Утверждён
приказом ООО ИЦ «Выбор»
от 21.06.2017 г. № 148

РЕГЛАМЕНТ

Удостоверяющего центра ООО ИЦ «Выбор»

1. ТЕРМИНЫ, СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

1.1. *Закон об электронной подписи* – Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

1.2. *Удостоверяющий центр (далее – Удостоверяющий центр, 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.

1.3. *Аннулирование сертификата ключа проверки электронной подписи* – объявление о прекращении действия признанного недействительным сертификата путём включения его серийного номера в актуальный список отозванных сертификатов Удостоверяющего центра и опубликования Удостоверяющим центром этого списка.

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

1.5. *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.

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

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

1.8. *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 Минкомсвязи России в рамках инфраструктуры электронного правительства с целью упорядочить и централизовать процессы регистрации, идентификации, аутентификации и авторизации пользователей.

1.9. *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.

1.10. *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.

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

1.12. *Идентификация пользователя* – предъявление пользователем данных о себе и характеру своей принадлежности к определённым организационным структурам.

1.13. *Квалифицированный сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат, КСКПЭП)* – сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Закон об электронной подписи и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее – уполномоченный федеральный орган).

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

1.15. *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*).

1.16. *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. утрата ключевых носителей, в т.ч. с последующим их обнаружением;

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

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

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

1.18. *Конфиденциальность информации* – обязанность лица, получившего доступ к определённой информации, не передавать такую информацию третьим лицам без согласия её обладателя.

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. *Пользователь сертификата ключа проверки электронной подписи (далее – пользователь сертификата, пользователь СКПЭП)* – физическое лицо, действующее от имени владельца сертификата на основании учредительных документов или доверенности и указываемое в издаваемом сертификате в поле «Субъект» в атрибутах имени SN = (фамилия) и G = (имя, отчество).

1.23. *Рабочий день Удостоверяющего центра* – период времени с 8:30 по 17:30 (мск) каждого дня недели за исключением выходных (суббота и воскресенье) и нерабочих праздничных дней.

1.24. *Реестр Удостоверяющего центра (далее – Реестр УЦ)* – информационный ресурс (база данных) удостоверяющего центра, содержащий разделы:

1.24.1. квалифицированные сертификаты ключей проверки электронной подписи, выданные физическим лицам;

1.24.2. квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам;

1.24.3. квалифицированные сертификаты ключей проверки электронной подписи, выданные физическим лицам, прекратившие своё действие;

1.24.4. квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам, прекратившие своё действие;

1.24.5. аннулированные сертификаты ключей проверки электронной подписи, выданные физическим лицам;

1.24.6. аннулированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам.

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 (COC, CRL*[1]*)* – электронный документ с электронной подписью уполномоченного лица удостоверяющего центра, включающий в себя список серийных номеров, дату и время 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. *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.

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

1.31. *Участники электронного взаимодействия* – осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане.

1.32. *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.

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

---

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

2. ПРАВОВОЙ СТАТУС РЕГЛАМЕНТА

2.1. Регламент **У**достоверяющего центра ООО ИЦ «Выбор» (далее по тексту – Регламент УЦ) разработан на основании положений Закона об электронной подписи, других федеральных законов, принимаемых в соответствии с ними нормативных правовых актов, 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 её 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 отказать на законных основаниях 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 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 доминирующим 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, д. 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
Банковские реквизиты	р/с 40702810559310000170 Смоленское отделение № 8609 ПАО Сбербанк г. Смоленск БИК 046614632 к/с 30101810000000000632
Пункты выдачи сертификатов:	
Центральное (Смоленское) отделение ООО ИЦ «Выбор»	
Адрес	214000 г. Смоленск, ул. Коммунистическая, 6
Телефон	(4812) 701-201
Факс	(4812) 388-898
Адрес электронной почты	info@icvibor.ru
Режим работы	соответствует рабочему дню Удостоверяющего центра
Сафоновское отделение ООО ИЦ «Выбор»	
Адрес	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
Режим работы	соответствует рабочему дню Удостоверяющего центра
Вяземское отделение ООО ИЦ «Выбор»	
Адрес	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
Режим 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 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 Удостоверяющего центра 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 Удостоверяющего центра, действующим на день обращения заявителя УЦ в подразделения УЦ, и (или) оговариваются в договоре, заключаемом с заявителем.

4.3. Действующий прейскурант 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 полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата;

5.1.2. устанавливает сроки действия сертификатов ключей проверки электронных подписей;

5.1.3. аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;

5.1.4. выдаёт по обращению заявителя 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;

5.1.5. ведёт Реестр УЦ, в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;

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

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

5.1.8. проверяет уникальность ключей проверки электронных подписей в Реестре УЦ;

5.1.9. осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

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

5.3. обеспечивает возможность получения заинтересованными лицами содержащейся в Реестре УЦ информации;

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

5.4.1. осуществляет иную связанную с использованием электронной подписи деятельность.

5.5. Удостоверяющий центр обязан:

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

5.5.2. обеспечить актуальность, целостность и доступность информации, содержащейся в Реестре УЦ, и её защиту от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий;

5.6. обеспечивать круглосуточную (за исключением периодов технического обслуживания и ремонта) доступность в информационно-телекоммуникационной сети «Интернет» полученной из Реестра УЦ актуальной информации о выданных или аннулированных сертификатах;

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

5.6.2. отказать заявителю в создании сертификата в случае, если не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата;

5.6.3. отказать заявителю в создании сертификата в случае отрицательного результата проверки в Реестре УЦ уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата;

5.6.4. издавать сертификаты в формах электронного документа и документа на бумажном носителе на основании заявления заявителей и в соответствии с порядком, определённым Регламентом УЦ;

5.6.5. для подписания издаваемых сертификатов и Реестре УЦ использовать только ключ электронной подписи уполномоченного лица Удостоверяющего центра, срок действия которого не истёк, и только с этой целью;

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

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

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

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

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

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

5.6.12. 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 и иных информационных ресурсов сведения, необходимые для осуществления проверки достоверности документов и сведений, представленных заявителем;

5.6.13. запрашивать и получать из государственных и иных информационных ресурсов:

- выписку из Единого государственного реестра юридических лиц в отношении заявителя-юридического лица;
- выписку из Единого государственного реестра индивидуальных предпринимателей в отношении заявителя-индивидуального предпринимателя;
- выписку из Единого государственного реестра налогоплательщиков в отношении Заявителя-иностранной организации;

5.6.14. отказать заявителю в выдаче сертификата в случае, если полученная с использованием государственных и иных 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;

5.6.15. 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;

5.6.16. до внесения в Реестр УЦ информации об аннулировании сертификата уведомить владельца сертификата об аннулировании его сертификата путём направления документа на бумажном носителе или электронного документа с указанием основания аннулирования его сертификата;

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

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

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

5.6.20. при выдаче квалифицированного сертификата Удостоверяющий центр по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществлять регистрацию указанного лица в ЕСИА.

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

5.6.22. обеспечивать превышение срока окончания действия сертификата ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра не менее 5 лет над сроками окончания действия сертификатов владельцев сертификатов;

5.6.23. соблюдать сроки действия ключей электронной подписи уполномоченного лица Удостоверяющего центра, используемых для подписания создаваемых клиентских сертификатов, чтобы все они были подписаны ключами, не прекратившими своё действие;

5.6.24. хранить информацию, внесённую в Реестр УЦ, в течение всего срока деятельности Удостоверяющего центра, если более короткий срок не установлены нормативными правовыми актами Российской Федерации.

5.7. Удостоверяющий центр имеет право:

5.7.1. 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;

5.7.2. не принимать от заявителя документы, не соответствующие требованиям нормативных правовых актов Российской Федерации и Регламента УЦ;

5.7.3. 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;

5.7.4. отказать Заявителю в аннулировании сертификата при ненадлежащем оформлении соответствующего заявления;

5.7.5. 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, включённой 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;

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

6. ПРАВА И ОБЯЗАННОСТИ ЗАЯВИТЕЛЯ (ВЛАДЕЛЬЦА СЕРТИФИКАТА)

6.1. Заявитель (владелец сертификата) обязан:

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

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

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

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

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

6.1.6. 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;

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

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

6.1.9. не использовать личный ключ электронной подписи до предоставления Удостоверяющему центру подписанного владельцем сертификата соответствующего сертификата на бумажном носителе.

6.2. Заявитель (владелец сертификата) имеет право:

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

6.2.2. получать сертификат уполномоченного лица Удостоверяющего центра;

6.2.3. получать актуальный список отозванных сертификатов, изготовленный Удостоверяющим центром;

6.2.4. генерировать личный ключ электронной подписи самостоятельно;

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

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

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

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

6.2.9. осуществлять экспорт выданного ему (сгенерированного им) ключа электронной подписи при условии соблюдения необходимых мер по обеспечению его конфиденциальности;

6.2.10. 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.

7. ОТВЕТСТВЕННОСТЬ СТОРОН И ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

7.1. При возникновении споров сторонами в них считаются Удостоверяющий центр и сторона, присоединившаяся к Регламенту УЦ.

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

7.2.1. неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг удостоверяющим центром;

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

7.3. 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 суде по месту нахождения Удостоверяющего центра в соответствии с его подведомственностью.

ПРЕДОСТАВЛЕНИЕ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

8. СОЗДАНИЕ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ ВЛАДЕЛЬЦАМИ СЕРТИФИКАТОВ.

8.1. Изготовление в Удостоверяющем центре ключей электронной подписи и соответствующих им сертификатов производится работниками, включёнными в Орган криптографической защиты информации Удостоверяющего центра, на автоматизированных рабочих местах, аттестованных на соответствие требованиям по безопасности информации.

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

8.3. Владелец или пользователь сертификата могут присутствовать при изготовлении им личного ключа электронной подписи работником Удостоверяющего центра.

8.4. Пользователь сертификата может 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 ключа проверки электронной подписи и запроса на издание сертификата, соответствующих предоставленному ключу электронной подписи.

8.5. Пользователь сертификата может 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 ключа проверки электронной подписи и запроса на издание сертификата, соответствующего предоставленному ключу электронной подписи.

8.6. Не санкционированное владельцем сертификата изготовление персоналом Удостоверяющего центра дубликатов ключа электронной подписи и их копирование на неучтённые ключевые носители **запрещены**.

9. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ УПОЛНОМОЧЕННОГО ЛИЦА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

9.1. Ключ электронной подписи уполномоченного лица Удостоверяющего центра используется для подписывания созданных Удостоверяющим центром сертификатов и СОС в течение срока его действия или до ввода в действие нового ключа.

9.2. Издание и ввод в обращение очередного ключа электронной подписи уполномоченного лица Удостоверяющего центра и сертификата к нему производится в связи окончанием срока действия предыдущего такого ключа.

9.3. Издание очередного ключа электронной подписи уполномоченного лица Удостоверяющего центра и сертификата к нему производится не позднее, чем через 1 год и 3 месяца (15 месяцев) после начала действия предыдущего такого ключа.

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

9.4.1. 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;

9.4.2. файл запроса на получение квалифицированного сертификата уполномоченного лица Удостоверяющего центра направляется в УФО (ГУЦ) по электронной почте на указанный Минкомсвязи России адрес с приложением анкеты Удостоверяющего центра установленной формы;

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

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

9.5. 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.

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

9.6.1. скачиванием с Портала (сайта) УФО (в разделе Удостоверяющего центра ООО ИЦ «Выбор»);

9.6.2. скачиванием с Информационного ресурса УЦ, в том числе с указанного в сертификате владельца сертификата (в поле «Доступ к информации о центрах сертификации») адреса;

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

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

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

10.2. 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).

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

10.4. 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.

10.5. 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.

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

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

10.8. 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 новые сертификаты (при необходимости – с ключами электронной подписи). При этом данные о владельце и назначения сертификатов должны быть аналогичны тем, что были указаны в аннулированных сертификатах.

10.9. 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.

10.10. 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.

11. Смена ключей электронной подписи владельцев сертификата.

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

11.2. Заявление на смену ключа электронной подписи владельца сертификата может быть создано в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца сертификата.

12. Изготовление сертификатов ключа проверки электронной подписи, их выдача владельцам сертификатов.

12.1. Сертификаты могут изготавливаться:

12.1.1. в связи с выдачей владельцу сертификата первого сертификата;

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

12.1.3. по обоснованной причине до окончания срока действия ранее выданных владельцу сертификатов.

12.2. Количество одновременно действующих сертификатов, выдаваемых одному владельцу сертификата, Удостоверяющим центром не ограничивается.

12.3. Для подтверждения сведений, вносимых в квалифицированный сертификат, в том числе для удостоверения личности заявителя, Удостоверяющий центр запрашивает у заявителя и (или) в государственных информационных системах:

от юридических лиц

12.3.1. заявление в УЦ о выпуске сертификата;

12.3.2. копию документа, удостоверяющего личность пользователя сертификата;

12.3.3. копии документов о наделении руководителя юридического лица полномочиями исполнительного органа;

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

12.3.5. выписку из ЕГРЮЛ;

12.3.6. СНИЛС пользователя сертификата;

12.3.7. при необходимости: доверенность от руководителя юридического лица представителю юридического лица, уполномоченному подписать заявление на выдачу сертификата, предоставить документы для изготовления сертификата и/или получить изготовленные ключи и сертификат;

12.3.8. при необходимости: копию документа, удостоверяющего личность лица (представителя юридического лица), уполномоченного на предоставление документов для изготовления сертификата и/или получение изготовленного сертификата;

от индивидуальных предпринимателей

12.3.9. заявление в УЦ о выпуске сертификата;

12.3.10. копию документа, удостоверяющего личность пользователя сертификата;

12.3.11. выписку из ЕГРИП;

12.3.12. СНИЛС пользователя сертификата;

12.3.13. при необходимости: доверенность от индивидуального предпринимателя представителю индивидуального предпринимателя, уполномоченному подписать заявление на выдачу сертификата, предоставить документы для изготовления сертификата и/или получить изготовленные ключи и сертификат;

12.3.14. при необходимости: заявление о наделении своего представителя (одного или нескольких) полномочиями подписать заявление на выдачу сертификата, предоставить документы для изготовления сертификата и/или получить изготовленные ключи и сертификат;

12.3.15. при необходимости: копию документа, удостоверяющего личность лица (представителя индивидуального предпринимателя), уполномоченного подписать заявление на выдачу сертификата, предоставить документы для изготовления сертификата и/или получить изготовленные ключи и сертификат;

от физических лиц

12.3.16. заявление в УЦ о выпуске сертификата;

12.3.17. копия документа, удостоверяющего личность пользователя сертификата;

12.3.18. СНИЛС пользователя сертификата;

12.3.19. копия свидетельства о постановке на учёт в налоговом органе.

12.4. Изготовление и выдача сертификатов ключа подписи их владельцам 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 актами, устанавливающими требования к сертификатам в системах электронного документооборота. В заявлении указываются:

12.4.1. сведения о заявителе;

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

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

12.4.4. сведения для регистрации пользователя сертификата в ЕСИА, в том числе паспортные данные;

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

12.4.6. дополнительные условия для создания ключа электронной подписи и сертификата к нему (используемые средства криптографической защиты информации, возможность копирования ключа на другой носитель, количество заказанных сертификатов, другие);

12.4.7. кодовая фраза и порядок её использования владельцем сертификата при компрометации его ключа электронной подписи;

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

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

12.4.10. должность и роспись представителя заявителя, его инициалы и фамилия;

12.4.11. дата заявления;

12.4.12. оттиск основной печати организации (для юридических лиц).

12.5. Заявление на создание и выдачу первого сертификата может быть оформлено на бумажном носителе с подписью заявителя и (для юридических лиц) печатью организации, а для второго и последующего сертификата – в виде электронного документа, подписанного квалифицированной электронной подписью владельца сертификата.

12.6. Удостоверяющий центр устанавливает личность заявителей - физических лиц (граждан Российской Федерации, иностранных государств, беженцев, вынужденных переселенцев и лиц без гражданства) по основным документам, удостоверяющим личность данных категорий лиц в соответствии с законным порядком и правилами, установленными на территории Российской Федерации.

12.7. Сведения, указанные владельцем сертификата для получения сертификата, которые удостоверяются предъявлением документов, подтверждающих эти сведения, или предоставлением их надлежащим образом заверенных копий:

12.7.1. 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;

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

12.7.3. 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.

12.8. Получение сертификата ключа проверки электронной подписи может быть осуществлено пользователем сертификата, 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.

12.9. Физическое лицо, при получении с действующее от имени заявителя-физического лица, должно предъявить в Удостоверяющий центр нотариально заверенную доверенность.

12.10. Достоверность сведений о владельце сертификата, 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 представляемых документов определяется российским законодательством и Регламентом УЦ.

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

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

12.11.2. быть действительными на дату их предъявления;

12.11.3. 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.);

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

12.11.5. не содержать признаков подделки или намеренных исправлений.

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

12.13. 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 для заполнения заявителям перед получением услуг удостоверяющего центра.

12.14. 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.

12.15. 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.

12.16. Срок создания и выдачи сертификата, а также иных услуг удостоверяющего центра устанавливаются заключённым с заявителем договором на оказание услуг удостоверяющего центра.

12.17. Квалифицированные сертификаты создаются в соответствии с требованиями приказа Федеральной службы безопасности от 27.12.2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

12.18. 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 при необходимости вводимые данные с копиями представленных клиентом документов, в том числе с выпиской из ЕГРЮЛ (ЕГРИП).

12.19. При генерации запроса на издание квалифицированного сертификата в него (при необходимости) вносятся объектные идентификаторы (OID), расширяющие область использования к в информационных системах, предъявляющих к сертификатам особые требования.

12.20. 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 средства Удостоверяющего центра и получение сертификатов осуществляется по защищённым каналам связи.

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

12.22. 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, Минкомсвязи). Выбор из числа разрешённых к использованию средств криптографической защиты информации для создания ключевой пары определяется заявителем и указывается в заявлении на выдачу сертификата.

12.23. 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).

12.24. После получения сертификата из Удостоверяющего центра работник УЦ с помощью специальных программ связывает его с соответствующим контейнером ключа электронной подписи владельца сертификата на носителе ключа.

12.25. По письменному заявлению заявителя для контейнера ключа электронной подписи задаётся возможность его копирования (экспорта) на другие совместимые носители.

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

12.27. 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.

12.28. Носители ключей электронной подписи после генерации, учёта и до выдачи пользователю ключей электронной подписи хранятся в личном сейфе подготовленного работника Удостоверяющего центра. Они выдаются пользователям сертификата под роспись.

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

12.30. 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.

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

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

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

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

12.32.3. один экземпляр принадлежащего ему сертификата ключа проверки электронной подписи (на бумажном носителе);

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

12.32.5. Заявитель указывает в своём заявлении на выдачу сертификата ключевую (парольную) фразу, необходимую для его аутентификации при выполнении процедур, связанных с компрометацией ключа электронной подписи.

13. ОТЗЫВ И АННУЛИРОВАНИЕ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ ВЛАДЕЛЬЦА СЕРТИФИКАТА.

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

13.1.1. по истечении срока их действия;

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

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

13.1.4. в случаях, установленных Законом об электронной подписи, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или Регламентом УЦ.

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

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

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

13.2.3. вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию или пользователь сертификата дисквалифицирован.

13.3. Приём заявлений на аннулирование сертификата (форма – в приложениях №№ 3 и 4) осуществляется в течение рабочего дня Удостоверяющего центра. Рассмотрение, обработка заявлений и официальное опубликование уведомлений об аннулировании сертификата осуществляются не позднее 30 минут после приёма заявления Удостоверяющим центром.

13.4. 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 или по доверенности, удостоверить свою личность).

13.5. Срок внесения информации о прекращении действия или аннулировании сертификата в Реестр УЦ не должен превышать 12 часов от времени наступления обстоятельств, указанных в пунктах 13.1 и 13.2, или 12 часов от времени, когда Удостоверяющему центру стало известно о наступлении таких обстоятельств.

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

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

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

14. ПОРЯДОК ВЕДЕНИЯ РЕЕСТРА КВАЛИФИЦИРОВАННЫХ СЕРТИФИКАТОВ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

14.1. Порядок формирования и ведения Реестра УЦ определяется Удостоверяющим центром в соответствии с требованиями, устанавливаемыми Минкомсвязи России.

14.2. Плановое техническое обслуживание Реестра УЦ проводится в сроки, совпадающие с регламентным обслуживанием оборудования Удостоверяющего центра.

14.3. Время, отводимое на плановое техническое обслуживание Реестра УЦ, не должно превышать 6 часов. Для проведения планового технического обслуживания Реестра УЦ выбирается промежуток от 22:00 до 06:00 московского времени в выходные дни.

14.4. Внеплановое техническое обслуживание Реестра УЦ проводится в случае непредвиденных неполадок в его функционировании. Для незамедлительной ликвидации неполадок в функционировании Реестра УЦ привлекаются все необходимые силы и средства Удостоверяющего центра.

14.5. Уведомление участников информационного взаимодействия о проведении технического обслуживания Реестра УЦ производится путём публикации сообщений на официальном сайте Удостоверяющего центра, а также по электронной почте через циркулярную рассылку сообщений владельцам действующих квалифицированных сертификатов. Публикация на сайте и рассылка сообщений производятся заблаговременно не позднее, чем за 24 часа до начала технического обслуживания Реестра УЦ.

15. ПОДТВЕРЖДЕНИЕ ПОДЛИННОСТИ ЭЛЕКТРОННОЙ ПОДПИСИ.

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

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

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

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

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

15.3. К заявлению должен обязательно прилагаться носитель информации с файлом сертификата, подвергающегося процедуре проверки, в формате PKCS#7 и DER-кодировке X.509 или кодировке Base64 (*.cer).

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

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

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

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

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

15.5. К заявлению должен обязательно прилагаться носитель информации 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).

15.6. 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.

15.7. 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 Удостоверяющего центра.

15.8. Результатом работ по подтверждению подлинности ЭП являются заключения Удостоверяющего центра, которые должны содержать:

15.8.1. дату и место проведения проверки;

15.8.2. состав комиссии, осуществлявшей проверку;

15.8.3. основание для проведения проверки;

15.8.4. данные, представленные для проведения проверки;

15.8.5. применённые методы и содержание проверки;

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

15.8.7. действовал или не действовал сертификат во время, указанное в заявлении;

15.8.8. обоснование результатов проверки;

15.8.9. подписи членов комиссии и лица утвердившего заключение;

15.8.10. печать Удостоверяющего центра.

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

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

16. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.

16.1. Удостоверяющий центр осуществляет информирование заявителя об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, выдачей под роспись пользователю сертификата на бумажном носителе руководства. Более подробные разъяснения по означенным условиям пользователь может получить, ознакомившись с Памяткой Удостоверяющего центра о порядке использования электронной подписи и средств электронной подписи (приложение № 10 к Регламенту УЦ).

16.2. Актуальность информации, содержащейся в Реестре УЦ, обеспечивается постоянным его ведением и публикацией обновлённых данных на Информационном ресурсе УЦ. Обновление или дополнение информации в Реестре УЦ производится незамедлительно (не позднее 8 рабочих

часов) после получения информации о выпуске или отзыве (аннулировании) квалифицированных сертификатов.

16.3. Защита информации, содержащейся в Реестре УЦ, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий обеспечивается мерами Удостоверяющего центра по информационной безопасности, состав и содержание которых определяются внутренними организационно-распорядительными документами Удостоверяющего центра.

16.4. Постоянная доступность информации из Реестра УЦ об изданных квалифицированных сертификатах и актуальных списках отозванных сертификатов обеспечивается её публикацией на Информационном ресурсе УЦ. Во время планового или внепланового технического обслуживания Реестра публикуемая информация из него может быть временно недоступной.

16.5. В соответствии с ч. 5 ст. 18 Закона об электронной подписи Удостоверяющий центр осуществляет регистрацию всех изданных им квалифицированных сертификатов в ЕСИА.

16.6. По желанию Заявителя, которому выдан квалифицированный сертификат, Удостоверяющий центр безвозмездно осуществляет регистрацию Заявителя в ЕСИА.

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

17. СТРУКТУРА И ПОРЯДОК ИСПОЛЬЗОВАНИЯ СЕРТИФИКАТОВ И СПИСКОВ ОТОЗВАННЫХ СЕРТИФИКАТОВ.

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

17.2. 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	<день месяц год час:минута:секунда>
по	<день месяц год час:минута:секунда>
Раздел (вкладка) «Состав»	
Версия	V3
Серийный номер	<уникальный номер из 32 символов в шестнадцатеричном исчислении>
Алгоритм подписи	<номер и год принятия ГОСТ>
Алгоритм хэширования подписи	<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	день месяц год час:минута:секунда
Действителен по	день месяц год час:минута:секунда
Субъект	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>

Наименование полей	Структура и значение полей
	C = RU ИНН = <12 цифр> ОГРН = <13 цифр> STREET = <улица, корпус, строение, дом и другие элементы топонимики>
Открытый ключ	<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) <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: РНС ФСС=<10 цифровых символов> <Дополнительные расширения (OID)>
Средство электронной подписи владельца	Средство электронной подписи: СКЗИ [наименование программы-криптопровайдера]
Идентификатор ключа субъекта	<уникальное значение из 40 символов в шестнадцатеричном исчислении>
Средство электронной подписи и УЦ издателя	Средство электронной подписи: СКЗИ <наименование от производителя> Заключение на средство ЭП: <номер и дата сертификата ФСБ> Средство УЦ: <наименование от производителя> Заключение на средство УЦ: <номер и дата сертификата ФСБ>
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=http://*.crl
Идентификатор ключа центра сертификатов	Идентификатор ключа= уникальное значение из 40 символов в шестнадцатеричном исчислении Поставщик сертификата: Адрес каталога: 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> Серийный номер сертификата= <уникальное значение из 32 символов в шестнадцатеричном исчислении>
Использование ключа	для СКПЭП владельцев сертификата: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0) для СКПЭП уполномоченного лица Удостоверяющего центра добавляются: Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL) (f6)

Наименование полей	Структура и значение полей
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	<тексто-графическое отображение цепочки доверия к сертификату>
Состояние сертификата	<текстовое заключение о статусе сертификата>

17.3. Структура списка отозванных сертификатов Удостоверяющего центра.

Наименование полей	Структура и значение полей
Раздел (вкладка) «Общие»	
Версия	V2
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	<день месяц год час:минута:секунда>
Следующее обновление	<день месяц год час:минута:секунда>
Алгоритм подписи	<номер и год принятия ГОСТ>
Алгоритм хэширования подписи	<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	<день месяц год час:минута:секунда>
Код причины списка отзыва (CRL)	<причина (цифровой код)>

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

17.4.1. наступило время начала его действия;

17.4.2. срок его действия не истёк;

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

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

17.5.1. минуло время начала его действия;

17.5.2. срок его действия не истёк;

17.5.3. сертификат не аннулирован.

17.6. Срок действия ключа электронной подписи уполномоченного лица Удостоверяющего центра не превышает 1 года и 3 месяцев (15 месяцев) и начинается от даты и времени его генерации.

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

17.8. Срок действия ключей электронной подписи владельцев сертификатов-клиентов УЦ не превышает 1 года и 3 месяцев (15 месяцев) и начинается от даты и времени начала действия соответствующего сертификата.

17.9. Срок действия сертификатов ключа проверки электронной подписи владельцев сертификатов-клиентов УЦ не превышает 1 года и 3 месяцев (15 месяцев).

18. БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

18.1. Информация, не относящаяся согласно законодательству Российской Федерации к информации ограниченного доступа, считается общедоступной.

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

18.3. Информация, включаемая в сертификат и списки отозванных сертификатов, издаваемые Удостоверяющим центром, не считается информацией ограниченного доступа на основании российского законодательства и письменного согласия владельцев сертификатов.

18.4. Ключ электронной подписи, соответствующий сертификату, является информацией ограниченного доступа, принадлежащей владельцу сертификата.

18.5. Удостоверяющий центр не осуществляет хранение ключевой информации после выдачи соответствующих ключей электронной подписи заявителям.

18.6. Персональная и (или) корпоративная информация о лицах, зарегистрированных в Удостоверяющем центре, содержащаяся в реестре Удостоверяющего центра, не подлежащая опубликованию в составе сертификата, относится к информации ограниченного доступа.

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

18.8. Хранение сертификата в Удостоверяющем центре осуществляется в течение всего периода его действия и пяти лет после окончания срока его действия или аннулирования. По истечении указанного срока хранения сертификаты переводятся в режим архивного хранения.

18.9. 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 представителям. Создание не оговорённых заявителями копий и постоянное хранение созданных для них Удостоверяющим центром ключей не допускается.

18.10. Невостребованные ключи уничтожаются назначенными и подготовленными работниками Удостоверяющего центра после принятия решения о выводе таких ключей из обращения. Технологические копии созданных Удостоверяющим центром ключей уничтожаются незамедлительно (не позднее конца рабочего дня Удостоверяющего центра).

19. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ (ФОРС-МАЖОР)

19.1.1. 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.

19.1.2. 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.

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

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

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

19.1.6. Если невозможность полного или частичного исполнения сторонами какого-либо обязательства по настоящему Регламенту УЦ обусловлена действием форс-мажора 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 аннулирование сертификата ключа проверки электронной подписи (форма; для юридических лиц).
4. Заявление на аннулирование сертификата ключа проверки электронной подписи (форма; для индивидуальных предпринимателей, физических лиц).
5. Заявление на подтверждение подлинности электронной подписи Уполномоченного лица УЦ в сертификате ключа проверки электронной подписи (форма; для юридических лиц).
6. Заявление на подтверждение подлинности электронной подписи Уполномоченного лица УЦ 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).
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

_____
наименование лица

в лице _____

действующего на основании _____

просит создать и выдать ключ электронной подписи и к нему 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. Дополнительные назначения (области использования) сертификата:

☐

22. Дополнительные условия:

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

☐ 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 Удостоверяющим центром ООО ИЦ «Выбор» его персональных данных, переданных заявителем, и признаёт отнесение его персональных данных, внесённых в выданный ему сертификат ключа проверки электронной подписи, к общедоступным.

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 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).

_____ _____ _____
должность руководителя заявителя подпись фамилия и инициалы

_____ 201 ____ г.

м.п.

Приложение № 2
к Регламенту Удостоверяющего центра
ООО ИЦ «ВЫБОР»
(примерная форма)

ДОВЕРЕННОСТЬ

г. Смоленск Дата выдачи доверенности: _____ _____ 201 ____ г.

Действительна до: _____ _____ 201 ____ 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 Обществе с ограниченной ответственностью Информационном центре «Выбор» (ОГРН 1026701454064, ИНН 6730025009) и совершать нижеуказанные действия.

1. Подписать и предоставить заявление на выдачу ключа электронной подписи и сертификата ключа проверки электронной подписи, а также другие документы, определённые Регламентом Удостоверяющего центра ООО ИЦ «Выбор» как необходимые для получения ключа электронной подписи, сертификата ключа проверки электронной подписи и иных средств электронной подписи, а также копии необходимых для этого документов.
2. 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.

3. Получить ключ электронной подписи и иные средства электронной подписи, а также право использования программ для ЭВМ и сопутствующие товары, работы и услуги.
4. 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 аннулирование сертификата ключа проверки электронной подписи

_____
полное наименование юридического лица согласно ЕГРЮЛ

ОГРН [ ] ИНН [ ] КПП [ ]

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	

_____ _____ _____
должность руководителя Заявителя | подпись | фамилия и инициалы

м.п.

_____ _____ 201___ г.

Служебные отметки (заполняется работниками Удостоверяющего центра)

Заявление на аннулирование сертификата ключа проверки электронной подписи принято «_____» _____ 201___ 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 «_____» _____ 201__ 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 аннулирование сертификата ключа проверки электронной подписи

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

ИНН ☐☐☐☐☐☐☐☐☐☐ ОГРНИП[1] ☐☐☐☐☐☐☐☐☐☐☐☐☐

в связи с _____
причина отзыва сертификата

прошу аннулировать сертификат ключа проверки электронной подписи со следующими данными:

Серийный номер сертификата	
СНИЛС пользователя сертификата	
Фамилия, имя, отчество пользователя сертификата	

Владелец сертификата _____ _____
подпись инициалы, фамилия

«____» _____ 201__ г.

м.п.

Служебные отметки (заполняется работниками Удостоверяющего центра)

Заявление на аннулирование сертификата ключа проверки электронной подписи принято «_____» _____ 201___ 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 «_____» _____ 201__ 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

«____» _____ 201___ г.

м.п.

Служебные отметки (заполняется работниками Удостоверяющего центра)

Заявление и дополнительные материалы к нему приняты
«_____» _____ 201___ 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

«____» _____ 201__ г.

М.П.

Служебные отметки (заполняется работниками Удостоверяющего центра)

Заявление и дополнительные материалы к нему приняты
«_____» _____ 201___ 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

«____» _____ 201___ г.

м.п.

Служебные отметки (заполняется работниками Удостоверяющего центра)

Заявление и дополнительные материалы к нему приняты
«_____» _____ 201___ 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

«____» _____ 201__ г.

М.П.

Служебные отметки (заполняется работниками Удостоверяющего центра)

Заявление и дополнительные материалы к нему приняты
«_____» _____ 201___ 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)

ООО Информационный центр "ВЫБОР" Юридический адрес: Россия, 214000, Смоленск, ул. Коммунистическая, д.6 ОГРН 1026701454064 ИНН 6730025009, КПП 673001001
т./ф. (4812) 701-201, e-mail: info@icvibor.ru, www.icvibor.ru

КВАЛИФИЦИРОВАННЫЙ СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

Номер квалифицированного сертификата: <32 шестнадцатеричных символа>
Действие квалифицированного сертификата: с <дата, время в часах, минутах>
по <дата, время в часах, минутах>

Сведения о владельце квалифицированного сертификата

Наименование юридического лица: <сокращённое>
Основной государственный регистрационный номер: <из 13 цифр>
Идентификационный номер налогоплательщика: <из 12 цифр>
Место нахождения юридического лица: <международный код страны, юридический адрес>

Сведения об издателе квалифицированного сертификата

Наименование удостоверяющего центра: <сокращённое>
Место нахождения удостоверяющего центра: <международный код страны, юридический адрес>
Номер квалифицированного сертификата удостоверяющего центра: <шестнадцатеричные символы>
Наименование средства электронной подписи: СКЗИ <наименование от производителя>
Реквизиты заключения о подтверждении соответствия средства электронной подписи: номер и дата
Наименование средства удостоверяющего центра:
Программный комплекс <наименование от производителя>
Реквизиты заключения о подтверждении соответствия средства удостоверяющего центра: номер и дата
Класс средств удостоверяющего центра:
Класс средства ЭП <буквенно-цифровое обозначение из трёх символов>

Сведения о ключе проверки электронной подписи

Используемый алгоритм: <номер и год принятия ГОСТ>
Используемое средство электронной подписи: СКЗИ <наименование от производителя>
Класс средства электронной подписи:
Класс средства ЭП <буквенно-цифровое обозначение из трёх символов>
Область использования ключа:
Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
Значение ключа:
<132 шестнадцатеричных символа>

Электронная подпись под квалифицированным сертификатом

Используемый алгоритм: <номер и год принятия ГОСТ>
Значение электронной подписи:
<128 шестнадцатеричных символов>

Подпись уполномоченного лица _____ /инициалы, фамилия/

Подпись владельца сертификата _____ /инициалы, фамилия/
М.П.

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

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Электронная подпись (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.

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

Сертификат ключа проверки электронной подписи (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.

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном Федеральным законом порядке выдан сертификат ключа проверки электронной подписи.

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

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

Список отозванных сертификатов (COC, CRL[1]) – электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, которые на определённый момент времени были отозваны пользователями и/или аннулированы Удостоверяющим центром или действие которых было приостановлено.

Отзыв сертификата ключа проверки электронной подписи – выраженное документально намерение пользователя аннулировать сертификат ключа проверки электронной подписи.

Аннулирование сертификата ключа проверки электронной подписи – прекращение его действия, признание его недействительным путём включения в актуальный список отозванных сертификатов Удостоверяющего центра.

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.

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:

- ключ используется или использовался ранее не его владельцем;
- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение работников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку информации или её искажение в системе конфиденциальной связи;

1 Certificate Revocation List (*англ.*)

- нарушение целостности печатей на сейфах с ключевыми носителями, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них ключевых носителей;
- утрата ключей от сейфов в момент нахождения в них ключевых носителей с последующим их обнаружением;
- доступ посторонних лиц к ключевой информации.

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 установленных 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, 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[4], упущенная выгода).

4.4. Выдача искажённого электронного документа за подлинный (задуманный автором) путём внесения изменений в файл на этапе подписания. Файл, передаваемый программе, которая ис-

---

1 для операционных систем семейства Windows

2 см. определение термина

3 подписание документа ключом электронной подписи без ведома его владельца

4 уголовная, материальная, административная

пользуется 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[1]. 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[2].

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[3] 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 потенциально опасных макросов[4], 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.

---

1 по принятой в ИТ терминологии имеют наименование «сниффер»

2 «рядовым» хакерам

3 например, локальной вычислительной сети

4 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

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.