



**Общество с ограниченной ответственностью «ЭТП ГПБ Консалтинг»
(ООО «ЭТП ГПБ Консалтинг»)**

УТВЕРЖДЕН

Приказом
ООО «ЭТП ГПБ Консалтинг»
№ К/Пр/2025/25 от 30 октября 2025 г.

Действует с:
01 ноября 2025 г.

**ПОРЯДОК
реализации функций
удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»
и исполнения его обязанностей
по созданию и выдаче неквалифицированных сертификатов ключа проверки
электронной подписи**

Редакция № 1
Москва
2025

1. СОДЕРЖАНИЕ

1.	СОДЕРЖАНИЕ	2
2.	ПОНЯТИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ.....	3
3.	ОБЩИЕ ПОЛОЖЕНИЯ	8
3.1.	Предмет регулирования	8
3.2.	Сведения об Удостоверяющем центре	9
3.3.	Порядок информирования о предоставлении услуг УЦ	9
3.4.	Стоимость услуг Удостоверяющего центра.....	9
3.5.	Подтверждение наличия инфраструктуры.....	10
4.	ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УЦ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ)	12
5.	ПРАВА И ОБЯЗАННОСТИ УЦ	14
6.	ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УЦ, В Т.Ч. ТРЕБОВАНИЯ К ДОКУМЕНТАМ, ПРЕДОСТАВЛЯЕМЫМ В УЦ В РАМКАХ ПРЕДОСТАВЛЕНИЯ УСЛУГ	18
6.1.	Процедура создания ключей ЭП и ключей проверки ЭП	18
6.2.	Процедура создания и выдачи неквалифицированных сертификатов	23
6.3.	Подтверждение действительности электронной подписи, использованной для подписания электронных документов	29
6.4.	Процедуры, осуществляемые при прекращении действия и аннулирования неквалифицированного сертификата	30
6.5.	Порядок ведения реестра неквалифицированных сертификатов:	33
6.6.	Порядок технического обслуживания реестра неквалифицированных сертификатов:	34
7.	ПРОЦЕДУРА ПОДТВЕРЖДЕНИЯ ВЛАДЕНИЯ ЗАЯВИТЕЛЕМ КЛЮЧОМ ЭЛЕКТРОННОЙ ПОДПИСИ ПРИ ВЫПУСКЕ УНЭП	35
8.	ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УЦ.....	37
8.1.	Информирование Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки	37
8.2.	Выдача по обращению Заявителя средств электронной подписи	37
8.3.	Обеспечение актуальности информации, содержащейся в реестре неквалифицированных сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий	37
8.4.	Обеспечение доступности реестра неквалифицированных сертификатов в информационно-телекоммуникационной сети Интернет в любое время, за исключением периодов технического обслуживания реестра неквалифицированных сертификатов	38
8.5.	Порядок обеспечения конфиденциальности созданных УЦ ключей электронных подписей:	38
8.6.	Предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре неквалифицированных сертификатов, включая информацию о прекращении действия неквалифицированного сертификата или об аннулировании неквалифицированного сертификата, в том числе путем публикации перечня прекративших свое действие (аннулированных) неквалифицированных сертификатов	39
9.	СПИСОК ПРИЛОЖЕНИЙ	40
9.1.	Приложение №1 к Порядку УЦ ООО «ЭТП ГПБ Консалтинг». Форма заявления на создание и выдачу неквалифицированного сертификата ключа проверки электронной подписи.	41
9.2.	Приложение №2 к Порядку УЦ ООО «ЭТП ГПБ Консалтинг». Форма заявления на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи.....	47
9.3.	Приложение №3 к Порядку УЦ ООО «ЭТП ГПБ Консалтинг». Форма заявления на подтверждение действительности электронной подписи в электронном документе	50
9.4.	Приложение №4 к Порядку УЦ ООО «ЭТП ГПБ Консалтинг». Руководство по обеспечению безопасности использования неквалифицированной электронной подписи и средств электронной подписи	51
9.5.	Приложение № 5 к Порядку УЦ ООО «ЭТП ГПБ Консалтинг». Форма неквалифицированного сертификата.....	56
9.6.	Приложение № 6 к Порядку УЦ ООО «ЭТП ГПБ Консалтинг». Профиль неквалифицированного сертификата.....	58

2. ПОНЯТИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ

2.1. Понятия, термины и определения гражданского, налогового законодательства Российской Федерации, законодательства Российской Федерации в сфере электронной подписи, других отраслей законодательства Российской Федерации, используемые в настоящем Порядке реализации функций удостоверяющего центра ООО «ЭТП ГПБ Консалтинг» и исполнения его обязанностей по созданию и выдаче НСКПЭП (далее – «Порядок»), применяются в том значении, в каком они используются в этих отраслях законодательства, федеральных законах, если иное не предусмотрено настоящим Порядком.

2.2. В Порядке используются следующие понятия, термины, определения и сокращения:

2.2.1. **Владелец сертификата ключа проверки электронной подписи (Владелец сертификата)** – лицо, которому в установленном Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» и настоящим Порядком выдан сертификат ключа проверки электронной подписи.

2.2.2. **Внеплановая смена ключа электронной подписи/сертификата** – создание нового ключа электронной подписи и ключа проверки электронной подписи в связи с компрометацией, изменением информации, внесенной в сертификат, или после окончания срока их действия.

2.2.3. **Доверенное лицо УЦ** – лицо, наделенное УЦ полномочиями по приему заявлений на создание и выдачу сертификатов ключей проверки электронной подписи, а также вручению сертификатов ключей проверки электронных подписей от имени этого удостоверяющего центра. При совершении порученных удостоверяющим центром действий доверенное лицо обязано идентифицировать заявителя при его личном присутствии в соответствии с требованиями Федерального закона от 06.04.2011 г. №63-ФЗ «Об электронной подписи».

2.2.4. **Единая система идентификации и аутентификации (ЕСИА)** - федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации, и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах.

2.2.5. **Заявитель** – коммерческая организация, некоммерческая организация, индивидуальный предприниматель, физическое лицо, не зарегистрированное в качестве индивидуального предпринимателя, но осуществляющее профессиональную деятельность, приносящую доход, в соответствии с федеральными законами на основании

государственной регистрации и (или) лицензии, в силу членства в саморегулируемой организации, а также любое иное физическое лицо, лица, замещающие государственные должности Российской Федерации или государственные должности субъектов Российской Федерации, должностные лица государственных органов, органов местного самоуправления, работники подведомственных таким органам организаций, нотариусы и уполномоченные на совершение нотариальных действий лица (далее - нотариусы), обращающиеся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата.

2.2.6. Сертификат ключа проверки электронной подписи (сертификат) – 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.

2.2.7. Ключ проверки электронной подписи (ключ проверки ЭП) – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

2.2.8. Ключ электронной подписи (ключ ЭП) – уникальная последовательность символов, предназначенная для создания электронной подписи.

2.2.9. Ключ электронной подписи Удостоверяющего центра (ключ ЭП УЦ) - ключ ЭП, использующийся УЦ для создания сертификатов ключей проверки ЭП и списков отозванных сертификатов.

2.2.10. Компрометация ключа ЭП – нарушение конфиденциальности ключа ЭП, а именно утрата доверия к тому, что используемые ключи ЭП обеспечивают безопасность информации (утрача носителя ключа ЭП или ключа ЭП (стирание, уничтожение с физического носителя), физическая порча носителя ключа ЭП, получение к ключу ЭП доступа третьих лиц, передача ключа ЭП по открытым каналам связи, например, по электронной почте, и прочее).

2.2.11. Общество - Общество с ограниченной ответственностью «ЭТП ГПБ Консалтинг» (ООО «ЭТП ГПБ Консалтинг»), ОГРН 5167746487651, ИНН 7728356929.

2.2.12. Оператор Удостоверяющего центра (Оператор УЦ) – работник УЦ, наделенный полномочиями по осуществлению действий по созданию и выдаче сертификатов ключей проверки ЭП, иными функциями и полномочиями, указанными в настоящем Порядке.

2.2.13. Плановая смена ключа ЭП/сертификата – создание нового ключа ЭП и сертификата ключа проверки ЭП до окончания срока действия ранее выданных неквалифицированного ключа ЭП и сертификата.

2.2.14. Прайс-лист на оказание услуг Удостоверяющего центра (Прайс-лист) – документ, разработанный и утвержденный в ООО «ЭТП ГПБ Консалтинг», размещенный в действующей редакции для ознакомления всеми заинтересованными лицами на Сайте УЦ и содержащий систематизированный перечень товаров, работ, услуг с указанием стоимости (цены) и кратких характеристик.

2.2.15. Подтверждение владения ключом ЭП - получение удостоверяющим центром, доказательств того, что лицо, обратившееся за получением сертификата ключа проверки ЭП, владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному таким лицом для получения сертификата.

2.2.16. Реестр неквалифицированных сертификатов ключей проверки электронных подписей (реестр сертификатов) – реестр созданных и аннулированных УЦ неквалифицированных сертификатов ключей проверки ЭП, в том числе включающий в себя информацию, содержащуюся в созданных УЦ неквалифицированных сертификатах, и информацию о датах прекращения действия или аннулирования неквалифицированных сертификатов, а также об основаниях прекращения действия или аннулирования неквалифицированных сертификатов.

2.2.17. Сайт УЦ – совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет») по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети Интернет, размещенный в сети Интернет по адресу: <https://uc-gpb.ru/> и содержащий информацию об УЦ, об услугах УЦ и их стоимости, инструкции и пояснения для заявителей и владельцев сертификатов, реестры сертификатов ключей проверки ЭП, а также другую информацию, необходимую к опубликованию в соответствии с Федеральным законом от 06.04.2011 г. №63-ФЗ «Об электронной подписи» и настоящим Порядком.

2.2.18. Сертификат ключа проверки электронной подписи Удостоверяющего центра (сертификат ЭП УЦ) – неквалифицированный сертификат ключа проверки ЭП, использующийся для проверки УЦ в созданных им неквалифицированных сертификатах ключей проверки ЭП и реестрах неквалифицированных сертификатов ключей проверки ЭП.

2.2.19. Система межведомственного электронного взаимодействия (СМЭВ) – федеральная государственная информационная система, позволяющая органам и организациям осуществлять информационный обмен на основе унифицированных правил взаимодействия между информационными системами органов и организаций (далее – электронные сервисы), а также обеспечивать единый технологический способ взаимодействия информационных систем органов и организаций (далее – единый электронный сервис) посредством технологии очередей электронных сообщений в соответствии с зарегистрированными форматами передаваемых сведений (далее – виды сведений) и фиксацией фактов движения электронных сообщений в системе взаимодействия.

2.2.20. Средства электронной подписи (средства ЭП) – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП, и соответствующие требованиям к средствам электронной подписи. УЦ ООО «ЭТП ГПБ Консалтинг» поддерживает использование сертифицированных средств ЭП производства ООО «КРИПТО-ПРО».

2.2.21. Средства УЦ – программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

2.2.22. Средства криптографической защиты информации (СКЗИ) – шифровальные (криптографические) средства защиты информации конфиденциального характера.

2.2.23. Удостоверяющий центр (УЦ) – структурное подразделение Общества, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 г. №63-ФЗ «Об электронной подписи».

2.2.24. Федеральный закон – Федеральный закон от 06.04.2011 года № 63-ФЗ «Об электронной подписи».

2.2.25. Формат сертификата ключа проверки электронной подписи (списка отозванных сертификатов) – упорядоченный набор допустимых полей данных сертификата ключа проверки ЭП (списка отозванных сертификатов).

2.2.26. 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.

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

2.3. Настоящий Порядок содержит также иные понятия, термины, определения и сокращения, которые используются в значениях, раскрытых в его соответствующих разделах.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Предмет регулирования

3.1.1. Порядок определяет условия предоставления услуг УЦ, включая права, обязанности и ответственность УЦ, в соответствии с Федеральным законом и иными нормативно-правовыми актами, принимаемыми в соответствии с Федеральным законом.

3.1.2. Порядок является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации, распространяется в форме электронного документа, размещенного на Сайте УЦ и является официальным уведомлением всех заинтересованных сторон о взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ, а также соглашением, налагающим обязанности на все вовлеченные в эти взаимоотношения стороны. Действие Порядка распространяется на Заявителей, Владельцев сертификатов, Доверенных лиц УЦ, а также на всех лиц, использующих предоставляемые УЦ услуги и информацию.

3.1.3. Присоединение к Порядку осуществляется путем подачи Заявителем заявки на регистрацию в УЦ. С момента подачи заявки Заявитель считается присоединившимся к Порядку и становится стороной Порядка.

3.1.4. Регистрация заявок Заявителей в УЦ осуществляется на основании поданных Заявителем в УЦ регистрационных данных Заявителя, включая информацию, подлежащую внесению в неквалифицированный сертификат, с использованием информационной системы УЦ.

3.1.5. Заявка на регистрацию может быть подана Заявителем одним из следующих способов:

- путем подачи заявки на регистрацию в форме электронного документа, сформированного Заявителем на Сайте УЦ;
- путем передачи в информационную систему УЦ заявки на регистрацию, сформированной по обращению Заявителя Уполномоченным сотрудником Доверенного лица УЦ на основании предоставленных Заявителем регистрационных данных.

3.1.6. Регистрация заявок в информационной системе УЦ осуществляется путем присвоения заявке порядкового номера с буквенно-цифровым идентификатором.

3.1.7. Факт присоединения Заявителя к Порядку является полным принятием им условий Порядка и всех его положений в редакции, действующей на момент подачи заявки на регистрацию в УЦ. Сторона, присоединившаяся к Порядку, принимает дальнейшие изменения (дополнения), вносимые в Порядок, в соответствии с условиями Порядка.

3.1.8. Порядок утверждается приказом Общества. Изменения и дополнения в Порядок вносятся УЦ в одностороннем порядке. Уведомление Сторон Порядка осуществляется путем публикации новой версии Порядка на Сайте УЦ.

3.1.9. В случае изменения законодательства Российской Федерации, Порядок действует в части, не противоречащей положениям действующих нормативных правовых актов, до внесения соответствующих изменений (дополнений) в настоящий Порядок.

3.2. Сведения об Удостоверяющем центре

3.2.1. Адрес (место нахождения):

Юридический адрес ООО «ЭТП ГПБ Консалтинг»: 117342, г. Москва, ул. Миклухо-Маклая, д. 40, этаж 1, помещение IV, комната 20.

Почтовый адрес ООО «ЭТП ГПБ Консалтинг»: 117342, г. Москва, ул. Миклухо-Маклая, д. 40, этаж 1, помещение IV, комната 20.

Адрес осуществления деятельности УЦ: 119180, г. Москва, Якиманская наб., д.2.

Адреса Доверенных лиц УЦ размещены на Сайте УЦ.

3.2.2. График работы УЦ осуществляется в круглосуточном режиме, включая выходные и нерабочие праздничные дни.

График работы Доверенных лиц УЦ (точек обслуживания) размещается на Сайте УЦ и соответствует местному времени.

3.3. Порядок информирования о предоставлении услуг УЦ

3.3.1. Многоканальный телефон УЦ (для справок, технической поддержки, оформления заявок): +7 (800) 100-65-49.

3.3.2. Адрес Сайта УЦ в сети Интернет: <https://uc-gpb.ru/>, адрес электронной почты УЦ: ca@etpgpb.ru.

По вопросам предоставления услуг УЦ Заявители получают информацию:

- на Сайте УЦ в порядке самостоятельного ознакомления с размещенной информацией или через форму обратной связи на сайте УЦ путём отправки заявки на консультацию;
- по многоканальному телефону УЦ в порядке консультации со специалистами УЦ в режиме реального времени;
- по адресу электронной почты путем отправки электронного письма с обращением в адрес УЦ.

3.4. Стоимость услуг Удостоверяющего центра

3.4.1. Стоимость услуг УЦ определяется, исходя из установленных Прайс-листом цен (тарифов), публикуемых на Сайте УЦ на день выставления счета, либо иными

договорами, соглашениями и внутренними (локальными) нормативными актами ООО «ЭТП ГПБ Консалтинг».

3.4.2. Сроки и порядок расчетов за оказанные услуги УЦ определяются публичным договором, заключаемым между Обществом и Заявителем (текст публичного договора размещен на Сайте УЦ), сублицензионным договором на использование программы для электронно-вычислительных машин (ЭВМ) СКЗИ «КриптоПро CSP», иными договорами, соглашениями и внутренними (локальными) нормативными актами ООО «ЭТП ГПБ Консалтинг».

3.4.3. Расчеты за услуги УЦ производятся в рублях в порядке, в размерах и на условиях, определенных действующим Прайс-листом, публичным договором, заключаемым между Обществом и Заявителем, сублицензионным договором на использование программы для ЭВМ СКЗИ «КриптоПро CSP», иными договорами, соглашениями и внутренними (локальными) нормативными актами ООО «ЭТП ГПБ Консалтинг».

3.4.4. Положения п.п. 3.4.1 – 3.4.3 Порядка могут не применяться в том случае, если Заявитель получает услуги УЦ на основании договора, заключенного между УЦ и Доверенным лицом УЦ. В этом случае Заявитель и Доверенное лицо УЦ руководствуются условиями, установленными таким договором. При этом все иные положения, установленные Порядком, являются обязательными для Заявителя и Доверенного лица УЦ.

3.5. Подтверждение наличия инфраструктуры

3.5.1. Во исполнение требований части 4 статьи 13 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», ООО «ЭТП ГПБ Консалтинг» (Удостоверяющий центр) подтверждает наличие организационно-технической инфраструктуры, обеспечивающей безопасное и непрерывное электронное взаимодействие доверенными лицами и УЦ, включая:

- взаимодействие между доверенными лицами:

УЦ обеспечивает функционирование защищённой информационной системы, предназначенной для обмена информацией, необходимой доверенным лицам при приёме заявлений на создание и выдачу неквалифицированных сертификатов ключей проверки электронной подписи и при их вручении.

- взаимодействие между доверенными лицами и УЦ:

Инфраструктура УЦ включает в себя:

- защищённые каналы связи, построенные с использованием криптографических алгоритмов в соответствии с ГОСТ TLS, ГОСТ 28147-89 и ГОСТ Р 34.12-2015;
- модули приёма, обработки и учёта электронных заявлений;

- механизмы идентификации и аутентификации доверенных лиц с разграничением прав доступа;
- средства регистрации и аудита действий доверенных лиц.
 - правовое закрепление полномочий доверенных лиц:

Порядок взаимодействия, а также права и обязанности доверенных лиц определяются внутренними локальными актами УЦ и договорами, заключёнными с организациями, привлекаемыми в качестве доверенных лиц.

- соответствие законодательств:

Созданная организационно-техническая инфраструктура обеспечивает соблюдение требований части 4 статьи 13 Федерального закона № 63-ФЗ, включая приём заявлений и вручение доверенными лицами от имени УЦ неквалифицированных сертификатов ключей проверки электронной подписи, а также гарантирует выполнение установленных требований к защите информации и устойчивости функционирования информационных систем УЦ.

4. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УЦ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ)

4.1. В соответствии с Федеральным законом УЦ реализует следующие функции и оказывает услуги:

4.1.1. Создает неквалифицированные сертификаты ключей проверки ЭП и выдает созданные неквалифицированные сертификаты лицам, обратившимся за их получением (Заявителям), при условии установления личности получателя неквалифицированного сертификата (Заявителя) либо полномочия лица, выступающего от имени Заявителя, по обращению за получением неквалифицированного сертификата с учетом требований, установленных в соответствии с Порядком;

4.1.2. осуществляет в соответствии с правилами подтверждения владения ключом ЭП подтверждение владения заявителем ключом ЭП, соответствующим ключу проверки ЭП, указанному им для получения неквалифицированного сертификата ключа проверки ЭП;

4.1.3. устанавливает сроки действия неквалифицированных сертификатов ключей проверки ЭП;

4.1.4. аннулирует выданные этим удостоверяющим центром неквалифицированные сертификаты ключей проверки ЭП;

4.1.5. выдает по обращению Заявителя средства ЭП, содержащие ключ ЭП и ключ проверки ЭП (в том числе созданные УЦ) или обеспечивающие возможность создания ключа ЭП и ключа проверки ЭП Заявителем;

4.1.6. ведет реестр выданных и аннулированных УЦ неквалифицированных сертификатов ключей проверки ЭП (далее – реестр неквалифицированных сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных УЦ неквалифицированных сертификатах ключей проверки ЭП, и информацию о датах прекращения действия или аннулирования неквалифицированных сертификатов ключей проверки ЭП и об основаниях таких прекращения или аннулирования;

4.1.7. создает по обращениям Заявителей ключи ЭП и ключи проверки ЭП;

4.1.8. проверяет уникальность ключей проверки ЭП в реестре неквалифицированных сертификатов;

4.1.9. обеспечивает доступ лиц к информации, содержащейся в реестре неквалифицированных сертификатов (к списку отозванных неквалифицированных сертификатов), в том числе с использованием сети Интернет;

4.1.10. осуществляет по обращениям участников электронного взаимодействия проверки электронных подписей;

4.1.11. предоставляет информацию, содержащуюся в реестре неквалифицированных сертификатов, в том числе информацию об аннулировании неквалифицированных сертификата ключа проверки ЭП.

4.2. УЦ осуществляет иную связанную с использованием ЭП УЦ деятельность.

5. ПРАВА И ОБЯЗАННОСТИ УЦ

5.1. УЦ в соответствии с Федеральным законом имеет право:

5.1.1. запросить у Заявителя документы для подтверждения информации, содержащейся в заявлении на создание и выдачу неквалифицированных сертификата;

5.1.2. запросить сведения у операторов базовых государственных информационных ресурсов, в т.ч. с использованием системы межведомственного электронного взаимодействия (СМЭВ) для проверки достоверности документов и сведений, представляемых Заявителями при подаче заявлений на создание и выдачу неквалифицированного сертификата;

5.1.3. не принимать от Заявителя документы, не соответствующие требованиям действующих нормативных правовых актов Российской Федерации;

5.1.4. отказать в регистрации заявления на создание и выдачу неквалифицированного сертификата в случае ненадлежащего его оформления и/или непредставления документов, указанных в Федеральном законе и Порядке;

5.1.5. отказать в прекращении действия неквалифицированного сертификата Владелец неквалифицированного сертификата в случае ненадлежащего оформления соответствующего заявления на прекращение действия неквалифицированного сертификата;

5.1.6. отказать в прекращении действия неквалифицированного сертификата ключа проверки ЭП Владелец неквалифицированного сертификата в случае, если неквалифицированный сертификат ключа проверки ЭП уже аннулирован или прекратил свое действие по другим основаниям, или истек установленный срок действия ключа ЭП, соответствующего неквалифицированному сертификату ключа проверки ЭП;

5.1.7. в одностороннем порядке вносить изменения в Порядок;

5.1.8. наделить третьих лиц (далее – Доверенные лица УЦ) полномочиями по приему заявлений на создание и выдачу неквалифицированных сертификатов ключей проверки ЭП, а также вручению неквалифицированных сертификатов ключей проверки ЭП от имени УЦ Общества;

5.1.9. выдавать неквалифицированные сертификаты ключей проверки ЭП как в форме электронных документов, так и в форме документов на бумажном носителе.

5.2. УЦ в соответствии с Федеральным законом обязан:

5.2.1. информировать Заявителей об условиях и о порядке использования электронных подписей и средств ЭП, о рисках, связанных с использованием электронных

подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

5.2.2. обеспечивать актуальность информации, содержащейся в реестре невалифицированных сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

5.2.3. предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру невалифицированных сертификатов информацию, содержащуюся в реестре невалифицированных сертификатов, в том числе информацию об аннулировании невалифицированного сертификата ключа проверки ЭП;

5.2.4. обеспечивать конфиденциальность созданных УЦ ключей ЭП;

5.2.5. отказать Заявителю в создании невалифицированного сертификата ключа проверки ЭП в случае, если не было подтверждено то, что Заявитель владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному Заявителем для получения невалифицированного сертификата;

5.2.6. отказать Заявителю в создании невалифицированного сертификата ключа проверки ЭП в случае отрицательного результата проверки в реестре невалифицированных сертификатов уникальности ключа проверки ЭП, указанного Заявителем для получения невалифицированного сертификата;

5.2.7. незамедлительно информировать владельца невалифицированного сертификата о выявленных случаях приостановления (прекращения) технической возможности использования ключа ЭП, не предусмотренных соглашением сторон, или возникновения у удостоверяющего центра обоснованных сомнений в получении поручения от уполномоченного соглашением сторон лица об использовании ключа ЭП;

5.2.8. внести в реестр невалифицированных сертификатов информацию о прекращении действия невалифицированного сертификата в течение двенадцати часов с момента наступления следующих обстоятельств:

- в связи с истечением установленного срока его действия;
- на основании заявления Владельца невалифицированного сертификата ключа проверки ЭП, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в случае прекращения деятельности УЦ без перехода его функций другим лицам;
- в иных случаях, установленных Федеральным законом, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами,

или в течение двенадцати часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие невалифицированного сертификата ключа проверки ЭП прекращается с момента внесения УЦ записи об этом в реестр невалифицированных сертификатов;

5.2.9. аннулировать невалифицированный сертификат ключа проверки ЭП в следующих случаях:

- не подтверждено, что Владелец невалифицированного сертификата владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в таком невалифицированном сертификате;

- установлено, что содержащийся в таком невалифицированном сертификате ключ проверки ЭП уже содержится в ином ранее созданном невалифицированном сертификате ключа проверки ЭП;

- вступило в силу решение суда, которым, в частности, установлено, что невалифицированный сертификат ключа проверки ЭП содержит недостоверную информацию;

- с внесением в реестр невалифицированных сертификатов в течение двенадцати часов с момента наступления указанных обстоятельств, или в течение двенадцати часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие невалифицированного сертификата ключа проверки ЭП прекращается с момента внесения записи об этом в реестр невалифицированных сертификатов;

5.2.10. уведомить Владельца невалифицированного сертификата об аннулировании его невалифицированного сертификата до внесения в реестр невалифицированных сертификатов информации об аннулировании невалифицированного сертификата путем направления документа на бумажном носителе или электронного документа;

5.2.11. хранить в течение срока деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации, в форме, позволяющей проверить ее целостность и достоверность, следующую информацию:

- реквизиты основного документа, удостоверяющего личность владельца невалифицированного сертификата - физического лица;

- сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением невалифицированного сертификата;

- сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца неквалифицированного сертификата действовать от имени юридических лиц, государственных органов, органов местного самоуправления, если информация о таких полномочиях владельца неквалифицированного сертификата включена в неквалифицированный сертификат;

5.2.12. для подписания от своего имени неквалифицированных сертификатов использовать неквалифицированную ЭП удостоверяющего центра;

5.2.13. В случае принятия решения о прекращении своей деятельности УЦ обязан:

1) с переходом его функций другим лицам:

- уведомить в письменной форме Владельцев неквалифицированных сертификатов, которые выданы УЦ и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций;

- передать информацию, внесенную в реестр неквалифицированных сертификатов, лицу, к которому перешли функции УЦ.

2) без перехода его функций другим лицам:

- уведомить в письменной форме Владельцев неквалифицированных сертификатов, которые выданы этим УЦ и срок действия которых не истек, не менее чем за один месяц до даты прекращения деятельности УЦ;

- в указанном случае после прекращения деятельности УЦ информация, внесенная в реестр неквалифицированных сертификатов, будет уничтожена.

5.2.14. выполнять Порядок в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций удостоверяющего центра и исполнения обязанностей, а также Федеральным законом и иными нормативными правовыми актами, принимаемыми в соответствии с Федеральным законом.

5.2.15. при выдаче неквалифицированного сертификата УЦ обязан в порядке, установленном Федеральным законом, идентифицировать Заявителя - физическое лицо, обратившееся к нему за получением неквалифицированного сертификата.

5.2.17. ознакомить Владельца неквалифицированного сертификата с информацией, содержащейся в неквалифицированном сертификате, выданном УЦ;

5.2.18. предоставить Владельцу неквалифицированного сертификата руководство по обеспечению безопасности использования ЭП и средств электронной подписи;

5.3. Иные обязанности УЦ определены положениями действующего законодательства Российской Федерации.

**6. ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ),
НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УЦ, В Т.Ч. ТРЕБОВАНИЯ К
ДОКУМЕНТАМ, ПРЕДОСТАВЛЯЕМЫМ В УЦ В РАМКАХ ПРЕДОСТАВЛЕНИЯ
УСЛУГ**

6.1. Процедура создания ключей ЭП и ключей проверки ЭП

6.1.1. Порядок создания ключей ЭП и ключей проверки ЭП с учетом следующих способов создания:

6.1.1.1. Заявитель создает ключ ЭП и ключ проверки ЭП в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09.02.2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (зарегистрирован Министерством юстиции Российской Федерации 03.03.2005 г., регистрационный N 6382), с изменениями, внесенными приказом ФСБ России 12.04.2010 г. N 173 «О внесении изменений в некоторые нормативные правовые акты ФСБ России» (зарегистрирован Министерством юстиции Российской Федерации 25.05.2010 г., регистрационный N 17350). Созданный Заявителем ключ проверки ЭП передается в УЦ в составе файла запроса на сертификат ключа проверки ЭП через личный кабинет в информационной системе УЦ и (или) путем доставки на отчуждаемом носителе в УЦ, при этом формат файла запроса на сертификат ключа проверки ЭП должен соответствовать формату PKCS#10.

6.1.1.2. УЦ создает ключ ЭП и ключ проверки ЭП для Заявителя в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09.02.2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» при выполнении требований, установленных постановлением Правительства Российской Федерации от 03.02.2012 г. N 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (Собрание законодательства Российской Федерации, 2012, N 7, ст. 863; 2016, N 26, ст. 4049) в отношении автоматизированного рабочего места УЦ, используемого для создания ключа ЭП и ключа проверки ЭП для Заявителя.

6.1.1.3. Ключ ЭП и ключ проверки ЭП, предназначенные для создания и проверки усиленного НСКПЭП создаются с использованием средства ЭП.

6.1.2. Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи УЦ:

- 1) истечение срока использования ключа ЭП УЦ для создания НСКПЭП;
- 2) переход на использование новых стандартов ЭП и функции хеширования в соответствии с руководящими документами органа исполнительной власти, уполномоченного в сфере использования ЭП.

6.1.2.1. плановая смена ключа ЭП УЦ выполняется не позднее 15 месяцев с момента начала его действия на основании требований и в соответствии с процедурами, установленными эксплуатационной документацией на средства УЦ;

6.1.2.2. выполнение плановой смены ключа ЭП УЦ осуществляется в следующем порядке:

- УЦ создает новый ключ ЭП и соответствующий ему ключ проверки ЭП;
- УЦ устанавливает в контейнер и формирует ключ электронной подписи.

6.1.2.3. сроки выполнения плановой смены ключа ЭП УЦ устанавливаются нормативно-правовыми и иными законодательными актами, регламентирующими указанное взаимодействие;

6.1.2.4. при плановой замене ключа ЭП УЦ все Владельцы сертификатов должны установить на своих компьютерах новый сертификат УЦ.

6.1.2.5. информирование Владельцев невалифицированных сертификатов о выполнении плановой смены ключа ЭП УЦ осуществляется путем размещения файла нового невалифицированного сертификата ключа проверки ЭП УЦ на Сайте УЦ;

6.1.2.6. Доверенным способом получения нового невалифицированного сертификата УЦ является его публикация на официальном сайте УЦ, доступная для скачивания.

6.1.2.7. ключ ЭП и соответствующий невалифицированный сертификат ключа проверки ЭП УЦ, действовавшие до ввода в действие нового ключа ЭП УЦ, используются УЦ в течение срока их действия для подписания списка аннулированных невалифицированных сертификатов, содержащего сведения о невалифицированных сертификатах, выданных УЦ до ввода в действие нового ключа ЭП УЦ;

6.1.3. Порядок осуществления смены ключей ЭП УЦ в случаях нарушения их конфиденциальности (компрометации):

6.1.3.1. внеплановая смена ключа ЭП УЦ производится при нарушении конфиденциальности (компрометации) ключа ЭП УЦ в случаях наступления событий, связанных со следующими видами угроз нарушения конфиденциальности ключа ЭП УЦ:

- физическая утрата ключевого носителя, содержащего ключ ЭП УЦ;
- нарушение правил хранения и использования ключа ЭП УЦ, установленных эксплуатационной документацией на средства УЦ;
- несанкционированное копирование ключа ЭП УЦ;
- несанкционированный доступ постороннего лица в место размещения технических средств УЦ или подозрение на то, что такое событие имело место быть (нарушение слепков печатей, повреждение замков и т. п.);
- нарушение работоспособности или нештатное функционирование технических средств защиты информации, обрабатываемой на средствах УЦ;

6.1.3.2. в случае компрометации ключа ЭП УЦ немедленно прекращает создание новых неквалифицированных сертификатов ключей проверки ЭП Заявителям с использованием скомпрометированного ключа ЭП УЦ и не позднее двух часов с момента, когда УЦ стало известно о наступлении обстоятельств, вызвавших компрометацию или угрозу компрометации ключа ЭП УЦ, прекращает действия неквалифицированного сертификата ключа проверки ЭП, соответствующего скомпрометированному ключу ЭП УЦ;

6.1.3.3. одновременно со сменой такого ключа ЭП УЦ прекращается действие всех неквалифицированных сертификатов, созданных с использованием этого ключа ЭП УЦ, с занесением сведений об этих неквалифицированных сертификатах в реестр неквалифицированных сертификатов;

6.1.3.4. сроки выполнения внеплановой смены ключа ЭП УЦ устанавливаются нормативно-правовыми и иными законодательными актами, регламентирующими указанное взаимодействие;

6.1.3.5. в случае выполнения внеплановой смены ключа ЭП УЦ прекращается действие всех неквалифицированных сертификатов, подписанных электронной подписью УЦ, созданной с использованием скомпрометированного ключа ЭП УЦ, с включением сведений о прекращении действия этих неквалифицированных сертификатов в реестр сертификатов;

6.1.3.6. в случае выполнения внеплановой смены ключа ЭП УЦ должны быть проведены работы по внеплановой смене ключей ЭП Владельцев неквалифицированных сертификатов, которые подписаны электронной подписью УЦ, созданной с использованием скомпрометированного ключа ЭП УЦ. Создание и выдача новых неквалифицированных сертификатов ключей проверки ЭП осуществляется УЦ безвозмездно в порядке, указанном в подразделе «Процедура создания и выдачи неквалифицированных сертификатов» настоящего документа на срок, указанный в поле

notAfter поля Validity сертификата, подлежащего внеплановой смене, с пролонгацией на срок равный времени (в днях) с момента прекращения действия и до момента выпуска нового неквалифицированного сертификата;

6.1.3.7. информирование Владельцев неквалифицированных сертификатов, подписанных электронной подписью УЦ, созданной с использованием скомпрометированного ключа ЭП УЦ, о внеплановой смене ключа ЭП УЦ и, соответственно, о прекращении действия выданных им неквалифицированных сертификатов, осуществляется путем размещения соответствующей информации на Сайте УЦ, а также путем уведомления по электронной почте;

6.1.3.8. Доверенным способом получения нового неквалифицированного сертификата УЦ является его публикация на официальном сайте УЦ, доступная для скачивания и исключающая уничтожение, модифицирование, блокирование при передаче и иные неправомерные действия с неквалифицированным сертификатом.

6.1.4. Порядок осуществления Удостоверяющим центром смены ключа ЭП владельца неквалифицированного сертификата:

6.1.4.1. смена ключа ЭП владельца неквалифицированного сертификата осуществляется в случаях, указанных в пунктах 1, 2, 4 части 6 и части 6.1 статьи 14 Федерального закона;

6.1.4.2. смена ключей ЭП Владельца неквалифицированного сертификата осуществляется вместе с процедурой создания и выдачи неквалифицированного сертификата в соответствии с требованиями подраздела «Процедура создания и выдачи неквалифицированных сертификатов» настоящего Порядка. При плановой и внеплановой смене ключей ЭП и неквалифицированного сертификата ключа проверки ЭП заявление от Владельца неквалифицированного сертификата подается по форме Приложения № 1 к Порядку в соответствии с категорией Заявителя (далее – «заявление на создание и выдачу неквалифицированного сертификата»). Требования к заявлению на создание и выдачу неквалифицированного сертификата, в том числе состав реквизитов такого заявления, указаны в подразделе «Процедура создания и выдачи неквалифицированных сертификатов» Порядка;

6.1.4.3. заявление на создание и выдачу неквалифицированного сертификата по форме Приложения № 1 к Порядку может быть создано в форме электронного документа, подписанного действующей квалифицированной электронной подписью Заявителя, либо подписанного неквалифицированной электронной подписью Заявителя, сформированной действующим неквалифицированным сертификатом ключа проверки электронной подписи, выданный ранее УЦ ООО «ЭТП ГПБ Консалтинг», либо

посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемыми Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" (далее - единая система идентификации и аутентификации) и информации из государственной информационной системы "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных" (далее - единая биометрическая система).

6.1.4.4. обязательным приложением к заявлению на создание и выдачу нового неквалифицированного сертификата является запрос на сертификат, сформированный с использованием средства ЭП, установленного на автоматизированном рабочем месте Заявителя, который должен быть подписан квалифицированной электронной подписью, Заявителя, либо неквалифицированной электронной подписью Заявителя, сформированной действующим сертификатом ключа проверки электронной подписи, выданным ранее УЦ ООО «ЭТП ГПБ Консалтинг», и передан в УЦ;

6.1.4.5. плановая смена ключей ЭП и неквалифицированного сертификата ключа проверки ЭП проводится Владелец сертификата не ранее одного календарного месяца до даты истечения действующего сертификата, указанной в поле notAfter поля Validity сертификата. Способ создания ключей ЭП при плановой смене ключей ЭП соответствует изложенному в настоящем разделе;

6.1.4.6. внеплановая смена ключа ЭП и ключа проверки ЭП осуществляется в следующих случаях, связанных с нарушением конфиденциальности ключа ЭП или угрозой нарушения его конфиденциальности:

- Владелец неквалифицированного сертификата не осуществил плановую смену в установленные настоящим Порядком сроки;
- произошла компрометация ключа ЭП Владельца неквалифицированного сертификата;
- изменились сведения, включенные в неквалифицированный сертификат;
- при компрометации ключа ЭП УЦ;

6.1.4.7. при внеплановой смене ключа ЭП и ключа проверки ЭП Владелец неквалифицированного сертификата немедленно прекращает использование скомпрометированного ключа ЭП и выполняет требования подраздела «Процедуры, осуществляемые при прекращении действия и аннулировании неквалифицированного сертификата» Порядка, способы создания ключей ЭП при внеплановой смене ключей ЭП соответствуют изложенному в настоящем разделе.

6.2. Процедура создания и выдачи неквалифицированных сертификатов

6.2.1. Порядок подачи заявления на создание и выдачу неквалифицированного сертификата:

6.2.1.1. Заявитель лично подаёт заявление на создание и выдачу неквалифицированного сертификата по форме Приложения № 1 к Порядку в соответствии с категорией Заявителя в форме документа на бумажном носителе в Удостоверяющий центр либо Доверенному лицу УЦ;

6.2.1.2. Заявитель лично подаёт заявление на создание и выдачу неквалифицированного сертификата по форме Приложения № 1 к Порядку в соответствии с категорией Заявителя в форме электронного документа, подписанного действующей электронной подписью Заявителя в УЦ.

6.2.2. Требования к заявлению на создание и выдачу неквалифицированного сертификата:

6.2.2.1. Заявление на создание и выдачу неквалифицированного сертификата по форме Приложения №1 к Порядку в соответствии с категорией Заявителя может быть подано Заявителем как в форме документа на бумажном носителе, так и в форме электронного документа, подписанного действующей квалифицированной электронной подписью Заявителя, либо подписанного неквалифицированной электронной подписью Заявителя, сформированной действующим сертификатом ключа проверки электронной подписи, выданный ранее УЦ ООО «ЭТП ГПБ Консалтинг», либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемыми Правительством Российской Федерации¹, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из федеральной государственной информационной системы "Единая система идентификации и аутентификации в

¹ Постановление Правительства Российской Федерации от 25.01.2013 г. N 33 "Об использовании простой электронной подписи при оказании государственных и муниципальных услуг".

инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" (далее - единая система идентификации и аутентификации)² и информации из государственной информационной системы "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных" (далее - единая биометрическая система)³

6.2.2.2. В заявлении на создание и выдачу сертификата по форме Приложения № 1 к Порядку для Владельца неквалифицированного сертификата – физического лица должны быть указаны: фамилия, имя, отчество (если имеется), страховой номер индивидуального лицевого счета и идентификационный номер налогоплательщика Владельца неквалифицированного сертификата - физического лица.

6.2.2.3. В заявлении на создание и выдачу сертификата по форме Приложения № 1 к Порядку для Владельца неквалифицированного сертификата – физического лица указываются и иные сведения в соответствии с требованиями Федерального закона, иных федеральных законов и нормативно-правовых актов Российской Федерации, относящих требования к данному виду документов.

6.2.3. Порядок идентификации Заявителя, обратившегося с заявлением на создание и выдачу неквалифицированного сертификата:

6.2.3.1. идентификация гражданина Российской Федерации осуществляется:

- при его личном присутствии по основному документу, удостоверяющему личность;
- без его личного присутствия:

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

² Постановление Правительства Российской Федерации от 28.11.2011 г. N 977 "О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме".

³ Пункт 4 статьи 2 Федерального закона от 29.12.2022 г. N 572-ФЗ "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации".

проведении эксперимента по совершенствованию применения технологии электронной подписи";

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

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

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

6.2.4. Перечень документов, запрашиваемых УЦ у Заявителя для создания и выдачи неквалифицированного сертификата:

- основной документ, удостоверяющий личность;
- страховой номер индивидуального лицевого счета Заявителя - физического лица (может предоставляться в виде сведений);
- идентификационный номер налогоплательщика Заявителя - физического лица (может предоставляться в виде сведений);

6.2.4.1. Заявитель вправе по собственной инициативе представить копии документов, содержащих сведения, необходимые для создания и выдачи неквалифицированного сертификата.

6.2.4.2. В случае если для подтверждения сведений, вносимых в неквалифицированный сертификат, законодательством Российской Федерации установлена определенная форма документа, заявитель представляет в УЦ документ соответствующей формы.

6.2.4.3. Надлежащим способом заверения копий документов может являться нотариальное заверение копий, заверение копий органом власти, заверение копий документов Заявителем самостоятельно. При необходимости копии с документов могут быть сняты и заверены работником УЦ или Доверенным лицом УЦ.

6.2.4.4. Нотариально заверенные копии документов должны содержать штамп нотариуса «копия верна», штамп с информацией о нотариусе, должны быть заверены печатью нотариуса и иметь подпись нотариуса. Нотариальное совершение заверения

документа должно быть осуществлено не позднее 30 (тридцати) дней до момента подачи в УЦ или Доверенному лицу УЦ.

6.2.4.5. Копии документов, изданных и хранимых Заявителем, должны быть заверены не позднее 30 (тридцати) дней до момента подачи в УЦ или Доверенному лицу УЦ. На последнем листе копии (выписки из документа) на свободном месте под текстом оформляется реквизит «Отметка о заверении копии», придающий копии документа юридическую силу и включающий: слова «Копия верна», указание о месте нахождения подлинника документа, наименование должности лица, заверившего копию, личную подпись, расшифровку подписи, дату заверения и оттиск печати. Листы многостраничных копий (выписок из документов) нумеруются, отметка о заверении копии дополняется указанием количества листов копии (выписки из документа): «Всего в копии (выписки из документа) ____ листов». Допускается заверять отметкой «Копия верна» каждый лист многостраничной копии документа.

6.2.4.6. Копии документов, заверенные органом власти, должны содержать подпись и расшифровку подписи должностного лица, их заверившего, а также печать (штамп) данного органа власти.

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

6.2.4.8. Документы и/или их надлежащим образом заверенные копии, представленные в УЦ для создания и выдачи неквалифицированного сертификата, остаются на хранении в УЦ и возврату не подлежат.

6.2.5. Порядок проверки достоверности документов и сведений, представленных Заявителем:

6.2.5.1. для заполнения неквалифицированного сертификата УЦ запрашивает и получает из государственных информационных ресурсов следующие сведения:

- Сведения о соответствии паспортных данных и ИНН физического лица;
- Сведения о соответствии фамильно-именной группы, даты рождения, пола и СНИЛС;
- Сведения о действительности паспорта.

6.2.5.2. в случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной Заявителем для включения в неквалифицированный сертификат, и УЦ (Доверенное лицо УЦ) идентифицировал Заявителя - физическое лицо, УЦ осуществляет процедуру создания и

выдачи Заявителю неквалифицированного сертификата. В ином случае УЦ отказывает Заявителю в выдаче неквалифицированного сертификата и приема заявления на создание и выдачу квалифицированного сертификата по форме Приложения № 1 к Порядку в соответствии с категорией Заявителя;

6.2.5.3. в случае подтверждения достоверности сведений, указанных в заявлении на создание и выдачу неквалифицированного сертификата по форме Приложения № 1 к Порядку и предоставленных документах, по информации, полученной из государственных информационных ресурсов, Оператор УЦ или Доверенное лицо УЦ осуществляет регистрацию заявления на создание и выдачу неквалифицированного сертификата.

6.2.6. Порядок создания неквалифицированного сертификата:

6.2.6.1. Оператор УЦ приступает к созданию неквалифицированного сертификата при получении от Заявителя запроса на сертификат, основанного на ключе проверки ЭП, созданного в соответствии с требованиями Порядка, после исполнения процедур по идентификации Заявителя, проверки документов, представленных Заявителем, и сведений из них в соответствии с Порядком;

6.2.6.2. Оператор УЦ создает неквалифицированный сертификат с данными, указанными в заявлении на создание и выдачу сертификата по форме Приложения № 1 к Порядку и запросе сертификата в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09.02.2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

6.2.6.3. при создании ключа ЭП и ключа проверки ЭП, созданного в соответствии с требованиями настоящего Порядка, Оператор УЦ создает неквалифицированный сертификат с данными, указанными в заявлении на создание и выдачу неквалифицированного сертификата по форме Приложения № 1 к Порядку и запросе сертификата в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09.02.2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

6.2.6.4. созданный неквалифицированный сертификат в электронной форме записывается на ключевой носитель Владельца сертификата либо Оператором УЦ, либо Владельцем сертификата самостоятельно с использованием личного кабинета информационной системы УЦ, в зависимости от того, какой способ формирования ключей ЭП был выбран Заявителем.

6.2.7. Порядок выдачи неквалифицированного сертификата:

6.2.7.1. при получении неквалифицированного сертификата Заявителем он должен быть ознакомлен УЦ с информацией, содержащейся в неквалифицированном сертификате. Подтверждение ознакомления с информацией, содержащейся в неквалифицированном сертификате, осуществляется под расписку посредством использования Заявителем квалифицированной ЭП при наличии у него действующего квалифицированного сертификата, либо подписанного неквалифицированной электронной подписью Заявителя, сформированной действующим сертификатом ключа проверки электронной подписи, выданный ранее УЦ ООО «ЭТП ГПБ Консалтинг», либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы. Указанное согласие, подписанное ЭП, в том числе простой ЭП, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного физического лица. УЦ обязан хранить информацию, подтверждающую ознакомление Заявителя с информацией, содержащейся в неквалифицированном сертификате, в течение всего срока осуществления своей деятельности.

6.2.7.2. при получении неквалифицированного сертификата Владелец ознакомливается с Руководством по обеспечению безопасности использования неквалифицированной электронной подписи и средств электронной подписи (Приложение № 4 к Порядку).

6.2.8. Срок создания и выдачи неквалифицированного сертификата с момента получения и регистрации УЦ или Доверенным лицом УЦ соответствующего заявления не должен превышать 3 (трех) рабочих дней при наличии запроса сертификата и подтверждения достоверности сведений и документов, предоставленных Заявителем.

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

6.3.1. Требования к заявлению на подтверждение действительности электронной подписи в электронном документе, в том числе перечень прилагаемых к такому заявлению документов:

6.3.1.1. подтверждение действительности ЭП, использованной для подписания электронных документов, созданной с использованием сертификата ЭП, созданным в УЦ, осуществляется на основании заявления заинтересованного лица. Заявление на подтверждение действительности электронной подписи в электронном документе оформляется по форме Приложения № 3 к Порядку.

6.3.1.2. заявление на подтверждение действительности электронной подписи в электронном документе должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные Заявителя, подлинность ЭП которого необходимо подтвердить в электронном документе;
- время и дата формирования ЭП электронного документа;
- время и дата, на момент наступления которых требуется установить подлинность ЭП.

6.3.1.3. обязательным приложением к заявлению на подтверждение действительности ЭП в электронном документе является носитель, содержащий:

- файл сертификата, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе;
- электронный документ – в виде одного файла, содержащего данные и значение ЭП этих данных, либо двух файлов: один из которых содержит данные, а другой значение ЭП этих данных.

6.3.2. Срок предоставления услуги по подтверждению действительности электронной подписи в электронном документе не может превышать 5 (пяти) рабочих дней с момента получения и регистрации Оператором УЦ соответствующего заявления.

6.3.3. Порядок оказания услуги:

6.3.3.1. УЦ обеспечивает подтверждение подлинности ЭП в электронном документе, если формат электронного документа с ЭП соответствует стандарту криптографических сообщений Criptographic Message Syntax (CMS – стандарт криптографических сообщений, описанный в RFC 3852 и RFC 3369). Решение о соответствии электронного документа с ЭП стандарту CMS принимает УЦ. В случае, если

электронный документ не соответствует стандарту CMS, УЦ отказывает Заявителю в проведении процедуры подтверждения действительности ЭП.

6.3.3.2. Проведение работ по подтверждению подлинности ЭП в электронном документе осуществляет комиссия, сформированная из числа работников УЦ.

6.3.3.3. Комиссия осуществляет проверку действительности всех сертификатов, включенных в последовательность проверки от проверяемого сертификата до сертификата УЦ, предназначенные для подтверждения подлинности ЭП в электронном документе.

6.3.3.4. Результатом проведения работ по подтверждению подлинности ЭП в электронном документе является заключение УЦ. Заключение УЦ содержит:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- результат проверки ЭП электронного документа;
- данные, представленные комиссии для проведения проверки;
- отчет по выполненной проверке.

6.3.3.5. Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- содержание и результаты проверки.

6.3.3.6. Заключение УЦ по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью УЦ. Один экземпляр заключения по выполненной проверке должен быть предоставлен Заявителю.

6.4. Процедуры, осуществляемые при прекращении действия и аннулирования невалифицированного сертификата

6.4.1. Основания прекращения действия или аннулирования невалифицированного сертификата:

6.4.1.1. невалифицированный сертификат прекращает свое действие в случаях, установленных статьей 14 Федерального закона;

6.4.1.2. УЦ признает невалифицированный сертификат аннулированным, если:

- не подтверждено, что Владелец невалифицированного сертификата владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в таком невалифицированном сертификате;

- установлено, что содержащийся в невалифицированном сертификате ключ проверки ЭП уже содержится в ином ранее созданном невалифицированном сертификате;
- вступило в силу решение суда, которым установлено, что невалифицированный сертификат содержит недостоверную информацию;

6.4.2. Порядок действий УЦ при прекращении действия (аннулировании) невалифицированного сертификата:

6.4.2.1. Заявление на прекращение действия невалифицированного ключа проверки электронной подписи (далее – «заявление на прекращение действия невалифицированного сертификата») сертификата оформляется Владелец невалифицированного сертификата по форме Приложения № 2 к Порядку и должно содержать:

- серийный номер невалифицированного сертификата;
- даты начала и окончания действия невалифицированного сертификата;
- фамилия, имя, отчество (при наличии) Владельца невалифицированного сертификата;
- страховой номер индивидуального лицевого счета;
- идентификационный номер налогоплательщика;
- наименование аккредитованного удостоверяющего центра, выдавшего невалифицированный сертификат;
- причины отзыва (аннулирования) невалифицированного сертификата;
- иные необходимые реквизиты, включая подпись, печать.

6.4.2.2. Заявление на прекращение действия невалифицированного сертификата может быть направлено как в форме документа на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной ЭП, либо невалифицированной электронной подписью Заявителя, сформированной действующим сертификатом ключа проверки электронной подписи, выданный ранее УЦ ООО «ЭТП ГПБ Консалтинг»:

6.4.2.2.1. заявление на прекращение действия сертификата, подаваемое в форме документа на бумажном носителе, должно быть подписано собственноручной подписью лица, указанного в качестве Владельца сертификата. Заявление на прекращение действия невалифицированного сертификата, выданного юридическому лицу, может быть подписано собственноручной подписью лица, имеющего право без доверенности действовать от имени юридического лица.

6.4.2.2.2. заявление на прекращение действия неквалифицированного сертификата, подаваемое в форме электронного документа, должно быть подписано усиленной квалифицированной ЭП Владельца неквалифицированного сертификата, либо неквалифицированной электронной подписью Заявителя, сформированной действующим сертификатом ключа проверки электронной подписи, выданный ранее УЦ ООО «ЭТП ГПБ Консалтинг», при этом в случае, если прекращение действия неквалифицированного сертификата связано с компрометацией ключа ЭП, то заявление на прекращение действия неквалифицированного сертификата должно быть подписано иной действующей усиленной неквалифицированной электронной подписью Владельца неквалифицированного сертификата.

6.4.2.3. УЦ осуществляет прием заявления на прекращение действия неквалифицированного сертификата при условии установления личности лица, подающего такое заявление, либо полномочий лица, подающего такое заявление от имени юридического лица, в случае подачи такого заявления в форме документа на бумажном носителе, или при установлении действительности электронной подписи, которой подписано заявление на прекращение действия неквалифицированного сертификата, подаваемое в форме электронного документа.

6.4.2.4. При ошибках в оформлении заявления на прекращение действия неквалифицированного сертификата или несовпадении данных из представленного заявления на прекращение действия неквалифицированного сертификата с данными, хранящимися в реестре УЦ, Оператор УЦ имеет право отказать Заявителю в регистрации заявления на прекращение действия неквалифицированного сертификата и прекращении действия (аннулирования) сертификата или запросить дополнительные документы, подтверждающие изменение данных по своему усмотрению.

6.4.3. Порядок внесения информации о прекращении действия или аннулировании неквалифицированного сертификата в реестр неквалифицированных сертификатов:

6.4.3.1. Внесение информации о прекращении действия или аннулировании неквалифицированного сертификата в реестр неквалифицированных сертификатов осуществляется путем внесения соответствующей информации в список прекративших действие или аннулированных неквалифицированных сертификатов.

6.4.3.2. УЦ вносит информацию о прекращении действия или аннулировании неквалифицированного сертификата в реестр неквалифицированных сертификатов в срок, не превышающий двенадцать часов с момента наступления обстоятельств, указанных в настоящем разделе или в течение двенадцати часов с момента получения УЦ соответствующих сведений.

6.4.3.3. До внесения в реестр невалифицированных сертификатов информации об аннулировании невалифицированного сертификата УЦ уведомляет Владельца сертификата об аннулировании его невалифицированного сертификата путем направления уведомления в форме бумажного или электронного документа.

6.4.3.4. Официальным уведомлением о факте прекращения действия невалифицированного сертификата является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения об аннулированном сертификате, и изданного не ранее времени наступления произошедшего случая.

6.4.3.5. Временем опубликования списка аннулированных невалифицированных сертификатов признается включенное в список аннулированных невалифицированных сертификатов время его создания.

6.4.3.6. Датой и временем аннулирования или прекращения действия невалифицированного сертификата признается дата и время внесения информации о невалифицированном сертификате, который был аннулирован или действие которого было досрочно прекращено, в список аннулированных невалифицированных сертификатов.

6.4.3.7. В случае прекращения действия невалифицированного сертификата по истечении установленного срока его действия временем прекращения действия сертификата признается время, хранящееся в поле `notAfter` поля `Validity` сертификата. В данном случае информация о невалифицированном сертификате в список отозванных невалифицированных сертификатов не заносится.

6.4.3.8. Информация о размещении списка отозванных невалифицированных сертификатов заносится в созданные УЦ сертификаты в расширение `CRL Distribution Point` сертификата ключа проверки ЭП.

6.4.3.9. УЦ осуществляет размещение реестра невалифицированных сертификатов и списков отозванных сертификатов в сети Интернет на Сайте УЦ.

6.5. Порядок ведения реестра невалифицированных сертификатов:

6.5.1. Реестр невалифицированных сертификатов ведется УЦ в электронной форме в соответствии с требованиями, установленными Порядком формирования и ведения реестров выданных удостоверяющими центрами невалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, включая требования к формату предоставления такой информации, утвержденным приказом Минцифры России от 08.11.2021 г. N 1138, и кроме информации, содержащейся в невалифицированных сертификатах, включает также информацию о датах прекращения действия или аннулирования невалифицированных сертификатов и об

основаниях прекращения действия или аннулирования, а также иную информацию, подлежащую включению в реестр в соответствии с требованиями нормативных правовых документов.

6.5.1.1. УЦ вносит информацию о созданном неквалифицированном сертификате ключа проверки электронной подписи в реестр сертификатов не позднее указанной в нем даты начала действия такого сертификата.

6.5.1.2. УЦ вносит информацию о неквалифицированном сертификате, который был аннулирован или действие которого было досрочно прекращено, в реестр неквалифицированных сертификатов в течение 12 (двенадцати) часов с момента возникновения обстоятельств, послуживших основанием для аннулирования или прекращения действия неквалифицированного сертификата или в течение 12 (двенадцати) часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств.

6.5.2. Информация, внесенная в реестр неквалифицированных сертификатов, подлежит хранению в течение всего срока деятельности УЦ, если более короткий срок не установлен нормативными правовыми актами Российской Федерации.

6.5.3. Хранение информации, содержащейся в реестре неквалифицированных сертификатов, осуществляется в защищенных базах данных УЦ и в электронных архивах в форме, позволяющей проверить ее целостность и достоверность. Формирование и ведение единого реестра осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему.

6.6. Порядок технического обслуживания реестра неквалифицированных сертификатов:

6.6.1. Максимальные сроки проведения технического обслуживания реестра неквалифицированных сертификатов не могут превышать 3 (трех) дней.

6.6.2. УЦ заблаговременно оповещает Владельцев неквалифицированных сертификатов и иных лиц, использующих реестр неквалифицированных сертификатов, о планируемом проведении планового или внепланового технического обслуживания реестра неквалифицированных сертификатов путем размещения соответствующего уведомления на Сайте УЦ.

7. ПРОЦЕДУРА ПОДТВЕРЖДЕНИЯ ВЛАДЕНИЯ ЗАЯВИТЕЛЕМ КЛЮЧОМ ЭЛЕКТРОННОЙ ПОДПИСИ ПРИ ВЫПУСКЕ УНЭП

7.1. Общие положения

7.1.1. Настоящий раздел определяет порядок подтверждения владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному для получения сертификата ключа проверки усиленной неквалифицированной электронной подписи (УНЭП).

7.1.2. Процедура установлена во исполнение Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и приказа ФСБ России от 20.04.2021 № 154 «Об утверждении Правил подтверждения владения ключом электронной подписи».

7.1.3. Настоящий порядок является частью локального нормативного акта УЦ и обязателен для сотрудников и доверенных лиц, участвующих в выпуске сертификатов УНЭП.

7.2. Участники процедуры

7.2.1. Подтверждение владения ключом осуществляется оператором УЦ или доверенным лицом, уполномоченным на приём заявлений и выдачу сертификатов УНЭП.

7.2.2. Руководитель УЦ обеспечивает контроль за правильностью исполнения процедуры.

7.3. Порядок подтверждения владения ключом

7.3.1. Подтверждение владения закрытым ключом заявителя осуществляется посредством его идентификации с использованием простой электронной подписи, ключ которой был получен при личной явке заявителя в соответствии с Правилами использования простой электронной подписи при оказании государственных и муниципальных услуг, утверждёнными постановлением Правительства РФ от 25.01.2013 № 33.

7.3.2. Организация взаимодействия с заявителем обеспечивается через Единую систему идентификации и аутентификации (ЕСИА) с применением средств защиты информации, прошедших процедуру оценки соответствия.

7.3.3. При успешной идентификации и проверке достоверности данных в ЕСИА владение заявителем закрытым ключом подтверждается.

7.3.4. В случае невозможности подтверждения владения ключом выпуск сертификата УНЭП прекращается, заявителю направляется мотивированный отказ.

7.4. Фиксация результатов

7.4.1. Все действия фиксируются в электронном журнале (логах УЦ) с обязательным указанием:

- даты и времени процедуры;
- данных заявителя (ФИО, идентификатор ЕСИА);
- результата проверки (успешно/отказ).

7.4.2. Журнал ведётся в электронном виде и хранится в сроки, установленные внутренними регламентами УЦ.

7.5. Заключительные положения

7.5.1. Настоящий порядок применяется исключительно к операциям по выпуску и выдаче неквалифицированных сертификатов (УНЭП).

7.5.2. Изменения и дополнения в процедуру вносятся в установленном порядке приказом генерального директора.

8. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УЦ

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

8.1.1. УЦ осуществляет информирование Заявителей об условиях и о порядке использования электронных подписей и средств ЭП, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, путем включения этой информации в выдаваемое каждому Владелецу неквалифицированного сертификата Руководство по обеспечению безопасности использования неквалифицированной электронной подписи и средств электронной подписи;

8.1.2. Руководство по обеспечению безопасности использования неквалифицированной электронной подписи и средств электронной подписи, содержащее указанную информацию, публикуется также на Сайте УЦ.

8.2. Выдача по обращению Заявителя средств электронной подписи

8.2.1. Средства ЭП, выдаваемые УЦ Заявителю, должны иметь подтверждение соответствия требованиям, установленным в соответствии с частью 4 статьи 6 Федерального закона и обеспечивать возможность проверки всех усиленных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными электронными подписями.

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

8.3.1. Актуальность информации, содержащейся в реестре неквалифицированных сертификатов, обеспечивается путем выполнения УЦ порядка ведения реестра неквалифицированных сертификатов, изложенного в настоящем Порядке, а также защиты указанной информации от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

8.3.2. Защита информации, содержащейся в реестре неквалифицированных сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий обеспечивается комплексом организационно-технических мероприятий, осуществляемых УЦ в соответствии с требованиями, установленными

эксплуатационной документацией на средства УЦ, а также требованиями, установленными в области технической защиты информации.

8.4. Обеспечение доступности реестра неквалифицированных сертификатов в информационно-телекоммуникационной сети Интернет в любое время, за исключением периодов технического обслуживания реестра неквалифицированных сертификатов

8.4.1. Информация, содержащаяся в реестре неквалифицированных сертификатов УЦ, доступна любому лицу в любое время, за исключением периодов технического обслуживания реестра неквалифицированных сертификатов на Сайте УЦ.

8.5. Порядок обеспечения конфиденциальности созданных УЦ ключей электронных подписей:

8.5.1. Конфиденциальность созданных УЦ ключей электронных подписей обеспечивается комплексом организационно-технических мероприятий, осуществляемых УЦ в соответствии с требованиями, установленными:

- нормативными документами федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, в отношении безопасности информации автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации;
- эксплуатационной документацией на средства УЦ и средства ЭП.

8.5.2. УЦ не осуществляет архивирование или хранение ключей электронных подписей, созданных по запросу Заявителей, за исключением случаев применения технологии дистанционного хранения ключей ЭП их Владельцев, при условии, что такая услуга указана в Прайс-листе.

8.5.3. В случае применения технологии дистанционного хранения ключей ЭП, конфиденциальность, условия временного хранения ключей ЭП, условия и сроки их уничтожения обеспечиваются комплексом организационно-технических мероприятий, осуществляемых УЦ в соответствии с требованиями, установленными:

- нормативными документами федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, в отношении безопасности информации автоматизированных систем,

предназначенных для хранения и обработки конфиденциальной информации;

– эксплуатационной документацией на средства УЦ и средства ЭП.

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

8.6.1. Доступ к информации, содержащейся в реестре невалифицированных сертификатов, включая информацию о прекращении действия или аннулировании невалифицированного сертификата, предоставляется безвозмездно любому лицу в соответствии с порядком, указанным в пункте 7.4 Порядка.

9. СПИСОК ПРИЛОЖЕНИЙ

Приложение №1. Форма заявления на создание и выдачу неквалифицированного сертификата ключа проверки электронной подписи.

Приложение №2. Форма заявления на прекращение действия (аннулирование) неквалифицированного сертификата ключа проверки электронной подписи.

Приложение №3. Форма заявления на подтверждение подлинности электронной подписи в электронном документе.

Приложение №4. Руководство по обеспечению безопасности использования неквалифицированной электронной подписи и средств электронной подписи.

Приложение №5. Форма сертификата на бумажном носителе.

Приложение № 6. Профиль неквалифицированного сертификата.

9.1. Приложение №1 к Порядку УЦ ООО «ЭТП ГПБ Консалтинг». Форма заявления на создание и выдачу неквалифицированного сертификата ключа проверки электронной подписи.

(для физических лиц)

Заявление на создание и выдачу неквалифицированного сертификата ключа проверки электронной подписи в Удостоверяющем центре ООО «ЭТП ГПБ Консалтинг» *

От _____
(фамилия, имя, отчество)

_____ (серия и номер паспорта, код подразделения, дата выдачи)

Прошу сформировать ключи электронной подписи и создать неквалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

CommonName (CN)	ФИО владельца сертификата
E-Mail (E)	Адрес электронной почты владельца сертификата
Surname	Фамилия владельца сертификата
GivenName	Имя и отчество владельца сертификата
StreetAddress	Адрес регистрации владельца сертификата
Locality (L)	Наименование населенного пункта по адресу регистрации владельца сертификата
State (S)	Субъект Федерации по адресу регистрации пользователя владельца сертификата
Country (C)	Страна (RU)
INN	ИНН владельца сертификата
SNILS	СНИЛС владельца сертификата

Полностью и безусловно присоединяюсь к Порядку УЦ ООО «ЭТП ГПБ Консалтинг», условия которого определены ООО «ЭТП ГПБ Консалтинг».

С Порядком УЦ ООО «ЭТП ГПБ Консалтинг», приложениями к нему и с Руководством по обеспечению безопасности использования неквалифицированной электронной подписи ознакомлен и обязуюсь соблюдать все положения указанных документов.

Настоящим подтверждаю факт ознакомления с указанным в Порядке перечнем рисков, возникающих при проведении операций с использованием неквалифицированной электронной подписи и средств электронной подписи. Я понимаю, что перечень рисков, указанный в Порядке, не может раскрыть все возможные риски и другие аспекты использования неквалифицированной электронной подписи и средств электронной подписи. Риски, связанные с использованием неквалифицированной электронной подписи и средств электронной подписи, мне понятны и принимаются полностью.

Я свободно, своей волей и своим интересе в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», в целях идентификации Заявителя,

* Заявление на создание и выдачу сертификата ключа проверки электронной подписи в УЦ ООО «ЭТП ГПБ Консалтинг» подается в УЦ или Доверенному лицу УЦ в двух экземплярах. После регистрации заявления один экземпляр предоставляется Заявителю. В случае создания формы Заявления в автоматизированной системе УЦ, приоритетной считается такая форма.

создания и выдачи Заявителю неквалифицированного сертификата ключа проверки электронной подписи, оказания консультационных услуг о создании и выдаче неквалифицированного сертификата, оказания услуг технической поддержки по использованию сопутствующего программного обеспечения для управления неквалифицированными сертификатами ключа проверки электронной подписи даю согласие на обработку в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» своих персональных данных, а именно: фамилии, имени и отчества, контактом(ых) телефоне(ах), адресе электронной почты, СНИЛС, ИНН, пола, паспортных данных (серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта, адрес регистрации) как с использованием средств автоматизации, так и без использования таких средств, включая совершение с ними следующих действий: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, блокирование, удаление, уничтожение и передачу.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

Заявитель

_____ / _____

"__" ____ 20__ г.

Отметка Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»

Данное заявление на создание и выдачу сертификата зарегистрировано в реестре УЦ.
Регистрационный № _____ от «__» _____ 20__ г.

(должность/полномочия)

_____ / _____

«__» _____ 20__ г.

(для индивидуальных предпринимателей)

Заявление на создание и выдачу неквалифицированного сертификата ключа проверки электронной подписи в Удостоверяющем центре ООО «ЭТП ГПБ Консалтинг» *

Настоящим _____
(наименование организации, включая организационно-правовую форму, ОГРНИП, ИНН)

Прошу сформировать ключи электронной подписи и создать неквалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

CommonName (CN)	ФИО владельца сертификата
E-Mail (E)	Адрес электронной почты владельца сертификата
Surname	Фамилия владельца сертификата
GivenName	Имя и отчество владельца сертификата
StreetAddress	Адрес регистрации владельца сертификата
Locality (L)	Наименование населенного пункта по адресу регистрации владельца сертификата
State (S)	Субъект Федерации по адресу регистрации пользователя владельца сертификата
Country (C)	Страна (RU)
OGRNIP	ОГРНИП владельца сертификата
INN	ИНН владельца сертификата
SNILS	СНИЛС владельца сертификата

Полностью и безусловно присоединяюсь к Порядку УЦ ООО «ЭТП ГПБ Консалтинг», условия которого определены ООО «ЭТП ГПБ Консалтинг».

С Порядком УЦ ООО «ЭТП ГПБ Консалтинг», приложениями к нему и с Руководством по обеспечению безопасности использования неквалифицированной электронной подписи ознакомлен и обязуюсь соблюдать все положения указанных документов.

Настоящим подтверждаю факт ознакомления с указанным в Порядке перечнем рисков, возникающих при проведении операций с использованием неквалифицированной электронной подписи и средств электронной подписи. Я понимаю, что перечень рисков, указанный в Порядке, не может раскрыть все возможные риски и другие аспекты использования неквалифицированной электронной подписи и средств электронной подписи. Риски, связанные с использованием неквалифицированной электронной подписи и средств электронной подписи, мне понятны и принимаются полностью.

Я свободно, своей волей и своим интересе в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», в целях идентификации Заявителя, создания и выдачи Заявителю неквалифицированного сертификата ключа проверки электронной подписи, оказания консультационных услуг о создании и выдаче неквалифицированного сертификата, оказания услуг технической поддержки по использованию сопутствующего программного обеспечения для управления

* Заявление на создание и выдачу сертификата ключа проверки электронной подписи в УЦ ООО «ЭТП ГПБ Консалтинг» подается в УЦ или Доверенному лицу УЦ в двух экземплярах. После регистрации заявления один экземпляр предоставляется Заявителю. В случае создания формы Заявления в автоматизированной системе УЦ, приоритетной считается такая форма.

неквалифицированными сертификатами ключа проверки электронной подписи даю согласие на обработку в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» своих персональных данных, а именно: фамилии, имени и отчества, контактом(ых) телефоне(ах), адресе электронной почты, СНИЛС, ИНН, пола, паспортных данных (серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта, адрес регистрации) как с использованием средств автоматизации, так и без использования таких средств, включая совершение с ними следующих действий: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, блокирование, удаление, уничтожение и передачу.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

Заявитель

_____/_____

"__" ____ 20__ г.

М.П.

Отметка Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»

Данное заявление на создание и выдачу сертификата зарегистрировано в реестре УЦ.
Регистрационный № _____ от «__» _____ 20__ г.

(должность/полномочия)

_____/_____

«__» _____ 20__ г.

(для юридических лиц)

**Заявление на создание и выдачу неквалифицированного сертификата ключа
проверки электронной подписи в Удостоверяющем центре ООО «ЭТП ГПБ
Консалтинг» ***

Настоящим _____
(наименование организации, включая организационно-правовую форму, ОГРН, ИНН)

в лице

(должность, фамилия, имя, отчество руководителя организации)

действующего на основании

(наименование документа, подтверждающего право действовать от имени юридического лица)

Прошу сформировать ключи электронной подписи и создать неквалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

CommonName (CN)	Наименование организации (владелец сертификата)
E-Mail (E)	Адрес электронной почты представителя владельца сертификата
Organization	Наименование организации
Title	Должность представителя владельца сертификата
Organization Unit	Наименование подразделения, сотрудником которого является представитель владельца сертификата
Surname	Фамилия представителя владельца сертификата
GivenName	Имя и отчество представителя владельца сертификата
StreetAddress	Адрес местонахождения юридического лица
Locality (L)	Наименование населенного пункта по адресу местонахождения организации
State (S)	Субъект Федерации по адресу местонахождения организации
Country (C)	Страна (RU)
OGRN	ОГРН организации
INNLE	ИНН организации
INN	ИНН представителя владельца сертификата
SNILS	СНИЛС представителя владельца сертификата

Полностью и безусловно присоединяюсь к Порядку УЦ ООО «ЭТП ГПБ Консалтинг», условия которого определены ООО «ЭТП ГПБ Консалтинг».

С Порядком УЦ ООО «ЭТП ГПБ Консалтинг», приложениями к нему и с Руководством по обеспечению безопасности использования неквалифицированной электронной подписи ознакомлен и обязуюсь соблюдать все положения указанных документов.

Настоящим подтверждаю факт ознакомления с указанным в Порядке перечнем рисков, возникающих при проведении операций с использованием неквалифицированной электронной подписи и средств электронной подписи. Я понимаю, что перечень рисков,

* Заявление на создание и выдачу сертификата ключа проверки электронной подписи в УЦ ООО «ЭТП ГПБ Консалтинг» подается в УЦ или Доверенному лицу УЦ в двух экземплярах. После регистрации заявления один экземпляр предоставляется Заявителю. В случае создания формы Заявления в автоматизированной системе УЦ, приоритетной считается такая форма.

указанный в Порядке, не может раскрыть все возможные риски и другие аспекты использования неквалифицированной электронной подписи и средств электронной подписи. Риски, связанные с использованием неквалифицированной электронной подписи и средств электронной подписи, мне понятны и принимаются полностью.

Я свободно, своей волей и своим интересе в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», в целях идентификации Заявителя, создания и выдачи Заявителю неквалифицированного сертификата ключа проверки электронной подписи, оказания консультационных услуг о создании и выдаче неквалифицированного сертификата, оказания услуг технической поддержки по использованию сопутствующего программного обеспечения для управления неквалифицированными сертификатами ключа проверки электронной подписи даю согласие на обработку в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» своих персональных данных, а именно: фамилии, имени и отчества, контактном(ых) телефоне(ах), адресе электронной почты, СНИЛС, ИНН, пола, паспортных данных (серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта, адрес регистрации) как с использованием средств автоматизации, так и без использования таких средств, включая совершение с ними следующих действий: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, блокирование, удаление, уничтожение и передачу.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

Заявитель

_____/_____
" ____ " _____ 20__ г.

Руководитель организации:

_____/_____
" ____ " _____ 20__ г.

М.П.

Отметка Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»

Данное заявление на создание и выдачу сертификата зарегистрировано в реестре УЦ.
Регистрационный № _____ от « ____ » _____ 20__ г.

(должность/полномочия)

_____/_____
« ____ » _____ 20__ г.

9.2. Приложение №2 к Порядку УЦ ООО «ЭТП ГПБ Консалтинг». Форма заявления на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи

(для физических лиц)

Заявление на прекращение действия (аннулирование) неквалифицированного сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «ЭТП ГПБ Консалтинг»

Прошу прекратить действие (аннулировать) сертификат ключа проверки электронной подписи, содержащий следующие поля:

Серийный номер сертификата	
Дата начала действия и дата окончания действия сертификата	
Ф.И.О.	
Причина отзыва сертификата	

Владелец сертификата

_____/_____
(ФИО)

«__»_____20__ г.

Отметка Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»

Данное заявление на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «ЭТП ГПБ Консалтинг», зарегистрировано в реестре УЦ. Регистрационный №_____ от «__»_____20__ г.

(должность/полномочия)

_____/_____
«__»_____20__ г.

(для индивидуальных предпринимателей)

Заявление на прекращение действия (аннулирование) невалифицированного сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «ЭТП ГПБ Консалтинг»

Прошу прекратить действие (аннулировать) сертификат ключа проверки электронной подписи, содержащий следующие поля:

Серийный номер сертификата	
Дата начала действия и дата окончания действия сертификата	
Ф.И.О.	
Причина отзыва сертификата	

Владелец сертификата

_____/_____/_____
(ФИО)

«__»_____20__ г.

М.П.

Отметка Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»

Данное заявление на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «ЭТП ГПБ Консалтинг», зарегистрировано в реестре УЦ. Регистрационный №_____ от «__»_____20__ г.

(должность/полномочия)

_____/_____/_____
«__»_____20__ г.

(для юридических лиц)

Заявление на прекращение действия (аннулирование) невалифицированного сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «ЭТП ГПБ Консалтинг»

Прошу прекратить действие (аннулировать) сертификат ключа проверки электронной подписи, содержащий следующие поля:

Серийный номер сертификата	
Дата начала действия и дата окончания действия сертификата	
Ф.И.О.	
Организация	
Причина отзыва сертификата	

Владелец сертификата

_____/_____/_____
(ФИО)
«__»_____20__ г.

Руководитель организации

_____/_____/_____
(ФИО)
«__»_____20__ г.

М.П.

Отметка Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»

Данное заявление на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «ЭТП ГПБ Консалтинг», зарегистрировано в реестре УЦ. Регистрационный №_____ от «__»_____20__ г.

(должность/полномочия)

_____/_____/_____
«__»_____20__ г.

9.3. Приложение №3 к Порядку УЦ ООО «ЭТП ГПБ Консалтинг». Форма заявления на подтверждение действительности электронной подписи в электронном документе

Заявление на подтверждение действительности электронной подписи в электронном документе

Прошу подтвердить подлинность электронной подписи в электронном документе на основании следующих данных:

1. Файл, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № _____;
2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи, на прилагаемом к заявлению носителе – рег. № _____
3. Время, на момент наступления которого требуется подтвердить подлинность электронной подписи: _____.

Заявитель _____/_____

«__» _____ 20__ г.

Отметка Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»

Данное заявление на подтверждение подлинности электронной подписи в электронном документе, созданной с сертификатом ключа проверки ЭП, изготовленным Удостоверяющим центром ООО «ЭТП ГПБ Консалтинг», зарегистрировано в реестре УЦ. Регистрационный № _____ от «__» _____ 20__ г.

(должность/полномочия)

_____/_____
«__» _____ 20__ г.

9.4. Приложение №4 к Порядку УЦ ООО «ЭТП ГПБ Консалтинг». Руководство по обеспечению безопасности использования неквалифицированной электронной подписи и средств электронной подписи

Руководство по обеспечению безопасности использования неквалифицированной электронной подписи и средств электронной подписи

Использование электронных подписей сопровождается рисками финансовых потерь при несанкционированном получении злоумышленниками ключей электронной подписи или несанкционированного использования рабочего места пользователя, на котором осуществляется выработка электронной подписи. В связи с этим необходимо выполнение приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

1. Обязанности владельца неквалифицированного сертификата ключа проверки электронной подписи

1.1. Обеспечить конфиденциальность ключей электронных подписей.

1.2. Применять для формирования электронной подписи только действующий ключ электронной подписи.

1.3. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

1.4. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.

1.5. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение или приостановление действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

1.6. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по моменту времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.

1.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено.

1.8. Использовать для создания и проверки неквалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства ЭП.

1.9. Обратиться в Удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, с заявлением о подтверждении подлинности электронной подписи в электронном документе в случае возникновения конфликтной ситуации, заключающейся в оспаривании авторства и/или содержимого документа, подписанного электронной подписью.

1.10. Обеспечить незамедлительное уничтожение ключей электронных подписей по истечении сроков действия данных ключей в отношении усиленных неквалифицированных электронных подписей. Для уничтожения ключей электронных подписей применять прошедшие в установленном порядке процедуру оценки соответствия средства электронной подписи, в составе которых реализована функция уничтожения информации.

2. Порядок применения средств неквалифицированной электронной подписи

2.1. Средства неквалифицированной электронной подписи должны применяться владельцем неквалифицированного сертификата ключа проверки электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство неквалифицированной электронной подписи.

2.2. При эксплуатации средств неквалифицированной электронной подписи должны использоваться только неквалифицированные сертификаты ключей проверки электронной подписи, выпущенные аккредитованным Удостоверяющим центром.

2.3. Средства неквалифицированной электронной подписи должны использоваться с сертифицированными средствами антивирусной защиты.

2.4. Установка средств неквалифицированной электронной подписи на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.

2.5. При установке и использовании средств неквалифицированной электронной подписи должна быть обеспечена защита аппаратного и программного обеспечения от несанкционированного доступа в соответствии с Руководством администратора безопасности из состава эксплуатационной документации на средство неквалифицированной электронной подписи.

2.6. Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства вычислительной техники с установленным средствами неквалифицированной электронной подписи, посторонних лиц, по роду своей

деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на средства неквалифицированной электронной подписи, средства вычислительной техники, на которых эксплуатируются средства неквалифицированной электронной подписи, и защищаемую информацию.

2.7. На средствах вычислительной техники, предназначенных для работы со средствами неквалифицированной электронной подписи, должно использоваться только лицензионное программное обеспечение фирм-изготовителей и не должны устанавливаться средства разработки программного обеспечения и отладчики.

2.8. Программное обеспечение, устанавливаемое на средствах вычислительной техники, предназначенных для работы со средствами неквалифицированной электронной подписи, не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

2.9. Для идентификации пользователя при входе в операционную систему и BIOS на технических средствах, предназначенных для работы со средствами неквалифицированной электронной подписи, необходимо использовать пароли в соответствии со следующими правилами:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;

- личный пароль пользователь не имеет права сообщать никому;

- периодичность смены пароля не должна превышать 6 месяцев.

2.10. Средствами BIOS должна быть исключена возможность работы на средствах вычислительной техники, предназначенных для работы со средствами неквалифицированной электронной подписи, если во время начальной загрузки не проходят встроенные тесты.

2.9. ЗАПРЕЩАЕТСЯ:

- оставлять без контроля средства вычислительной техники, на которых эксплуатируются средства неквалифицированной электронной подписи, после ввода ключевой информации либо иной конфиденциальной информации;

- вносить какие-либо изменения в программное обеспечение средств электронной подписи;

- осуществлять копирование ключевых носителей;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;

- использовать ключевые носители в режимах, не предусмотренных функционированием средств неквалифицированной электронной подписи;

- записывать на ключевые носители постороннюю информацию;

- изменять настройки, установленные программой установки средства ЭП или администратором;

- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами ЭП.

3. Правила использования ключевых носителей

3.1. Хранить ключ неквалифицированной электронной подписи необходимо исключительно на защищенном ключевом носителе.

3.2. При создании и записи на ключевой носитель ключ неквалифицированной электронной подписи должен быть отмечен как неэкспортируемый.

3.3. На ключевой носитель должен быть установлен индивидуальный PIN-код доступа (отличный от установленного по умолчанию).

3.4. Владелец ключа неквалифицированной электронной подписи обязан обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц (хранить и использовать носитель таким образом, чтобы исключался несанкционированный доступ к нему других лиц) и сохранять в конфиденциальности PIN-код доступа. Владелец ключа несет персональную ответственность за хранение личных ключевых носителей.

3.5. В случае утери ключевого носителя или наличия оснований подозревать о получении к нему несанкционированного доступа сторонних лиц владелец ключа электронной подписи обязан обратиться в Удостоверяющий центр с заявлением о прекращении или приостановлении действия сертификатов ключей проверки электронной подписи, ключи электронной подписи которых хранятся на носителе.

3.6. Максимальный срок действия ключа неквалифицированной электронной подписи составляет 1 (один) год 3 (три) месяца. Ключи неквалифицированной электронной подписи, срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами неквалифицированной электронной подписи, после чего ключевые носители могут использоваться для записи на них новой ключевой информации.

9.5. Приложение № 5 к Порядку УЦ ООО «ЭТП ГПБ Консалтинг». Форма невалифицированного сертификата

Сертификат ключа проверки электронной подписи

Сведения о сертификате:

Версия: _____

Серийный номер: _____

Издатель сертификата: CN=ООО "ЭТП ГПБ КОНСАЛТИНГ", O=ООО "ЭТП ГПБ КОНСАЛТИНГ", STREET=улица

Миклухо-Маклая, дом 40, эт.1 пом. IV ком.20, L=г. Москва, S=77 Москва, C=RU, INN=007728356929,

OGRN=5167746487651, E=ca@etpgpb.ru

Владелец сертификата: SN=_____, G=_____, L=_____, STREET=_____
S=_____, E=_____, SNILS=_____, T=_____, OU=_____, O=_____,
INN=_____, OGRN=_____, CN=_____, C=RU

Тип идентификации при выдаче сертификата: <identificationKind>

Срок действия:

Действителен с: 00.00.0000 00:00:00

Действителен по: 00.00.0000 00:00:00

Ключ проверки электронной подписи:

Алгоритм: ГОСТ Р 34.10-2012 256 бит (1.2.643.7.1.1.1.1)

Параметры: _____

Значение: _____

Расширения сертификата X.509

Расширение: Использование ключа (критичное)

Идентификатор: _____

Значение: _____

Расширение: Идентификатор ключа субъекта

Идентификатор: _____

Значение: _____

Расширение: Идентификатор ключа центра сертификатов

Идентификатор: _____

Значение: Идентификатор ключа= _____,

Поставщик сертификата: Адрес каталога: CN= ООО "ЭТП ГПБ КОНСАЛТИНГ",
ИНН=007728356929, ОГРН=5167746487651,

O= ООО "ЭТП ГПБ КОНСАЛТИНГ", STREET улица

Миклухо-Маклая, дом 40, эт.1 пом. IV ком.20, L=г. Москва, S=77 Москва, C=RU,
E=ca@etpgpb.ru

Серийный номер сертификата= _____

Расширение: Улучшенный ключ

Идентификатор: _____

Значение: _____

Расширение: Политики сертификата

Идентификатор: _____

Значение: [1]Политика сертификата: Идентификатор политики=Класс средства ЭП КС1,
[2]Политика

сертификата: Идентификатор политики=Класс средства ЭП КС2

Расширение: Период использования закрытого ключа

Идентификатор: _____

Действителен с: 00.00.0000 00:00:00

Действителен по: 00.00.0000 00:00:00

Расширение: Средства электронной подписи и УЦ издателя

Идентификатор: _____

Значение: Средство электронной подписи: _____ (заключение: Сертификат соответствия № _____), средство удостоверяющего центра: _____ (заключение: Сертификат соответствия № _____)

Общество с ограниченной ответственностью "ЭТП ГПБ Консалтинг"

Удостоверяющий Центр

Расширение: Средство электронной подписи владельца

Идентификатор: _____

Значение: Средство электронной подписи: _____

Расширение: Ограниченная лицензия КРИПТО-ПРО

Идентификатор: _____

Значение: _____

Расширение: Точки распространения списков отзыва (CRL)

Идентификатор: _____

Значение: [1]Точка распределения списка отзыва (CRL): Имя точки распространения:

Полное имя: URL=_____, [2]Точка распределения списка отзыва (CRL): Имя точки распространения: Полное имя: URL=_____

Расширение: Доступ к информации о центрах сертификации

Идентификатор: _____

Значение: [1]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации

(1.3.6.1.5.5.7.48.2), дополнительное имя=URL=_____

[2]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации

(1.3.6.1.5.5.7.48.2), дополнительное имя=URL=_____

Подпись Удостоверяющего центра:

Алгоритм: ГОСТ Р 34.11-2012/34.10-2012 256 бит (1.2.643.7.1.1.3.2)

Параметры:

Значение:

Подпись владельца сертификата: _____/_____

" ____ " _____ Г.

Подпись доверенного лица: _____/_____

" ____ " _____ Г.

М. П.

9.6. Приложение № 6 к Порядку УЦ ООО «ЭТП ГПБ Консалтинг». Профиль неквалифицированного сертификата

1. Общие сведения.

1.1. Неквалифицированный сертификат создается и выдается в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ, иными нормативными актами.

1.2. Владельцем неквалифицированного сертификата может быть физическое лицо.

2. Сведения о владельце сертификата.

2.1. Атрибутами поля идентификационных данных Владельца сертификата, являющегося физическим лицом, являются:

Наименование	Ограничение длины	Описание
Common Name	64	Фамилия, имя и отчество (при наличии) владельца сертификата - обязательно
Surname	40	Фамилия владельца сертификата - обязательно
Given name	64	Имя и отчество (при наличии) владельца сертификата - обязательно
Email	255	Адрес электронной почты владельца сертификата - обязательно
SNILS	11	СНИЛС владельца сертификата - обязательно
INN	12	ИНН владельца сертификата - обязательно
Country	2	RU - обязательно
State Or Province	128	Код и наименование субъекта РФ по адресу регистрации владельца сертификата – опционально
Locality	128	Наименование населенного пункта по адресу регистрации владельца сертификата – опционально
Street	128	Часть адреса регистрации владельца сертификата, включающая наименование улицы, номер дома, корпуса, строения, квартиры, помещения, – опционально

3. Тип идентификации при выдаче неквалифицированного сертификата.

3.1. Для указания в неквалифицированном сертификате идентификатора, однозначно указывающего на то, что идентификация Заявителя при выдаче неквалифицированного сертификата проводилась при его личном присутствии или

без его личного присутствия должно использоваться некритичное дополнение identificationKind. Объектный идентификатор типа IdentificationKind имеет вид 1.2.643.100.114.

Значение дополнения	Значение (INTEGER)	Описание
personal	0	Идентификация Заявителя при выдаче неквалифицированного сертификата проводилась при его личном присутствии
remote_cert	1	Идентификация Заявителя при выдаче неквалифицированного сертификата проводилась без его личного присутствия с использованием КЭП при наличии действующего сертификата
remote_passport	2	Идентификация Заявителя – гражданина Российской Федерации при выдаче неквалифицированного сертификата проводилась без его личного присутствия с применением информационных технологий путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные
remote_system	3	Идентификация заявителя – гражданина Российской Федерации при выдаче неквалифицированного сертификата проводилась без его личного присутствия с применением информационных технологий путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Лист регистрации изменений

[illegible]