Утверждён
приказом ООО ИЦ «Выбор»
от 28.12.2020 г. № 235

ПОРЯДОК

реализации функций и исполнения обязанностей аккредитованного Удостоверяющего центра ООО ИЦ «Выбор»

Смоленск, 2020

ОГЛАВЛЕНИЕ

1. ТЕРМИНЫ, СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

1.1. *Аннулирование сертификата ключа проверки электронной подписи* – объявление на основаниях, предусмотренных ч. 6.1 ст. 14 Закона об электронной подписи, о прекращении (временном приостановлении) действия сертификата путём включения его серийного номера в актуальный список отозванных сертификатов Удостоверяющего центра и опубликования Удостоверяющим центром этого списка.

1.2. *Аутентификация заявителя* – проверка подлинности предъявленных заявителем данных путём сравнения их с данными, содержащимися в подтверждающих их документах или информационных ресурсах.

1.3. *Владелец сертификата ключа проверки электронной подписи (далее – владелец сертификата, владелец СКПЭП)* – лицо, которому в установленном Законом об электронной подписи порядке выдан сертификат ключа проверки электронной подписи.

1.4. *Вручение сертификата ключа проверки электронной подписи* – передача работником Удостоверяющего центра изготовленного этим Удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу.

1.5. *Головной удостоверяющий центр (далее – ГУЦ)* – его функции в отношении аккредитованных удостоверяющих центров осуществляет Минцифры России.

1.6. *Единая система идентификации и аутентификации (далее – ЕСИА)* – федеральная государственная информационная система Российской Федерации (ФГИС), обеспечивающая санкционированный доступ участников информационного взаимодействия (граждан-заявителей и должностных лиц органов исполнительной власти) к информации, содержащейся в государственных информационных системах и иных информационных системах. ФГИС ЕСИА создана и развивается Минцифры России в рамках инфраструктуры электронного правительства с целью упорядочить и централизовать процессы регистрации, идентификации, аутентификации и авторизации пользователей.

1.7. *Единый государственный реестр индивидуальных предпринимателей (далее – ЕГРИП)* – государственный реестр, содержащий сведения о приобретении физическими лицами статуса индивидуального предпринимателя, прекращении физическими лицами деятельности в качестве индивидуальных предпринимателей, иные сведения об индивидуальных предпринимателях и соответствующие документы.

1.8. *Единый государственный реестр юридических лиц (далее – ЕГРЮЛ)* – государственный реестр, содержащий сведения о создании, реорганизации и ликвидации юридических лиц, иные сведения о юридических лицах и соответствующие документы.

1.9. *Закон об электронной подписи* – Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

1.10. *Заявитель* – физическое лицо, в т.ч. имеющее статус индивидуального предпринимателя, или юридическое лицо, обратившиеся в Удостоверяющий центр с заявлением об оказании им услуг удостоверяющего центра.

1.11. *Идентификация заявителя* – предъявление заявителем данных о себе и характере своей принадлежности к определённым организационным структурам.

1.12. *Информационный ресурс Удостоверяющего центра* – технические и программные средства ООО ИЦ «Выбор», в совокупности выполняющие функции по определённому законодательством и нормативными актами информированию (в том числе через информационно-телекоммуникационную сеть Интернет) неопределённого круга лиц о деятельности Удостоверяющего центра.

1.13. *Квалифицированный сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат, КСКПЭП)* – сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Законом об электронной подписи и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитован-

ным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (*далее – уполномоченный федеральный орган*).

1.14. *Ключ проверки электронной подписи (далее – КПЭП)* – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее – *проверка электронной подписи*).

1.15. *Ключ электронной подписи (КЭП)* – уникальная последовательность символов, предназначенная для создания электронной подписи.

1.16. *Ключевой носитель* – устройство, содержащее в доступной для использования по прямому назначению форме ключ электронной подписи.

1.17. *Компрометация ключевых документов* – утрата доверия к тому, что используемые ключи электронной подписи недоступны посторонним лицам. К событиям, определяющим компрометацию ключей, относятся, в том числе, следующие:

1.17.1. ключ используется или использовался ранее не его владельцем;

1.17.2. выявленное похищение носителей ключей у владельца сертификата;

1.17.3. утрата (утеря) носителей ключей, даже с их последующим обнаружением;

1.17.4. утрата ключей от сейфов в момент нахождения в них ключевых носителей, в т.ч. с последующим их обнаружением;

1.17.5. не санкционированное владельцем сертификата копирование ключей;

1.17.6. обнаруженная владельцем ключа возможность копирования ключевой информации посторонними лицами.

1.17.7. обнаруженная доступность ключей несанкционированным процессам;

1.17.8. увольнение сотрудников, имевших доступ к служебной ключевой информации;

1.17.9. нарушение правил хранения и уничтожения ключа (по окончании срока его действия);

1.17.10. подозрения на утечку информации или её искажение, подделка в защищённых каналах связи;

1.17.11. нарушение целостности печатей на сейфах, где хранились ключевые носители, если используется процедура опечатывания таких сейфов.

1.18. *Конфиденциальность информации* – обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя, предотвращать её разглашение.

1.19. *Отзыв сертификата ключа проверки электронной подписи* – выраженное документально или по установленной процедуре намерение владельца сертификата или уполномоченного органа аннулировать сертификат.

1.20. *Официальный информационный ресурс Удостоверяющего центра (Информационный ресурс УЦ)* – имеющие принадлежность ООО ИЦ «Выбор» общедоступные информационные ресурсы в информационно-телекоммуникационной сети «Интернет» (сайты, папки и файлы), предназначенные для предоставления в электронном виде информационных и технологических материалов Участникам электронного взаимодействия.

1.21. *Подтверждение владения ключом электронной подписи* – получение Удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата.

1.22. *Прекращение действия сертификата ключа проверки электронной подписи* – определение состояния сертификата как прекратившего своё действие в связи с истечением установленного

срока его действия, на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа, при прекращении деятельности УЦ без перехода его функций другим лицам, а также в иных случаях, установленных Законом об электронной подписи и другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между Удостоверяющим центром и владельцем сертификата.

1.23. *Рабочий день Удостоверяющего центра* – период времени с 08:30 по 17:30 (мск) каждого дня недели за исключением выходных (суббота и воскресенье) и нерабочих праздничных дней.

1.24. *Реестр сертификатов Удостоверяющего центра (далее – Реестр сертификатов)* – информационный ресурс (база данных) удостоверяющего центра, содержащий данные о выданных Удостоверяющим центром квалифицированных сертификатах ключей проверки электронной подписи, в том числе о прекративших своё действие и аннулированных.

1.25. *Сертификат ключа проверки электронной подписи (далее – сертификат, СКПЭП)* – электронный документ или документ на бумажном носителе, выданные Удостоверяющим центром либо доверенным лицом Удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

1.26. *Список отозванных (аннулированных) сертификатов (СОС, CRL[1])* – электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров, дату, время и причину аннулирования сертификатов ключей проверки электронной подписи, которые до окончания срока их действия на момент издания СОС были на законном основании аннулированы удостоверяющим центром.

1.27. *Средства Удостоверяющего центра* – программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

1.28. *Средства электронной подписи* – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

1.29. *Удостоверяющий центр (далее – УЦ)* – юридическое лицо ООО ИЦ «ВЫБОР», осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Законом об электронной подписи.

1.30. *Уполномоченное лицо Удостоверяющего центра (далее – уполномоченное лицо УЦ)* – лицо, решением единоличного исполнительного органа ООО ИЦ «Выбор» наделённое полномочиями по заверению (в т.ч. подписанию электронной подписью) сертификатов ключей проверки электронных подписей и списков отозванных сертификатов, издаваемых Удостоверяющим центром.

1.31. *Уполномоченный федеральный орган (далее – УФО) в области использования электронной подписи* – Минкомсвязь России.

1.32. *Участники электронного взаимодействия* – осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане (физические лица).

1.33. *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.

1.34. *Электронный документ* – документ, в котором информация представлена в электронной форме.

---

[1] Certificate Revocation List (*англ.*)

ОБЩИЕ ПОЛОЖЕНИЯ

2. ПРАВОВОЙ СТАТУС ДОКУМЕНТА

2.1. Порядок реализации функций и исполнения обязанностей аккредитованного Удостоверяющего центра ООО ИЦ «Выбор» (равнозначное название далее по тексту – Регламент Удостоверяющего центра ООО ИЦ «Выбор», Регламент УЦ, Порядок) разработан на основании положений Закона об электронной подписи, других федеральных законов, нормативных правовых актов уполномоченных федеральных органов, регулирующих деятельность удостоверяющих центров. Он определяет порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей.

2.2. Регламент УЦ является договором присоединения в соответствии со ст. 428 ГК РФ и определяет условия оказания услуг Удостоверяющего центра, включая права, обязанности, ответственность сторон, формы и форматы документов, а также основные организационно-технические мероприятия, направленные на обеспечение работы Удостоверяющего центра.

2.3. Регламент УЦ распространяется (публикуется) в форме электронного документа на официальном сайте Удостоверяющего центра. Доступ к информации на официальном сайте осуществляется на основе распространенных программ-обозревателей Интернета (в частности: Internet Explorer, Mozilla Firefox, Opera, Google Chrome) без использования специального программного обеспечения, установка которого на технические средства пользователя требует заключения лицензионного или иного соглашения с правообладателем программного обеспечения, предусматривающего взимание с пользователя платы. Для доступа к документам и информации на официальном сайте регистрация и идентификация пользователей, ввод паролей или предоставление персональных данных не требуется. Документы и информация размещаются на официальном сайте без применения шифрования и иных методов, не позволяющих осуществить ознакомление пользователя с их содержанием без использования иного программного обеспечения или технологических средств, кроме программ-обозревателей Интернета, и размещается на официальном сайте в формате, обеспечивающем возможность поиска средствами пользователей без использования специально созданного для доступа к информации программного обеспечения. Размещаемые на страницах официального сайта информация и электронные документы (файлы) имеют индикацию даты последнего изменения информации или размещения файла.

2.4. Присоединение к Регламенту УЦ осуществляется в целом путём подписания заявителем заявления по форме Удостоверяющего центра. После присоединения к Регламенту УЦ заявитель безусловно принимает все условия Регламента УЦ и вступает с Удостоверяющим центром в договорные отношения на определённых Регламентом УЦ условиях.

2.5. Удостоверяющий центр вправе на законных основаниях отказать любому лицу в присоединении к Регламенту УЦ.

2.6. Владелец сертификата вправе в одностороннем порядке отказаться от присоединения к Регламенту УЦ, в т.ч. при нарушении Удостоверяющим центром условий Регламента УЦ. Отказ должен быть выражен в письменной документальной форме.

2.7. Отказ от присоединения к Регламенту УЦ не освобождает стороны от исполнения обязательств, возникших до отказа, и не освобождает от ответственности за их неисполнение (ненадлежащее исполнение).

2.8. Внесение изменений в Регламент УЦ производится Удостоверяющим центром в одностороннем порядке путём размещения новой редакции Регламента УЦ на своём официальном сайте. Все приложения, изменения и дополнения к Регламенту УЦ являются его составной и неотъемлемой частью.

2.9. Все изменения, вносимые Удостоверяющим центром в Регламент УЦ по его инициативе и не связанные с изменением законодательства Российской Федерации, вступают в силу по истечении 30 дней с даты их размещения на официальном сайте Удостоверяющего центра.

2.10. Все изменения, вносимые Удостоверяющим центром в Регламент УЦ в связи с изменением

нормативных правовых актов, вступают в силу в сроки, установленные законодательством Российской Федерации.

2.11. Изменения Регламента УЦ с момента их вступления в силу распространяются на всех владельцев сертификатов. Владельцы и пользователи сертификатов обязаны самостоятельно и своевременно контролировать изменения в Регламенте УЦ и руководствоваться его редакцией, актуальной на момент приобретения услуг удостоверяющего центра.

2.12. Стороны понимают термины, применяемые в Регламенте УЦ, буквально и в контексте общего содержания Регламента УЦ.

2.13. В случае противоречия и (или) расхождения названия какого-либо раздела Регламента УЦ со смыслом какого-либо в нём содержащегося пункта стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

2.14. В случае противоречия и (или) расхождения положений какого-либо приложения к Регламенту УЦ с положениями собственно Регламента УЦ стороны считают доминирующими смысл и формулировки Регламента УЦ.

3. СВЕДЕНИЯ ОБ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ

3.1. ООО ИЦ «Выбор» является юридическим лицом, зарегистрированным Администрацией г. Смоленска 08.11.1995 г. за № 5483, о котором 15.12.2002 г. Инспекцией ФНС России по Промышленному р-ну г. Смоленска внесена запись в ЕГРЮЛ за ОГРН 1026701454064.

3.2. Реквизиты Удостоверяющего центра и данные для контактов:

Полное наименование	Общество с ограниченной ответственностью Информационный центр «Выбор»
Сокращённое наименование	ООО ИЦ «Выбор»
Адрес места нахождения	Российская Федерация, г. Смоленск, ул. Коммунистическая, д. 6
Почтовый адрес	214000 г. Смоленск, ул. Коммунистическая, 6
ОГРН	1026701454064
ИНН	6730025009
КПП	673001001
Телефон	(4812) 701-201 (автоинформатор)
Факс	(4812) 388-898
Адрес электронной почты	info@icvibor.ru
Официальный сайт	www.icvibor.ru
График работы	соответствует рабочему дню Удостоверяющего центра
Пункты выдачи сертификатов:	
Центральное (Смоленское) отделение ООО ИЦ «Выбор»	
Адрес места нахождения	214000 г. Смоленск, ул. Коммунистическая, 6
Телефон	(4812) 701-201
Факс	(4812) 388-898
Адрес электронной почты	info@icvibor.ru
График работы	соответствует рабочему дню Удостоверяющего центра
Сафоновское отделение ООО ИЦ «Выбор»	
Адрес места нахождения	215500 Смоленская область, г. Сафоново, ул. Ленина, 16-А
Телефон	(4812) 701-201 доб. 304; (48142) 221-91
Факс	(48142) 265-36
Адрес электронной почты	ac-safonovo@icvibor.ru
График работы	соответствует рабочему дню Удостоверяющего центра
Вяземское отделение ООО ИЦ «Выбор»	
Адрес места нахождения	215116 Смоленская область, г. Вязьма, ул. Смоленская, 6
Телефон	(4812) 701-201 доб. 156; (48131) 619-89;
Факс	(48131) 619-89
Адрес электронной почты	ac-vyazma@icvibor.ru
График работы	соответствует рабочему дню Удостоверяющего центра

3.3. Информирование получателей услуг Удостоверяющего центра по всем вопросам деятельности Удостоверяющего центра осуществляется:

- работниками ООО ИЦ «Выбор» по прибытии заявителей (клиентов) в одно из его подразделений;
- администрацией ООО ИЦ «Выбор» через Почту России;
- работниками ООО ИЦ «Выбор» по электронной почте;
- работниками ООО ИЦ «Выбор» по телефону;
- работниками ООО ИЦ «Выбор» по факсимильной связи;
- на официальном сайте ООО ИЦ «Выбор».

3.4. Удостоверяющий центр является профессиональным участником рынка услуг по созданию и выдаче сертификатов ключей проверки электронной подписи и в этом качестве осуществляет свою деятельность на территории Российской Федерации на основании:

- Свидетельства Минкомсвязи России об аккредитации удостоверяющего центра;
- лицензии Управления ФСБ России по Смоленской области на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- лицензии Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций на телематические услуги связи.

3.5. Сведения об актуальных лицензиях и иных разрешительных документах УЦ размещаются на официальном сайте Удостоверяющего центра.

4. ЦЕНА УСЛУГ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

4.1. Удостоверяющий центр оказывает свои услуги на платной основе, за исключением тех из них, оказание которых определено безвозмездным согласно требованиям российского законодательства.

4.2. Ассортимент услуг удостоверяющего центра, их стоимость, сроки выполнения и порядок расчётов за оказанные услуги определяются прейскурантом цен на услуги Удостоверяющего центра, действующим на день обращения заявителя в подразделения УЦ, и (или) оговариваются в договоре, заключаемом с заявителем.

4.3. Действующий прейскурант цен на услуги УЦ публикуется на официальном сайте Удостоверяющего центра.

5. ФУНКЦИИ И УСЛУГИ, РЕАЛИЗУЕМЫЕ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

5.1. В рамках своей деятельности Удостоверяющий центр реализует следующие услуги:

5.1.1. создаёт сертификаты ключей проверки электронных подписей и выдаёт такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо правомочий лица, выступающего от имени заявителя, обращаться за получением данного сертификата;

5.1.2. осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи, соответствующим

ключу проверки электронной подписи, указанному им для получения сертификата;

5.1.3. устанавливает сроки действия сертификатов ключей проверки электронных подписей;

5.1.4. аннулирует выданные им сертификаты ключей проверки электронных подписей на основаниях, установленных Законом об электронной подписи;

5.1.5. выдаёт по обращениям заявителей средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные Удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

5.1.6. ведёт Реестр выданных и аннулированных Удостоверяющим центром сертификатов ключей проверки электронных подписей (далее – Реестр сертификатов), включающий в себя в том числе информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах, и информацию о датах прекращения действия или аннулирования сертификатов и об основаниях таких прекращения или аннулирования;

5.1.7. устанавливает порядок ведения Реестра сертификатов, не являющихся квалифицированными, и доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в Реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети «Интернет»;

5.1.8. создаёт по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;

5.1.9. проверяет уникальность ключей проверки электронных подписей в Реестре сертификатов;

5.1.10. осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей в электронных документах;

5.1.11. подтверждает владение владельцем сертификата ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата;

5.1.12. обеспечивает возможность получения заинтересованными лицами содержащейся в Реестре сертификатов информации;

5.1.13. публикует в Информационном ресурсе УЦ перечни документов, обязательных для предъявления заявителями при подаче заявлений на оказание услуг Удостоверяющего центра;

5.1.14. осуществляет иную связанную с использованием электронной подписи деятельность.

6. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

6.1. Удостоверяющий центр обязан:

6.1.1. информировать заявителей об условиях и порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

6.1.2. обеспечивать актуальность, целостность и доступность информации, содержащейся в Реестре сертификатов, и её защиту от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий;

6.1.3. обеспечивать безвозмездную круглосуточную (за исключением периодов технического обслуживания и ремонта) доступность (также и посредством информационно-телекоммуникационной сети «Интернет») актуальной информации, содержащейся в Реестре сертификатов, в том числе об аннулировании выданных сертификатов ключа проверки электронной подписи;

6.1.4. обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей до их выдачи владельцам сертификатов;

6.1.5. отказывать заявителю в создании сертификата в случае, если не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки элек-

тронной подписи, указанному заявителем для получения сертификата;

6.1.6. отказывать заявителю в создании сертификата в случае отрицательного результата проверки в Реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата;

6.1.7. издавать сертификаты в формах электронного документа и документа на бумажном носителе (форма – в приложении № 9) на основании заявления заявителей и в соответствии с порядком, определённым Регламентом УЦ;

6.1.8. для подписания издаваемых сертификатов и списков отозванных сертификатов использовать только ключ электронной подписи уполномоченного лица УЦ, срок действия которого не истёк, и только с этой целью;

6.1.9. принимать меры по защите ключа электронной подписи уполномоченного лица Удостоверяющего центра от несанкционированного доступа;

6.1.10. вести отсчёт (указание) времени в средствах Удостоверяющего центра, электронных документах и документах на бумажном носителе по московскому поясному времени;

6.1.11. синхронизировать с точным мировым временем и периодически поверять системное время средств Удостоверяющего центра;

6.1.12. вносить в создаваемые сертификаты только достоверную и актуальную информацию, подтверждённую соответствующими документами и сведениями, полученными с использованием государственных информационных ресурсов;

6.1.13. обеспечить уникальность серийных номеров сертификатов ключа проверки электронной подписи, издаваемых Удостоверяющим центром, а также изготовленных ключей проверки электронной подписи владельцев сертификатов;

6.1.14. при выдаче сертификатов устанавливать личность заявителя-физического лица, обратившегося к нему за получением сертификата, или получать от лица, выступающего от имени заявителя-юридического лица, подтверждение правомочия обращаться за получением сертификата;

6.1.15. с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, запрашивать и получать у операторов базовых государственных информационных ресурсов сведения, необходимые для проверки достоверности документов и сведений, представленных заявителем;

6.1.16. запрашивать и получать из государственных информационных ресурсов подтверждение достоверности документов и сведений, представленных в соответствии с Законом об электронной подписи заявителем для заполнения квалифицированного сертификата;

6.1.17. отказывать заявителю в выдаче сертификата, если полученная с использованием государственных информационных ресурсов информация не подтверждает достоверность представленных заявителем документов и сведений, или не установлена личность заявителя-физического лица, либо не получено подтверждение правомочий лица, выступающего от имени заявителя-юридического лица, на обращение за получением квалифицированного сертификата;

6.1.18. уведомлять об аннулировании сертификатов посредством публикации в Информационном ресурсе УЦ актуальных СОС (CRL) в течение 30 минут после поступления в Удостоверяющий центр соответствующего заявления об аннулировании сертификата или вступившего в законную силу решения суда о дисквалификации руководителя либо иного документа уполномоченного органа, подтверждающего факт невозможности осуществления руководства;

6.1.19. до внесения в Реестр сертификатов информации об аннулировании сертификата на основаниях, предусмотренных ч. 9 ст. 14 Закона об электронной подписи, уведомлять владельца сертификата об аннулировании его сертификата путём направления документа на бумажном носителе или электронного документа с указанием основания аннулирования его сертификата;

6.1.20. издавать не реже 1 раза в 24 часа актуальные списки отозванных сертификатов и публиковать их в Информационном ресурсе УЦ;

6.1.21. по электронной почте направлять владельцам сертификатов уведомления о дате окончания действия их сертификатов за 30, 14 и 10 календарных дней до её наступления;

6.1.22. направлять для регистрации в ЕСИА сведения в установленном объёме о лице, получившем сертификат ключа проверки электронной подписи, и о полученном им квалифицированном сертификате;

6.1.23. при выдаче квалифицированного сертификата по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществлять регистрацию указанного лица в ЕСИА;

6.1.24. по заявлениям участников электронного взаимодействия осуществлять проверку электронной подписи в электронных документах, электронной подписи уполномоченного лица Удостоверяющего центра в сертификатах;

6.1.25. таким образом соблюдать сроки действия ключей электронной подписи уполномоченного лица Удостоверяющего центра, используемых для подписания создаваемых клиентских сертификатов, чтобы последние были подписаны ключами, не прекратившими своё действие;

6.1.26. хранить информацию, внесённую в Реестр сертификатов, в течение всего срока деятельности Удостоверяющего центра, если более короткий срок не установлен нормативными правовыми актами Российской Федерации.

6.2. Удостоверяющий центр имеет право:

6.2.1. запрашивать у заявителя дополнительные, подтверждающие достоверность представленных им сведений, документы при наличии противоречий между сведениями, представленными заявителем, и сведениями, полученными в соответствии с ч. 2.2 ст. 18 Закона об электронной подписи;

6.2.2. не принимать к рассмотрению поступившие от заявителя документы, не соответствующие требованиям нормативных правовых актов Российской Федерации и Регламента УЦ;

6.2.3. отказать заявителю в выдаче сертификата при невыполнении им обязанностей и условий, установленных ч.ч. 2÷2.3 ст. 18 Закона об электронной подписи, иными нормативными правовыми актами Российской Федерации и Регламентом УЦ;

6.2.4. отказать Заявителю в аннулировании сертификата при ненадлежащем обращении за этим или ненадлежащем оформлении соответствующего заявления;

6.2.5. досрочно (без заявления владельца сертификата) аннулировать сертификат:

- при наличии у Удостоверяющего центра достоверных сведений о нарушении конфиденциальности ключа электронной подписи владельца сертификата;
- при наличии у Удостоверяющего центра достоверных сведений о том, что документы, ранее представленные заявителем в целях создания и получения им сертификата, не являются подлинными и/или не подтверждают достоверность всей информации, включенной в созданный сертификат;
- при наличии у Удостоверяющего центра достоверных сведений о невыполнении владельцем сертификата обязанностей, установленных законодательством Российской Федерации в области электронной подписи;
- если не подтверждено, что владелец сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- если установлено, что содержащийся в сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном Удостоверяющим центром сертификате ключа проверки электронной подписи;
- если вступило в силу решение суда, которым, в частности, установлено, что сертификат содержит недостоверную информацию или о дисквалификации пользователя сертификата;

- при отказе владельца сертификата от присоединения к Регламенту УЦ или от его исполнения.

6.2.6. устанавливать срок действия сертификатов в интервалах, определённых законами и иными нормативными правовыми актами, а также техническими характеристиками применяемых средств Удостоверяющего центра.

7. ПРАВА И ОБЯЗАННОСТИ ЗАЯВИТЕЛЯ (ВЛАДЕЛЬЦА СЕРТИФИКАТА)

7.1. Заявитель (владелец сертификата) обязан:

7.1.1. представить Удостоверяющему центру документы, подтверждающие сведения, вносимые в его сертификат ключа проверки электронной подписи, и правомочия владельца сертификата;

7.1.2. при необходимости предоставить Удостоверяющему центру надлежащим образом заверенные копии документов, подтверждающих сведения, вносимые в сертификат, и правомочия владельца сертификата;

7.1.3. соблюдать конфиденциальность личного ключа электронной подписи, принимая все возможные меры для предотвращения его утери, несанкционированного (скрытого) копирования и использования;

7.1.4. применять для подписания электронных документов только личный, действующий на данный момент времени, ключ электронной подписи;

7.1.5. не использовать личный ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа была нарушена;

7.1.6. в течение не более, чем 1 рабочего дня от получения информации о компрометации его ключа электронной подписи, обращаться в Удостоверяющий центр с заявлением об аннулировании сертификата ключа проверки электронной подписи, а также уведомлять об этом иных участников электронного взаимодействия;

7.1.7. со времени подачи в Удостоверяющий центр заявления об аннулировании сертификата не использовать личный ключ электронной подписи, связанный с этим сертификатом;

7.1.8. не использовать личный ключ электронной подписи, связанный с сертификатом, который аннулирован.

7.2. Заявитель (владелец сертификата) имеет право:

7.2.1. в порядке выполнения оплаченной им услуги получать личный сертификат в форме электронного документа и заверенного Удостоверяющим центром экземпляра сертификата на бумажном носителе;

7.2.2. получать сертификат уполномоченного лица Удостоверяющего центра в форме электронного документа;

7.2.3. получать актуальный список отозванных сертификатов, изготовленный Удостоверяющим центром, в форме электронного документа;

7.2.4. создавать (генерировать) личный ключ электронной подписи самостоятельно;

7.2.5. направлять в Удостоверяющий центр запрос на получение сертификата ключа проверки электронной подписи, созданный с соблюдением требований к такому запросу и соответствующий ключу электронной подписи, сгенерированному им самостоятельно;

7.2.6. поручать изготовление личного ключа электронной подписи Удостоверяющему центру, в том числе в личном присутствии заявителя;

7.2.7. применять СОС, изготовленный Удостоверяющим центром, для проверки статуса сертификатов ключа проверки электронной подписи, изготовленных Удостоверяющим центром;

7.2.8. применять для хранения личного ключа электронной подписи любой носитель, поддерживаемый средствами электронной подписи Удостоверяющего центра, если использование такого носителя не запрещено российским законодательством;

7.2.9. осуществлять экспорт выданного ему (сгенерированного им) ключа электронной подписи

при условии соблюдения необходимых мер по обеспечению его конфиденциальности;

7.2.10. обращаться в Удостоверяющий центр с заявлениями:

- об изготовлении ему сертификата ключа проверки электронной подписи и (при необходимости) ключа электронной подписи;
- об аннулировании сертификата ключа проверки электронной подписи в течение срока действия соответствующего ключа электронной подписи;
- о подтверждении подлинности электронной подписи уполномоченного лица Удостоверяющего центра в сертификате ключа проверки электронной подписи;
- о подтверждении подлинности электронной подписи в электронном документе.

8. ОТВЕТСТВЕННОСТЬ СТОРОН И ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

8.1. При возникновении споров сторонами в них считаются Удостоверяющий центр и заявитель (владелец сертификата).

8.2. Все споры, связанные с исполнением Регламента УЦ, будут разрешаться сторонами в претензионном порядке. Сторона, получившая претензию, обязана её рассмотреть и предоставить ответ направившей стороне в течение 10 рабочих дней со дня её получения. При неурегулировании спора в досудебном порядке, он подлежит рассмотрению в установленном порядке.

8.3. Каждая сторона несёт ответственность за вред, причинённый другой стороне и третьим лицам в результате:

8.3.1. неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг Удостоверяющим центром;

8.3.2. неисполнения или ненадлежащего исполнения обязанностей, предусмотренных Законом об электронной подписи.

8.4. Удостоверяющий центр не несёт ответственности за невозможность использования в отдельных информационных системах электронной подписи, основанной на квалифицированном сертификате, выданном Удостоверяющим центром, при предъявлении операторами этих информационных систем требований к форме квалифицированного сертификата, к аккредитованному удостоверяющему центру и иных, в том числе к условиям признания электронных документов, подписанных электронной подписью, и электронной подписи в них имеющими юридическую силу, превышающих требования, установленные Законом об электронной подписи и принятыми в соответствии с ним нормативными правовыми актами, если дополнительные требования не были обеспечены за дополнительную оплату.

ПРЕДОСТАВЛЕНИЕ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

9. ПРОЦЕДУРА СОЗДАНИЯ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ И КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

9.1. Изготовление в Удостоверяющем центре ключей электронной подписи и соответствующих им сертификатов производится работниками Удостоверяющего центра на автоматизированных рабочих местах, имеющих документальное подтверждение их соответствия требованиям по безопасности информации.

9.2. Ключ электронной подписи и ключ проверки электронной подписи создаются заявителем или работниками УЦ с использованием 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, установленными постановлением Правительства Российской Федерации от 03.02.2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

9.3. После успешной аутентификации владельца сертификата и проверки правильности составления (оформления) представленных документов работник Удостоверяющего центра изготавливает ключ электронной подписи и соответствующие ему ключ проверки электронной подписи и сертификат, записав их на ключевой носитель.

9.4. Ключевые носители с изготовленными для владельцев сертификата ключами электронной подписи до выдачи их владельцам сертификата временно хранятся в личных опечатываемых сейфах работников Удостоверяющего центра, ответственных за их изготовление. Выдача носителей с ключами электронной подписи их владельцам производится под роспись в Журнале поэкземплярного учёта СКЗИ, эксплуатационной и технической документации к ним, ключевых документов органа криптографической защиты информации.

9.5. Изготовление персоналом Удостоверяющего центра дубликатов ключа электронной подписи, не санкционированное владельцем соответствующего сертификата или не предусмотренное технологическим процессом, а также копирование ключей электронной подписи на неучтённые ключевые носители, **запрещены**.

9.6. Технологические копии ключей электронной подписи после записи ключей на учтённые носители подлежат уничтожению (стиранию) не позднее 30 минут после проверки работоспособности учтённого ключа электронной подписи.

9.7. Владелец или пользователь сертификата имеют право присутствовать при изготовлении работником Удостоверяющего центра их личного ключа электронной подписи.

9.8. Пользователь сертификата имеет право самостоятельно вне Удостоверяющего центра изготовить для личного использования ключ электронной подписи (ключевой набор). Полученный таким образом ключевой набор пользователь представляет в Удостоверяющий центр для создания в его присутствии работником Удостоверяющего центра запроса на издание сертификата, соответствующего предоставленному ключу электронной подписи.

9.9. Пользователь сертификата имеет право самостоятельно (в присутствии работника Удостоверяющего центра) изготовить для личного использования ключ электронной подписи (ключевой набор) в Удостоверяющем центре на специально предназначенных для этого автоматизированных рабочих местах, аттестованных на соответствие требованиям по безопасности информации. Полученный таким образом ключевой набор пользователь представляет в Удостоверяющий центр для создания в его присутствии работником Удостоверяющего центра запроса на издание сертификата, соответствующего предоставленному ключу электронной подписи.

10. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ УПОЛНОМОЧЕННОГО ЛИЦА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

10.1. Ключ электронной подписи уполномоченного лица Удостоверяющего центра используется для подписывания созданных Удостоверяющим центром сертификатов и СОС в течение срока его действия.

10.2. Издание и ввод в обращение очередного ключа электронной подписи уполномоченного лица Удостоверяющего центра и сертификата к нему производится (как правило) в связи окончанием срока действия таких ключей, используемых Удостоверяющим центром для целей согласно п. 10.1 настоящего Регламента.

10.3. Издание очередного ключа электронной подписи уполномоченного лица Удостоверяющего центра и сертификата к нему производится в плановом порядке, но не позднее, чем через 15 месяцев после начала действия предыдущего ключа такого назначения.

10.4. Порядок издания и оформления ключей электронной подписи уполномоченного лица Удостоверяющего центра и сертификатов к ним:

10.4.1. уполномоченное лицо Удостоверяющего центра с помощью средств Удостоверяющего центра генерирует для себя очередной ключ электронной подписи и файл запроса на получение квалифицированного сертификата к этому ключу;

10.4.2. файл запроса на получение квалифицированного сертификата уполномоченного лица Удо-

стоверяющего центра направляется в УФО (ГУЦ) по электронной почте на указанный Минцифры России адрес или через Портал госуслуг с приложением анкеты Удостоверяющего центра установленной формы;

10.4.3. уполномоченное лицо Удостоверяющего центра по получении из УФО (ГУЦ) файла запрошенного сертификата производит его связывание с ранее созданным ключом электронной подписи;

10.4.4. полученный из УФО (ГУЦ) сертификат уполномоченного лица УЦ устанавливается в качестве текущего (действующего) в средствах Удостоверяющего центра.

10.5. Информирование неограниченного круга лиц, в том числе владельцев сертификата, о смене текущего (действующего) сертификата уполномоченного лица Удостоверяющего центра производится путём публикации его в Информационном ресурсе УЦ.

10.6. Доверенные способы получения очередного сертификата уполномоченного лица Удостоверяющего центра:

10.6.1. скачиванием с Портала (сайта) УФО (в разделе УЦ ООО ИЦ «Выбор»);

10.6.2. скачиванием с Информационного ресурса УЦ, в том числе по указанному в сертификате владельца сертификата адресу (в поле «Доступ к информации о центрах сертификации»);

10.6.3. обращением непосредственно или по электронной почте в Удостоверяющий центр.

11. СМЕНА КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ УПОЛНОМОЧЕННОГО ЛИЦА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА И ВЛАДЕЛЬЦЕВ СЕРТИФИКАТА ПРИ ИХ КОМПРОМЕТАЦИИ

11.1. Угрозами нарушения конфиденциальности ключа электронной подписи уполномоченного лица Удостоверяющего центра являются:

11.1.1. атаки на информационные системы (несанкционированный доступ извне, проникновение вредоносных программ);

11.1.2. удаленное администрирование персоналом Удостоверяющего центра;

11.1.3. хищение ключа сотрудником УЦ (инсайдером);

11.1.4. нарушение режима охраны и физического доступа к оборудованию.

11.2. Владелец сертификата самостоятельно делает вывод о компрометации ключа электронной подписи, владельцем которого он является.

11.3. При компрометации своего личного ключа электронной подписи владелец сертификата должен подать в Удостоверяющий центр заявление на аннулирование сертификата, соответствующего скомпрометированному ключу электронной подписи. Для срочного (связанного с компрометацией) отзыва сертификата владелец сертификата должен сообщить в Удостоверяющий центр по телефону идентифицирующие его и аннулируемый сертификат данные, в том числе: кодовую фразу, серийный номер сертификата, фамилию, имя, отчество пользователя сертификата, ОГРН организации (для юридических лиц) или ИНН (для индивидуальных предпринимателей и физических лиц).

11.4. Выдача владельцу сертификата новых (вместо скомпрометированных) ключей электронной подписи производится после аннулирования сертификата скомпрометированного ключа электронной подписи в соответствии с порядком, определённым Регламентом УЦ.

11.5. Компрометация ключа электронной подписи уполномоченного лица Удостоверяющего центра является основанием для обязательного аннулирования его сертификата, для чего в УФО (ГУЦ) Удостоверяющим центром незамедлительно направляется заявление об отзыве сертификата уполномоченного лица Удостоверяющего центра, соответствующего скомпрометированному ключу электронной подписи.

11.6. Скомпрометированный ключ электронной подписи уполномоченного лица Удостоверяющего центра незамедлительно выводится из обращения в Удостоверяющем центре, подписание

скомпрометированным ключом электронной подписи уполномоченного лица Удостоверяющего центра новых сертификатов и списков отозванных сертификатов прекращается с момента установления факта компрометации ключа.

11.7. Все действующие сертификаты, подписанные с использованием скомпрометированного ключа электронной подписи уполномоченного лица Удостоверяющего центра, подлежат аннулированию Удостоверяющим центром.

11.8. Занесение сведений об аннулированных сертификатах в Реестр сертификатов производится после получения из УФО (ГУЦ) нового (вместо отозванного) сертификата уполномоченного лица Удостоверяющего центра.

11.9. Взамен аннулированных вследствие факта компрометации ключа электронной подписи уполномоченного лица Удостоверяющего центра сертификатов Удостоверяющий центр досрочно (не позднее 10 рабочих дней от получения из ГУЦ нового сертификата уполномоченного лица Удостоверяющего центра) и безвозмездно издаёт для владельцев сертификата по их заявлениям аналогичные скомпрометированным новые сертификаты (при необходимости – с ключами электронной подписи).

11.10. Уведомление владельцев сертификата о компрометации ключа электронной подписи уполномоченного лица Удостоверяющего центра осуществляется посредством размещения информации об этом в информационном ресурсе УЦ, рассылок соответствующих сообщений по электронной почте или почтовой связью.

11.11. Процедуры создания ключа электронной подписи и получения сертификата уполномоченного лица Удостоверяющего центра, информирования неограниченного круга лиц, в том числе владельцев сертификата, о смене текущего (действующего) сертификата, доверенные способы его получения при компрометации ключа электронной подписи уполномоченного лица Удостоверяющего центра соответствуют тем, что применяются при плановой смене такого ключа.

12. СМЕНА КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ ВЛАДЕЛЬЦЕВ СЕРТИФИКАТА

12.1. Смена ключа электронной подписи владельца сертификата осуществляется по заявлению владельца сертификата.

12.2. Заявление на смену ключа электронной подписи владельца сертификата может быть подано в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца сертификата. Если смена КЭП связана с его компрометацией, то заявление в форме электронного документа должно быть подписано квалифицированной электронной подписью, созданной с помощью другого ключа электронной подписи.

13. ИЗГОТОВЛЕНИЕ СЕРТИФИКАТОВ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ, ИХ ВЫДАЧА ВЛАДЕЛЬЦАМ СЕРТИФИКАТОВ

13.1. Сертификаты могут изготавливаться:

13.1.1. в связи с выдачей Удостоверяющим центром владельцу сертификата первого сертификата в УЦ ООО ИЦ «Выбор»;

13.1.2. в связи с окончанием срока действия ранее выданных владельцу сертификатов;

13.1.3. до окончания срока действия ранее выданных владельцу сертификатов по причине, обоснованной п.п. 1, 2, 4 ч. 6 и ч. 6.1 ст. 14 Закона об электронной подписи.

13.2. Количество одновременно действующих сертификатов, выдаваемых одному лицу-заявителю, Удостоверяющим центром не ограничивается.

13.3. Для подтверждения сведений, вносимых в квалифицированный сертификат, в том числе для удостоверения личности заявителя, Удостоверяющий центр получает (проверяет) от заявителя и (или) запрашивает в государственных информационных ресурсах следующие документы и сведения:

от юридических лиц

13.3.1. заявление в УЦ о выпуске сертификата;

13.3.2. документ, удостоверяющий личность пользователя сертификата на территории РФ;

13.3.3. копии документов о наделении руководителя юридического лица (иного лица) полномочиями исполнительного органа;

13.3.4. при необходимости: копии документов, определяющих передачу полномочий единоличного исполнительного органа юридического лица управляющей организации/управляющему;

13.3.5. выписку из ЕГРЮЛ;

13.3.6. СНИЛС физического лица - пользователя сертификата;

13.3.7. при необходимости: доверенность от руководителя юридического лица представителю юридического лица, уполномоченному получить изготовленные ключи и сертификат;

13.3.8. при необходимости: документ, удостоверяющий личность лица (представителя юридического лица), уполномоченного на получение изготовленного сертификата;

от индивидуальных предпринимателей

13.3.9. заявление в УЦ о выпуске сертификата;

13.3.10. документ, удостоверяющий личность пользователя сертификата на территории РФ;

13.3.11. выписку из ЕГРИП;

13.3.12. СНИЛС пользователя сертификата;

13.3.13. при необходимости: нотариально заверенную доверенность от индивидуального предпринимателя представителю индивидуального предпринимателя, уполномоченному получить изготовленные ключи и сертификат;

13.3.14. при необходимости: заявление о наделении своего представителя (одного или нескольких) полномочиями получить изготовленные ключи и сертификат;

13.3.15. при необходимости: документ, удостоверяющий личность лица, уполномоченного получить изготовленные ключи и сертификат;

от физических лиц

13.3.16. заявление в УЦ о выпуске сертификата;

13.3.17. документ, удостоверяющий личность пользователя сертификата на территории РФ;

13.3.18. СНИЛС пользователя сертификата;

13.3.19. при необходимости: свидетельство о постановке физического лица на учёт в налоговом органе.

13.4. Изготовление и выдача сертификатов заявителям осуществляется Удостоверяющим центром в соответствии с заявлением установленной формы (приложение № 1), поданным заявителем в Удостоверяющий центр и содержащим сведения, необходимость указания которых установлена нормативными правовыми и иными актами, устанавливающими требования к сертификатам в системах электронного документооборота. В заявлении указываются:

13.4.1. сведения о заявителе;

13.4.2. просьба создать и выдать сертификат ключа проверки электронной подписи и (при необходимости) ключ электронной подписи к нему;

13.4.3. сведения (данные) о владельце (пользователе) сертификата, необходимые для внесения в состав сертификата;

13.4.4. сведения о владельце (пользователе) сертификата, необходимые для регистрации в ЕСИА согласно ч. 5 ст. 18 Закона об электронной подписи, в том числе данные из документа, удосто-

веряющего личность пользователя сертификата;

13.4.5. дополнительные назначения (области использования) сертификата, полномочия и роли владельца сертификата, если таковые нужны;

13.4.6. дополнительные условия по созданию ключа электронной подписи и сертификата к нему (метод идентификации заявителя, используемые средства криптографической защиты информации, возможность копирования ключа на другой носитель, количество заказываемых сертификатов, другие);

13.4.7. кодовая фраза и порядок её использования;

13.4.8. заявление владельца сертификата о присоединении к Регламенту УЦ, осведомлённости об использовании персональных данных пользователя сертификата, условиях использования средств электронной подписи;

13.4.9. заявление владельца сертификата о согласии осуществлять с Удостоверяющим центром юридически значимый документооборот по электронной почте с указанием адреса электронной почты, используемого для такого документооборота;

13.4.10. должность (если есть), роспись правомочного представителя заявителя, его инициалы и фамилия;

13.4.11. дата заявления;

13.4.12. оттиск основной печати организации (для юридических лиц, имеющих основную печать).

13.5. Кодовая (парольная) фраза в заявлении на выдачу сертификата необходима для аутентификации владельца сертификата при выполнении процедур, связанных с компрометацией ключа электронной подписи.

13.6. Заявление на создание и выдачу первого (для данного лица) квалифицированного сертификата должно быть оформлено на бумажном носителе с подписью заявителя и (для юридических лиц, имеющих основную печать) печатью организации, а для второго и последующих сертификатов данного лица может быть оформлено и в виде электронного документа, подписанного квалифицированной электронной подписью владельца сертификата.

13.7. Данные, вносимые в квалифицированный сертификат из заявления в виде электронного документа, подписанного квалифицированной электронной подписью заявителя, должны совпадать с аналогичными данными в квалифицированном сертификате, с помощью которого эта электронная подпись была создана.

13.8. Первым методом установления Удостоверяющим центром личности (идентификации) полностью дееспособных и правоспособных заявителей - физических лиц является предъявление в натуральном виде работникам Удостоверяющего центра основных документов, удостоверяющих личность физических лиц-заявителей или физических лиц-правомочных представителей юридических лиц, являющихся заявителями.

13.9. Документами, удостоверяющими личность граждан Российской Федерации, иностранных государств, беженцев, вынужденных переселенцев и лиц без гражданства в соответствии с законным порядком и правилами, установленными на территории РФ, являются:

13.9.1. паспорт гражданина Российской Федерации;

13.9.2. удостоверение личности военнослужащего Российской Федерации;

13.9.3. военный билет гражданина Российской Федерации;

13.9.4. временное удостоверение личности гражданина Российской Федерации;

13.9.5. военный билет офицера запаса Российской Федерации;

13.9.6. паспорт (в т.ч. заграничный) иностранного гражданина;

13.9.7. вид на жительство в Российской Федерации;

13.9.8. разрешение на временное проживание в Российской Федерации;

13.9.9. удостоверение беженца (российского образца);

13.9.10. свидетельство о предоставлении временного убежища на территории РФ;

13.9.11. свидетельство о рассмотрении ходатайства о признании лица беженцем на территории Российской Федерации по существу;

13.9.12. иные документы, в соответствии с текущим законодательством РФ установленные на территории Российской Федерации как удостоверяющие личность граждан РФ и иностранных государств.

13.10. Вторым методом идентификации заявителей (физических и юридических лиц) является предъявление (в т.ч. по электронной почте) работникам Удостоверяющего центра электронных документов (в т.ч. заявления на выдачу квалифицированного сертификата), подписанных квалифицированной электронной подписью физических лиц-заявителей или физических лиц-правомочных представителей юридических лиц, являющихся заявителями. Идентификация считается пройденной, если программно подтверждена действительность электронной подписи, и данные о лице, подписавшем электронный документ, в самом документе и в квалифицированном сертификате, с помощью которого была создана электронная подпись под электронным документом, совпадают.

13.11. Сведения, указанные заявителем для получения сертификата, которые удостоверяются данными, полученными из государственных информационных ресурсов (электронных реестров), предъявлением документов, подтверждающих эти сведения, или предоставлением их надлежащим образом заверенных копий:

13.11.1. для заявителя-юридического лица – полное или сокращённое наименование юридического лица, основной государственный регистрационный номер (далее по тексту – ОГРН), адрес местонахождения, идентификационный номер налогоплательщика (далее по тексту – ИНН), код причины постановки на учёт;

13.11.2. для заявителя-физического лица – номер Страхового свидетельства обязательного пенсионного страхования (СНИЛС), ИНН;

13.11.3. для заявителя-физического лица, являющегося индивидуальным предпринимателем – номер страхового свидетельства обязательного пенсионного страхования (СНИЛС), ИНН и ОГРН записи о государственной регистрации физического лица в качестве индивидуального предпринимателя.

13.12. Для заполнения полей квалифицированного сертификата Удостоверяющий центр в соответствии с ч. 2 ст. 17 Закона об электронной подписи запрашивает и получает из государственных информационных ресурсов сведения, предусмотренные ч. 2.2 ст. 18 того же Закона.

13.13. Удостоверяющий центр с использованием государственных информационных ресурсов проверяет действительность документов, удостоверяющих личность, предъявленных заявителями или их правомочными представителями в целях получения квалифицированного сертификата.

13.14. Если достоверность сведений, указанных заявителем в заявлении на получение сертификата, подтверждена информацией, полученной из государственных информационных ресурсов, и личность заявителя удостоверена, УЦ создаёт и выдаёт заявителю квалифицированный сертификат. В противном случае Удостоверяющий центр отказывает заявителю в выдаче квалифицированного сертификата.

13.15. Получение сертификата ключа проверки электронной подписи может быть осуществлено лицом, действующим на основании доверенности (примерные полномочия – в приложении № 2). Срок действия такой доверенности должен заканчиваться не ранее окончания срока действия сертификата, ключ электронной подписи к которому был получен по доверенности.

13.16. Физическое лицо, при получении сертификата действующее от имени заявителя-физического лица, должно предъявить в Удостоверяющий центр нотариально заверенную доверенность на право совершения таких действий.

13.17. Достоверность сведений о заявителе, указанных в заявлении на выдачу сертификата, подтверждается предъявлением документов, достоверно содержащих эти сведения и подтверждающих правомочия заявителя и иных получателей услуги удостоверяющего центра. При необходимости заявитель предоставляет в Удостоверяющий центр надлежащим образом заверенные копии подтверждающих документов, при этом перечень и форма представляемых документов определяется российским законодательством и Регламентом УЦ.

13.18. Необходимые для издания сертификата документы или их должным образом заверенные копии должны:

13.18.1. соответствовать требованиям к формату и содержанию, установленным действующим законодательством Российской Федерации и/или органами государственной власти;

13.18.2. быть действительными в день их предъявления;

13.18.3. иметь чётко выраженные и неискажённые реквизиты (например, учётные номера, даты выдачи или регистрации, подписи лиц, печати организаций, логотипы организаций или герб РФ, фотографии лиц и др.);

13.18.4. иметь текст или графические объекты документа, отпечатанные с качеством, позволяющим без искажений или изъятий воспринять их подлинный смысл (содержание);

13.18.5. быть надлежащим образом заверены, если это – копии;

13.18.6. сохранять стандартную целостность, не содержать признаков подделки или намеренных исправлений.

13.19. К предъявляемым документам, не имеющим в своём составе содержательной части, изложенной на русском языке, должен быть приложен их квалифицированный перевод на русский язык, заверенный нотариусом или консульскими органами Российской Федерации.

13.20. Формы документов (не имеющих государственного образца), применяемых при взаимодействии заявителей (владельцев сертификатов) и Удостоверяющим центром, устанавливаются Удостоверяющим центром. Их актуальные версии публикуются на официальном сайте Удостоверяющего центра, а также предлагаются заявителям для заполнения перед получением услуг Удостоверяющего центра.

13.21. Персонал Удостоверяющего центра проверяет правомочия заявителя на получение и владение сертификатом и достоверность сведений (данных), представленных им для внесения в сертификат, в пределах, необходимых и достаточных для реализации на законных основаниях функций аккредитованного удостоверяющего центра.

13.22. Документы и сведения (на бумажном носителе или электронные), а также их копии, подтверждающие данные, вносимые в сертификат ключа проверки электронной подписи, и правомочия заявителей, подлежат хранению в течение деятельности Удостоверяющего центра, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации.

13.23. Сроки создания и выдачи сертификата, а также исполнения иных услуг Удостоверяющего центра устанавливаются заключённым с заявителем договором на оказание услуг Удостоверяющего центра.

13.24. На создание и выдачу сертификата отводится 10 рабочих дней от оплаты заявителем заказа, предоставления полного и валидного комплекта документов и (при необходимости) носителя ключа электронной подписи.

13.25. При оплате заявителем тарифа срочного исполнения заказа и выполнении прочих необходимых условий (см. п. 14.21 настоящего Регламента) оказание услуги производится в течение 1 рабочего дня (8 рабочих часов).

13.26. Квалифицированные сертификаты создаются в соответствии с требованиями приказа ФСБ России от 27.12.2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

13.27. При создании квалифицированных сертификатов работник Удостоверяющего центра вносит данные для включения в сертификат (в запрос на создание сертификата) в соответствии со сведениями, указанными заявителем в заявлении на выдачу сертификата, сверяя вводимые данные с данными из государственных информационных ресурсов (сервисов СМЭВ), а также (при необходимости) и с копиями представленных клиентом документов.

13.28. По требованию клиента в издаваемый для него квалифицированный сертификат Удостоверяющим центром вносятся специальные объектные идентификаторы (OID).

13.29. Формирование запросов на создание сертификата и получение сертификатов из Удостоверяющего центра осуществляется подготовленными работниками на специально оснащённых автоматизированных рабочих местах, аттестованных на соответствие требованиям нормативной документации по безопасности информации. Отправка запросов в программно-аппаратный комплекс Удостоверяющего центра и получение оттуда сертификатов осуществляется по защищённым каналам связи.

13.30. Сертификаты ключа проверки электронной подписи, изданные Удостоверяющим центром, подписываются электронной подписью уполномоченного лица Удостоверяющего центра.

13.31. При создании ключевой пары и запроса на выдачу сертификата работниками Удостоверяющего центра используются только средства, в том числе криптографической защиты информации, соответствие которых требованиям безопасности информации подтверждено уполномоченными на то государственными органами (Федеральная служба безопасности, ФСТЭК). Выбор из числа разрешённых к использованию средств криптографической защиты информации для создания ключевой пары определяется заявителем и указывается в заявлении на выдачу сертификата.

13.32. Для записи контейнера ключа электронной подписи Удостоверяющим центром используются применяемые в Российской Федерации носители, соответствие которых требованиям безопасности информации подтверждено уполномоченными на то государственными органами (Федеральная служба безопасности) и руководящей документацией на СКЗИ.

13.33. После получения сертификата из программно-аппаратного комплекса Удостоверяющего центра работник УЦ с помощью специальных программ связывает его с соответствующим контейнером ключа электронной подписи владельца сертификата на носителе ключа.

13.34. Возможность копирования (экспорта) контейнера ключа электронной подписи на другие совместимые носители задаётся по письменному заявлению заявителя.

13.35. При формировании запроса на создание сертификата может использоваться созданный владельцем сертификата ключевой набор (контейнер ключа электронной подписи).

13.36. Носители с ключами электронной подписи после генерации, учёта и до их выдачи пользователям хранятся в личном сейфе работника Удостоверяющего центра, изготовившего ключи электронной подписи. Носители с ключами электронной подписи выдаются пользователям сертификата под роспись.

13.37. Невостребованные владельцем сертификата ключи электронной подписи подлежат уничтожению (стиранию с носителя) по истечении 45 суток со дня их генерации. Об уничтожении ключей электронной подписи их владельцы предупреждаются Удостоверяющим центром по электронной почте и/или телефону за 3 рабочих дня до удаления ключей с носителя или его уничтожения.

13.38. Сертификат выдаётся пользователю в электронной форме и на бумажном носителе. При необходимости одновременно с сертификатом выдаётся ключ электронной подписи, соответствующий выданному сертификату.

13.39. При получении сертификата пользователь должен быть под роспись ознакомлен Удостоверяющим центром с информацией, содержащейся в сертификате. Для этого созданные сертификаты распечатываются работником Удостоверяющего центра на бумажном носителе (форма – в приложении № 9) в 2 экземплярах, каждый из которых подписывается пользователем сертификата, а также работником Удостоверяющего центра, подпись которого скрепляется печатью

Удостоверяющего центра.

13.40. Оба экземпляра сертификата на бумажном носителе, один из которых остаётся на хранении в Удостоверяющем центре, а второй выдаётся владельцу сертификата, имеют равную силу.

13.41. Вместо сертификата на бумажном носителе владельцу сертификата может быть отправлена информация о содержании квалифицированного сертификата в электронном виде. Факт ознакомления с информацией о содержании квалифицированного сертификата владелец сертификата фиксирует подписанием файла с информацией личной квалифицированной электронной подписью и направлением подписанного файла в Удостоверяющий центр.

13.42. При оказании услуги Удостоверяющего центра по созданию и выдаче сертификата владельцу сертификата выдаются:

13.42.1. сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра (в виде файла);

13.42.2. принадлежащий ему сертификат ключа проверки электронной подписи, соответствующий его ключу электронной подписи (в виде файла);

13.42.3. один экземпляр принадлежащего ему сертификата ключа проверки электронной подписи (на бумажном носителе) или информация о содержании квалифицированного сертификата (в виде файла);

13.42.4. ключ электронной подписи (если он изготавливался в Удостоверяющем центре), записанный на ключевой носитель.

13.43. Все квалифицированные сертификаты, выданные Удостоверяющим центром, подлежат обязательной регистрации в Единой системе идентификации и аутентификации путём направления в неё установленных законом сведений о лице, получившем квалифицированный сертификат, и о полученном им квалифицированном сертификате.

13.44. По желанию лица, которому выдан квалифицированный сертификат, Удостоверяющий центр осуществляет безвозмездную регистрацию этого лица в ЕСИА.

14. ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ И АННУЛИРОВАНИЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

14.1. Сертификаты, выданные Удостоверяющим центром, прекращают свое действие:

14.1.1. до начала или по истечении срока их действия;

14.1.2. по инициативе владельца сертификата на основании заявления, поданного в форме документа на бумажном носителе или электронного документа;

14.1.3. при прекращении деятельности Удостоверяющего центра без передачи его функций другим лицам;

14.1.4. в случаях, установленных ст. 14 Закона об электронной подписи, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или Регламентом УЦ.

14.2. Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи если:

14.2.1. не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;

14.2.2. установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном Удостоверяющим центром сертификате;

14.2.3. вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

14.3. Приём заявлений на прекращение действия сертификата осуществляется в течение рабочего дня Удостоверяющего центра.

14.4. Заявление на прекращение действия сертификата (форма – в приложениях №№ 3 и 4) должно содержать данные об отзываемом сертификате и его владельце, в том числе:

14.4.1. наименование юридического лица (согласно ЕГРЮЛ) или фамилию, имя, отчество индивидуального предпринимателя или физического лица, от которых подаётся заявление;

14.4.2. должность, фамилия, имя и отчество руководителя юридического лица;

14.4.3. на основании какого акта (документа) действует заявитель;

14.4.4. причину отзыва сертификата;

14.4.5. данные сертификата: серийный номер сертификата, ОГРН юридического лица или СНИЛС физического лица, фамилия, имя и отчество пользователя сертификата;

14.4.6. срок прекращения действия (временный или постоянный);

14.4.7. должность, фамилия и инициалы правомочного представителя заявителя и его подпись, печать организации;

14.4.8. дата подачи заявления.

14.5. На заявлении работники Удостоверяющего центра делают отметки об идентификации личности заявителя, подтверждении его полномочий на подачу заявления, проверке указанных в Заявлении сведений, дате и времени приёма заявления и аннулирования сертификата Удостоверяющим центром (внесения в список отозванных сертификатов).

14.6. Рассмотрение, обработка заявлений и официальное опубликование уведомлений об аннулировании сертификата осуществляются не позднее 30 минут после приёма заявления Удостоверяющим центром.

14.7. Лицо, подавшее (подписавшее) заявление на аннулирование сертификата, обязано подтвердить свои правомочия на отзыв сертификата (право действовать от имени юридического лица, индивидуального предпринимателя или физического лица без доверенности, удостоверить свою личность).

14.8. Срок внесения информации о прекращении действия или аннулировании сертификата в Реестр УЦ не должен превышать 12 часов от времени наступления обстоятельств, указанных в п.п. 15.1 и 15.2 настоящего Регламента, или 12 часов от времени, когда Удостоверяющему центру стало известно о наступлении таких обстоятельств.

14.9. Официальным уведомлением об аннулировании сертификата является опубликование списка отозванных сертификатов, содержащего сведения об аннулированном сертификате. Время аннулирования сертификата считается временем внесения записи об этом в Реестр УЦ.

14.10. Список отозванных сертификатов подписывается электронной подписью Уполномоченного лица Удостоверяющего центра.

14.11. Информация об адресе размещённого в информационно-телекоммуникационной сети «Интернет» СОС заносится в изданные Удостоверяющим центром сертификаты в поле «Точки распространения списков отзыва (CRL)».

14.12. Заявления о прекращении действия сертификата могут направляться в Удостоверяющий центр как на бумажном носителе, так и в форме электронного документа, подписанного квалифицированной электронной подписью.

15. ПОРЯДОК ВЕДЕНИЯ РЕЕСТРА КВАЛИФИЦИРОВАННЫХ СЕРТИФИКАТОВ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

15.1. Формирование и ведение реестра сертификатов осуществляется Удостоверяющим центром в соответствии с Законом об электронной подписи, Порядком формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров (утв. приказом Минкомсвязи России от 22.08.2017 г. № 436), иными принимаемыми в соответствии с Законом об электронной подписи и Федеральным законом «Об информации, информа-

ционных технологиях и о защите информации» нормативными правовыми актами и настоящим Регламентом.

15.2. Формирование реестра сертификатов включает в себя внесение в реестр сертификатов информации о квалифицированных сертификатах, выданных Удостоверяющим центром.

15.3. Ведение реестра сертификатов включает в себя:

15.3.1. внесение корректировок и дополнений в реестр сертификатов в случае изменения содержащихся в нём сведений;

15.3.2. внесение в реестр сертификатов сведений о прекращении действия или об аннулировании квалифицированных сертификатов.

15.4. Хранение информации, содержащейся в реестре сертификатов, осуществляется Удостоверяющим центром в форме, позволяющей проверить её целостность и достоверность.

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

15.6. Формирование и ведение реестра сертификатов осуществляется Удостоверяющим центром с соблюдением требований к мерам и способам защиты информации, обеспечивающих предотвращение несанкционированного доступа к нему.

15.7. В целях обеспечения целостности информации, в том числе предотвращения утраты сведений о квалифицированных сертификатах, содержащихся в реестре сертификатов, Удостоверяющий центр осуществляет резервное копирование баз данных, обрабатываемых с использованием сертифицированных средств УЦ, а также реестра сертификатов.

15.8. Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре сертификатов.

15.9. Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, к реестру сертификатов в любое время в течение срока деятельности УЦ, за исключением периодов технического обслуживания реестра.

15.10. Удостоверяющий центр предоставляет безвозмездно любому лицу по его обращению сведения, содержащиеся в реестре сертификатов, в том числе информацию об аннулировании квалифицированного сертификата. Указанная информация предоставляется в форме выписки из реестра сертификатов и направляется обратившемуся лицу как в форме документа на бумажном носителе с использованием почтового отправления, так и с в форме электронного документа использованием информационно-телекоммуникационных сетей, в том числе с использованием электронной почты (по выбору лица, обратившегося за получением информации из реестра сертификатов).

15.11. Срок предоставления Удостоверяющим центром запрошенной заявителем информации, содержащейся в реестре сертификатов, не превышает 7 дней со дня получения запроса от заявителя, если Удостоверяющий центр направляет запрошенную информацию в форме документа на бумажном носителе с использованием почтового отправления, и 24 часов для направления выписки посредством информационно-телекоммуникационных сетей, в том числе с использованием электронной почты.

15.12. Информация, внесённая в реестр сертификатов, подлежит хранению в течение всего срока деятельности Удостоверяющего центра.

15.13. При принятии решения о прекращении своей деятельности Удостоверяющий центр обязан передать в уполномоченный федеральный орган реестр сертификатов в соответствии с Порядком передачи реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи, в случае прекращения деятельности аккредитованного удостоверяющего центра (утв.

приказом Минкомсвязи России от 14.08.2017 г. № 416).

15.14. Реестр сертификатов УЦ включает реестр сертификатов юридических лиц и реестр сертификатов физических лиц.

15.15. Реестр сертификатов юридических лиц состоит из следующих разделов:

15.15.1. квалифицированные сертификаты, выданные юридическим лицам;

15.15.2. квалифицированные сертификаты, выданные юридическим лицам, прекратившие свое действие;

15.15.3. аннулированные квалифицированные сертификаты, выданные юридическим лицам.

15.16. Реестр сертификатов физических лиц состоит из следующих разделов:

15.16.1. квалифицированные сертификаты, выданные физическим лицам;

15.16.2. квалифицированные сертификаты, выданные физическим лицам, прекратившие своё действие;

15.16.3. аннулированные квалифицированные сертификаты, выданные физическим лицам.

15.17. Информация о выданных Удостоверяющим центром квалифицированных сертификатах вносится в реестр сертификатов одновременно с их выдачей, но не позднее даты начала действия квалифицированного сертификата, указанной в квалифицированном сертификате.

15.18. Информация о прекращении действия и аннулировании квалифицированного сертификата вносится Удостоверяющим центром в реестр сертификатов УЦ в течение 12 часов с момента наступления обстоятельств, указанных в настоящем Регламенте, или в течение 12 часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

15.19. Информация об аннулировании квалифицированного сертификата вносится Удостоверяющим центром в реестр сертификатов не позднее 1 рабочего дня со дня вступления в законную силу решения суда, явившегося основанием для аннулирования, а также при аннулировании Удостоверяющим центром квалифицированных сертификатов по основаниям, указанным в п.п. 1 и 2 ч. 6.1 ст. 14 Закона об электронной подписи:

15.19.1. не подтверждено, что владелец сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком квалифицированном сертификате;

15.19.2. установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате.

15.20. При аннулировании (в соответствии с п.п. 16.25, 16.25.1, 16.25.2 настоящего Регламента) выданного Удостоверяющим центром квалифицированного сертификата не позднее, чем за 1 рабочий день до внесения в реестр сертификатов УЦ информации об аннулировании квалифицированного сертификата Удостоверяющий центр уведомляет об этом владельца сертификата путём направления документа на бумажном носителе или электронного документа.

16. ПОРЯДОК ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ РЕЕСТРА КВАЛИФИЦИРОВАННЫХ СЕРТИФИКАТОВ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

16.1. Плановые работы по техническому обслуживанию реестра сертификатов, а также процедуры его резервного копирования, проводятся Удостоверяющим центром в выходные дни либо в ночное время с целью минимизации и по возможности исключения перерывов в функционировании реестра.

16.2. Плановое техническое обслуживание реестра сертификатов осуществляется не более 8 часов от начала работ.

16.3. Внеплановые работы по техническому обслуживанию реестра сертификатов проводятся только при авариях и неполадках в его работе за минимально возможное время.

16.4. Время проведения планового технического обслуживания может быть увеличено при наличии объективных оснований и причин, но не более чем на 5 дней со дня их начала, если такие работы могут повлиять на возможность создания или проверки электронной подписи участниками электронного взаимодействия.

16.5. Перед проведением работ по техническому обслуживанию реестра сертификатов, если такие работы могут повлиять на возможность создания или проверки электронной подписи участниками электронного взаимодействия, Удостоверяющий центр оповещает о проведении вышеуказанных работ посредством публикации соответствующей информации на сайте Удостоверяющего центра и (или) направлением уведомления в электронной форме с использованием информационно-телекоммуникационных сетей, в том числе электронной почты.

17. ПОДТВЕРЖДЕНИЕ ДЕЙСТВИТЕЛЬНОСТИ ЭЛЕКТРОННОЙ ПОДПИСИ, ИСПОЛЬЗОВАННОЙ ДЛЯ ПОДПИСАНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

17.1. При необходимости для стороны, присоединившейся к Регламенту УЦ, Удостоверяющий центр осуществляет проверку подлинности электронной подписи уполномоченного лица УЦ в изданных сертификатах или подлинности ЭП владельца сертификата в электронном документе.

17.2. Для подтверждения подлинности ЭП уполномоченного лица УЦ в сертификате владелец сертификата подаёт в Удостоверяющий центр заявление (по форме в приложениях №№ 5 и 6), которое должно содержать:

17.2.1. идентификационные данные владельца сертификата, в сертификате которого необходимо подтвердить подлинность ЭП уполномоченного лица Удостоверяющего центра;

17.2.2. серийный номер сертификата, в котором необходимо подтвердить подлинность ЭП уполномоченного лица Удостоверяющего центра;

17.2.3. дату и время, на которые требуется установить статус сертификата.

17.3. К заявлению обязательно должен быть приложен носитель информации (желательно компакт-диск одноразовой записи) с файлом сертификата, подвергающегося проверке, в формате PKCS#7 и DER-кодировке X.509 или кодировке Base64 (*.cer).

17.4. Для подтверждения подлинности ЭП в электронном документе владелец сертификата подаёт в Удостоверяющий центр заявление (по форме в приложениях №№ 7 и 8), которое должно содержать:

17.4.1. идентификационные данные владельца сертификата, подлинность ЭП которого в электронном документе необходимо подтвердить;

17.4.2. серийный номер сертификата, применённого для подписания электронного документа;

17.4.3. имя, дату и время создания, объём файла электронного документа, подпись в котором необходимо подтвердить;

17.4.4. дату и время, на которые требуется установить статус электронной подписи.

17.5. К заявлению обязательно должен быть приложен носитель информации (желательно компакт-диск одноразовой записи) с файлом электронного документа, подлинность ЭП в котором необходимо подтвердить, файл электронной подписи (если она отделена от файла электронного документа), файл сертификата ключа проверки электронной подписи (если электронную подпись создавал заявитель).

17.6. Удостоверяющий центр определяет состав комиссии, набор исходных данных для проведения проверки, перечень и содержание отчётных документов, сроки проведения необходимых работ для составления заключений Удостоверяющего центра по результатам проведённых проверок.

17.7. Проверка действительности всех сертификатов, включённых в цепочку доверия для данного сертификата (включительно до сертификата Удостоверяющего центра, выданного ему Головным удостоверяющим центром) производится с применением средств УЦ, в том числе автоматизированного рабочего места разбора конфликтных ситуаций.

17.8. Результатом работ по подтверждению подлинности ЭП являются заключение Удостоверяющего центра, которое должно содержать:

17.8.1. дату и место проведения проверки;

17.8.2. состав комиссии, осуществлявшей проверку;

17.8.3. основание для проведения проверки;

17.8.4. данные, представленные для проведения проверки;

17.8.5. применённые методы и содержание проверки;

17.8.6. результат проверки ЭП уполномоченного лица Удостоверяющего центра в проверяемом сертификате или ЭП в электронном документе (верна/неверна);

17.8.7. был ли действителен сертификат на дату и время, указанные в заявлении;

17.8.8. обоснование результатов проверки;

17.8.9. подписи членов комиссии и лица, утвердившего заключение;

17.8.10. печать Удостоверяющего центра.

17.9. Заключения Удостоверяющего центра по выполненным проверкам составляются в письменной форме на бумажном носителе в двух экземплярах, один из которых выдаётся (высылается) заявителю.

17.10. Срок проверки подлинности ЭП и предоставления заявителям заключений по проверке не должен превышать 3 рабочих дней от оплаты данной услуги при условии поступления соответствующего заявления в Удостоверяющий центр.

18. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

18.1. Удостоверяющий центр осуществляет информирование заявителя об условиях и порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и мерах, необходимых для обеспечения безопасности электронных подписей и их проверки:

18.1.1. выдачей пользователям под роспись на бумажном носителе или в виде текстового файла Руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи;

18.1.2. ознакомлением пользователей с Памяткой Удостоверяющего центра о порядке использования электронной подписи и средств электронной подписи (приложение № 10 к Регламенту УЦ).

18.2. Средства электронной подписи выдаются заявителям (владельцам сертификата) за плату, если иное не предусмотрено действующим законодательством.

18.3. Средства криптографической защиты информации выдаются с соблюдением процедур, предусмотренных руководящими документами ФСБ России, под роспись в Журнале поэкземплярного учёта СКЗИ, эксплуатационной и технической документации к ним, ключевых документов органа криптографической защиты информации.

18.4. Средства электронной подписи должны обеспечивать возможность проверки всех квалифицированных электронных подписей, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные квалифицированной электронной подписью, или электронный документ подписан несколькими квалифицированными электронными подписями.

18.5. Актуальность информации, содержащейся в Реестре сертификатов, обеспечивается постоянным его обновлением или дополнением, производимыми незамедлительно после получения информации о выпуске или отзыве (аннулировании) квалифицированных сертификатов.

18.6. Защита информации, содержащейся в Реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий обеспечивается ме-

рами Удостоверяющего центра по информационной безопасности, состав и содержание которых определяются организационно-распорядительными документами государственных органов регулирования, технической документацией и внутренними организационно-распорядительными документами Удостоверяющего центра.

18.7. Постоянная доступность информации из Реестра сертификатов об изданных и отозванных (аннулированных) квалифицированных сертификатах обеспечивается круглосуточным приёмом запросов на её получение на Информационном ресурсе УЦ. Во время планового или внепланового технического обслуживания Реестра информация из него может быть временно недоступной.

18.8. В соответствии с ч. 5 ст. 18 Закона об электронной подписи сведения в объёме, необходимом для регистрации в ЕСИА, о лицах, получивших квалифицированный сертификат, и о полученных ими сертификатах Удостоверяющий центр направляет в ЕСИА.

18.9. При выдаче квалифицированного сертификата Удостоверяющий центр по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществляет регистрацию указанного лица в ЕСИА.

18.10. Удостоверяющий центр безвозмездно предоставляет обратившимся к нему лицам (в том числе не являющимся владельцами выданных Удостоверяющим центром сертификатов) информацию, содержащуюся в Реестре сертификатов, в том числе о прекращении действия или аннулировании сертификатов, с использованием любых доступных средств связи. Срок отправки указанной информации не должен превышать 3 рабочих дней от даты приёма обращения.

18.11. Удостоверяющий центр публикует списки отозванных сертификатов на своих общедоступных информационных ресурсах в глобальной сети Интернет.

19. СТРУКТУРА И ПОРЯДОК ИСПОЛЬЗОВАНИЯ СЕРТИФИКАТОВ И СПИСКОВ ОТОЗВАННЫХ СЕРТИФИКАТОВ

19.1. Используемые УЦ сертификаты соответствуют стандарту X.509 версии 3.

19.2. Структура квалифицированных сертификатов владельцев сертификатов.

Наименование полей	Структура и значение полей
Раздел (вкладка) «Общие (Сведения о сертификате)»	
Этот сертификат предназначается для:	• <Класс средства ЭП (буквенно-цифровое значение)> • Политики применения <выраженные словесно или объектными идентификаторами [OID]> • Области применения <выраженные словесно или объектными идентификаторами [OID]>
Кому выдан:	<Значение атрибута CN из поля «Субъект» в разделе «Состав»>
Кем выдан:	<Значение атрибута CN из поля «Издатель» в разделе «Состав»>
Действителен с	<выраженные цифрами день.месяц.год>
по	<выраженные цифрами день.месяц.год>
Раздел (вкладка) «Состав»	
Версия	V3
Серийный номер	<уникальный номер из 32 символов в шестнадцатеричном исчислении>
Алгоритм подписи	<алгоритм (номер и год принятия ГОСТ)>
Алгоритм хеширования подписи	<алгоритм (номер и год принятия ГОСТ)>
Издатель	CN = <наименование организации> OU = <наименование подразделения> O = <наименование организации> E = <адрес ящика электронной почты> S = <код и название региона Российской Федерации> L = <название населённого пункта> C = RU ИНН = <12 цифр> ОГРН = <13 цифр> STREET = <улица, корпус, строение, дом и другие элементы топонимики>
Действителен с	<выраженные цифрами день, словом месяц, цифрами год, цифрами час:минута:секунда>
Действителен по	<выраженные цифрами день, словом месяц, цифрами год, цифрами час:минута:секунда>

Наименование полей	Структура и значение полей
Субъект	CN = <наименование организации (юридического лица) или фамилия, имя, отчество физического лица> OU = <наименование подразделения организации (если есть)> O = <наименование организации (юридического лица)> E = <адрес ящика электронной почты> S = <код и название региона Российской Федерации> L = <название населённого пункта (муниципального образования)> C = RU ИНН = <12 цифр> ОГРН = <13 цифр> STREET = <улица, корпус, строение, дом и другие элементы топонимики> Неструктурированное имя = <добавляется при наличии>
Открытый ключ	<алгоритм (номер и год принятия ГОСТ)> <уникальное значение из 132 символов в шестнадцатеричном исчислении>
Возможности SMIME	[1]Возможности SMIME Идентификатор объекта=1.2.643.2.2.21
Улучшенный ключ	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищённая электронная почта (1.3.6.1.5.5.7.3.4) Установка отметки времени (1.3.6.1.5.5.7.3.8) <Дополнительные расширения (OID)>
Политики сертификата	[1]Политика сертификата: Идентификатор политики=<буквенно-цифровое обозначение из 3 символов> [2]Политика сертификата: Идентификатор политики=<буквенно-цифровое обозначение из 3 символов>
Дополнительное имя субъекта	Адрес каталога: <добавляется при наличии>
Средство электронной подписи владельца (Subject Sign Tool)	Средство электронной подписи: СКЗИ <наименование программы-криптопровайдера>
Идентификатор ключа субъекта	<уникальное значение из 40 символов в шестнадцатеричном исчислении>
Средство электронной подписи и УЦ издателя (Issuer Sign Tool)	Средство электронной подписи: СКЗИ <наименование от производителя> Заключение на средство ЭП: <номер и дата заключения ФСБ России> Средство УЦ: <наименование от производителя> Заключение на средство УЦ: <номер и дата заключения ФСБ России >
Доступ к информации о центрах сертификации	[1]Доступ к сведениям центра сертификации Метод доступа=Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://212.3.135.212:8777/ocsp [2]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://*.cer
Точки распространения списков отзыва (CRL)	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://*.crl [2]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=ftp://*.crl

Наименование полей	Структура и значение полей
Идентификатор ключа центра сертификатов	Идентификатор ключа= уникальное значение из 40 символов в шестнадцатеричном исчислении Поставщик сертификата: Адрес каталога: CN = <наименование организации (юридического лица)> OU = <наименование подразделения> O = <наименование организации (юридического лица)> E = <адрес ящика электронной почты> S = <код и название региона Российской Федерации> L = <название населённого пункта (муниципального образования)> C = RU ИНН = <12 цифр> ОГРН = <13 цифр> STREET = <улица, корпус, строение, дом и другие элементы топонимики> Серийный номер сертификата = <уникальное значение из 32 символов в шестнадцатеричном исчислении>
Использование ключа	Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
Основные ограничения	Тип субъекта=Конечный субъект Ограничение на длину пути=Отсутствует
Алгоритм отпечатка	sha1
Отпечаток	<уникальное значение из 40 символов в шестнадцатеричном исчислении>
Раздел (вкладка) «Путь сертификации»	
Путь сертификации	<текстово-графическое отображение цепочки доверия к сертификату>
Состояние сертификата	<текстовое заключение о статусе сертификата>

19.3. Структура списка отозванных сертификатов Удостоверяющего центра.

Наименование полей	Структура и значение полей
Раздел (вкладка) «Общие»	
Версия	V2
Издатель	CN = <наименование организации (юридического лица)> OU = <наименование подразделения> O = <наименование организации (юридического лица)> E = <адрес ящика электронной почты> S = <код и название региона Российской Федерации> L = <название населённого пункта> C = RU ИНН = <12 цифр> ОГРН = <13 цифр> STREET = <улица, корпус, строение, дом и другие элементы топонимики>
Действителен с	<выраженные цифрами день, словом месяц, цифрами год, цифрами час:минута:секунда>
Следующее обновление	<выраженные цифрами день, словом месяц, цифрами год, цифрами час:минута:секунда>
Алгоритм подписи	<алгоритм (номер и год принятия ГОСТ)>
Алгоритм хеширования подписи	<алгоритм (номер и год принятия ГОСТ)>
Номер CRL	<Номер CRL=уникальный номер в шестнадцатеричном исчислении>
Идентификатор ключа центра сертификатов	<Идентификатор ключа=уникальный идентификатор в шестнадцатеричном исчислении>
Раздел (вкладка) «Список отзыва»	
Серийный номер	<уникальный номер аннулированного сертификата в шестнадцатеричном исчислении>
Дата отзыва	<выраженные цифрами день, словом месяц, цифрами год, цифрами час:минута:секунда>
Код причины списка отзыва (CRL)	<причина текстом и её цифровой код>

19.4. Ключ электронной подписи действует на определённый момент времени (действующий ключ электронной подписи), если:

19.4.1. наступило поясное время начала его действия;

19.4.2. не наступило поясное время окончания его действия;

19.4.3. сертификат, соответствующий данному ключу электронной подписи, не аннулирован.

19.5. Сертификат ключа проверки электронной подписи действует на определённый момент времени (действующий сертификат), если:

19.5.1. наступило поясное время начала его действия;

19.5.2. не наступило поясное время окончания его действия;

19.5.3. данный сертификат не аннулирован.

19.6. Срок действия ключа электронной подписи уполномоченного лица Удостоверяющего центра не превышает 15 месяцев и начинается от даты и времени начала действия сертификата, соответствующего этому ключу и выданного ГУЦ УФО.

19.7. Срок действия сертификата уполномоченного лица Удостоверяющего центра устанавливается ГУЦ УФО при выдаче сертификата.

19.8. Срок действия ключей электронной подписи владельцев сертификатов-клиентов УЦ не превышает 15 месяцев и начинается от даты и времени начала действия соответствующего им сертификата.

19.9. Срок действия (использования для создания электронной подписи) сертификатов ключа проверки электронной подписи владельцев сертификатов-клиентов УЦ не превышает 15 месяцев. Возможность использования сертификатов ключа проверки электронной подписи для проверки действительности электронной подписи, созданной с их использованием, по сроку не ограничена.

20. БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

20.1. Информация, обрабатываемая Удостоверяющим центром и согласно законодательству Российской Федерации не относящаяся к информации ограниченного доступа, считается общедоступной.

20.2. Общедоступная информация может публиковаться по решению Удостоверяющего центра. Место, способ и время публикации общедоступной информации определяется Удостоверяющим центром.

20.3. Информация, вносимая в сертификаты, издаваемые Удостоверяющим центром, в том числе фамилия, имя, отчество, сведения о месте работы и занимаемой должности, ИНН, СНИЛС, адрес электронной почты, с письменного согласия владельцев сертификатов включается в источники общедоступных персональных данных, которыми являются квалифицированный сертификат ключа проверки электронной подписи и реестр сертификатов УЦ.

20.4. Ключ электронной подписи, соответствующий выданному Удостоверяющим центром сертификату, является информацией ограниченного доступа, принадлежащей владельцу сертификата.

20.5. Если в Удостоверяющем центре имеется персональная и (или) корпоративная информация о владельцах сертификата, содержащаяся в Реестре сертификатов и не подлежащая опубликованию в составе сертификата, то такая информация относится к информации ограниченного доступа.

20.6. Удостоверяющий центр имеет право раскрывать информацию ограниченного доступа третьим лицам только в случаях, установленных законодательством Российской Федерации.

20.7. Хранение сертификата в Удостоверяющем центре осуществляется в течение всего периода его действия и пяти лет после окончания срока (прекращения) его действия. По истечении указанного срока хранения сертификаты переводятся в режим архивного хранения.

20.8. Созданные Удостоверяющим центром ключи электронной подписи заявителей записываются на отчуждаемые ключевые носители, которые до их вручения заявителям хранятся в специальном хранилище (сейфе) и вручаются только заявителям или их полномочным представителям.

20.9. Создание не оговоренных заявителями копий и постоянное хранение созданных для них Удостоверяющим центром ключей не допускается. Технологические копии созданных Удосто-

веряющим центром ключей уничтожаются незамедлительно (не позднее конца текущего рабочего дня Удостоверяющего центра).

20.10. Удостоверяющий центр не осуществляет хранение ключевой информации ограниченного доступа после выдачи соответствующих ключей электронной подписи заявителям.

20.11. Невостребованные ключи электронной подписи уничтожаются назначенными и подготовленными работниками Удостоверяющего центра после принятия решения о выводе таких ключей из обращения. Соответствующие таким ключам электронной подписи сертификаты решением Удостоверяющего центра аннулируются.

21. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ (ФОРС-МАЖОР)

21.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по Регламенту УЦ, если это неисполнение явилось следствием обстоятельств непреодолимой силы (форс-мажорных), возникших после присоединения к Регламенту УЦ.

21.2. Обстоятельствами непреодолимой силы признаются чрезвычайные (т.е. находящиеся вне разумного контроля сторон) и неотвратимые при данных условиях обстоятельства, включая военные действия, массовые беспорядки, террористические акты, стихийные бедствия, забастовки, техногенные катастрофы, технические сбои в функционировании аппаратных и программных средств (систем), пожары, взрывы, действия (бездействие) государственных и муниципальных органов, повлёкшие невозможность исполнения одной или обеими сторонами своих обязательств по Регламенту УЦ.

21.3. При возникновении обстоятельств непреодолимой силы срок исполнения сторонами своих обязательств по Регламенту УЦ сдвигается соразмерно времени, в течение которого действовали такие обстоятельства.

21.4. Сторона, потерявшая возможность исполнения своих обязательств по Регламенту УЦ, обязана незамедлительно извещать в письменной форме другую сторону о наступлении, предполагаемом сроке действия и прекращении обстоятельств непреодолимой силы, а также представлять доказательства возникновения таких обстоятельств.

21.5. Отсутствие извещения или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечёт за собой утрату права ссылаться на такие обстоятельства.

21.6. Если невозможность полного или частичного исполнения сторонами какого-либо обязательства по настоящему Регламенту УЦ обусловлена действием обстоятельств непреодолимой силы и длится свыше одного месяца, то каждая из сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства. В этом случае ни одна из сторон не вправе требовать от другой стороны возмещения возникших у неё убытков.

ПРИЛОЖЕНИЯ

1. Заявление на выдачу сертификата ключа проверки электронной подписи (примерная форма; для юридических лиц, индивидуальных предпринимателей, физических лиц).
2. Доверенность (на осуществление действий в рамках Регламента УЦ; примерная форма).
3. Заявление на прекращение действия сертификата ключа проверки электронной подписи (форма; для юридических лиц).
4. Заявление на прекращение действия сертификата ключа проверки электронной подписи (форма; для индивидуальных предпринимателей, физических лиц).
5. Заявление на подтверждение подлинности электронной подписи Уполномоченного лица УЦ ООО ИЦ «Выбор» в сертификате ключа проверки электронной подписи (форма; для юридических лиц).
6. Заявление на подтверждение подлинности электронной подписи Уполномоченного лица УЦ ООО ИЦ «Выбор» в сертификате ключа проверки электронной подписи (форма; для индивидуальных предпринимателей, физических лиц).
7. Заявление на подтверждение подлинности электронной подписи в электронном документе (форма; для юридических лиц).
8. Заявление на подтверждение подлинности электронной подписи в электронном документе (форма; для индивидуальных предпринимателей, физических лиц).
9. Сертификат ключа проверки электронной подписи Пользователя УЦ (форма для распечатки на бумажном носителе).
10. Памятка Пользователю УЦ о порядке использования электронной подписи и средств электронной подписи.

Приложение № 1
к Регламенту Удостоверяющего центра ООО ИЦ «ВЫБОР»
(*примерная форма*)

В Удостоверяющий центр ООО ИЦ «Выбор»

ЗАЯВЛЕНИЕ

_____
полное наименование лица

в лице _____

действующего на основании _____

просит создать и выдать квалифицированный сертификат ключа проверки электронной подписи своему уполномоченному представителю (далее – пользователю) согласно нижеуказанным данным.

1. Фамилия, имя, отчество: _____
2. Подразделение: _____
3. Должность: _____
4. Электронная почта (e-mail): _____
5. Сокращённое наименование организации: _____
6. Юридический адрес: _____
7. Код и наименование субъекта РФ: | | |
8. ИНН: | | 9. КПП: | | 10. ОГРН: | |

Сведения для регистрации сертификата в ЕСИА:

11. СНИЛС: | | 12. Документ, удост. личн. | | 13. Гражданство | |
14. Серия | | 15. Номер | | 16. Код подразделения | | 17. Дата выдачи | | 18. Пол | |
19. Дата рождения | | 20. Место рождения | |

21. Назначения (области использования) сертификата:

☐

22. Дополнительные условия:

Ключ электронной подписи создать с использованием криптопровайдера (СКЗИ)
☐ КриптоПро CSP ☐ ViPNet CSP
☐ Криптотокен (JaCarta-2) ☐ Рутокен ЭЦП 2.0 (Rutoken ECP 2.0)

☐ Ключ электронной подписи создать в Удостоверяющем центре ООО ИЦ «Выбор»
☐ Идентификацию пользователя провести с использованием квалифицированной электронной подписи заявителя
☐ Ключ электронной подписи создать с возможностью его копирования на другой носитель
☐ Ключ электронной подписи записать на съёмный ключевой носитель, приобретённый заявителем в УЦ
☐ Ключ электронной подписи записать на предоставленный заявителем в УЦ съёмный ключевой носитель
☐ Создать на разных носителях ☐ разных ключей электронной подписи и сертификатов к ним для указанного пользователя

23. Кодовая фраза: | |

Заявитель подтверждает, что указанная кодовая фраза является паролем для начала действий, предусмотренных регламентом Удостоверяющего центра ООО ИЦ «Выбор» при компрометации ключа электронной подписи, и обязуется:
- обеспечить конфиденциальность ключа электронной подписи и неразглашение кодовой фразы (пароля);
- при компрометации ключа электронной подписи без промедления проинформировать об этом УЦ.

24. Подписав настоящее заявление, заявитель подтверждает, что он и пользователь ознакомлены с Регламентом УЦ ООО ИЦ «Выбор», размещённом на сайте http://icvibor.ru/, и безусловно присоединились к этому Регламенту. Заявитель и пользователь обязуются самостоятельно и своевременно контролировать изменения в Регламенте и руководствоваться его редакцией, актуальной на момент приобретения услуг удостоверяющего центра.

25. Пользователь согласен на обработку (включая сбор, запись, систематизацию, накопление, хранение, обновление, изменение, использование, распространение, предоставление, блокирование и уничтожение) его персональных данных, указанных в настоящем заявлении, в течение всего срока деятельности УЦ, в т.ч. с использованием программно-аппаратных средств УЦ ООО ИЦ «Выбор», и признаёт отнесение к общедоступным его персональных данных, включённых в выданный ему квалифицированный сертификат.

26. Заявитель и пользователь осведомлены, что для создания квалифицированной электронной подписи с помощью выданного ключа проверки электронной подписи они обязаны использовать средства электронной подписи, получившие подтверждение соответствия требованиям Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

27. Заявитель согласен для получения услуг удостоверяющего центра осуществлять с Удостоверяющим центром ООО ИЦ «Выбор» юридически значимый документооборот по электронной почте, для которого заявитель использует адрес электронной почты, указанный в п. 4 настоящего заявления, а Удостоверяющий центр ООО ИЦ «Выбор» – любой адрес, расположенный в домене @icvibor.ru (ст. 165.1 ГК РФ).

Пользователь сертификата _____ _____ _____
подпись фамилия и инициалы

_____ _____ _____
должность руководителя заявителя подпись фамилия и инициалы

_____ 20 _____ г.

м.п.

Приложение № 2
к Регламенту Удостоверяющего центра
ООО ИЦ «ВЫБОР»
(примерная форма,
только для юридических лиц)

ДОВЕРЕННОСТЬ

г. Смоленск Дата выдачи доверенности: _____ _____ 20 ____ г.

Действительна до: _____ _____ 20 ____ г.

_____
полное наименование лица

ОГРН [ ] ИНН [ ] КПП [ ]

в лице _____
должность, фамилия, имя и отчество руководителя

действующего на основании _____

уполномочивает _____
фамилия, имя и отчество представителя

_____ _____
дата рождения место рождения

_____ _____ _____ _____
(наименование документа, удостоверяющего личность) серия номер дата выдачи

_____
кем выдан

быть представителем в Удостоверяющем центре Общество с ограниченной ответственностью Информационный центр «Выбор» (ОГРН 1026701454064, ИНН 6730025009) и совершать нижеуказанные действия.

1. Подписать договор (контракт) на приобретение прав использования программ для ЭВМ, ключа электронной подписи, сертификата ключа проверки электронной подписи и иных средств электронной подписи, а также сопутствующих товаров, работ и услуг.

2. Получить ключ электронной подписи и иные средства электронной подписи, а также право использования программ для ЭВМ и сопутствующие товары, работы и услуги.

3. Подписать и получить сертификат ключа проверки электронной подписи, первичные учётные и иные документы, определённые Регламентом Удостоверяющего центра ООО ИЦ «Выбор», а также необходимые для исполнения договора (контракта).

_____ _____ _____
должность руководителя заявителя подпись фамилия и инициалы

м.п.

Приложение № 3
к Регламенту Удостоверяющего центра
ООО ИЦ «ВЫБОР»
(форма для юридических лиц)

В Удостоверяющий центр
ООО ИЦ «Выбор»

ЗАЯВЛЕНИЕ
на прекращение действия сертификата ключа проверки электронной подписи

_____
полное наименование юридического лица согласно ЕГРЮЛ

в лице _____
должность, фамилия, имя и отчество руководителя

действующего на основании _____
устава, положения, приказа и т.п.

в связи с _____
причина отзыва сертификата

просит аннулировать сертификат ключа проверки электронной подписи со следующими данными:

Серийный номер сертификата	
ОГРН организации	
Фамилия, имя, отчество Пользователя сертификата	

Срок прекращения действия (выбрать):

☐ постоянный

☐ до ☐ . ☐ . ☐ г. включительно.
дата цифрами: день месяц год

_____ _____ _____
должность руководителя Заявителя подпись фамилия и инициалы

м.п.

_____ _____ 20____г.

Служебные отметки (заполняется работниками Удостоверяющего центра)

Заявление на прекращение действия сертификата ключа проверки электронной подписи принято «_____» _____ 20___ г. в _____ час _____ мин (мск).
Личность заявителя идентифицирована, полномочия на подачу заявления подтверждены, указанные в Заявлении сведения сверены.

Работник Удостоверяющего центра _____ _____
подпись инициалы, фамилия

Сертификат аннулирован «_____» _____ 20__ г. в _____ час _____ мин (мск).

Работник Удостоверяющего центра _____ _____
подпись инициалы, фамилия

Приложение № 4
к Регламенту Удостоверяющего центра
ООО ИЦ «ВЫБОР»
(форма для индивидуальных предпринимателей,
физических лиц)

В Удостоверяющий центр
ООО ИЦ «Выбор»

ЗАЯВЛЕНИЕ
на прекращение действия сертификата ключа проверки электронной подписи

Я _____
фамилия, имя и отчество индивидуального предпринимателя или физического лица

в связи с _____
причина отзыва сертификата

прошу аннулировать сертификат ключа проверки электронной подписи со следующими данными:

Серийный номер сертификата	
СНИЛС пользователя сертификата	
ОГРН индивидуального предпринимателя[1]	
Фамилия, имя, отчество пользователя сертификата	

Срок прекращения действия (выбрать):

☐ постоянный

☐ до ☐ . ☐ . ☐ г. включительно.
дата цифрами: день месяц год

Владелец сертификата _____
подпись инициалы, фамилия

«____» _____ 20__ г.

М.П.

Служебные отметки (заполняется работниками Удостоверяющего центра)

Заявление на прекращение действия сертификата ключа проверки электронной подписи принято «_____» _____ 20___ г. в _____ час _____ мин (мск).
Личность заявителя идентифицирована, полномочия на подачу заявления подтверждены, указанные в Заявлении сведения сверены.

Работник Удостоверяющего центра _____ _____
подпись инициалы, фамилия

Сертификат аннулирован «_____» _____ 20__ г. в _____ час _____ мин (мск).

Работник Удостоверяющего центра _____ _____
подпись инициалы, фамилия

[1] заполняют только индивидуальные предприниматели

Приложение № 5
к Регламенту Удостоверяющего центра
ООО ИЦ «ВЫБОР»
(форма для юридических лиц)

В Удостоверяющий центр
ООО ИЦ «Выбор»

ЗАЯВЛЕНИЕ
на подтверждение подлинности электронной подписи уполномоченного лица
Удостоверяющего центра ООО ИЦ «ВЫБОР»
в сертификате ключа проверки электронной подписи

_____
полное наименование организации, включая организационно-правовую форму

в лице _____
должность

_____
фамилия, имя, отчество

действующего на основании _____

просит подтвердить подлинность электронной подписи Уполномоченного лица УЦ в изданном Удостоверяющим центром сертификате ключа проверки электронной подписи и установить его статус (действует/не действует) на основании предоставленных исходных данных:

1. Файл сертификата ключа проверки электронной подписи на прилагаемом к заявлению носителе.
2. Время и дата[1], на которые требуется установить статус сертификата:

_____:_____ (мск) _____
часов минут день месяц год

должность руководителя Заявителя _____ подпись _____ инициалы, фамилия

«____» _____ 20___ г.

м.п.

Служебные отметки (заполняется работниками Удостоверяющего центра)

Заявление и дополнительные материалы к нему приняты
«_____» _____ 20___ г. в _____ час _____ мин (мск).

Личность Заявителя идентифицирована, полномочия на подачу заявления подтверждены.

Работник Удостоверяющего центра _____ подпись _____ инициалы, фамилия

[1] время и дата должны быть указаны по Московскому времени; если время и дата не были указаны, то статус сертификата устанавливается на время подачи заявления в Удостоверяющий центр

Приложение № 6
к Регламенту Удостоверяющего центра
ООО ИЦ «ВЫБОР»
(форма для индивидуальных предпринимателей,
физических лиц)

В Удостоверяющий центр
ООО ИЦ «Выбор»

ЗАЯВЛЕНИЕ
на подтверждение подлинности электронной подписи уполномоченного лица
Удостоверяющего центра ООО ИЦ «ВЫБОР»
в сертификате ключа проверки электронной подписи

Я, _____
фамилия, имя, отчество

прошу подтвердить подлинность электронной подписи Уполномоченного лица УЦ в изданном Удостоверяющим центром сертификате ключа проверки электронной подписи и установить его статус (действует или не действует) на основании предоставленных исходных данных:

1. Файл сертификата ключа проверки электронной подписи на прилагаемом к заявлению носителе.
2. Время и дата[1], на которые требуется установить статус сертификата:
   : (мск)
   часов минут день месяц год

_____
подпись инициалы, фамилия

«____» _____ 20__ г.

м.п.

Служебные отметки (заполняется работниками Удостоверяющего центра)

Заявление и дополнительные материалы к нему приняты
«_____» _____ 20___ г. в _____ час _____ мин (мск).

Личность Заявителя идентифицирована, полномочия на подачу заявления подтверждены.

Работник Удостоверяющего центра _____ _____
подпись инициалы, фамилия

[1] время и дата должны быть указаны по Московскому времени; если время и дата не были указаны, то статус сертификата устанавливается на время подачи заявления в Удостоверяющий центр

Приложение № 7
к Регламенту Удостоверяющего центра
ООО ИЦ «ВЫБОР»
(форма для юридических лиц)

В Удостоверяющий центр
ООО ИЦ «Выбор»

ЗАЯВЛЕНИЕ
на подтверждение подлинности электронной подписи в электронном документе

_____
полное наименование организации, включая организационно-правовую форму

в лице _____
должность

_____
фамилия, имя, отчество

действующего на основании _____

просит подтвердить подлинность электронной подписи в электронном документе (верна/не верна) на основании предоставленных исходных данных:

1. Пользователь, подлинность ЭП которого в электронном документе необходимо подтвердить: _____
общее имя владельца сертификата, подписавшего электронный документ (CN)

2. СКПЭП, применённый для подписания электронного документа: _____
серийный номер сертификата

3. Файл документа, ЭП в котором необходимо подтвердить (на прилагаемом к заявлению носителе): _____
имя файла дата и время создания объём (байт)

4. Время и дата[1], на которые требуется установить статус электронной подписи:
_____ : _____ (мск) _____
часов минут день месяц год

_____ _____
должность руководителя Заявителя подпись инициалы, фамилия

«____» _____ 20___ г.
м.п.

Служебные отметки (заполняется работниками Удостоверяющего центра)

Заявление и дополнительные материалы к нему приняты
«_____» _____ 20___ г. в _____ час _____ мин (мск).

Личность Заявителя идентифицирована, полномочия на подачу заявления подтверждены.

Работник Удостоверяющего центра _____ _____
подпись инициалы, фамилия

[1] время и дата должны быть указаны по Московскому времени; если время и дата не были указаны, то статус сертификата устанавливается на время подачи заявления в Удостоверяющий центр

Приложение № 8
к Регламенту Удостоверяющего центра
ООО ИЦ «ВЫБОР»
(форма для индивидуальных предпринимателей,
физических лиц)

В Удостоверяющий центр
ООО ИЦ «Выбор»

ЗАЯВЛЕНИЕ
на подтверждение подлинности электронной подписи в электронном документе

Я, _____
фамилия, имя, отчество

прошу подтвердить подлинность электронной подписи в электронном документе (верна/не верна) на основании предоставленных исходных данных:

1. Пользователь, подлинность ЭП которого в электронном документе необходимо подтвердить: _____
общее имя владельца сертификата, подписавшего электронный документ (CN)

2. СКПЭП, применённый для подписания электронного документа: _____
серийный номер сертификата

3. Файл документа, ЭП в котором необходимо подтвердить (на прилагаемом к заявлению носителе): _____
имя файла дата и время создания объём (байт)

4. Время и дата[1], на которые требуется установить статус электронной подписи:
_____ : _____ (мск) _____
часов минут день месяц год

_____
подпись инициалы, фамилия

«____» _____ 20__ г.

М.П.

Служебные отметки (заполняется работниками Удостоверяющего центра)

Заявление и дополнительные материалы к нему приняты
«_____» _____ 20___ г. в _____ час _____ мин (мск).

Личность Заявителя идентифицирована, полномочия на подачу заявления подтверждены.

Работник Удостоверяющего центра _____ _____
подпись инициалы, фамилия

[1] время и дата должны быть указаны по Московскому времени; если время и дата не были указаны, то статус сертификата устанавливается на время подачи заявления в Удостоверяющий центр

Приложение № 9
к Регламенту Удостоверяющего центра
ООО ИЦ «ВЫБОР»
(форма)

КВАЛИФИЦИРОВАННЫЙ СЕРТИФИКАТ
КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

Серийный номер: < >
Действие сертификата: с < >
по < >

Издатель: CN=< > OU=< > O=< > E=< > S=< > L=< > C=< > INN=< > OGRN=< > STREET=< >

Владелец: CN=< > SN=< > G=< > C=< > S=< > L=< > STREET=< > O=< > T=< > OGRN=< > SNILS=< > INN=< > E=< >

1.2.643.2.2.19 Алгоритм открытого ключа: < >

Открытый ключ:
< >

2.5.29.15 Использование ключа: <OID>

2.5.29.37 Улучшенный ключ:
<OID>

2.5.29.14 Идентификатор ключа субъекта: < >

1.3.6.1.5.5.7.1.1 Доступ к информации о центрах сертификации:
<URL=>

2.5.29.31 Точки распространения списков отзыва (CRL):
<URL=>

Поставщик сертификата уполномоченного лица Удостоверяющего центра:
CN=< > C=< > S=< > L=< > O=< > STREET=< > E=< > OGRN=< > INN=< > Серийный номер сертификата=< >

1.2.643.2.2.3 Алгоритм подписи: < >
Подпись:
< >

Отпечаток сертификата:
< >

Уполномоченное лицо УЦ _____ <фамилия, имя, отчество>
м.п.

Ключ электронной подписи, сертификат и Руководство по безопасному использованию ЭП получил(-а), с их содержанием ознакомлен(-а).

Владелец сертификата _____ <фамилия, имя, отчество>

Примечание: символами < > обозначены поля, заполняемые переменными данными.

Приложение № 10
к Регламенту Удостоверяющего центра
ООО ИЦ «ВЫБОР»

ПАМЯТКА
пользователю Удостоверяющего центра
о порядке использования электронной подписи и средств электронной подписи

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная памятка содержит положения, предлагаемые Пользователю УЦ в качестве предостережений и рекомендаций, которые следует учитывать при работе со средствами электронной подписи и электронной подписью.

1.2. При наличии требований к порядку использования и проверки электронной подписи, а также к средствам электронной подписи, установленных оператором информационной системы, организующим юридически значимый документооборот, Пользователю УЦ следует руководствоваться требованиями этого оператора.

1.3. Основная часть рекомендаций основана на положениях Федерального закона от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи», нормативных документов государственных органов, в чьей компетенции находятся вопросы информационной безопасности, а также на сформировавшемся в этой сфере отечественном и зарубежном опыте.

2. ПОРЯДОК ИСПОЛЬЗОВАНИЯ СРЕДСТВ ЭЛЕКТРОННОЙ ПОДПИСИ

2.1. При создании электронной подписи для использования в информационной системе общего пользования должны применяться только сертифицированные средства электронной подписи (криптографические и прикладные), на которые у Пользователей УЦ имеются лицензии производителей (правообладателей).

2.2. Средства электронной подписи должны иметь документ, подтверждающий их соответствие требованиям, установленным Федеральной службой безопасности РФ.

2.3. Создание ключей электронной подписи осуществляется для использования в информационной системе общего пользования её участником, по его обращению удостоверяющим центром или в корпоративной информационной системе в порядке, установленном в этой системе.

2.4. Использование криптографических и прикладных средств электронной подписи должно осуществляться в соответствии с руководящей и технической документацией производителей этих средств.

2.5. Внесение Пользователями УЦ (или иными лицами) изменений в конструкцию аппаратных или программные коды программных средств электронной подписи не допускается.

3. ПОРЯДОК ИСПОЛЬЗОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

3.1. Электронная подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

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

3.1.2. подтверждена подлинность электронной подписи в электронном документе;

3.1.3. электронная подпись используется в соответствии со сведениями, указанными в сертификате ключа проверки электронной подписи.

3.2. Сертификат действует с момента его выдачи, если в сертификате не указана иная дата начала его действия, и прекращает своё действие в соответствии с условиями, предусмотренными ч. 6 ст. 14 Закона об электронной подписи.

3.3. Сертификаты для участников электронного взаимодействия создаются с учётом установлен-

ных эксплуатационной документацией на используемое средство электронной подписи сроков действия ключей электронных подписей.

3.4. Участник информационной системы может быть одновременно владельцем любого количества сертификатов ключей проверки электронной подписи. При этом электронный документ с электронной подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате.

3.5. Для юридически значимого электронного документооборота очень важно, чтобы не нарушалась связь между документом и электронной подписью. Для этого получателю должен отправляться «контейнер», содержащий электронный документ и электронную подпись, дающий возможность проверить целостность отправленного электронного документа и идентифицировать лицо, подписавшее электронный документ.

3.6. В информационных системах участников электронного взаимодействия дальнейшей обработке (после проверки) подлежат электронные документы, которые подписаны электронной подписью, признанной действительной.

3.7. Электронная подпись признается действительной при одновременном соблюдении условий, предусмотренных п.п. 1, 3 и 4 ст. 11 Закона об электронной подписи, а также при условии, что сертификат ключа проверки электронной подписи, соответствующий ей, не прекратил своё действие или не был аннулирован на момент подписания электронного документа. Основным средством подтверждения того, что сертификат не был аннулирован, является установка в хранилище (реестр) операционной системы[1] актуального списка отозванных сертификатов, изданного удостоверяющим центром, выпустившим этот сертификат.

3.8. Проверку подписи осуществляют участники электронного взаимодействия с использованием средств электронной подписи или средств Удостоверяющего центра.

3.9. Документ должен иметь метку времени (информацию о моменте подписания), которая присоединена к указанному электронному документу.

3.10. Участнику электронного взаимодействия, направившему электронный документ, который подписан электронной подписью, признанной недействительной, направляется уведомление об отказе в приёме к обработке такого документа. Указанное уведомление подписывается электронной подписью участника электронного взаимодействия, признавшего электронную подпись недействительной.

3.11. Прекращение действия сертификата, выданного участнику электронного взаимодействия на имя его уполномоченного лица, осуществляется в обязательном порядке при смене такого уполномоченного лица, а также в случае нарушения конфиденциальности ключа электронной подписи (компрометации ключа).

3.12. При прекращении полномочий уполномоченного лица участника электронного взаимодействия по подписанию документов в электронной форме участник электронного взаимодействия незамедлительно извещает об этом удостоверяющий центр для прекращения действия сертификата, выданного указанному уполномоченному лицу.

4. РИСКИ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОЙ ПОДПИСИ

4.1. Компрометация ключа электронной подписи[2] и, как следствие: 1) лишение возможности использовать электронную подпись по назначению; 2) возможная ответственность владельца сертификата ключа проверки электронной подписи за содержание электронного документа, электронная подпись которого признана верной, но авторство ему (владельцу) не принадлежит.

4.2. Несанкционированное подписание[3] электронных документов (в том числе и продолжительное по времени) и, как следствие, возможная ответственность владельца сертификата ключа проверки электронной подписи за содержание электронного документа, электронная подпись которого признана верной. Например, вредоносная программа может инициировать подписание документа, сымитировав работу «правильной» программы. Предположение основывается на том,

---

[1] для операционных систем семейства Windows

[2] см. определение термина

[3] подписание документа ключом электронной подписи без ведома его владельца

что средство создания электронной подписи не сможет определить, какой процесс к нему обращается.

4.3. Неисправность носителя ключа электронной подписи, лишение возможности использовать электронную подпись по назначению и получение неблагоприятных последствий (различные виды ответственности[1], упущенная выгода).

4.4. Выдача искажённого электронного документа за подлинный (задуманный автором) путём внесения изменений в файл на этапе подписания. Файл, передаваемый программе, которая используется для подписания документов электронной подписью, перехватывается вредоносной программой, которая на этом этапе может внести в файл изменения или даже подменить его.

4.5. Компрометация (хищение) пин-кода (пароля) носителя, содержащего ключ электронной подписи. Если пин-код вводится с клавиатуры компьютера, то есть теоретическая вероятность его хищения вредоносными программами, отслеживающими нажатия клавиш[2]. В данном случае лучше защищёнными оказываются терминалы, оборудованные специальной клавиатурой для ввода пин-кода, при этом посторонние процессы, запущенные на компьютере, не имеют доступа к пин-коду.

4.6. Фальсификация интерфейса программы. Большинство программ используют стандартные средства ОС Windows для вывода на экран информации о результатах работы и представления подписываемого документа в окне предварительного просмотра. Вредоносное ПО может перехватить этот процесс и отобразить в окне программы ложное изображение подписываемого документа или результатов проверки подписи.

4.7. Для реализации описанных выше угроз не требуется никакого специального оборудования, особых знаний и навыков, они вполне доступны лицам, имеющим заурядный уровень подготовки в области ИТ[3].

5. МЕРЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ПОДПИСИ

5.1. У Пользователя УЦ должна функционировать система комплексной безопасности, обеспечивающая:

5.1.1. безопасность обмена электронными документами;

5.1.2. защиту конфиденциальности и целостности ключей электронной подписи;

5.1.3. чёткое разграничение прав доступа пользователей к информационным ресурсам;

5.1.4. контроль за устанавливаемыми программами;

5.1.5. регулярные проверки на наличие вредоносных программ;

5.1.6. защиту собственных информационных систем[4] от внешних угроз;

5.1.7. анализ появляющихся угроз и разработку мер противодействия им.

5.2. Для подписания документа электронной подписью следует применять надёжные инструменты (криптопровайдеры, системы электронного документооборота, носители для записи ключа электронной подписи). Рекомендуется для этих целей использовать программные и аппаратные средства, прошедшие государственную сертификацию в Российской Федерации.

5.3. Использование несертифицированных средств электронной подписи и созданных ими ключей электронных подписей в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления не допускается.

5.4. Следует использовать для электронного документооборота надёжные, распространённые или взаимно согласованные форматы электронных документов. Прежде чем подписать электронный документ электронной подписью, отправитель должен быть уверен, что формат, в котором документ будет отправлен контрагенту, позволит ему увидеть (воспринимать) документ точно таким, каким видит (воспринимает) его отправитель.

5.5. Перед подписанием электронного документа следует убедиться, что он не содержит потенци-

---

[1] уголовная, материальная, административная

[2] по принятой в ИТ терминологии имеют наименование «сниффер»

[3] «рядовым» хакерам

[4] например, локальной вычислительной сети

ально опасных макросов[1], скрытого текста, элементов оформления, которые могут произвольно искажать смысл документа и (самое важное!) его файл не несёт в себе вредоносных программ. Наиболее подходящим средством противодействия этой угрозе являются специализированные (антивирусные) программы.

5.6. После подписания документа следует проверить, не были ли внесены в документ на этапе подписания какие-либо искажения. Рекомендуется также самим проверить верность электронной подписи перед её отправкой получателю.

5.7. В случае возникновения обстоятельств, не позволяющих Участнику электронного взаимодействия (уполномоченному лицу Участника электронного взаимодействия) правомерно использовать электронную подпись и средства электронной подписи при осуществлении электронного взаимодействия, Участник электронного взаимодействия обязан незамедлительно (не позднее 1 рабочего дня со дня наступления таких обстоятельств) уведомить об этих обстоятельствах удостоверяющий центр, выдавший сертификат, для прекращения действия сертификата.

5.8. По правилам делопроизводства срок хранения документа устанавливается в зависимости от его значимости и информации, которая в нём содержится, и не зависит от вида носителя и наличия электронной подписи. Хранение документов, подписанных электронной подписью, должно быть организовано таким образом, чтобы гарантировать возможность проверки подлинности подписи. Если организация сдаёт какую-либо отчётность в электронном виде, то у неё должен быть определён порядок долговременного хранения файлов электронных документов, обеспечивающий целостность, подлинность и аутентичность электронных документов на протяжении заданных сроков.

---

[1] другое название – макрокоманда; программный объект, который во время вычисления заменяется на новый объект, создаваемый определением макроса на основе его аргументов, затем выражается обычным образом; набор команд, которые можно применить, нажав всего лишь одну клавишу, автоматизировать любое действие, которое выполняется в используемом приложении, и даже выполнять действия, о возможности выполнения которых пользователь не догадывается