документов.

21. ИСО/МЭК 14888-1:2008. Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения.

22. ИСО/МЭК 14888-3:2018. Информационная технология. Методы и средства обеспечения безопасности. Цифровые подписи с приложением. Часть 3. Механизмы на основе дискретного логарифма.

### **Международные документы**

23. Типовой закон ЮНСИТРАЛ «Об электронной торговле». Издание ООН, Нью-Йорк, 2006 год.

24. Типовой закон ЮНСИТРАЛ «Об электронных подписях и Руководство по применению». Издание ООН, Нью-Йорк, 2001 год.

25. ISO/IEC 14888-1:2008. Information technology - Security techniques - Digital signatures with appendix - Part 1: General.

26. ISO/IEC 14888-3:2018. Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms.

## **II. Литература**

27. Бобылева М.П. Управленческий документооборот: от бумажного к электронному. Вопросы теории и практики./ Бобылева М.П.// Изд-во «Термика», 2016.-360 с.

28. Бондаренко А.В. Открытая платформа ВЭД: опыт Сингапура и перспективы создания в России./ Бондаренко А.В. //PKI – Форум 2020. XVIII международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи //URL: <https://odin.mgimo.ru/nov-pod-mgimo/3482-aleksey-bondarenko-vystupil-na-xviii-mezhdunarodnoj-konferentsii-po-problematike-infrastruktury-otkrytykh-klyuchey-i-elektronnoj-podpisi> (дата обращения 16.11.2020).

29. Гомалеев А.О. Перспективы применения электронной, в том числе дистанционной электронной, подписи в целях повышения эффективности предоставления государственных услуг / Гомалеев О.А. // «Научно-практический электронный журнал Аллея науки» №2 (18) 2018.

30. Горовой А. Выбор системы электронного документооборота. [Электронный ресурс]. UML: <https://fossdoc.com/ru/vybor-sed> (дата обращения 16.11.2020).

31. Ермолаева А.В. Совершенствование управления документами в органах государственной власти /Ермолаева А.С.//Делопроизводство. №4. 2020. С. 16-21.

32. Ермолаева А.В. Электронный документ и электронная подпись: проблемы регламентации и практики применения / Ермолаева А.В. //Региональная власть, местное самоуправление и гражданское общество: механизмы взаимодействия: сб. научных трудов. Изд-во Поволжского института управления им. П.А. Столыпина, 2017. С 77-80.

33. Концепция безбумажного документооборота и электронного архива. [Электронный ресурс]. UML: <https://upr.ru/upload/adminFiles/2020/koncepciia-bezbumazhnogo-dokumentoorota-i-elektronnogo-arhiva.pdf> (дата обращения 15.01.2021).

34. С.Л. Кузнецов. Современные технологии документационного обеспечения управления /С.Л. Кузнецов – 3-е изд.// Изд-во ООО «Термика.РУ», 2017.

35. Смышляев С.В., Смирнов П.В. Дистанционное создание электронной подписи: настоящее и будущее / Смышляев С.В.// PKI – Форум 2020. XVIII международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи URL: [https://pki-forum.ru/files/files/2\\_3\\_%20Smirnov\\_Smyshlyayev\\_2020.pdf](https://pki-forum.ru/files/files/2_3_%20Smirnov_Smyshlyayev_2020.pdf). (дата обращения 16.01.2021).

36. Славинская А.Н. Что такое электронная подпись [Электронный ресурс] / Славинская А.Н.// Секретарь-референт, №1, 2020 URL: [https://www.profiz.ru/sr/1\\_2020/elektronnaya\\_podpis/](https://www.profiz.ru/sr/1_2020/elektronnaya_podpis/)

37. Соловяненко Н.И. Федеральный закон №476-ФЗ «О внесении изменений в ФЗ «Об электронной подписи...»: Проблемы применения и юридические риски»/ Соловяненко Н.И. // PKI – Форум 2020. XVIII международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи //URL: [https://pki-forum.ru/files/files/1\\_%20Solovyanenko\\_1%20session.pdf](https://pki-forum.ru/files/files/1_%20Solovyanenko_1%20session.pdf) (дата обращения 16.01.2021).

38. Ульяновцева С.Э. Концепция безбумажного документооборота и электронного архива / Ульяновцева С.Э.// Делопроизводство. №4. 2020. С. 22-31.

39. Туркин Р. Сравнительный анализ использования ЭП в России и за рубежом./Туркин Р. // URL: [https://zakon.ru/blog/2013/3/29/sravnitelnyj\\_analiz\\_ispolzovaniya\\_ep\\_v\\_rossii\\_i\\_za\\_rubezhom](https://zakon.ru/blog/2013/3/29/sravnitelnyj_analiz_ispolzovaniya_ep_v_rossii_i_za_rubezhom) (дата обращения 15.01.2021).

40. Храмцовская Н.А. Европейский закон eIDAS: Усиленные электронные подписи на основе квалифицированного сертификата – какой стандарт ETSI применим?/ Храмцовская Н.А.// URL: <http://rusrim.blogspot.com/2018/02/eidas-etsi.html>.

41. Щепеткова А.В. О правовой регламентации применения электронной подписи / Щепеткова А.В., Шокорова Н.Н. // Информационные технологии в науке и образовании. Проблемы и перспективы. : сб. ст. по материалам VI Всерос. межвуз. науч-практ. конф. (г.Пенза, 13 марта 2019 г.) /под ред. Л.Р. Фионовой. – Пенза: Изд-во ПГУ, 2019, с. 393-395.

42. Щепеткова А.В. Правовая регламентация применения электронных подписей за рубежом /Щепеткова А.В., Шокорова Н.Н. // Информационные технологии в науке и образовании. Проблемы и перспективы. : сб. ст. по материалам VII Всерос. межвуз. науч-практ. конф. (г.Пенза, 18 марта 2020 г.) /под ред. Л.Р. Фионовой. – Пенза: Изд-во ПГУ, 2020, с. 70-72.

43. Щепеткова А.В. Технологии реализации электронной подписи в России / Шокорова Н.Н., Щепеткова А.В. // Информационные технологии в науке и образовании. Проблемы и перспективы. : сб. ст. по материалам VII Всерос. межвуз. науч-практ. конф. (г.Пенза, 18 марта 2020 г.) /под ред. Л.Р. Фионовой. – Пенза: Изд-во ПГУ, 2020, с. 68-70.

## **Интернет-ресурсы**

44. Единый портал Электронной подписи // URL: <https://iesp.ru/>
45. PKI – Форум 2020. XVIII международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи //URL: <http://pki-forum.ru> (дата обращения 16.11.2020)
46. Применение электронной подписи. Официальный сайт ФНС //URL: [https://www.nalog.ru/rn77/related\\_activities/el\\_doc/use\\_electronic\\_sign/](https://www.nalog.ru/rn77/related_activities/el_doc/use_electronic_sign/) (дата обращения 13.01.2021).
47. Официальный сайт «Цифровая экономика РФ» //URL: <https://digital.gov.ru/ru/activity/directions/858/#section-docs>
48. Электронная подпись // URL: <https://ru.wikipedia.org/wiki/>

## **Приложение А**

*(обязательное)*

**Комплект документов при получении электронной  
подписи и сертификата ключа**



## ДОГОВОР № №1529П-КЭ/10

г. Пенза

12 апреля 2018 г.

ООО «РПЦ «Партнер», именуемое в дальнейшем «Исполнитель», в лице директора Пензенского филиала Залетова Андрея Сергеевича, действующего на основании генеральной доверенности, положения о филиале и выданных Лицензий, размещенных на официальном сайте [parc.ru/penza](http://parc.ru/penza) с одной стороны, и ГАСУСОССЗН ПО "Сердобский дом ветеранов труда", именуемое в дальнейшем «Заказчик», в лице директора Щетинина Александра Владимировича, действующего на основании Устава, с другой стороны, именуемые в дальнейшем также «Стороны», заключили настоящий Договор о нижеследующем:

### 1. ПРЕДМЕТ ДОГОВОРА.

1.1. «Исполнитель» по настоящему договору обязуется предоставить «Заказчику» право использования Системы «Контур-Экстерн», оказать услуги по обслуживанию в Системе и передать иные права на ПО, а «Заказчик» обязуется принять и оплатить оказываемые услуги и права в соответствии с условиями Договора.  
1.2. Оказание услуг и передача прав по настоящему договору осуществляются в соответствии с актом согласования стоимости услуг и передачи прав (Приложение №1) с учетом выбранного «Заказчиком» тарифного плана (таблица сервисов, входящих в тарифный план опубликована в сети интернет на официальном сайте «Исполнителя» [parc.ru/penza](http://parc.ru/penza)).

### 2. ОБЯЗАННОСТИ СТОРОН.

2.1. «Исполнитель» обязуется:  
2.1.1. Осуществлять функции оператора электронного документооборота, функции удостоверяющего Центра (УЦ) в соответствии с Федеральным законом N 63-ФЗ от 06.04.2011 г., иными актами законодательства РФ.  
2.1.2. Обеспечивать защиту информации о персональных данных «Заказчика» согласно действующему законодательству РФ.  
2.1.3. Своевременно предоставлять бухгалтерскую и иную необходимую документацию (счета, счета-фактуры, акты и пр.)  
2.1.4. В течение действия договора осуществлять техническую поддержку «Заказчика» по телефону горячей линии 8 (8412) 233-433.  
2.1.5. Не допускать разглашения конфиденциальных данных «Заказчика», ставших известными при его регистрации в ходе оказания услуг, передачи прав или иным образом.  
2.1.6. Проводить профилактические работы в течение не более чем двух рабочих дней в течение месяца, в период с 1 по 10 число месяца.  
2.2. «Заказчик» обязуется:  
2.2.1. Согласовать и заключить настоящий договор с приложениями, текст которых опубликован в сети интернет на официальном сайте «Исполнителя» [parc.ru/penza](http://parc.ru/penza).  
2.2.2. Предоставить заявление на изготовление сертификата электронной подписи (опубликовано в сети интернет на официальном сайте «Исполнителя» [parc.ru/penza](http://parc.ru/penza)).  
2.2.3. Произвести оплату по счету за услуги и права, согласно Приложению №1.  
2.2.4. При работе, эксплуатации и хранении СКЗИ соблюдать приказ ФАПСИ №152 от 13.06.2001 г., в т.ч. подготовить рабочее место.  
2.2.5. Издать приказ /распоряжение о назначении ответственного лица по работе с СКЗИ. По настоящему договору ответственным лицом считается владелец сертификата. Если ответственным лицом является иное лицо, то «Заказчик» обязуется уведомить Исполнителя дополнительно.  
2.2.6. Соблюдать меры безопасности, изложенные в Инструкции по безопасности на рабочем месте Заказчика (текст инструкции опубликован в сети интернет на официальном сайте «Исполнителя» [parc.ru/penza](http://parc.ru/penza)). При установке сертификатов и лицензий пользоваться необходимым программным обеспечением и соответствующими инструкциями (текст инструкции опубликован в сети интернет на официальном сайте «Исполнителя» [parc.ru/penza](http://parc.ru/penza)).  
2.2.7. Соглашаясь с условиями договора «Заказчик» признает, что ознакомлен с Регламентом УЦ с условиями Сублицензионного договора на право пользования Системой «Контур-Экстерн», в случае приобретения лицензии СКЗИ КриптоПро – с условиями Сублицензионного договора на поставку программных продуктов, под торговой маркой КриптоПро, в случае приобретения право пользования программы для ЭВМ «Контур-Отчет ПФ» право использования ПО для управления сертификатом - с условиями соответствующих Лицензионных/Сублицензионных договоров, текст которых опубликован в сети интернет на официальном сайте «Исполнителя» [parc.ru/penza](http://parc.ru/penza), и обязуется выполнять их требования.

### 3. ЦЕНА ДОГОВОРА И ПОРЯДОК РАСЧЕТОВ.

3.1. Общая стоимость по настоящему договору определяется в акте согласования стоимости услуг и передачи права и составляет 7 200,00 рублей, в том числе НДС 183,05 руб.  
3.2. «Исполнитель» выставляет «Заказчику» счет за услуги и права, который оплачивается в порядке 100% предоплаты до момента оказания услуг, передачи права.  
3.3. Срок начала оказания услуг, передачи права: не позднее 5 дней с момента предоставления надлежаще оформленного полного пакета документов (опубликован в сети интернет на официальном сайте «Исполнителя» [www.parc.ru/penza](http://www.parc.ru/penza)), поступления на расчетный счет Исполнителя оплаты от «Заказчика», а также присутствия представителя «Заказчика» в офисе «Исполнителя».  
3.4. Для бюджетных организаций оплата по настоящему договору может быть осуществлена в авансовом порядке в размере 30% от общей стоимости путем перечисления денежных средств на расчетный счет «Исполнителя» в течение 5 (пяти) банковских дней после подписания настоящего Договора на основании счета, выставленного «Исполнителем». Оставшаяся сумма в размере 70% подлежит оплате в течение 10 (десяти) дней после получения Акта приема-передачи и /или иных бухгалтерских документов.  
3.5. Моментом оплаты услуг, передачи права считается зачисление денежных средств на расчетный счет «Исполнителя».  
3.6. По факту оказания услуг, передачи права стороны подписывают акт сдачи-приемки (приложение №2), иные бухгалтерские документы.

### 4. СРОК ДЕЙСТВИЯ И ПОРЯДОК РАСТОРЖЕНИЯ ДОГОВОРА.

4.1. Настоящий договор вступает в силу со дня его подписания сторонами и действует в течение двенадцати месяцев с момента подписания к системе.  
4.2. Для бюджетных организаций настоящий договор вступает в силу с момента подписания и действует до 31 декабря текущего года, а в части оказания услуг до полного их исполнения.

4.3. Договор может быть продлен на следующий период, при этом обязательным условием продления действия договора является согласие «Заказчика», выраженное до истечения действия договора, в виде предоставления надлежащим образом оформленного полного пакета документов (опубликован в сети интернет на официальном сайте «Исполнителя» [www.parc.ru/penza](http://www.parc.ru/penza)), поступления на расчетный счет Исполнителя оплаты от «Заказчика», а также присутствия представителя «Заказчика» в офисе «Исполнителя». При невыполнении этого условия действие договора прекращается.

4.4. Договор может быть расторгнут по соглашению сторон в соответствии с действующим законодательством РФ.

4.5. Действие настоящего договора может быть досрочно прекращено в следующих случаях:

- «Заказчиком» в одностороннем порядке, при условии письменного уведомления «Исполнителя» и компенсации фактически оказанных услуг, передачи прав;
- «Исполнителем» в одностороннем порядке при просрочке оплаты «Заказчиком» более чем на 1(один) месяц от установленного договором срока.

В случае досрочного расторжения договора либо неоплаты и (или) неполной оплаты, ответом «Исполнителя» является отзыв (аннулирование) сертификата «Заказчика».

#### 5. ОТВЕТСТВЕННОСТЬ СТОРОН И ПОРЯДОК РАССМОТРЕНИЯ СПОРОВ

5.1. За неисполнение или ненадлежащее исполнение своих обязательств по настоящему договору стороны несут друг перед другом ответственность в порядке, установленном настоящим договором и действующим законодательством РФ.

5.2. По настоящему договору «Исполнитель» несет перед «Заказчиком» ответственность только за реальный ущерб, установленный решением суда. Возмещение «Заказчику» упущенной выгоды, морального вреда и иного не предусматривается.

5.3. В случае нарушения стороной своих обязательств по договору, виновная сторона уплачивает пени в размере 1/300 став рефинансирования Центрального Банка РФ, за каждый день просрочки исполнения обязательств.

5.4. Все споры, разногласия и претензии, стороны будут стремиться решить путем переговоров с соблюдением обязательно претензионного порядка. Срок рассмотрения 10 дней со дня получения соответствующих разногласий/претензий. Если претензия не получена в связи с отсутствием представителя в месте получения (адрес регистрации либо местонахождения), либо в связи с отказом представителя от получения сообщения, стороны признают такое сообщение полученным.

5.5. При неурегулировании спора в претензионном порядке, спор подлежит рассмотрению в Арбитражном суде Пензенской области.

5.6. Стороны договорились, что любые авансы, предварительные оплаты, не дают кредитору по соответствующему денежному обязательству права и не выступают основаниями для начисления и взимания процентов за пользование денежными средствами на условиях и в порядке, предусмотренных ст. 317.1. Гражданского кодекса РФ.

#### 6. ФОРС-МАЖОР

6.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по настоящему договору, если оно вызвано обстоятельствами непреодолимой силы, таких как стихийные бедствия, массовые беспорядки, террористические акты, противоправные действия третьих лиц, изменения в законодательстве, при условии, что данные обстоятельства непосредственно повлияли на выполнение условий по настоящему договору. Сторона, которая на них ссылается, обязана предоставить официальное подтверждение таких обстоятельств, подписанное уполномоченными государственными органами.

#### 7. ПРОЧИЕ УСЛОВИЯ

7.1. Все изменения к настоящему договору оформляются с помощью дополнительных соглашений, которые подписываются уполномоченными представителями и заверяются печатями Сторон.

7.2. В случае изменения данных «Заказчика», указанных в заявлении на изготовление сертификата электронной подписи последний обязан немедленно известить об этом «Исполнителя». При этом «Исполнитель» производит бесплатный перевыпуск сертификата на основании данных вновь предоставленного заявления, сроком не более первоначального, при условии, что к концу срока действия сертификата осталось не менее одного месяца. В случае последующих изменений, перевыпуск производится по действующим ценам «Исполнителем».

7.3. При необходимости «Исполнитель» выдает дополнительные сертификаты ключа подписи по заявлению «Заказчика» согласно Регламента УЦ по ценам, действующим на момент заказа. Оплата «Заказчиком» производится на основании выставленного счета.

7.4. Действие сертификата ключа подписи может быть приостановлено «Исполнителем» на основании указания лиц или органов имеющих такое право в силу закона, а в системе электронного документооборота также в силу установленных для нее правил пользования.

7.5. Стороны согласились на использование факсимиле (клише) подписи уполномоченных лиц Сторон под настоящим договором в случае, если положения условий настоящего договора не изменяются. Стороны признают, что договор, подписанный с помощью факсимиле, имеет такую же юридическую силу, какую имеет документ, собственноручно подписанный уполномоченным лицом Сторон. При этом «Заказчик» заверяет собственноручной подписью данные в заявлении на изготовление сертификата ЭП.

7.6. Настоящий договор составлен в двух подлинных экземплярах, имеющих равную юридическую силу, по одному для каждой Стороны.

«ИСПОЛНИТЕЛЬ»  
ООО «РПЦ «Партнер»  
410005, г. Саратов, ул. Б.Садовая, д.239, к.42, оф.422  
440000, г. Пенза, ул. Московская, д.29  
т/ф (8412) 233-433  
ИНН 6454066437 КПП 583643001  
р/счет № 40702810412240001390  
в Филиал ПАО Банк ВТБ в г. Нижнем Новгороде  
кор/счет № 3040161020000000837БИК 042202837



/А.С. Залетов /

«ЗАКАЗЧИК»  
ГАСУ СОСЗН ПО "Сердобский дом ветеранов труда"  
442894, Пензенская обл, Сердобск г, Ленина ул, дом № 291  
тел./факс 5-24-38, 2-01-06  
ИНН 5805000612 КПП 580501001  
р/с 40601410956553000001  
в Отделении Пенза 2 Пенза  
и/с  
БИК 045655001



М.П.

И.И.И.И.И.

Приложение №1

к договору № №1529П-КЭ

Акт согласования стоимости услуг и прав к договору № №1529П-КЭ/10

| № | Наименование                                                                                                                                       | Кол-во | Ед. | Цена за единицу(руб) | Стоимость без налога (руб) | Стоимость налогом НДС(руб) |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------|--------|-----|----------------------|----------------------------|----------------------------|
| 1 | Лицензия СКЗИ КриптоПро CSP версии 4.0 (годовая)                                                                                                   | 1      | шт  | 700,00               | 700,00                     | 70                         |
| 2 | Право использования ПО для управления Сертификатом с выдачей квалифицированного Сертификата для Системы «Контур-Экстерн» сроком действия один год. | 1      | шт  | 1 000,00             | 1 000,00                   | 1 00                       |
| 3 | Право использования программы для ЭВМ "Контур-Отчет ПФ" сроком на 1 год.                                                                           | 1      | шт  | 1 000,00             | 1 000,00                   | 1 00                       |
| 4 | Право использования программы для ЭВМ Система "Контур-Экстерн" сроком на 1 год (без НДС)                                                           | 1      | шт  | 3 300,00             | 3 300,00                   | 3 30                       |
| 5 | Сопровождение Системы "Контур-Экстерн" сроком на 1 год (в т.ч. НДС 18%)                                                                            | 1      | шт  | 1 200,00             | 1 016,95                   | 1 20                       |

Итого: 7 201  
В том числе НДС: 18:  
Всего к оплате: 7 201

Всего наименований 5, на сумму 7 200,00 руб  
Семь тысяч двести рублей 00 копеек

Лицензия на право использования СКЗИ «КриптоПро CSP», право пользования программой для ЭВМ «Контур-Экстерн», право пользования программой для ЭВМ «Контур-Отчет ПФ», право использования ПО управления сертификатом НДС не облагается на основании пп. 26 пункта 2 статьи 149 главы 21 Налогового Кодекса Российской Федерации

Приобретая Лицензию на право использования СКЗИ «КриптоПро CSP», право пользования программой для ЭВМ «Контур-Экстерн», право пользования программой для ЭВМ «Контур-Отчет ПФ», право использования ПО управления сертификатом, Вы соглашаетесь с текстом Лицензионных/ Сублицензионных договоров размещенных на сайте [parc.ru/pei](http://parc.ru/pei)

«ИСПОЛНИТЕЛЬ»  
ООО «РПЦ «Партнер»  
410005, г. Саратов, ул. Б.Садовая, д.239, к.42, оф.422  
440000, г. Пенза, ул. Московская, д.29  
(8412) 233-433  
ИНН 6454066437 КПП 583643001  
р/счет № 40702810412240001390  
в Филиал ПАО Банк ВТБ в г. Нижнем Новгороде  
кор/счет № 30101810200000000837БИК 042202837



А.С. Залетов /

«ЗАКАЗЧИК»  
ГАСУ СОСЗН ПО "Сердобский дом ветеранов труда"  
442894, Пензенская обл, Сердобск г, Ленина ул, дом № 29  
тел./факс 5-24-38, 2-01-06  
ИНН 5805000612 КПП 580501001  
р/с 4060181095655300001  
в Отделении Пенза / Пенза  
к/с  
БИК 045655001



М.П.

## Регистрационная карта абонента

Краткое наименование в соответствии с учредительными документами

ГАСУСОССЗН ПО "Сердобский дом ветеранов труда"

Тарифный план: №договора 1529П-КЭ/10

ИНН: 5805000612

КПП: 580501001

РНС ФСС: 5802005267

КП ФСС: 58021

ОГРН: 1025800598031

Код ИФНС:

Юридический адрес: 442894, Пензенская область, город Сердобск, улица Ленина, дом 291

☒ Почтовый адрес совпадает с юридическим

Почтовый адрес: 442894, Пензенская область, город Сердобск, улица Ленина, дом 291

Р/С 40601810956553000001

К/С

БИК: 045655001

В к: Отделение Пенза г. Пенза

Тел. Факс: 8(84167)2-01-06

## Сведения о руководителе

Фамилия: Щетинин

Имя: Александр

Отчество: Владимирович

Должность: Директор

Действующий на основании:

Устава

Телефон/факс:

8(84167)2-01-06

## 2. Сведения о владельце сертификата:

Фамилия: Щетинин

Имя: Александр

Отчество: Владимирович

Должность: Директор

Идентификационный номер: 580502563322

Паспорт:

Серия: 56

08

Номер: 783492

выдан: ОУФМС России по Пензенской обл. в Сердобском районе

когда: 16 09 2008

СНИЛС: 154 - 394 - 318 74

e-mail:

телефон:

Подтверждаю свое согласие на использование ИСПОЛНИТЕЛЕМ принадлежащих мне персональных данных в целях исполнения настоящего Договора.

(подпись) Щетинин А.В.

(расшифровка подписи)

## 3. Правильность сведений, указанных в пп. 1-2, гарантирую.

Щетинин А.В.

ФИО

Директор

подпись

дата: 12 04 2018 г.

Необходимо заполнить все поля регистрационной карты в электронном виде. В случае отсутствия реквизита

ООО "КРИПТО-ПРО" <http://www.CryptoP>  
info@CryptoP

**Лицензия на использование программного продукта  
КриптоПро CSP**

Настоящая лицензия действует на основании Лицензионного договора между ООО «КРИПТОПРО» и ЗАО «ПФ «СКБ Контур» в рамках Сублицензионного договора, заключенного между ЗАО «ПФ «СКБ Контур» и ООО «РПЦ «Партнер» (наименование СОС), по Сублицензионному договору между ООО «РПЦ «Партнер» (Наименование СОС) и Пользователем (физическим и юридическим лицом).

Настоящая лицензия дает право Пользователю на установку и использование одной копии Изделия (программного продукта) «КриптоПро CSP» в соответствии с Сублицензионным договором и правилами пользования, изложенными в эксплуатационной документации.

*Предупреждение. Перед установкой дистрибутива требуется проверить его целостность в соответствии с рекомендациями, изложенными в эксплуатационной документации.*

Выдана организации (пользователю)

Серийный номер «КриптоПро CSP»

1-1 -8 -I

Ключ установки

Действует до: 26.05.2019

Лицензия сформирована

Дата 26.02.2018

