

«УТВЕРЖДАЮ»
Генеральный директор
ООО «СберКорус»



Тарасов В.Г.

«30» августа 2024

Порядок (Регламент)
реализаций функций и исполнения обязанностей
аккредитованного Удостоверяющего центра
ООО «СберКорус»

г. Санкт-Петербург
2024 г.

ООО «СберКорус»

Оглавление

1. Основные понятия	3
2. Общие положения	4
2.1. Предмет регулирования	4
2.2. Сведения об Удостоверяющем центре	5
2.3. Порядок информирования о предоставлении услуг Удостоверяющего центра	5
2.4. Стоимость услуг Удостоверяющего центра	5
2.5. Присоединение к Регламенту	6
2.6. Изменение (дополнение) Регламента	6
2.7. Односторонний отказ от Регламента	6
3. Перечень реализуемых Удостоверяющим центром функций (оказываемых услуг)	7
4. Права и обязанности Удостоверяющего центра и других Субъектов	8
4.1. Права Удостоверяющего центра:	8
4.2. Обязанности Удостоверяющего центра	9
4.3. Ответственность Удостоверяющего центра	11
4.4. Обязанности Заявителя	12
4.5. Права Владельца КСКПЭП	12
4.6. Обязанности Владельца КСКПЭП	12
4.7. Ответственность Заявителя и/или Владельца КСКПЭП:	13
5. Порядок и сроки выполнения процедур, необходимых для предоставления услуг Удостоверяющим центром	13
5.1. Процедура создания ключей электронной подписи и ключей проверки электронной подписи	13
5.2. Процедура создания и выдачи КСКПЭП для Владельцев	17
5.3. Подтверждение действительности электронной подписи, использованной для подписания электронных документов	22
5.4. Процедуры, осуществляемые при прекращении действия или аннулирования КСКПЭП	23
5.5. Порядок ведения реестра сертификатов	24
5.6. Порядок технического обслуживания реестра сертификатов	25
6. Порядок исполнения обязанностей Удостоверяющего центра	25
7. Сроки действия ключей ЭП и сертификатов	28
8. Список приложений	28
Приложение №1 Форма Заявления физического лица на изготовление КСКПЭП	29
Приложение №2 Перечень документов, представляемых Заявителем УЦ для изготовления и включения в КСКПЭП	30
Приложение №3 Форма заявления на прекращение действия КСКПЭП	31
Приложение №4. Форма заявления на проверку подлинности электронной подписи в электронном документе	32
Приложение №5 Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи	33

1. Основные понятия

В деятельности Удостоверяющего центра ООО «СберКорус» используются основные понятия в значениях, указанных в Федеральном законе от 06.04.2011 № 63-ФЗ «Об электронной подписи» и в настоящем Регламенте:

Квалифицированный сертификат ключа проверки электронной подписи (далее – КСКПЭП или Сертификат) – сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, и являющийся в связи с этим официальным документом.

Список отозванных сертификатов (далее – СОС) – файл в формате crl опубликованный Удостоверяющим центром, содержащий в себе серийные номера аннулированных КСКПЭП и КСКПЭП, прекративших свое действие, на определенный момент времени, до истечения установленного срока их действия.

Отзыв КСКПЭП – операция Удостоверяющего центра, направленная на аннулирование или прекращение действия КСКПЭП, до истечения установленного срока его действия, влекущая за собой включение в СОС серийного номера этого КСКПЭП.

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

Вручение сертификата ключа проверки электронной подписи – передача сотрудником/доверенным лицом Удостоверяющего центра изготовленного этим Удостоверяющим центром Сертификата его Владелцу.

Доверенное лицо Удостоверяющего центра – физическое лицо, являющееся сотрудником юридического лица или индивидуального предпринимателя, с которым Удостоверяющий центр заключил договор, наделенное полномочиями по идентификации личности Заявителя при его личном присутствии, проверке и приему от него документов сертификата, созданного Удостоверяющим центром.

Заявитель – физическое лицо, обращающееся в Удостоверяющий центр с соответствующим заявлением за услугой по изготовлению (выдаче) КСКПЭП в качестве будущего Владельца такого сертификата.

Усиленная квалифицированная электронная подпись (далее – УКЭП) – усиленная квалифицированная электронная подпись, соответствующая следующим признакам:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после его подписания;
- создается с использованием средств электронной подписи;
- ключ проверки электронной подписи указан в квалифицированном сертификате ключа проверки электронной подписи;
- для создания и проверки используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи».

Субъекты – это все лица, которые в силу настоящего Регламента, договора об оказании услуг УЦ или действующего законодательства обязаны соблюдать правила и выполнять все требования, предусмотренные настоящим Регламентом. Субъектами, на которых распространяется действие настоящего Регламента, являются – Заявитель УЦ, Владелец КСКПЭП, Доверенное лицо УЦ и/или Удостоверяющий центр (если это соответствует смысловой нагрузке соответствующего условия).

Ключевой носитель – аппаратное или программно-аппаратное устройство хранения ключей ЭП, являющееся персональным средством, обеспечивающим защиту хранения ключей ЭП.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Компрометация ключа подписи – нарушение конфиденциальности или подозрение в нарушении конфиденциальности ключа электронной подписи, хищение, утрата, и иные действия/бездействия Владельца КСКПЭП, в результате которых ключи электронной подписи могут стать доступными неуполномоченным и/или посторонним лицам.

Доверенная информационная система – любая информационная система (программа для ЭВМ), участниками которой может быть ограниченный круг лиц, определенный ее оператором или соглашением участников этой информационной системы, и в которой работает и/или планирует работать Заявитель УЦ.

Корректная (подлинная) электронная подпись – электронная подпись, проверка которой с помощью средства электронной подписи и с использованием сертификата ключа подписи, действующего на момент создания подписи, дала положительный результат.

Некорректная (неподлинная) электронная подпись – электронная подпись, проверка которой с помощью средства электронной подписи и с использованием сертификата ключа подписи, действующего на момент создания подписи, дала отрицательный результат.

Сотрудник Удостоверяющего центра - уполномоченное лицо Удостоверяющего центра, наделенное Удостоверяющим центром полномочиями по осуществлению действий по созданию, регистрации и управлению КСКПЭП Владельцев сертификата Удостоверяющего центра, а также иными полномочиями согласно настоящего Регламента.

Средство криптографической защиты информации (СКЗИ):

- программное, аппаратное или аппаратно-программное средство, реализующее криптографические алгоритмы преобразования данных и предназначенное для защиты информации от несанкционированного доступа при ее обработке, хранении и передаче по каналам связи;

- программное, аппаратное или аппаратно-программное средство, реализующее криптографические алгоритмы преобразования данных и предназначенное для защиты информации от искажения информации и навязывания ложной информации;

- программное, аппаратное или аппаратно-программное средство, предназначенное для изготовления и распределения криптографических ключей.

Фотофиксация – осуществление фотосъемки будущего владельца КСКПЭП. Производится в целях сбора доказательственной базы исполнения Удостоверяющим центром требований Федерального закона № 63-ФЗ с помощью специально предназначенного для данных целей фотоаппарата.

Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Электронная подпись – (далее – ЭП) - 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.

2. Общие положения

2.1. Предмет регулирования:

Настоящий документ содержит и регламентирует порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей (далее – Регламент), учитывает положения действующего законодательства Российской Федерации, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите

информации», Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных», и иными нормативными правовыми актами РФ, осуществляющих правовое регулирование отношений в области использования электронной подписи, является руководящим документом аккредитованного Удостоверяющего центра ООО «СберКорус» (далее – Удостоверяющий центр, УЦ) и иных Субъектов УЦ, и устанавливает общий порядок и условия предоставления Удостоверяющим центром услуг по созданию и выдаче КСКПЭП и дополнительных услуг, в т.ч. связанных с управлением КСКПЭП.

Действующая редакция настоящего Регламента размещена в сети Интернет по адресу www.esphere.ru, в разделе «Удостоверяющий центр».

2.2. Сведения об Удостоверяющем центре:

2.2.1. Общество с ограниченной ответственностью «СберКорус» (ИНН 7801392271, КПП 780201001), именуемое в дальнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Санкт-Петербург. Свидетельство о регистрации серия 78 № 005628307 выдано 03 ноября 2005 Межрайонной инспекцией Федеральной налоговой службы №15 по Санкт-Петербургу.

2.2.2. Удостоверяющий центр осуществляет функции по созданию и выдаче КСКПЭП и иные функции удостоверяющего центра в соответствии с требованиями действующей редакции Федерального закона № 63-ФЗ от 06.04.2011 «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативно- правовыми актами.

2.2.3. УЦ осуществляет свою деятельность на территории Российской Федерации в качестве профессионального участника рынка на основании аккредитации в соответствии с решением Правительственной комиссии, уполномоченной на принятие решения об аккредитации удостоверяющих центров, лицензии Управления Федеральной службы безопасности Российской Федерации по г. Санкт-Петербургу и Ленинградской области, размещенных в сети «Интернет» по адресу: www.esphere.ru в разделе «О Компании - Документы».

2.2.4. Юридический адрес и фактическое местонахождение Удостоверяющего центра: 194100, г. Санкт-Петербург, Б. Сампсониевский проспект, д.68, лит.Н, пом.1Н.

2.2.5. Адреса офисов Удостоверяющего центра опубликованы на сайте <https://www.esphere.ru/products/uc/>

2.2.6. Удостоверяющий центр осуществляет свою работу в круглосуточном режиме.

Рабочий день офисов Удостоверяющего центра (далее – рабочий день) – промежуток времени с 09:00 по 18:00 (МСК.) каждого рабочего дня недели, за исключением выходных и нерабочих праздничных дней. Информация о времени посещения офиса Удостоверяющего центра предоставляется при обращении Заявителя УЦ по контактным данным, указанным на сайте Удостоверяющего центра.

2.2.7. УЦ зарегистрирован в реестре мирового пространства идентификаторов объектов под номером 1.2.643.3.285, осуществляет свою деятельность с использованием программно-аппаратного комплекса «Удостоверяющий центр «КриптоПро УЦ».

2.3. Порядок информирования о предоставлении услуг Удостоверяющего центра

2.3.1. Информирование по вопросам предоставления услуг Удостоверяющего центра осуществляется следующими способами:

- 1) по контактному номеру телефона: 8 (800) 100-8-812;
- 2) по адресу электронной почты, e-mail: help@esphere.ru;
- 3) путем опубликования информации на официальном сайте: www.esphere.ru

2.3.2. Информирование Субъектов по вопросам предоставления услуг Удостоверяющим центром производится либо в результате общения по контактными телефонам, либо посредством направления электронного письма на адрес, указанный при обращении и/или ином взаимодействии с Удостоверяющим центром, либо посредством направления SMS-уведомлений на телефонный номер, представленный Заявителем УЦ и/или Владелец КСКПЭП в Удостоверяющий центр, и/или посредством размещения информации на сайте по адресу www.esphere.ru, или сочетание таких способов.

2.4. Стоимость услуг Удостоверяющего центра

Удостоверяющий центр осуществляет свою деятельность на платной основе.

Стоимость и состав услуг УЦ, порядок и способы их получения размещены на сайте Удостоверяющего центра (www.esphere.ru) в разделе «Электронная подпись». Данная информация может изменяться УЦ в одностороннем порядке и/или по условиям заключаемого договора по согласованию с Заявителем.

Текущую информацию о стоимости услуг Удостоверяющего центра любое лицо может получить способами, указанными в п.2.3.1 Регламента.

2.5. Присоединение к Регламенту

Присоединение Заявителя УЦ к настоящему Регламенту и оказание такому лицу услуг, предусмотренных настоящим Регламентом, осуществляется либо путем подписания двустороннего договора, либо путем представления заявления на заключение договора и присоединение к Условиям о предоставлении услуг и иных обязательствах ООО «СберКорус», либо путем представления (подписания) заявления на изготовление КСКПЭП, в т.ч. электронной подписью, либо путем оплаты счета, оформленного согласно Договору (Оферты) на оказание услуг удостоверяющего центра, или выражением волеизъявления на его оплату.

При использовании Субъектом доверенной информационной системы для создания и получения КСКПЭП, присоединяясь к настоящему Регламенту, Субъект УЦ подтверждает своё ознакомление с руководством пользователя доверенной информационной системы по работе в ней.

Факт присоединения указанного Субъекта к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент присоединения к нему одним из вышеописанных способов. Субъект, присоединившийся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями п.2.6 настоящего Регламента.

Удостоверяющий центр оформляет указанному Субъекту счет на оплату услуг по изготовлению КСКП ЭП с теми наименованием, составом и объемом услуг, которые получены им от Субъекта в ходе письменной или устной консультации. Субъект, оплачивая счет на оплату услуг по изготовлению КСКПЭП в рамках определенного договора, и/или подписывая заявление на изготовление КСКПЭП с «дополнительными услугами», подтверждает свою готовность получить указанную в нем услугу согласно наименованию, в составе и объеме, указанных в таком счете или в заявлении на изготовление КСКПЭП.

2.6. Изменение (дополнение) Регламента

Внесение изменений в настоящий Регламент, включая приложения к нему, производится УЦ в одностороннем порядке путем опубликования новой редакции Регламента на своем сайте по адресу: www.esphere.ru в разделе «Удостоверяющий центр».

Любые изменения, вносимые в настоящий Регламент, с момента вступления в силу распространяются на всех лиц, присоединившихся к настоящему Регламенту, в том числе присоединившихся к настоящему Регламенту ранее даты вступления изменений в силу.

2.7. Односторонний отказ от Регламента

Субъект, присоединившийся к Регламенту, вправе в любое время, в том числе в случае несогласия с изменениями (дополнениями), внесенными Удостоверяющим центром в Регламент, в одностороннем внесудебном порядке отказаться от исполнения Регламента:

- направив в Удостоверяющий центр заявление на прекращение действия, выданного ему КСКПЭП;

- направив в Удостоверяющий центр уведомление, в т.ч. о расторжении договора об оказании услуг УЦ. Указанное уведомление должно быть оформлено в письменной форме и направлено в Удостоверяющий центр способом, позволяющим достоверно установить факт его получения Удостоверяющим центром. Данное письменное уведомление, полученное Удостоверяющим центром, является основанием для обязательного досрочного прекращения действия КСКПЭП лица, предоставившего уведомление об отказе от исполнения Регламента, в порядке, установленном настоящим Регламентом и Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи».

После получения указанного заявления/уведомления Удостоверяющим центром на лицо, предоставившее данное заявление/уведомление, действие Регламента не распространяется.

Прекращение действия настоящего Регламента не освобождает Субъекта от исполнения обязательств, возникших до указанного дня прекращения его действия, и не освобождает от ответственности за их неисполнение (ненадлежащее исполнение).

Удостоверяющий центр вправе в одностороннем внесудебном порядке отказаться от исполнения настоящего Регламента в случае нарушения Субъектом, присоединившимся к Регламенту, условий настоящего Регламента и/или заключенного договора об оказании услуг УЦ. Отказ от исполнения Регламента не влияет на действительность электронных подписей Субъекта, присоединившегося к Регламенту, созданных до даты такого отказа.

Выполнение ООО «СберКорус» функций Удостоверяющего центра может быть прекращено в порядке, установленном законодательством Российской Федерации, и на основании локально-нормативных актов ООО «СберКорус». В случае прекращения выполнения ООО «СберКорус» функций Удостоверяющего центра реестр выданных сертификатов передается головному удостоверяющему центру в соответствии с Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами.

3. Перечень реализуемых Удостоверяющим центром функций (оказываемых услуг)

3.1. Создание и выдача КСКПЭП в соответствии с требованиями, указанными в Федеральном законе № 63-ФЗ от 06.04.2011 «Об электронной подписи».

3.2. Осуществление в соответствии с правилами подтверждения владения ключом электронной подписи, описанного в п. 5.1.1. настоящего Регламента, подтверждения владения Заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения Сертификата.

3.3. Установление сроков действия КСКПЭП.

3.4. Отзыв КСКПЭП в виде аннулирования КСКПЭП или прекращения действия КСКЭП, до истечения установленного его срока, выданных Удостоверяющим центром, в случаях, установленных федеральными законами РФ, принимаемыми в соответствии с ними нормативными правовыми актами, соглашением между Удостоверяющим центром и Заявителем, или настоящим Регламентом.

3.5. Выдача средств электронной подписи, содержащих ключ электронной подписи и ключ проверки электронной подписи или обеспечивающих возможность создания ключа электронной подписи и ключа проверки электронной подписи Заявителем.

3.6. Ведение реестров выданных Удостоверяющим центром КСКПЭП, аннулированных или прекративших действие КСКПЭП, до истечения установленного срока их действия, (далее – реестр сертификатов), в том числе включающего в себя информацию, содержащуюся в выданных этим УЦ КСКПЭП, и информацию о датах прекращения действия или аннулирования КСКПЭП и об основаниях таких прекращений действия или аннулирования.

3.7. Создание ключей электронной подписи и ключей проверки электронной подписи по обращению Заявителя УЦ с гарантией обеспечения конфиденциальности ключей ЭП.

3.8. Проверка уникальности ключей проверки электронной подписи в реестре сертификатов.

3.9. Осуществление проверки электронных подписей электронных документов на подлинность (корректность) по обращению участников электронного взаимодействия и/или предоставление информации о статусе сертификата ключа проверки электронной подписи в порядке, предусмотренном в п. 5.3 настоящего Регламента.

3.10. Отправка в единую систему идентификации и аутентификации сведений о лице, получившем КСКПЭП, в объеме, необходимом для его регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате.

3.11. Осуществление по желанию Владельца КСКПЭП безвозмездной регистрации в единой системе идентификации и аутентификации в порядке, предусмотренном в п.4.1.16, п.4.5.6 Регламента.

3.12. Осуществление иной связанной с использованием электронной подписи и/или средств электронной подписи деятельности.

4. Права и обязанности Удостоверяющего центра и других Субъектов

в рамках исполнения функций, предусмотренных статьями 13 - 15, 17 и 18 Федерального закона № 63-ФЗ от 06.04.2011 «Об электронной подписи», в т.ч.:

4.1. Права Удостоверяющего центра:

4.1.1. Запрашивать у Заявителя УЦ документы и/или сведения для подтверждения любой содержащейся в заявлении на изготовление КСКПЭП информации, а также запрашивать дополнительные, подтверждающие достоверность представленных им сведений документы в случае наличия противоречий между сведениями, представленными Заявителем и данными в иных представленных документах.

4.1.2. Обрабатывать персональные данные Заявителя – физического лица с использованием технических средств.

4.1.3. Не принимать от Заявителя документы, не соответствующие требованиям действующих нормативных актов Российской Федерации, требованиям настоящего Регламента.

4.1.4. Отказать Заявителю в принятии заявления в случае невыполнения им обязанностей указанных в п.4.4 Регламента и/или установленных частью 2 статьи 18 Федерального закона № 63-ФЗ от 06.04.2011 «Об электронной подписи», и принимаемыми в соответствии с ним нормативными правовыми актами РФ, а также в случае, если услуга по созданию и выдаче КСКПЭП не оплачена в надлежащем порядке.

4.1.5. Отказать Заявителю в принятии заявления в случае подачи заявления на изготовление КСКПЭП с ошибками, исправлениями, подчистками и/или приписками, не подтвержденными собственноручной подписью Заявителя.

4.1.6. Отказать Заявителю в принятии заявления в случае, если Заявитель-физическое лицо не предоставил письменного согласия на обработку своих персональных данных и/или не согласился с обработкой и хранением персональных данных.

4.1.7. Отказать Заявителю в принятии заявления в случае, если Заявитель отказывается или уклоняется от посещения Удостоверяющего центра лично, когда это необходимо в целях подтверждения его волеизъявления, предоставленной информации и документов или удостоверения его личности.

4.1.8. Без заявления Владельца КСКПЭП на прекращение действия КСКПЭП прекратить действие КСКПЭП до истечения срока его действия:

- в случае наличия у УЦ достоверных сведений о нарушении конфиденциальности ключа электронной подписи Владельца КСКПЭП;
- невыполнения владельцем КСКПЭП обязанностей, установленных законодательством Российской Федерации в области электронной подписи;
- в случае появления у УЦ достоверных сведений о том, что документы и/или сведения, предоставленные Заявителем в целях создания и получения им Сертификата, не являются подлинными и/или не подтверждают достоверность всей информации, включенной в данный Сертификат;
- в случае отсутствия оплаты за услугу по созданию и выдаче данного сертификата в сроки и в порядке, описанные в договоре, заключенном между УЦ и Заявителем;
- в случае обнаружения в КСКПЭП «опечатки» в сведениях, внесённых в Сертификат;
- в случае одностороннего внесудебного отказа Заявителя /Клиента /Владельца КСКПЭП от исполнения настоящего Регламента путем предоставления в Удостоверяющий центр соответствующего заявления/уведомления (п.2.7 Регламента);
- в случае непредставления Заявителем подтверждения ознакомления с информацией, содержащейся в КСКПЭП согласно п. 4.6.8 Регламента;
- в случае получения Удостоверяющим центром подтверждения факта смерти Владельца КСКПЭП – физического лица;

- в иных случаях, установленных Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между Субъектами.

4.1.9. Отказать в прекращении срока действия КСКПЭП в случае ненадлежащего оформления соответствующего заявления (Приложение № 3 к настоящему Регламенту).

4.1.10. Осуществить проверку подлинности электронной подписи в электронном документе и/или предоставить информацию о статусе сертификата ключа проверки электронной подписи в порядке, предусмотренном в п. 5.3 настоящего Регламента.

4.1.11. Наделять Доверенных лиц УЦ полномочиями по установлению личности Заявителя, проверке и приему документов, по вручению КСКПЭП, ключевого носителя от имени УЦ.

4.1.12. Отказать в изготовлении КСКПЭП Заявителю в случае, если использованный Заявителем формат запроса на изготовление КСКПЭП не поддерживается УЦ.

4.1.13. Требовать от Субъекта, присоединившегося к Регламенту, безусловного выполнения всех его положений.

4.1.14. Использовать предоставленные Заявителем и указанные в соответствующем заявлении номера телефонов мобильной связи и адреса электронной почты для рассылки уведомлений об окончании срока действия Сертификата, другой информации, которую Удостоверяющий центр сочтет необходимой донести до сведения Заявителя и/или Владельца Сертификата.

4.1.15. Произвести фотофиксацию будущего Владельца КСКПЭП. В отдельных случаях фотофиксация будущего Владельца КСКПЭП производится в анфас со страницей паспорта, на которой размещена фотография. В случае отказа произвести фотофиксацию Удостоверяющий центр вправе потребовать предоставить письменный отказ, выполненный будущим Владельцем КСКПЭП. Письменный отказ в полном объеме должен быть выполнен собственноручно и должен содержать ссылку на факт отказа от проведения фотофиксации, а также фамилию, имя, отчество, дату и расшифровку подписи.

4.1.16. . Отказать в выдаче КСКПЭП в случае, если будущий Владелец КСКПЭП не согласился произвести фотофиксацию в том числе со страницей паспорта, на которой размещена фотография, или выполненный собственноручно отказ от проведения фотофиксации.

4.2. Обязанности Удостоверяющего центра

4.2.1. Информировать Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

4.2.2. Предоставить безвозмездно любому лицу по его обращению, в соответствии с установленным порядком доступа к реестру сертификатов, информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании КСКПЭП.

4.2.3. Обеспечить актуальность информации, содержащейся в реестр сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

4.2.4. Обеспечить конфиденциальность созданных Удостоверяющих центром ключей электронной подписи.

4.2.5. Отказать Заявителю в создании КСКПЭП в случае, если не было подтверждено то, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному Заявителем для получения сертификата.

4.2.6. Отказать Заявителю в создании КСКПЭП в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного Заявителем для получения сертификата.

4.2.7. Не указывать в создаваемом им КСКПЭП ключ проверки электронной подписи, который содержится в КСКПЭП, выданном этому удостоверяющему центру любым другим удостоверяющим центром.

4.2.8. Оказывать услуги в соответствии с требованиями, устанавливаемыми Федеральным законом № 63-ФЗ, другими федеральными законами РФ и принимаемыми в соответствии с ними нормативными правовыми актами.

4.2.9. Создать ключ электронной подписи, ключ проверки электронной подписи согласно п.5.1.1 настоящего Регламента, и КСКПЭП на основании оформленного заявления на изготовление КСКПЭП в соответствии с требованиями к заявлению, указанными в п. 5.2.2, и порядком, определенным в настоящем Регламента.

4.2.10. Использовать для создания ключей электронной подписи и ключей проверки электронной подписи (п.5.1.1 Регламента) сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

4.2.11. Осуществлять проверку достоверности документов и сведений, представленных Заявителем, способами и с использованием инфраструктуры, указанных в ст.18 Федерального закона № 63-ФЗ от 06.04.2011 «Об электронной подписи».

4.2.12. Вносить в создаваемые КСКПЭП только достоверную и актуальную информацию, подтвержденную соответствующими документами и/или сведениями (информацией). Выдавать КСКПЭП его Владельцу в форме электронного документа или на бумажном носителе.

4.2.13. При выдаче КСКПЭП установить (идентифицировать) личность Заявителя – физического лица, обратившегося за получением КСКПЭП, способами, указанными в п. 5.2.3.

4.2.14. В течение срока деятельности Удостоверяющего центра, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации, хранить информацию о реквизитах основного документа, удостоверяющего личность Владельца сертификата – физического лица; о наименовании органа, выдавшего документ, удостоверяющий личность.

4.2.15. Использовать ключ электронной подписи УЦ, выданный Головным удостоверяющим центром, только для заверения создаваемых им (УЦ) КСКПЭП, а также для заверения СОС.

4.2.16. Принять меры по защите ключа электронной подписи УЦ от несанкционированного доступа.

4.2.17. Организовать свою работу по московскому времени. УЦ синхронизирует все свои программные и технические средства обеспечения деятельности.

4.2.18. Обеспечить уникальность серийных номеров создаваемых КСКПЭП.

4.2.19. Обеспечить уникальность значений ключей проверки электронной подписи в созданных КСКПЭП.

4.2.20. Уведомить об отзыве КСКПЭП всех лиц, зарегистрированных в УЦ, посредством публикации СОС, ссылка на который размещена в каждом КСКПЭП, а также на портале уполномоченного федерального органа в области использования электронной подписи <https://e-trust.gosuslugi.ru/CA> в профиле ООО «СберКорус».

Период публикации актуального СОС – не более 12 часов.

При этом при наличии у доверенных информационных систем, для которых Удостоверяющим центром осуществляется выдача сертификатов ключей проверки электронной подписи, требований о публикации СОС в более короткие сроки применяются сроки публикации СОС, предусмотренные требованиями соответствующих информационных систем.

4.2.21. Обеспечивать безвозмездную круглосуточную доступность реестра сертификатов в информационно-коммуникационной сети «Интернет», за исключением периодов планового или внепланового технического обслуживания.

4.2.22. При выдаче КСКПЭП:

- ознакомить с информацией, содержащейся в КСКПЭП.

Подтверждение ознакомления с информацией, содержащейся в КСКПЭП, осуществляется под расписку посредством использования Заявителем УКЭП при наличии у него действующего КСКПЭП либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из

единой системы идентификации и аутентификации и информации из единой биометрической системы. Указанное согласие, подписанное электронной подписью, в том числе простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного физического лица. Удостоверяющий центр обязан хранить информацию, подтверждающую ознакомление заявителя с информацией, содержащейся в квалифицированном сертификате, в течение всего срока осуществления своей деятельности.

- направить в единую систему идентификации и аутентификации сведения о лице, получившем КСКПЭП, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им КСКПЭП (уникальный номер Сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра).

- при получении от лица, которому выдается КСКПЭП, запроса (обращения), адресованного сотруднику Удостоверяющего центра или на адрес электронной почты Удостоверяющего центра (п.2.3), о желании такого лица быть зарегистрированным в единой системе идентификации и аутентификации осуществляет на безвозмездной основе такую регистрацию указанного лица в соответствии с пунктом 5 статьи 18 Федерального закона № 63-ФЗ «Об электронной подписи».

- предоставить Владельцу КСКПЭП руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств криптографической защиты информации (Приложение № 5 к настоящему Регламенту или путем предоставления документа, размещенного в сети Интернет на сайте УЦ).

4.2.23. В случае принятия решения о прекращении своей деятельности как аккредитованного Удостоверяющего центра:

- 1) сообщить об этом в уполномоченный федеральный орган не позднее чем за 1 (Один) месяц до даты прекращения своей деятельности;
- 2) передать в уполномоченный федеральный орган в установленном порядке реестр выданных этим аккредитованным Удостоверяющим центром КСКПЭП;
- 3) передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном Удостоверяющем центре.

4.2.24. Отказать Заявителю в создании КСКПЭП в случае, отсутствия какого-либо документа, предусмотренного Приложением № 2 к Регламенту, и/или отсутствия подтверждения от государственных информационных ресурсов сведений о достоверности информации, представленной Заявителем для включения в КСКПЭП, согласно с ч.2.2, 2.3 ст.18 Федерального закона № 63-ФЗ от 06.04.2011 «Об электронной подписи».

4.2.25. Строго соблюдать срок использования ключей электронной подписи УЦ в соответствии с правилами использования СКЗИ, а также с учетом того, чтобы по окончании сроков действия, соответствующих им КСКПЭП, все подписанные этими ключами сертификаты пользователей и СОС уже прекратили свое действие.

4.2.26. Осуществлять иные действия по реализации прав, предоставленных Заявителю или третьему лицу настоящим Регламентом и/или законодательством Российской Федерации.

4.2.27. Обеспечивать конфиденциальность фотоизображений будущего Владельца КСКПЭП

4.3. Ответственность Удостоверяющего центра

4.3.1. Удостоверяющий центр несет гражданско-правовую и (или) административную ответственность, а его работники несут гражданско-правовую и (или) административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим Регламентом.

4.3.2. Удостоверяющий центр в соответствии с законодательством Российской Федерации будет нести ответственность за вред, причиненный третьим лицам в результате:

- неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг Удостоверяющего центра;

- неисполнения или ненадлежащего исполнения обязанностей, предусмотренных действующим законодательством и настоящим Регламентом.

4.3.3. Удостоверяющий центр не будет нести ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также убытки, возникшие в связи с этим, которые бы получены другим Субъектом в случаях:

- если Удостоверяющий центр обоснованно полагался на сведения, представленные Заявителем;
- подделки, подлога либо иного искажения Заявителем, Владелец КСКПЭП либо третьими лицами информации, содержащейся в заявлении либо иных документах, представленных в Удостоверяющий центр.

4.3.4. Удостоверяющий центр не будет нести ответственность за невозможность использования КСКПЭП в случае, если такая невозможность возникла после создания КСКПЭП и вызвана изменением требований информационных систем или действующих нормативных правовых актов РФ.

4.3.5. Удостоверяющий центр не будет нести ответственность за невозможность выдачи КСКПЭП в случае, если такая невозможность вызвана изменением действующих нормативно-правовых актов РФ.

4.4. Обязанности Заявителя

4.4.1. Предъявить документы, удостоверяющие личность Заявителя – физического лица в соответствии с подразделом 5.2.3. настоящего Регламента.

4.4.2. Обеспечить личную явку в Удостоверяющий центр или к Доверенному лицу УЦ Заявителя – физического лица, в случаях, указанных в п. 5.2.3 настоящего Регламента.

4.4.3. Представить Удостоверяющему центру документы, предусмотренные Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи», иными нормативными правовыми актами РФ, локальными документами доверенных информационных систем. Перечень и порядок предоставления соответствующих документов приведены в Приложении № 2 к настоящему Регламенту.

4.4.4. Безусловно соблюдать положения настоящего Регламента.

4.5. Права Владельца КСКПЭП

4.5.1. Получить под расписку от Удостоверяющего центра КСКПЭП в форме электронного документа и/или в форме документа на бумажном носителе.

4.5.2. Обратиться в УЦ для подачи заявления на прекращение действия КСКПЭП в течение срока действия, соответствующего ключу электронной подписи такого КСКПЭП.

4.5.3. В порядке, предусмотренном настоящим Регламентом, обратиться в УЦ для проверки подлинности электронной подписи в электронном документе и/или предоставления информации о статусе КСКПЭП в порядке, предусмотренном в п. 5.3 настоящего Регламента.

4.5.4. Получить средства (средство) электронной подписи, получившие (получившее) подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи», и право использования программного или программно-аппаратного средства (при его выдаче) на условиях простой (неисключительной) лицензии.

4.5.5. При получении КСКПЭП выразить своё желание о безвозмездной регистрации в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона № 63-ФЗ «Об электронной подписи» путем обращения к сотруднику Удостоверяющего центра или на адрес электронной почты Удостоверяющего центра (п. 2.3).

4.5.6. При обращении за получением КСКПЭП получить информацию о рисках, связанных с использованием ЭП.

4.6. Обязанности Владельца КСКПЭП

4.6.1. Хранить в тайне ключ электронной подписи, принимать все возможные меры для предотвращения его компрометации (т.е. потери, раскрытия, искажения и несанкционированного использования), в частности, не допускать использование принадлежащих ему ключей электронной подписи без своего согласия.

4.6.2. Обеспечить выполнение требований руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение № 5 к настоящему Регламенту или путем предоставленного документа, размещенного в сети Интернет на сайте УЦ.).

4.6.3. Применять для формирования электронной подписи только ключ, соответствующий действующему КСКПЭП.

4.6.4. Не применять ключ электронной подписи, если есть основания полагать, что конфиденциальность данного ключа нарушена.

4.6.5. Уведомить и немедленно обратиться в УЦ с заявлением на прекращение действия КСКПЭП (Приложение № 3 к настоящему Регламенту) в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи, в течение не более чем 1 (Одного) рабочего дня со дня получения информации о таком нарушении.

4.6.6. Не использовать ключ электронной подписи, связанный с КСКПЭП, заявление на прекращение действия которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в УЦ до момента официального уведомления Удостоверяющим центром о досрочном прекращении действия сертификата (до истечения установленного срока его действия), либо об отказе в прекращении действия.

4.6.7. Не использовать ключ электронной подписи, связанный с КСКПЭП, действие которого прекращено.

4.6.8. При получении КСКПЭП ознакомиться с информацией, содержащейся в КСКПЭП, подтвердив этот факт предоставлением расписки в бумажном виде или в электронном виде в соответствии с подразделом 5.2.7 настоящего Регламента.

4.6.9. Информировать Удостоверяющий центр об изменении регистрационных данных Владельца КСКПЭП, влияющих на актуальность сведений, содержащихся в таком Сертификате.

4.6.10. Обеспечивать незамедлительное уничтожение принадлежащих Владельцу сертификата ключей ЭП по истечении сроков действия данных ключей в КСКПЭП. Для уничтожения ключей ЭП должны применяться прошедшие в установленном порядке процедуру оценки соответствия средства электронной подписи, в составе которых реализована функция уничтожения информации.

4.7. Ответственность Заявителя и/или Владельца КСКПЭП предусмотрена:

4.7.1. за полноту и достоверность сведений, указанных в соответствующем заявлении.

4.7.2. за сохранность и правильность эксплуатации СКЗИ и своих ключей электронной подписи.

4.7.3. за ущерб, причиненный другим лицам, случае несвоевременного сообщения о факте компрометации ключей ЭП.

4.7.4. За неисполнение или ненадлежащее исполнение обязательств по настоящему Регламенту Заявитель/Владелец КСКПЭП несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного потерпевшей стороне неисполнением или ненадлежащим исполнением своих обязательств.

5. Порядок и сроки выполнения процедур, необходимых для предоставления услуг Удостоверяющим центром

5.1. Процедура создания ключей электронной подписи и ключей проверки электронной подписи (совместно именуемые далее по тексту - ключи).

5.1.1. Порядок создания ключей электронных подписей и ключей проверки электронных подписей.

Ключи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, с выполнением требований в

отношении автоматизированного рабочего места Удостоверяющего центра, используемого для создания ключей Заявителя.

Создание ключей осуществляется одним из способов:

- а) Заявителем самостоятельно. Заявитель создаёт ключи на своём рабочем месте с использованием предоставленных Удостоверяющим центром, либо с использованием собственных средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности и в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), в т.ч. совместимыми со средствами Удостоверяющего центра.
- б) В Удостоверяющем центре. Ключи создаются Заявителем-физическим лицом или сотрудником УЦ для Заявителя в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), на автоматизированном рабочем месте, аттестованном на соответствие требованиям по технической защите конфиденциальной информации, размещенном в помещении, доступ в которое ограничен. Ключ электронной подписи, созданный таким образом, записывается только на ключевой носитель.

Создание ключей осуществляется Удостоверяющим центром в соответствии с требованиями постановления Правительства Российской Федерации от 03 февраля 2012 г. №79 «О лицензировании деятельности по технической защите конфиденциальной информации», с использованием автоматизированных рабочих мест Удостоверяющего центра, а также средств защиты информации и средств криптографической защиты информации, прошедших процедуру оценки соответствия, аттестованных и(или) сертифицированных по требованиям безопасности информации.

Факт создания ключа электронной подписи и соответствующего ему ключа проверки электронной подписи, содержащегося в КСКПЭП, Удостоверяющим центром, или факт создания данных ключей Заявителем самостоятельно при помощи собственных средств электронной подписи, либо выданных ему Удостоверяющим центром, подтверждается фактом его ознакомления с информацией, указанной в КСКПЭП, согласно требованиям п. 4.6.8 настоящего Регламента, и является документом, подтверждающим его владение ключом проверки, указанным в составе данной информации.

5.1.2. Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра, порядок информирования Владельцев КСКПЭП об осуществлении такой смены.

Плановая смена ключей ЭП УЦ выполняется в период действия ключа ЭП УЦ и выполняется не ранее, чем через 1 (один) год и не позднее, чем через 1 (один) год и 3 (три) месяца после даты начала действия ключа ЭП УЦ.

Плановая смена ключей ЭП УЦ производится по следующим основаниям:

- истечение срока использования ключа ЭП;
- переход на использование новых стандартов ЭП и функции хеширования в соответствии с руководящими документами органа исполнительной власти, уполномоченного в сфере использования электронной подписи.

Процедура плановой смены ключей УЦ осуществляется в течение 1 (одного) рабочего дня в следующем порядке:

- УЦ создает новый ключ ЭП и соответствующий ему ключ проверки ЭП;
- УЦ направляет соответствующее заявление и запрос на сертификат в головной удостоверяющий центр, функции которого осуществляет уполномоченный орган в порядке, предусмотренном Регламентом головного удостоверяющего центра. Головной удостоверяющий центр выдает квалифицированный сертификат и вручает его Удостоверяющему центру.
- УЦ осуществляет информирование Владельцев КСКПЭП о проведении плановой смены ключей уполномоченного лица удостоверяющего центра (о вводе в действие нового сертификата издателя сертификатов) посредством публикации информации на официальном сайте Удостоверяющего центра по адресу: <https://www.esphere.ru>. Доверенным способом получения нового квалифицированного сертификата УЦ является его публикация на официальном сайте Удостоверяющего центра по адресу: <https://www.esphere.ru>, доступного для скачивания или на портале уполномоченного федерального органа в области использования электронной подписи <https://e-trust.gosuslugi.ru/> в профиле ООО «СберКорус».

Старые ключи УЦ Удостоверяющий центр использует в течение их срока действия для формирования СОС, изданных УЦ в период действия старых ключей ЭП УЦ.

- Все Заявители/Владельцы КСКПЭП должны установить на своих компьютерах/рабочих местах новый квалифицированный сертификат УЦ.

5.1.3. Порядок осуществления смены ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности: основания, процедуры и сроки осуществления смены ключей электронной подписи Удостоверяющего центра. Порядок информирования владельцев Сертификатов об осуществлении такой смены.

Основания для внеплановой смены ключей по причине нарушения конфиденциальности ключа ЭП Удостоверяющего центра:

- произошла компрометация ключа электронной подписи УЦ и/или есть подозрение, что ключ электронной подписи УЦ мог быть скомпрометирован;
- ключ электронной подписи УЦ не доступен (ключевой носитель поврежден, уничтожен, потерян с последующим обнаружением);
- увольнение работников УЦ, обладавших ключевой информацией;
- нарушение печати на опломбированном пенале с ключевыми носителями, находящемся в опечатываемом сейфе.

Актуальными угрозами нарушения конфиденциальности (компрометации) ключа электронной подписи Удостоверяющего центра относятся угрозы, представляющие собой целенаправленные действия с использованием следующих возможностей:

- Подготовка и проведение атак из контролируемой зоны.
- Подготовка и проведение атак без использования доступа к функциональным возможностям программно-аппаратных средств взаимодействия с Удостоверяющим центром.
- Самостоятельное осуществление создания способов атак, подготовки и проведения атак на: документацию на средства УЦ; защищаемые электронные документы; ключевую (аутентифицирующую, парольную) информацию; средства УЦ и их программные и аппаратные компоненты; данные, передаваемые по каналам связи; помещения, в которых находятся аппаратные средства, на которых реализованы средства Удостоверяющего центра, а также другие защищаемые ресурсы информационной системы.
- Внесение на этапах разработки, производства, хранения, транспортировки и ввода в эксплуатацию средств Удостоверяющего центра: негативных функциональных возможностей в средства Удостоверяющего центра, в том числе с использованием вредоносных программ; несанкционированных изменений в документацию на средства Удостоверяющего центра.
- Получение следующей информации:

- общих сведений об информационной системе, в которой используются средства Удостоверяющего центра (назначение, состав, объекты, в которых размещены ресурсы информационной системы);
- сведений об информационных технологиях, базах данных, автоматизированной системы, программном обеспечении, используемых в информационной системе совместно со средствами Удостоверяющего центра;
- сведений о физических мерах защиты объектов, в которых размещены средства Удостоверяющего центра;
- сведений о мерах по обеспечению защиты контролируемой зоны объектов информационной системы, в которой используются средства Удостоверяющего центра;
- сведений о мерах по разграничению доступа в помещения, в которых размещены средства Удостоверяющего центра;
- содержания находящейся в свободном доступе технической документации на средства Удостоверяющего центра;
- сведений о защищаемой информации, используемой в процессе эксплуатации средств Удостоверяющего центра (виды защищаемой информации: служебная информация, парольная и аутентифицирующая информация, конфигурационная информация, управляющая информация, информация в электронных журналах регистрации; общие сведения о содержании каждого вида защищаемой информации; характеристики безопасности для каждого вида защищаемой информации);
- всех возможных данных, передаваемых в открытом виде по каналам связи, не защищенным от несанкционированного доступа организационно-техническими мерами;
- сведений о линиях связи, по которым передается защищаемая с использованием средств Удостоверяющего центра информация;
- сведений обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами, нарушениях правил эксплуатации средств Удостоверяющего центра;
- сведений обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами, неисправностях и сбоях средств Удостоверяющего центра;
- сведений, получаемых в результате анализа любых доступных для перехвата сигналов от аппаратных компонентов средств Удостоверяющего центра.
- Использование:
 - находящихся в свободном доступе или за пределами контролируемой зоны автоматизированной системы и программного обеспечения, включая программные и аппаратные компоненты средств Удостоверяющего центра;
 - специально разработанных автоматизированных систем и программного обеспечения.
- Использование в качестве каналов атак не защищенных от несанкционированного доступа к информации организационно-техническими мерами каналов связи (как вне контролируемой зоны, так и в ее пределах), по которым передается информация, обрабатываемая средствами Удостоверяющего центра.
- Подготовка и проведение атак без использования доступа к автоматизированной системе, на которых реализованы средства Удостоверяющего центра.
- Использование штатных средств информационной системы, в которой используются средства Удостоверяющего центра.

Для предотвращения угроз нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра реализован изолированный режим работы программно-аппаратного комплекса Удостоверяющего центра – комплекс организационно-технических мер, при выполнении

которых нарушитель не располагает программно-аппаратными средствами взаимодействия с Удостоверяющим центром.

Хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых ключ ЭП Удостоверяющего центра может стать доступным несанкционированным лицам и (или) процессам, является основанием полагать, что конфиденциальность такого ключа ЭП нарушена.

В случае нарушения конфиденциальности ключа ЭП Удостоверяющего центра или угрозы нарушения конфиденциальности такого ключа электронной подписи выполняется внеплановая смена соответствующего ключа.

Процедура внеплановой смены ключей УЦ выполняется в порядке, определенном процедурой плановой смены ключей УЦ п. 5.1.2.

В случае компрометации ключа ЭП УЦ сертификат УЦ досрочно прекращает свой срок действия. Владельцы КСКПЭП извещаются УЦ об указанном факте путем публикации информации о компрометации на сайте УЦ по адресу: <https://www.esphere.ru>. Все КСКПЭП, подписанные с использованием скомпрометированного ключа УЦ, досрочно прекращают действие, с занесением соответствующих сведений об этих квалифицированных сертификатах в СОС.

Доверенным способом получения нового квалифицированного сертификата УЦ является его публикация на официальном сайте Удостоверяющего центра по адресу: <https://www.esphere.ru>, доступного для скачивания или на портале уполномоченного федерального органа в области использования электронной подписи <https://e-trust.gosuslugi.ru/> в профиле ООО «СберКорус».

5.1.4. Порядок осуществления Удостоверяющим центром смены ключа электронной подписи Владельца КСКПЭП.

Смена ключа ЭП Владельца КСКПЭП осуществляется в случаях:

- истечения срока действия КСКПЭП;
- на основании заявления владельца КСКПЭП о досрочном прекращении его действия (согласно Приложения № 3 к Регламенту), подаваемого в форме документа на бумажном носителе или в форме электронного документа в порядке, описанном в п. 5.4.2. Регламента;
- если не подтверждено, что Владелец КСКПЭП владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в таком Сертификате;
- если установлено, что содержащийся в таком КСКПЭП ключ проверки ЭП уже содержится в ином ранее созданном КСКПЭП;
- если вступило в силу решение суда, которым, в частности, установлено, что КСКПЭП содержит недостоверную информацию;
- иных случаях, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между УЦ и Заявителем.

При смене ключа ЭП Владелец КСКПЭП подает заявление на изготовление КСКПЭП в соответствии с требованиями раздела 5.2.1. настоящего Регламента. При этом в случае, подписания такого заявления в электронном виде с использованием квалифицированной ЭП (при наличии действующего сертификата) по причине смены ключа электронной подписи Владельца КСКПЭП из-за нарушения его конфиденциальности или угрозы нарушения конфиденциальности, соответствующее заявление должно быть подписано иной усиленной квалифицированной электронной подписью Владельца КСКПЭП.

Процедура выдачи КСКПЭП и ключа электронной подписи (при необходимости) осуществляется в соответствии со статьей 18 Федерального закона № 63-ФЗ «Об электронной подписи».

5.2. Процедура создания и выдачи КСКПЭП для Владельцев.

5.2.1. Порядок подачи заявления на создание и выдачу КСКПЭП.

Создание и выдача КСКПЭП осуществляется на основании Заявления на изготовление КСКПЭП (далее по тексту – заявление) с предоставлением документов и сведений, указанных в п. 5.2.4 Регламента.

Заявление предоставляется в УЦ либо в форме документа на бумажном носителе, либо в форме электронного документа в порядке, предусмотренном в п. 5.2.2. Регламента.

Сотрудник УЦ/ Доверенное лицо УЦ в момент принятия заявления на изготовление КСКПЭП к рассмотрению выполняет процедуру идентификации лица, обратившегося в УЦ, путем установления личности обратившегося согласно п. 5.2.3. Регламента.

В случае внесения в КСКПЭП персональных данных физического лица, Заявитель предоставляет свое письменное согласие на обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и на основании «Политики обработки персональных данных ООО «СберКорус», которая размещена на сайте Компании. Текст согласия включен в заявление на изготовление КСКПЭП и подписывается собственноручно Заявителем в момент предоставления такого заявления. Персональные данные Владельца КСКПЭП, внесенные в КСКПЭП, становятся общедоступными в соответствии с Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи».

5.2.2. Требование к заявлению на изготовление КСКПЭП.

Заявление на изготовление КСКПЭП может быть оформлено как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью, либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемыми Правительством Российской Федерации¹, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме"² и информации из государственной информационной системы "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных"³.

Заявление заполняется Заявителем на русском языке по форме в соответствии с Приложением № 1 к настоящему Регламенту и/или по форме, отдельно предоставленной Удостоверяющим центром Заявителю, в том числе согласно соглашению/договору⁴, с указанием достоверных и полных сведений, без подчисток и исправлений. Подписание заявления в форме документа на бумажном носителе производится собственноручно (без применения факсимиле) чернилами (пастой) синего или черного цвета.

5.2.3. Порядок идентификации Заявителя.

Идентификация Заявителя устанавливается одним из следующих способов:

- а) При личном присутствии Заявителя в Удостоверяющем центре или у Доверенного лица Удостоверяющего центра.

¹ Постановление Правительства Российской Федерации от 25 января 2013 г. N 33 "Об использовании простой электронной подписи при оказании государственных и муниципальных услуг"

² Постановление Правительства Российской Федерации от 28 ноября 2011 г. N 977 "О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме".

³ Пункт 4 статьи 2 Федерального закона от 29 декабря 2002 г. N 572-ФЗ "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации".

⁴ Актуальную форму заявления УЦ определяет самостоятельно и по своей инициативе вправе вносить в нее любые изменения без уведомления Заявителя.

Сотрудник УЦ/Доверенное лицо УЦ выполняет процедуру идентификации Заявителя УЦ путем установления его личности по документам, удостоверяющим личность. Для его идентификации требуется только оригинал соответствующего документа, удостоверяющего личность.

Порядок идентификации Заявителя следующий:

- идентификация гражданина Российской Федерации осуществляется по основному документу, удостоверяющему личность, – паспорту гражданина Российской Федерации. В исключительных случаях отсутствия у гражданина Российской Федерации основного документа, удостоверяющего личность, Удостоверяющий центр может удостоверить его личность по иному документу, удостоверяющему личность, в соответствии с законодательством Российской Федерации;

- идентификация гражданина иностранного государства осуществляется по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства.

- идентификация беженца, вынужденного переселенца и лица без гражданства осуществляется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.

К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

б) Без личного присутствия Заявителя:

- с использованием его УКЭП при наличии КСКПЭП, действующего на момент подачи заявления, который принадлежит лицу, личность которого устанавливается.

- путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные. Реализация данного способа осуществляется с учетом требований постановления Правительства Российской Федерации от 8 ноября 2019 г. N 1427 "О проведении эксперимента по совершенствованию применения технологии электронной подписи";

- путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

5.2.4. Перечень документов, запрашиваемых Удостоверяющим центром у Заявителя для изготовления и выдачи КСКПЭП.

Перечень документов и сведений, запрашиваемых Удостоверяющим центром у Заявителя, необходимых для изготовления и выдачи КСКПЭП, в том числе для идентификации личности Заявителя, устанавливается в соответствии с частью 2 статьи 17 и частью 2 статьи 18 Федерального закона № 63-ФЗ от 06.04.2011 «Об электронной подписи».

Удостоверяющий центр выполняет свою обязанность по внесению в КСКПЭП только достоверной и актуальной информации путем сбора и хранения копий документов, предоставленных Заявителем с учетом обязанностей в п. 4.4.3 Регламента, перечень документов и сведений, необходимых для изготовления и выдачи КСКПЭП указан в Приложении № 2 к настоящему Регламенту (далее по тексту – пакет документов). В случае если для подтверждения сведений, вносимых в КСКПЭП, законодательством Российской Федерации установлена определенная форма документа, Заявитель представляет в Удостоверяющий центр документ соответствующей формы.

5.2.5. Порядок проверки достоверности документов и сведений, представленных Заявителем.

Для заполнения информации о Заявителе в состав КСКПЭП в соответствии с частью 2 статьи 17 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» Удостоверяющий

центр запрашивает и получает из государственных информационных ресурсов сведения, предусмотренные частью 2.2 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». В случае, если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной Заявителем для включения в КСКПЭП, и Заявитель был идентифицирован, УЦ принимает решение о принятии пакета документов и осуществляет процедуру создания и выдачи КСКПЭП. В ином случае, УЦ отказывает Заявителю в принятии пакета документов и в выдаче КСКПЭП.

При проверке пакета документов Сотрудник УЦ/Доверенное лицо УЦ осуществляет следующие действия:

- 1) проверяет данные в заявлении на изготовление КСКПЭП на соответствие данным, содержащимся в иных представленных Заявителем документах, на полноту, достаточность и достоверность внесенных сведений (информации) и представленных документов, в том числе на соответствие настоящему Регламенту;
- 2) устанавливает:
 - факт принадлежности документов предоставившему их лицу;
 - факт соответствия сведений, указанных в заявлении, представленным документам и/или сведениям, а также сведениям/информации, полученным Удостоверяющим центром из государственных информационных ресурсов в соответствии с п.2.2 ст.18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
 - факт отсутствия признаков подделки представленных документов.

При отклонении заявления на изготовление КСКПЭП Сотрудник УЦ/Доверенное лицо УЦ уведомляет об этом обратившееся лицо с указанием причины отклонения пакета документов.

При принятии заявления на изготовление КСКПЭП Сотрудник УЦ/Доверенное лицо УЦ проставляет отметку о принятии на заявлении и/или иным образом подтверждает факт принятия такого пакета документов.

Субъект, присоединившийся к Регламенту, обязан предоставлять в Удостоверяющий центр только достоверную информацию. В случае если после создания КСКПЭП выяснится факт предоставления поддельных копий документов, Удостоверяющий центр вправе в одностороннем порядке прекратить действие такого Сертификата, а Субъект несет материальную ответственность в размере стоимости оказанных услуг УЦ.

5.2.6. Порядок создания КСКПЭП.

На основе принятого пакета документов Сотрудник УЦ выполняет действия по созданию КСКПЭП.

Процедура создания КСКПЭП зависит от способа создания ключа электронной подписи.

а) Процедура создания в УЦ ключа электронной подписи и соответствующего ему КСКПЭП включает в себя:

- внесение регистрационной информации в отношении будущего Владельца КСКПЭП в базу данных УЦ;
- создание ключа подписи, устанавливаемого на ключевой носитель, допустимого эксплуатационной документацией к СКЗИ УЦ;
- формирование запроса на создание КСКПЭП;
- создание КСКПЭП;
- установка КСКПЭП в соответствующий контейнер на ключевом носителе (токен);
- ознакомление Заявителя (Владельца КСКПЭП) с информацией, содержащейся в КСКПЭП;
- предоставление Владельцу КСКПЭП руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи;
- внесение данных об изготовленных КСКПЭП и ключевых носителях в журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
- передача Владельцу КСКПЭП ключевого носителя типа токен с ключевой парой под

роспись в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, сотрудником/доверенным лицом УЦ.

- а) Процедура создания Заявителем самостоятельно ключа электронной подписи и запроса на изготовление КСКПЭП включает в себя:
- получение уведомления от УЦ о необходимости создания ключей электронной подписи и запроса на КСКПЭП на своем персональном компьютере с использованием сертифицированных ФСБ России средств СКЗИ;
 - в случаях, предусмотренных условиями договора, Заявителю может быть предоставлен доступ к доверенной информационной системе, с возможностью создания запроса на изготовление КСКПЭП⁵;
 - предоставление запроса в УЦ для изготовления КСКПЭП;
 - проверка сведений в запросе;
 - создание КСКПЭП непосредственно УЦ;
 - ознакомление Заявителя (Владельца КСКПЭП) с информацией, содержащейся в КСКПЭП;
 - предоставление Владелцу КСКПЭП руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи;
 - получение Владелцем КСКПЭП, КСКПЭП соответствующего его ключу электронной подписи.
 - установка КСКПЭП его Владелцем в соответствующий контейнер на ключевом носителе (в т.ч. токен).

5.2.7. Порядок выдачи КСКПЭП.

По окончании процедуры создания КСКПЭП и положительного результата процедуры установления личности Заявителя Сотрудник УЦ/Доверенное лицо УЦ знакомит такое лицо с информацией, содержащейся в КСКПЭП и предоставляет руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

При получении КСКПЭП владелец КСКПЭП должен быть ознакомлен с информацией, содержащейся в КСКПЭП, под расписку, в том числе посредством использования ЭП при наличии у него действующего КСКПЭП, а также иными способами, предусмотренными Федеральным законом N 63-ФЗ «Об электронной подписи».

При положительном результате процедуры ознакомления с информацией, содержащейся в КСКПЭП, УЦ выдает Заявителю КСКПЭП либо путем его записи на ключевой носитель (с последующей передачей такого носителя), либо путем предоставления Заявителю возможности самостоятельно на своем рабочем месте осуществить установку КСКПЭП (в т.ч. на ключевой носитель), на котором хранится сформированный ключ электронной подписи.

Вручение ключей электронной подписи, КСКПЭП, информации, содержащейся в нем, и руководства по обеспечению безопасности (Приложение № 5 к Регламенту или предоставленного документа, размещенного в сети Интернет на сайте УЦ.) осуществляется только Владелцу КСКПЭП.

5.2.8. Срок создания и выдачи КСКПЭП. Условия для срочного создания и выдачи КСКПЭП.

Создание КСКПЭП осуществляется в течение не более 5 (пяти) рабочих дней с момента подачи Заявителем соответствующего заявления, при условии подтверждения УЦ всех фактов соответствия сведений в заявлении и соблюдения Заявителем порядка оплаты за услуги, если более короткий срок не предусмотрен в соглашении/договоре между Субъектами. Срок оказания услуги по изготовлению КСКПЭП увеличивается пропорционально сроку предоставления требуемых документов и сведений.

⁵ Особенности аутентификации владельца КСКПЭП в доверенной информационной системе и работы в ней регулируются руководствами пользователя и/или отдельно заключаемыми договорами/соглашениями.

Срочное создание и выдача КСКПЭП производится УЦ в соответствии с условиями прайс-листа Удостоверяющего центра и соблюдением требований, указанных в соответствующем договоре с Заявителем.

5.3. Подтверждение действительности электронной подписи, использованной для подписания электронных документов.

5.3.1. Требования к заявлению на подтверждение действительности электронной подписи. Перечень прилагаемых к заявлению документов.

Подтверждение действительности электронной подписи, использованной для подписания электронных документов и выданной Удостоверяющим центром, проводящим проверку действительности электронной подписи осуществляется на основании заявления (Приложение №4 к настоящему Регламенту), которое предоставляется в УЦ в форме документа на бумажном носителе или в форме электронного документа. Подписание заявления в форме документа на бумажном носителе производится собственноручно (без применения факсимиле) чернилами (пастой) синего или черного цвета, а в форме электронного документа - производится усиленной квалифицированной электронной подписью.

Обязательным приложением к заявлению на проверку подлинности электронной подписи в электронном документе является носитель, содержащий документ и файл ЭП, подвергающийся процедуре проверки.

5.3.2. Срок предоставления услуг по подтверждению действительности электронной подписи в электронном документе.

Срок проведения работ по подтверждению действительности ЭП в электронном документе составляет не более 15 (пятнадцать) рабочих дней с момента поступления заявления в Удостоверяющий центр и при условии поступления оплаты стоимости данных услуг на расчетный счет Удостоверяющего центра.

5.3.3. Порядок оказания услуг по подтверждению действительности электронной подписи в электронном документе.

Сотрудник УЦ проверяет полноту и достаточность внесенных в заявление сведений/предоставленных приложений и при достаточности - проставляет на заявлении обратившегося лица отметку о получении и/или принятии такого заявления, при недостаточности – сообщает об этом Заявителю с указанием причин.

Процедура подтверждения действительности ЭП осуществляется с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи», комиссией, сформированной из числа сотрудников УЦ и/или сотрудников информационной безопасности.

Проверка действительности ЭП включает в себя:

- определение сертификата или нескольких сертификатов, необходимых для проверки ЭП;
- проверка действительности всех квалифицированных сертификатов, включенных в последовательность проверки от проверяемого квалифицированного сертификата до квалифицированного сертификата аккредитованного удостоверяющего центра, выданного ему головным удостоверяющим центром;
- проверка ЭП электронного документа с использованием каждого сертификата;
- определение даты формирования каждой ЭП в электронном документе;
- проверка действительности сертификатов на текущий момент времени;
- проверка отсутствия сертификатов в списках отозванных сертификатов (CRL).

По результатам проведения работ, УЦ оформляет в произвольной форме документ (справку, заключение и т.п.), заверенный подписью УЦ, в двух экземплярах, один из которых предоставляется Заявителю.

Заключение содержат: 1) основание для проведения проверки; 2) данные, предоставленные для проведения проверки; 3) результат проверки действительности электронной подписи в электронном документе.

5.4. Процедуры, осуществляемые при прекращении действия или аннулирования КСКПЭП.

5.4.1. Основания прекращения действия или аннулирования КСКПЭП.

КСКПЭП прекращает свое действие в случаях, указанных в п. 4.1.8. настоящего Регламента, а также в следующих случаях, установленных статьей 14 Федерального закона № 63-ФЗ от 06.04.2011 «Об электронной подписи»:

- в связи с истечением установленного срока его действия;
- на основании заявления Владельца КСКПЭП по форме Приложения № 3 к Регламенту;
- в случае прекращения деятельности УЦ без перехода его функций другим лицам;
- в иных случаях, установленных Федеральным законом №63-ФЗ от 06.04.2011 «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами РФ, или соглашением между Удостоверяющим центром и Заявителем, а также настоящим Регламентом.

УЦ аннулирует КСКПЭП, если:

- не подтверждено, что владелец КСКПЭП владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- установлено, что содержащийся в КСКПЭП ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате;
- вступило в силу решение суда, которым установлено, что КСКПЭП содержит недостоверную информацию.

5.4.2. Порядок действий Удостоверяющего центра при прекращении действия (аннулировании) КСКПЭП.

Заявление заполняется Заявителем на русском языке по форме в соответствии с Приложением № 3 к настоящему Регламенту и/или по форме, отдельно предоставленной Удостоверяющим центром Заявителю, в том числе согласно соглашению/договору⁶, с указанием достоверных и полных сведений, без подчисток и исправлений.

Заявление о прекращении действия квалифицированного сертификата должно предусматривать указание в заявлении серийного номера квалифицированного сертификата, даты начала и окончания действия квалифицированного сертификата, наименования аккредитованного удостоверяющего центра, выдавшего квалифицированный сертификат, причины прекращения действия квалифицированного сертификата, а также:

в отношении физического лица, не являющегося индивидуальным предпринимателем: фамилии, имени, отчества (при наличии), страхового номера индивидуального лицевого счета, идентификационного номера налогоплательщика.

Подписание заявления в форме документа на бумажном носителе производится собственноручно (без применения факсимиле) чернилами (пастой) синего или черного цвета, а в форме электронного документа - производится с использованием УКЭП, КСКПЭП которой является действующим на момент подписания, выданным удостоверяющим центром, аккредитованным в соответствии с Федеральным законом № 63-ФЗ «Об электронной подписи», в том числе с использованием федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)»⁷ (далее – Единый портал). Подтверждение полномочий Сотрудником УЦ обращаться за прекращением действия КСКПЭП осуществляется в порядке, предусмотренном для изготовления КСКПЭП.

⁶ Актуальную форму заявления УЦ определяет самостоятельно и по своей инициативе вправе вносить в нее любые изменения без уведомления Заявителя

⁷ Положение о федеральной государственной информационной системе "Единый портал государственных и муниципальных услуг (функций)", утвержденное постановлением Правительства Российской Федерации от 24 октября 2011 г. N 861.

Информация о прекращении действия КСКПЭП вносится УЦ в Реестр сертификатов в течение 12 (Двенадцати) часов с момента, указанного в настоящем Регламенте и/или в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», либо в течение 12 (Двенадцати) часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие КСКПЭП прекращается согласно п. 5.5.2 Регламента.

В случае направления заявителем заявления о прекращении действия квалифицированного сертификата с использованием Единого портала принятое по такому заявлению решение удостоверяющего центра в форме электронного документа, подписанного усиленной квалифицированной электронной подписью удостоверяющего центра, размещается в личном кабинете Заявителя на Едином портале после проведения проверки действительности усиленной квалифицированной электронной подписи удостоверяющего центра, которой такое решение подписано, и подтверждения ее действительности. В случае принятия по такому заявлению решения о прекращении действия квалифицированного сертификата удостоверяющий центр после внесения соответствующей информации в реестр квалифицированных сертификатов направляет на Единый портал информацию о прекращении действия квалифицированного сертификата. Взаимодействие удостоверяющего центра с Единым порталом в рамках реализации норм, предусмотренных настоящим абзацем, осуществляется посредством единой системы межведомственного электронного взаимодействия⁸.

5.5. Порядок ведения реестра сертификатов.

5.5.1. Формы ведения реестра сертификатов.

Реестр сертификатов ведётся УЦ в электронной форме и публикуется в сети Интернет согласно п. 6.4 Регламента.

Удостоверяющий центр осуществляет непосредственное управление реестром сертификатов, обеспечивая требуемый уровень доступности и целостности информации.

Формирование реестра сертификатов включает в себя внесение КСКПЭП, выданных Владельцам КСКПЭП Удостоверяющим центром, в реестр сертификатов. Ведение реестра сертификатов включает в себя внесение изменений в реестр сертификатов в случае изменения содержащихся в нем сведений, внесение в реестр сертификатов сведений о прекращении действия или об аннулировании КСКПЭП.

Под процессом ведения реестра сертификатов понимаются следующие действия УЦ:

- внесение изменений в реестр сертификатов в случае изменения сведений;
- внесение в реестр сертификатов сведений о прекращении действия или об аннулировании квалифицированных сертификатов

Информация, внесенная в реестр сертификатов, подлежит хранению в течение всего срока деятельности Удостоверяющего центра, если более короткий срок не установлен законодательством Российской Федерации.

Хранение информации, содержащейся в реестре сертификатов, должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре сертификатов.

Удостоверяющий центр обеспечивает защиту информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

Формирование и ведение реестра сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему. Для предотвращения утраты сведений о сертификатах, содержащихся в реестре, формируется его резервная копия. Удостоверяющий центр обязан обеспечивать актуальность информации, содержащейся в реестре сертификатов.

Структура Реестра сертификатов формируется и ведется в соответствии с требованиями Федерального органа исполнительной власти, осуществляющего функции по выработке и

⁸ Положение о единой системе межведомственного электронного взаимодействия, утвержденное постановлением Правительства Российской Федерации от 8 сентября 2010 г. N 697.

реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий. Удостоверяющий центр

5.5.2. Сроки внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов.

Информация о прекращении действия или аннулировании КСКПЭП вносится в реестр сертификатов. Действие КСКПЭП прекращается/аннулируется с момента публикации СОС, в который внесён этот КСКПЭП. Срок внесения в СОС сведений о прекращении действия или аннулировании сертификата указан в п. 4.2.20. Регламента.

5.6. Порядок технического обслуживания реестра сертификатов.

5.6.1. Максимальные сроки проведения технического обслуживания.

Плановые технические работы по обслуживанию реестра сертификатов проводятся Удостоверяющим центром в выходные дни либо в ночное время (с учетом часовых поясов на территории Российской Федерации) с целью минимизации и возможности исключения перерывов в работе при использовании КСКПЭП их Владельцами и в доступе к реестру сертификатов Удостоверяющего центра.

Внеплановые технические работы проводятся при появлении такой необходимости в оперативном режиме.

Максимальные сроки проведения технического обслуживания реестра сертификатов составляют не более 12 часов. Время проведения технического обслуживания может быть увеличено при наличии объективных оснований и причин.

5.6.2. Порядок уведомления участников информационного взаимодействия о проведении технического обслуживания.

УЦ оповещает лиц, использующих реестр сертификатов, о проведении планового или внепланового технического обслуживания реестра сертификатов путем публикации информации на официальном сайте УЦ.

6. Порядок исполнения обязанностей Удостоверяющего центра

6.1 . Информирование Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

Информирование Заявителя об условиях и о порядке использования электронной подписи, о рисках, связанных с их использованием и о мерах, необходимых для обеспечения безопасности ключей электронной подписи и процедур проверки электронных подписей осуществляется посредством ознакомления их с руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, которое выдается Заявителю одновременно с выдачей КСКПЭП.

6.2 Выдача по обращению Заявителя средств электронной подписи.

Удостоверяющий центр по обращению Заявителя выдает средства электронной подписи, которые в соответствии с частью 4 статьи 6 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» должны обеспечивать возможность проверки всех УКЭП в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные УКЭП, или в случае, если электронный документ подписан несколькими УКЭП.

Порядок использования средств электронной подписи определяются эксплуатационной документацией на такие средства и/или лицензионным соглашением, условия которого определяет правообладатель.

6.3 Обеспечение актуальности информации в реестре сертификатов и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий.

УЦ обеспечивает актуальность информации, содержащейся в реестре сертификатов, защиту информации от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий. Актуальность обеспечивается путем своевременного внесения записи о выпуске, прекращении действия или аннулировании КСКПЭП в реестр сертификатов. Режим защиты является общим требованием в отношении всей сферы применения электронной подписи, он обеспечивается посредством применения специальных шифровальных средств, способствующих защите информации от несанкционированного доступа. Для предотвращения утраты сведений о сертификатах, содержащихся в реестре, формируется его резервная копия.

6.4 Обеспечение доступности реестра сертификатов в информационно-телекоммуникационной сети «Интернет» в любое время, за исключением технического обслуживания реестра сертификатов.

УЦ обеспечивает на безвозмездной основе доступность реестра сертификатов, выданных данным УЦ, круглосуточно в любое время с использованием информационно-телекоммуникационных сети «Интернет» на странице <https://www.esphere.ru/products/uc/reestr>, за исключением периодов планового или внепланового технического обслуживания реестра сертификатов

6.5 Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей

При изготовлении ключей электронной подписи в УЦ, ключей проверки электронной подписи, КСКПЭП используются средства электронной подписи и средства удостоверяющего центра, соответствующие требованиям безопасности, установленным федеральным органом исполнительной власти в области обеспечения безопасности. Ключ электронной подписи, соответствующий КСКПЭП, является конфиденциальной информацией Владельца КСКПЭП. Владельцу КСКПЭП обязан обеспечивать конфиденциальность ключа электронной подписи, в частности не допускать использование ключа ЭП без его согласия.

Владельцу КСКПЭП необходимо немедленно обратиться в Удостоверяющий центр с заявлением на прекращение действия КСКПЭП (Приложение № 3 к Регламенту) в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

Владельцу КСКПЭП запрещается:

- оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ (в т.ч. средства усиленной электронной подписи), после ввода ключевой информации;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители посторонним и/или неуполномоченным лицам, к ним не допущенным;
- использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;
- записывать на ключевые носители постороннюю информацию;
- оставлять без присмотра ключевые носители (на столе, подключенным к ПЭВМ и пр.);
- разглашать пароль (пин-код) ключевого носителя и/или допускать использование принадлежащих им ключей электронной подписи без его согласия;
- применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

Ключи ЭП на ключевом носителе защищаются паролем (пин-кодом). Пароль (пин-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство криптографической защиты информации. Сотрудник УЦ сообщает сформированный пароль (пин-код) Владельцу КСКПЭП. Ответственность за сохранение пароля (пин-кода) в тайне возлагается на Владельца КСКПЭП.

Условия временного хранения ключей электронной подписи:

Удостоверяющий центр может осуществлять временное хранение ключа электронной подписи, ключа проверки электронной подписи, КСКПЭП до наступления обстоятельств, позволяющих УЦ

выполнить действия, предусмотренные статьей 18 Федерального закона Российской Федерации от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

- при хранении ключей ЭП необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Владелец КСКПЭП несет персональную ответственность за хранение своих ключевых носителей и/или ключей ЭП;
- в случае централизованного хранения ключевых носителей в организации, эксплуатирующей СКЗИ, администратор безопасности (если он имеется) несет персональную ответственность за хранение ключевых носителей и/или ключей ЭП. Владелец КСКПЭП.

Сроки уничтожения ключей электронной подписи.

Ключи на ключевых носителях, в том числе срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации. Срок уничтожения ключей электронной подписи Владелец КСКПЭП устанавливает самостоятельно.

6.6 Осуществление регистрации КСКПЭП в единой системе идентификации и аутентификации.

При выдаче КСКПЭП Удостоверяющий центр направляет в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра).

6.7 Осуществление по желанию лица, которому выдан КСКПЭП, безвозмездной регистрации указанного лица в единой системе идентификации и аутентификации.

При выдаче КСКПЭП Удостоверяющий центр по желанию лица, которому выдан КСКПЭП, безвозмездно осуществляет регистрацию указанного лица в единой системе идентификации и аутентификации.

6.8 Предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре сертификатов, включая информацию о прекращении действия КСКПЭП или об аннулировании КСКПЭП, в том числе путем публикации перечня прекративших свое действие (аннулированных) сертификатов.

Доступ к реестру выданных сертификатов осуществляется безвозмездно на основании запроса, содержащего необходимые УЦ сведения, позволяющие идентифицировать сертификат в реестре выданных сертификатов, сведения о запрашиваемом лице и о самом Заявителе УЦ, а также указание на способ получения запрашиваемой выписки из реестра и контактные данные её получателя.

Сведения из реестра выданных сертификатов по каждому отдельному выданному сертификату представляются на основании отдельного запроса.

Запрос о предоставлении информации из реестра сертификатов представляется в УЦ лично или направляется на бумажном носителе или в форме электронного документа, по контактным адресам УЦ, указанным в настоящем Регламенте, и/или посредством доверенной информационной системы (при наличии в ней такой возможности) или круглосуточно через форму на сайте УЦ <https://www.esphere.ru/products/uc/reestr>, за исключением периодов планового или внепланового технического обслуживания реестра сертификатов. Подписание запроса в форме документа на бумажном носителе производится собственноручно (без применения факсимиле) чернилами (пастой) синего или черного цвета, а в форме электронного документа - производится усиленной квалифицированной электронной подписью или иным видом электронной подписи, который прямо предусмотрен соглашением/договором между Субъектами.

Информация предоставляется в форме выписки из реестра выданных сертификатов и предоставляется путем представления КСКПЭП в форме электронного документа, либо в форме копии КСКПЭП на бумажном носителе по выбору лица, обратившегося за её получением.

7. Сроки действия ключей ЭП и сертификатов

Срок действия КСКПЭП, изготовленного УЦ, указан в полях «notBefore» и «not After» поля «Validity» сертификата.

Начало периода действия ключа электронной подписи исчисляется с даты и времени начала действия КСКПЭП.

Время начала периода действия КСКПЭП и его окончания заносится Удостоверяющим центром в поля «notBefore» и «not After» поля «Validity» КСКПЭП соответственно.

Срок действия КСКЭП Удостоверяющего центра составляет не более 15 лет.

Максимальный срок действия ключа электронной подписи Владельца КСКПЭП устанавливается эксплуатационной документацией средства электронной подписи (системы криптографической защиты информации), с использованием которого такой ключ создается. Начало периода действия ключа электронной подписи Владельца КСКПЭП исчисляется с момента начала действия КСКПЭП, соответствующего данному ключу.

Срок действия КСКПЭП, создаваемого Удостоверяющим центром для Владельца, равен сроку действия ключа электронной подписи, соответствующего данному КСКЭП, если иное не предусмотрено договором УЦ или Заявитель не указал иной срок действия КСКПЭП в Заявлении, но не более срока, , определенного требованиями, установленными в соответствии с пунктом 2 части 5 статьи 8 Федерального закон 06.04.2011 N 63-ФЗ "Об электронной подписи"

8. Список приложений

- 11.1. Приложение №1. Форма Заявления на изготовление КСКПЭП удостоверяющим центром для Заявителя.
- 11.2. Приложение № 2. Перечень документов, представляемых Заявителем УЦ для изготовления и включения в КСКПЭП.
- 11.3. Приложение № 3. Форма заявления на прекращение действия КСКПЭП.
- 11.4. Приложение № 4. Форма заявления на проверку подлинности электронной подписи в электронном документе.
- 11.5. Приложение № 5. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

ФОРМА

Приложение №1 к Регламенту
Удостоверяющего центра
ООО «СберКорус»
от «30» августа 2024г.

Заявление

физического лица на изготовление квалифицированного сертификата ключа проверки электронной подписи

(Фамилия, имя, отчество полностью)

(далее – Заявитель ИЦ) просит сформировать ключи электронной подписи и изготовить квалифицированный сертификат ключа проверки электронной подписи (далее – сертификат) согласно Федеральному закону №63-ФЗ от 06.04.2011 «Об электронной подписи» для себя как владельца такого сертификата в соответствии со следующими данными: наименование, указанным в настоящем Заявлении и сроком действия сертификата _____ год/лет»;

Адрес регистрации	
Идентификационный номер налогоплательщика (ИНН)	
Номер страхового свидетельства государственного пенсионного страхования (СНИЛС)	
Дата рождения владельца сертификата	
Гражданство владельца сертификата	
Пол владельца сертификата	
Место рождения владельца сертификата	
Серия и номер паспорта гражданина РФ (или иного основного документа, удостоверяющего личность) владельца сертификата	
Дата выдачи паспорта гражданина РФ (или иного основного документа, удостоверяющего личность)	
Наименование органа, выдавшего паспорт гражданина РФ (или иного основного документа, удостоверяющего личность)	
Код подразделения органа, выдавшего паспорт гражданина РФ	
Адрес электронной почты владельца сертификата	
Номер мобильного телефона владельца сертификата	
Информационная система-сайт, портал, сервис, где планирует работать с ЭП	

Я, Владелец сертификата, зарегистрированного(ой) по адресу: указанному выше, даю свое согласие ООО «СберКорус» (ОГРН 1037812752302, ИНН 7801392271), расположенному по адресу: 194100 г. Санкт-Петербург, Б. Самойковского пр-кт, д.63, литер Н помещению №145 (далее – Компания), с содержанием: с Федеральным агентством по техническому развитию и обработке информации, систематизации, накоплению, хранению, уточнению (обновлению, изменению), извлечению, использованию, передаче (распространению, предоставлению, доступу), обеспечению безопасности, удалению, уничтожению, и иному иному средству автоматизации информации без использования таких средств, моих персональных данных, указанных в настоящем Заявлении и к иному иному сертификату, а также к иному иному документу, необходимому для исполнения функций Регистратора Уполномоченного центра Компании, что подтверждает мою личную волю. Настоящее согласие на обработку моих персональных данных даю(а) лично: полученный и некая обязательности от Компании, а также для возможности проверки достоверности, подлинности и целостности моей электронной подписи в электронных документах лицам, с которыми у Компании допущено использование электронной подписи, а также с целью идентификации и аутентификации моих в доверенных информационных системах, в т.ч. для заполнения сведений в единую систему идентификации и аутентификации с соответствии с ч.5 ст.18 Федерального закона № 63-ФЗ от 06.04.2011 № 63-ФЗ об электронной подписи. Настоящим признаю, что мои персональные данные, записанные в сертификате, относятся к общедоступным персональным данным. В случае необходимости также даю Компании право предоставлять мои персональные данные третьим лицам для выполнения Компанией принятых на себя обязательств, в том числе установленных законодательством Российской Федерации.

Данное согласие действително с момента его подписания и на весь период действия моего сертификата и до истечения срока хранения информации или документа, содержащего вышеуказанную информацию, определенную в соответствии с действующим законодательством Российской Федерации. Данное согласие может быть отозвано мной посредством направления в Компанию письменного уведомления. После этого Компания вправе продолжить обработку персональных данных только в случаях, предусмотренных действующим законодательством (п.2 ст.9, п.2-п.11 ч1 ст.6, ч.2 ст.10 и ч.2 ст.11 Закона о персональных данных). Также в случае(х) о том, что информация (непредоставление в указанный срок) мной данного письменного согласия является основанием для прекращения обработки персональных данных, мне также предоставляется право отозвать данное согласие.

Настоятели д. Захектөлә УЦ, он же Владлен сәртифисовна.

- подтверждая, что ознакомлен(а) с опубликованным в сети Интернет по адресу: www.ezrnye.ru Регламентом Удостоверяющего центра Компании, присоединился к нему и обязуется его соблюдать;

- понимаю и принимаю на себя риск любых неблагоприятных последствий при использовании настоящего Заглавия неполной и/или неадекватной информации

Заместитель УЦ - Власов И.С. (с. 10)

INDEX

ФИО

20 T

Отметки уполномоченного лица Удостоверяющего центра ООО «СберКорпус»

Заявление	принято	и	проверено	на	полноту	и	достоверность	данных.	Идентификация	Заявителя
проведена:					/		«__»	20__г.		
(Должность)			(Подпись)			(ФИО)		(Дата)		

⁹ В соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ "Об электронной подписи", ст. 15, ч. 9, но не более срока, определенного требованиями, установленными в соответствии с пунктом 2 части 5 статьи 8 Федерального закон 06.04.2011 N 63-ФЗ "Об электронной подписи"

**Перечень документов, либо их надлежащим образом заверенные копии и (или) сведения,
представляемые Заявителем для изготовления и включения
в квалифицированный сертификат ключа проверки электронной подписи¹⁰**

Для физических лиц:

1. Заявление на изготовление квалифицированного сертификата ключа проверки электронной подписи.
2. Основной документ, удостоверяющий личность Заявителя.
3. Номер страхового свидетельства государственного пенсионного страхования заявителя (СНИЛС) Владельца КСКПЭП.
4. Идентификационный номер налогоплательщика заявителя – физического лица.

Документы, указанные выше, кроме основного документа, удостоверяющего личность Заявителя, могут быть представлены в УЦ в виде надлежащим образом заверенных копий документов, под которыми понимаются копии:

- для физических лиц – заверенные нотариусом

В случае, если для подтверждения сведений, вносимых в КСКПЭП, законодательством Российской Федерации установлена определенная форма документа, Заявитель представляет в Удостоверяющий центр документ соответствующей формы.

Для установления личности Владельца КСКП ЭП представляется только оригинал основного документа, удостоверяющего его личность.

В случае представления Заявителем оригиналов документов Удостоверяющий центр осуществляет их копирование и самостоятельное заверение для последующего хранения в Удостоверяющем центре.

¹⁰ Удостоверяющий центр вправе запросить иные документы, подтверждающие сведения, содержащиеся в заявлении на изготовление КСКПЭП и подлежащие внесению в КСКПЭП.

ФОРМА

Приложение №3 к Регламенту
Удостоверяющего центра
ООО «СберКорус»
от «30» августа 2024г.

Руководителю ООО «СберКорус»

Заявление на прекращение действия
квалифицированного сертификата ключа проверки электронной подписи

ФИО физического лица

серия и номер паспорта, дата выдачи и кем выдан

просит прекратить действие квалифицированного сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «СберКорус» (ОГРН: 1057812752502) в соответствии с Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи» и Порядком (Регламентом) реализаций функций и исполнения обязанностей аккредитованного УЦ, содержащего следующие идентификационные данные:

Серийный (уникальный) номер квалифицированного сертификата			
Дата начала и окончания действия сертификата			
Фамилия, имя и отчество владельца сертификата			
ИНН ФЛ	СНИЛС ФЛ		
Основание прекращения действия квалифицированного сертификата			

Лицо, подписывающее настоящее заявление, понимает и принимает на себя риск последствий, следующих за выбранным действием, направленным на прекращение действия сертификата ключа проверки электронной подписи.

подпись

Ф.И.О.

« ____ » _____ 20__ г.

Отметки уполномоченного лица Удостоверяющего центра ООО «СберКорус»:

Заявление принял и проверил на полноту и достоверность данных:

(Должность)

(Подпись)

(ФИО)

(Дата)

ФОРМА

Приложение №4 к Регламенту
Удостоверяющего центра
ООО «СберКорус»
от «30» августа 2024г.

Заявление на проверку подлинности электронной подписи электронного документа

полное наименование юридического лица, являющегося организационно-правовой формой, либо статус и полное ФИО индивидуального предпринимателя, либо полное ФИО физического лица

должность и фамилия, имя, отчество руководителя юридического лица или уполномоченного сотрудника (заполняется при необходимости)

действующий на основании

основание полномочий (устав, положение, доверенность №___от___) (заполняется при необходимости)

просит проверить подлинность электронной подписи электронного документа в соответствии со следующими идентификационными данными:

- Файл сертификата ключа проверки электронной подписи на прилагаемом к заявлению носителе.
- Файл, содержащий подписанные электронной подписью данные, на прилагаемом к заявлению носителе.
- Время подписания электронной подписью электронного документа:

___ часов ___ мин МСК «___» _____ 20__ г.

Если момент подписания электронного документа не определен, то необходимо указать время, на момент наступления которого необходимо проверить подлинность электронной подписи:

___ часов ___ мин МСК «___» _____ 20__ г.

Должность Заявителя или уполномоченного
сотрудника ЮЛ

подпись

Ф.И.О.

«___» _____ 20__ г.

Отметки уполномоченного лица Удостоверяющего центра ООО «СберКорус»:

Заявление принял и проверил на полноту и достоверность данных:

(Должность)

(Подпись)

(ФИО)

/ «___»

(Дата)

20__ г.

**Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств
квалифицированной электронной подписи**

1. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи.
 - 1.1. Обеспечить конфиденциальность ключей электронных подписей.
 - 1.2. Применять для формирования электронной подписи только ключ электронной подписи, соответствующий действующему сертификату ЭП.
 - 1.3. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.
 - 1.4. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.
 - 1.5. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении сертификата, либо об отказе в прекращении.
 - 1.6. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, действие которого прекращено.
 - 1.7. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.
2. Порядок применения средств квалифицированной электронной подписи
 - 2.1. Средства квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата ключа проверки электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи, размещенной на сайте <https://www.esphere.ru/support/download> в разделе «Электронная подпись», либо на сайте производителя, в т.ч. не разглашать содержимое носителей ключевой информации и/или не передавать сами носители лицам, к ним не допущенным, не выводить ключевую информацию на дисплей, принтер и иные средства отображения информации, а также не записывать на ключевые носители постороннюю информацию и т.д.
 - 2.2. Для предотвращения заражения компьютера с установленными средствами электронной подписи необходимо обеспечить непрерывную комплексную защиту компьютера от вирусов, хакерских атак, спама, шпионского программного обеспечения и других вредоносных программ антивирусным программным обеспечением с рекомендуемым разработчиком периодом обновления антивирусных баз.
 - 2.3. В помещениях владельцев средств электронной подписи для хранения выданных им носителей ключей электронной подписи, эксплуатационной и технической документации, устанавливающих средства электронной подписи, необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих владельцев средств квалифицированной электронной подписи.
 - 2.4. Заявителем Удостоверяющего центра соответствующими приказами должны быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации средств ЭП, назначены должностные лица, ответственные за обеспечение безопасности информации и эксплуатации этих средств; средства ЭП и ключевые носители в соответствии с их серийными номерами должны быть взяты на поквартирный учет в выделенных для этих целей журналах.

Настоящее Руководство получено: _____ / _____ /
(подпись) (ФИО)

« _____ » _____ 20 ____ г.