УСЛОВИЯ ПОЛЬЗОВАНИЯ СЕРВИСОМ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. ООО «Бухгалтерские и банковские технологии» (далее по тексту — «ББС») предлагает пользователю сети Интернет (далее — Пользователь) использовать свой сервис по подготовке полного комплекта документов, необходимого при государственной регистрации общества с ограниченной ответственностью при создании и/или при регистрации физического лица в качестве индивидуального предпринимателя (далее по тексту — «Сервис»), на условиях, изложенных в настоящем Пользовательском соглашении (далее — «Соглашение», «ПС»). Соглашение вступает в силу с момента выражения Пользователем согласия с его условиями в порядке, предусмотренном п. 1.5 Соглашения.
1.2. Адрес Сервиса в сети Интернет reg.open.ru
1.3. Сервис является брендированной версией оригинального сервиса. Сервис брендирован в соответствии с требованиями ПАО Банк «ФК Открытие» (далее по тексту — «Банк») в соответствии с условиями заключённого между ББС и Банком соглашения.
1.4. Все вопросы, связанные с функциональными возможностями Сервиса, процедурами подготовки документов в Сервисе, вопросы по итоговыми документами, создаваемыми Сервисом, а также обращения Пользователей по вопросам работы Сервиса и качеству итоговых документов, лежат в зоне ответственности ББС.
Банк является информационным партнёром Сервиса исключительно в рамках размещаемой на страницах Сервиса информации о банковских продуктах и услугах для предприятий малого и среднего бизнеса, включая, но не ограничиваясь информацией:

- расчетно-кассовом обслуживании;
- об услугах кредитовании;
- о банковских картах;
- о депозитах,
- о зарплатных проектах,

Банк не несёт никакой ответственности по вопросам, касающимся государственной регистрации общества с ограниченной ответственностью при создании и регистрации физического лица в качестве индивидуального предпринимателя.
1.5. Использование Сервиса регулируется настоящим Соглашением, Политикой конфиденциальности и регламентом взаимодействия с УЦ ООО «Астрал-М» . Соглашение может быть изменено ББС без какого-либо специального уведомления, новая редакция Соглашения вступает в силу с момента ее размещения в сети Интернет по указанному в настоящем абзаце адресу, если иное не предусмотрено новой редакцией Соглашения. Действующая редакция ПС всегда находится на странице по адресу https://reg.open.ru/reg-open_agreement.pdf
1.6. Начиная использовать Сервис либо пройдя процедуру регистрации в Сервисе, Пользователь считается принявшим условия Соглашения в полном объеме без всяких оговорок и исключений. В случае несогласия Пользователя с какими-либо из положений Соглашения, Пользователь не в праве использовать Сервис. В случае если ББС были внесены какие-либо изменения в Соглашение в порядке, предусмотренном пунктом 1.5 Соглашения, с которыми Пользователь не согласен, он обязан прекратить использование Сервиса.

2. РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЯ. УЧЕТНАЯ ЗАПИСЬ ПОЛЬЗОВАТЕЛЯ

2.1. Для того чтобы воспользоваться Сервисом или некоторыми отдельными функциями Сервиса, Пользователю необходимо пройти процедуру регистрации, в результате которой для Пользователя будет создана уникальная учетная запись.

2.2. Для регистрации Пользователь обязуется предоставить достоверную и полную информацию о себе по вопросам, предлагаемым в форме регистрации, и поддерживать эту информацию в актуальном состоянии. Если Пользователь предоставляет неверную информацию или у ББС есть основания полагать, что предоставленная Пользователем информация неполна или недостоверна, ББС имеет право по своему усмотрению заблокировать либо удалить учетную запись Пользователя и отказать Пользователю в использовании Сервиса.
2.3. ББС оставляет за собой право в любой момент потребовать от Пользователя подтверждения данных, указанных при регистрации (в частности адрес электронной почты и номер телефона), непредоставление которых, по усмотрению ББС, может быть приравнено к предоставлению недостоверной информации и повлечь последствия, предусмотренные п. 2.2 Соглашения.
2.4. В случае если данные Пользователя, указанные в предоставленных им документах, не соответствуют данным, указанным при регистрации, а также в случае, когда данные, указанные при регистрации, не позволяют идентифицировать Пользователя, ББС вправе отказать Пользователю в доступе к учетной записи и использованию Сервиса.
2.5. Персональная информация Пользователя, содержащаяся в учетной записи Пользователя, а также используемая им при работе с Сервисом, хранится и обрабатывается ББС в соответствии с условиями Политики конфиденциальности.
2.6. При регистрации Пользователь самостоятельно вводит адрес своей электронной почты, после чего получается на свой адрес реквизиты доступа к его новой учётной записи. При необходимости Пользователь может изменить пароль доступа к Сервису из своей учётной записи.
2.7. Пользователь самостоятельно обеспечивает конфиденциальность своего пароля. Пользователь самостоятельно несет ответственность за все действия (а также их последствия) в рамках или с использованием Сервиса под учетной записью Пользователя, включая случаи добровольной передачи Пользователем данных для доступа к учетной записи Пользователя третьим лицам на любых условиях (в том числе по договорам или соглашениям). При этом все действия в рамках или с использованием Сервиса под учетной записью Пользователя считаются произведенными самим Пользователем, за исключением случаев, когда Пользователь в порядке, предусмотренном п. 2.8., уведомил ББС о несанкционированном доступе к Сервису с использованием учетной записи Пользователя и/или о любом нарушении (подозрениях о нарушении) конфиденциальности своего пароля.
2.8. Пользователь обязан немедленно уведомить ББС о любом случае несанкционированного (не разрешенного Пользователем) доступа к Сервису с использованием учетной записи Пользователя и/или о любом нарушении (подозрениях о нарушении) конфиденциальности своего пароля. В целях безопасности Пользователь обязан самостоятельно осуществлять безопасное завершение работы под своей учетной записью (кнопка «Выход») по окончании каждой сессии работы с Сервисом. ББС не отвечает за возможную потерю или порчу данных, а также другие последствия любого характера, которые могут произойти из-за нарушения Пользователем положений этой части Соглашения.
2.9. Пользователь не в праве воспроизводить, повторять и копировать, продавать и перепродавать, а также использовать для каких-либо коммерческих целей какие-либо части Сервиса (включая контент, доступный Пользователю посредством Сервиса), или доступ к нему, кроме тех случаев, когда Пользователь получил такое разрешение от ББС. Исключением из требований данного пункта являются пакеты документов, сгенерированные Сервисом в процессе работы с ним Пользователем и необходимые Пользователю для проведения регистрационных действий.
2.10. ББС вправе заблокировать или удалить учетную запись Пользователя, а также запретить доступ с использованием какой-либо учетной записи к Сервису и удалить любой контент без объяснения причин, в том числе в случае нарушения Пользователем условий Соглашения или условий иных документов, предусмотренных Соглашением, а также в случае неиспользования сервисов ББС в течение 6 месяцев.
2.11. Удаление учетной записи Пользователя.
2.11.1. Пользователь вправе в любой момент удалить свою учетную запись или прекратить ее действие в

отношении некоторых из них, воспользовавшись соответствующей функцией в персональном разделе.

2.11.2. Удаление учетной записи Пользователя в Сервисе осуществляется в следующем порядке:

2.11.2.1. учетная запись блокируется на срок один месяц, в течение которого размещенные с ее использованием контент и иные пользовательские данные не удаляются, однако доступ к ним становится невозможен как для Пользователя – владельца учетной записи, так и для других пользователей;

2.11.2.2. если в течение указанного выше срока учетная запись Пользователя будет восстановлена, доступ к указанным данным возобновляется в объеме, существовавшем на момент блокирования (за исключением контента, нарушающего условия Соглашения или иных документов, регулирующих соответствующий сервис);

2.11.2.3. если в течение указанного выше срока учетная запись Пользователя не будет восстановлена, весь контент, размещенный с ее использованием, будет удален. С этого момента восстановление учетной записи, какой-либо информации, относящейся к ней, а равно доступов к сервисам ББС с использованием этой учетной записи - невозможны.

3. ОБЩИЕ ПОЛОЖЕНИЯ ОБ ИСПОЛЬЗОВАНИИ И ХРАНЕНИИ

3.1. ББС вправе устанавливать ограничения в использовании Сервиса для всех Пользователей либо для отдельных Пользователей (например, в зависимости от места пребывания Пользователя и т.д.), в том числе: максимальное количество обращений к Сервису за указанный период времени, максимальный срок хранения контента/комплектов документов, условия доступа к Сервису и т.д. ББС может запретить автоматическое обращение к Сервису, а также прекратить прием любой информации, сгенерированной автоматически (например, почтового спама или автозаполнение форм).

3.2. ББС вправе посылать своим пользователям информационные сообщения, а также информационные сообщения, содержащие информацию о продуктах и услугах партнёров ББС.

4. ДАННЫЕ ПОЛЬЗОВАТЕЛЯ

4.1. Пользователь самостоятельно несет ответственность за корректность данных, вводимых им в процесс использования Сервиса, а также за соответствие вводимых данных требованиям действующего законодательства, включая ответственность перед третьим лицами в случаях, когда Пользователь вводит данные, не имеющие к нему прямого отношения (например, данные третьих лиц), или нарушает права и законные интересы третьих лиц.

4.2. Пользователь признает и соглашается с тем, что ББС не обязан проверять вводимые Пользователем данные на предмет их корректности.

4.3. Пользователь осознает и соглашается с тем, что Сервис используется вводимые Пользователем данные для подготовки запрошенных Пользователем документов.

4.4. Пользователь уведомлён о том, что в целях обеспечения эффективного взаимодействия между Пользователем и Банком, ББС передаёт в Банк следующие публичные данные Пользователя:

4.4.1. по создаваемому обществу с ограниченной ответственностью:

- наименование создаваемого Пользователем общества;
- город регистрации общества;
- перечень кодов ОКВЭД создаваемого Пользователем общества;
- дата создания Пользователем комплекта документов;
- ФИО Пользователя (при наличии);
- e-mail Пользователя;
- контактный телефон Пользователя (при наличии);
- ФИО единоличного исполнительного органа создаваемого общества;
- e-mail единоличного исполнительного органа создаваемого общества (при наличии);

- информацию о желании Пользователя открыть в Банке счёт для создаваемого им общества.

4.4.2. при регистрации Пользователя в качестве ИП:

- город регистрации;
- дата создания Пользователем комплекта документов;
- ФИО Пользователя;
- e-mail Пользователя;
- контактный телефон Пользователя;
- перечень кодов ОКВЭД регистрируемого ИП;
- информацию о желании Пользователя открыть в Банке счёт.

4.5. Пользователь уведомлён о том, что ББС не передаёт в Банк и другим третьим лицам следующие данные:

- любые паспортные данные (за исключением ФИО Пользователя, ФИО единоличного исполнительного органа создаваемого общества и ФИО регистрируемого ИП);
- сведения об учредителях общества (их данные и количество), а также информацию о долях в уставном капитале общества;
- адреса регистрации физического лица;
- подготовленные Пользователем документы для создаваемого общества либо для регистрации в качестве ИП.

5. УСЛОВИЯ ИСПОЛЬЗОВАНИЯ СЕРВИСОВ ББС

5.1. Пользователь самостоятельно несет ответственность перед третьими лицами за свои действия, связанные с использованием Сервиса, в том числе, если такие действия приведут к нарушению прав и законных интересов третьих лиц, а также за соблюдение законодательства при использовании Сервиса.
5.2. При использовании сервисов ББС Пользователь не вправе:
5.2.1. выдавать себя за другого человека или представителя организации и/или сообщества без достаточных на то прав;
5.2.2. несанкционированно собирать и хранить персональные данные других лиц;
5.2.3. нарушать нормальную работу Сервиса;
5.2.4. содействовать действиям, направленным на нарушение ограничений и запретов, налагаемых Соглашением;
5.2.5. другим образом нарушать нормы законодательства, в том числе нормы международного права.

6. САЙТЫ И КОНТЕНТ ТРЕТЬИХ ЛИЦ

6.1. Все объекты, доступные при помощи Сервиса, в том числе элементы дизайна, текст, графические изображения, базы данных, готовые документы в форматах XLS и DOC и другие объекты, а также любой контент, размещенный в Сервисе, являются объектами исключительных прав ББС и других правообладателей.
6.2. Использование Сервиса, а также каких-либо иных элементов Сервиса возможно только в рамках функционала Сервиса. Никакие элементы содержания Сервиса, а также любой контент, размещенный на сервисах ББС, не могут быть использованы иным образом без предварительного разрешения ББС. Под использованием подразумеваются, в том числе распространение на любой основе, отображение во фрейме и т.д. Исключение составляют случаи, прямо предусмотренные законодательством РФ или условиями

использования Сервиса ББС.
6.3. Использование Пользователем элементов содержания Сервиса, а также любого контента для личного некоммерческого использования допускается при условии сохранения всех знаков охраны авторского права, смежных прав, товарных знаков, других уведомлений об авторстве, сохранения имени (или псевдонима) автора/наименования правообладателя в неизменном виде, сохранении соответствующего объекта в неизменном виде.

7. САЙТЫ И КОНТЕНТ ТРЕТЬИХ ЛИЦ

7.1. Сервис может:
- содержать ссылки на другие сайты в сети Интернет (сайты третьих лиц);
- использовать базы данных третьих лиц (например, базы данных ОКВЭД, КЛАДР, СОУН, СПРО и другие);
- использовать формы документов третьих лиц (заявления по форме Р11001, Р21001, формы платёжных квитанций и другие).

Третьи лица и их контент не проверяются ББС на соответствие тем или иным требованиям (достоверности, полноты, законности и т.п.). ББС не несет ответственность за любую информацию, материалы, размещенные на сайтах третьих лиц, к которым Пользователь получает доступ с использованием Сервиса.
7.2. Ссылка (в любой форме) на любой сайт, продукт, услугу, любую информацию коммерческого или некоммерческого характера, размещенная в Сервисе, не является одобрением или рекомендацией данных продуктов (услуг, деятельности) со стороны ББС.

8. РЕКЛАМА НА СЕРВИСЕ ББС

8.1. ББС несет ответственность за рекламу, размещенную на сервисах ББС, в пределах, установленных законодательством РФ.

9. ОТСУТСТВИЕ ГАРАНТИЙ, ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

9.1. Пользователь использует сервисы ББС на свой собственный риск. Сервис предоставляется «как есть». ББС не принимает на себя никакой ответственности, в том числе за соответствие Сервиса целям Пользователя;
9.2. ББС не гарантирует, что Сервис соответствует/будет соответствовать требованиям Пользователя; что Сервис будет предоставляться непрерывно, быстро, надежно и без ошибок.
9.3. Любые информацию и/или материалы (в том числе загружаемые документы, письма, какие-либо инструкции и руководства к действию и т.д.), доступ к которым Пользователь получает с использованием Сервиса ББС, Пользователь может использовать на свой собственный страх и риск и самостоятельно несет ответственность за возможные последствия использования указанных информации и/или материалов, в том числе за ущерб, который это может причинить Пользователю или третьим лицам, за потерю данных, времени, денежных средств или любой другой вред;
9.4. ББС не несет ответственности за любые виды убытков, произошедшие вследствие использования Пользователем Сервиса ББС или отдельных частей/функций Сервиса;
9.5. При любых обстоятельствах ответственность ББС в соответствии со статьей 15 Гражданского кодекса России ограничена 10 000 (десятью тысячами) рублей РФ и возлагается на него при наличии в его действиях вины.

10. ИНЫЕ ПОЛОЖЕНИЯ

10.1. Настоящее Соглашение представляет собой договор между Пользователем и ББС относительно порядка использования Сервиса и заменяет собой все предыдущие соглашения между Пользователем и ББС в отношении Сервиса.
10.2. Настоящее Соглашение регулируется и толкуется в соответствии с законодательством Российской Федерации. Вопросы, не урегулированные настоящим Соглашением, подлежат разрешению в соответствии с законодательством Российской Федерации. Все возможные споры, вытекающие из отношений, регулируемых настоящим Соглашением, разрешаются в порядке, установленном действующим законодательством Российской Федерации, по нормам российского права. Везде по тексту настоящего Соглашения, если явно не указано иное, под термином «законодательство» понимается законодательство Российской Федерации.
10.3. Ввиду безвозмездности услуг, оказываемых в рамках настоящего Соглашения, нормы о защите прав потребителей, предусмотренные законодательством Российской Федерации, не могут быть применимыми к отношениям между Пользователем и ББС.
10.4. Ничто в Соглашении не может пониматься как установление между Пользователем и ББС агентских отношений, отношений товарищества, отношений по совместной деятельности, отношений личного найма либо каких-то иных отношений, прямо не предусмотренных Соглашением.
10.5. Если по тем или иным причинам одно или несколько положений настоящего Соглашения будут признаны недействительными или не имеющими юридической силы, это не оказывает влияния на действительность или применимость остальных положений Соглашения.
10.6. Бездействие со стороны ББС в случае нарушения Пользователем либо иными пользователями положений Соглашений не лишает ББС права предпринять соответствующие действия в защиту своих интересов позднее, а также не означает отказа ББС от своих прав в случае совершения в последующем подобных либо сходных нарушений.

ООО «ББС»
Директор: Булаев Антон Сергеевич
Email: to@regme.online
Адрес: 115191, Москва г, Духовской пер, дом 17, офис 47
ИНН: 7726365491
КПП: 772601001
ОГРН: 5157746229746

«УТВЕРЖДАЮ»

Директор ООО «Астрал-М»

_____Мео Ю.Н.

от «31» августа 2019 г.

Регламент взаимодействия с клиентами ПАО «ФК Открытие» и ООО "ББС" в сервисе reg.open.ru по электронной отправке документов на регистрацию ООО и ИП

2019 г.

СОДЕРЖАНИЕ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

Сертификат ключа проверки электронной подписи – 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;

Квалифицированная электронная подпись – электронная подпись, которая соответствует всем признакам квалифицированной электронной подписи, определенным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) – сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного Удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее – уполномоченный федеральный орган);

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи; *Ключ электронной подписи* - уникальная последовательность символов, предназначенная для создания электронной подписи;

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

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

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.

Ключевой документ – физический носитель определенной структуры, содержащий ключевую информацию (ключи электронной подписи).*Удостоверяющий центр* – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

Администратор Удостоверяющего центра – полномоченный сотрудник Удостоверяющего центра, ответственный за бесперебойную работу программно-аппаратного комплекса удостоверяющего центра, а так же выполнение операций по изготовлению и обслуживанию сертификатов Пользователей УЦ;

Аккредитация Удостоверяющего центра – признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи; *Средства удостоверяющего центра* - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

Участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане; *Корпоративная информационная система* – информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

Информационная система общего пользования – информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Компрометация ключа электронной подписи – утрата доверия к тому, что используемые ключи электронной подписи недоступны посторонним лицам или подозрение, что ключи электронной подписи были временно доступны неуполномоченным лицам.

Конфиденциальная информация – информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ.

Несанкционированный доступ к информации – доступ к информации лиц, не имеющих на то полномочий в соответствии с законодательством РФ.

Плановая смена ключей подписи – смена ключей электронной подписи, не вызванная компрометацией ключей электронной подписи, производимая пользователем.

Пользователь Удостоверяющего центра (Пользователь УЦ) – клиент ООО «БСС», пользующийся услугами аккредитованного Удостоверяющего центра и присоединяющийся к Регламенту Удостоверяющего центра;

Реестр Удостоверяющего центра – набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий следующую информацию: реестр заявлений на регистрацию в Удостоверяющем центре, реестр

зарегистрированных пользователей Удостоверяющего центра, реестр заявлений на изготовление сертификатов ключей проверки электронных подписей, реестр заявлений на аннулирование (отзыв) сертификатов ключей проверки электронных подписей, реестр заявлений на приостановление/возобновление действия сертификатов ключей проверки электронных подписей, реестр заявлений на подтверждение подлинности электронной подписи в электронном документе, реестр сертификатов ключей проверки электронных подписей;*Список отозванных сертификатов (СОС)* – созданный Удостоверяющим центром список сертификатов ключей проверки электронных подписей, отозванных до окончания срока их действия;

Уполномоченное лицо Удостоверяющего центра – сотрудник Удостоверяющего центра, являющийся владельцем ключа электронной подписи и соответствующего ему квалифицированному сертификату ключа проверки электронной подписи Удостоверяющего центра и наделенный Удостоверяющим центром полномочиями по заверению квалифицированных сертификатов ключей проверки электронных подписей и списков отозванных сертификатов;

Шифрование – процесс преобразования открытой информации с целью сохранения ее в тайне от третьих лиц при помощи некоторого алгоритма, называемого шифром;

Штамп времени электронного документа (штамп времени) – электронный документ, подписанный электронной подписью и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе;

Электронный документ (ЭД) – документ, в котором информация представлена в электронной форме. Электронный документ может создаваться на основе документа на бумажном носителе, на основе другого электронного документа либо порождаться в процессе информационного взаимодействия.

2. СВЕДЕНИЯ ОБ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ

Общество с ограниченной ответственностью «АСТРАЛ-М», именуемое в дальнейшем «Удостоверяющий центр» или «УЦ», зарегистрировано на территории © ООО «АСТРАЛ-М», 2019| Порядок реализации функций АУЦ и исполнения его обязанностей (Регламент) Российской Федерации в городе Москве. Свидетельство о государственной регистрации № 011634160 от 03 июля 2008 года. Свидетельство о внесении записи в Единый государственный реестр юридических лиц за основным государственным регистрационным номером 1087746806311 от 03 июля 2008 года.

Удостоверяющий центр в качестве участника рынка услуг по созданию и выдаче сертификатов ключей проверки электронных подписей осуществляет свою деятельность на территории Российской Федерации на основании следующих документов:

- Свидетельства об аккредитации удостоверяющего центра № 804 от 03.10.2017 г. (Удостоверяющий центр аккредитован в соответствии с Приказом Минкомсвязи России № 604 от 03.10.2017 г. «Об аккредитации удостоверяющих центров»);
- Лицензии Центра по лицензированию, сертификации и защите государственной тайны ФСБ России № 16382 Н от 29.12.2017 г. на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

Реквизиты:

Реквизиты Удостоверяющего центра:
Полное наименование: Общество с ограниченной ответственностью «АСТРАЛ-М»
Сокращенное наименование: ООО «АСТРАЛ-М»
ИНН/КПП: 7720623379/772001001
ОГРН: 1087746806311
Юридический адрес: 111123 г. Москва, ул. Шоссе Энтузиастов, д. 56, стр. 32, офис 214
Фактический (почтовый адрес): 111123 г. Москва, ул. Шоссе Энтузиастов, д. 56, стр. 32,

офис 214
Банковские реквизиты:
Банк: АО ЮниКредит Банк
БИК 044525545
р/с 40702810800014707483
к/с 30101810300000000545
Контактные телефоны call-центра, адреса электронной почты:
+7 (495) 663-73-58 – г. Москва
Web-сайт: https://astral.ru;
Адрес электронной почты Удостоверяющего центра: ca@astralm.ru
Адрес электронной почты Клиентской службы: ca@astralm.ru

3. ОБЩИЕ ПОЛОЖЕНИЯ

- Регламент деятельности Удостоверяющего центра ООО «Астрал-М», именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность Удостоверяющих центров.
- Настоящий Регламент является документом, устанавливающим правила и порядок предоставления и пользования услугами ООО «Астрал-М» в качестве Удостоверяющего центра.
- Настоящий Регламент определяет форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы Удостоверяющего центра.
- Регламент утверждается директором ООО «Астрал-М» и вводится в действие его приказом.
- Внесение изменений (дополнений) в Регламент, а также в приложения к нему, производится путем подготовки и утверждения очередной редакции Регламента и производится Удостоверяющим центром в одностороннем порядке.
- Уведомление пользователей о внесении изменений (дополнений) в Регламент осуществляется ООО «Астрал-М» путем размещения очередной редакции Регламента, включающей указанные изменения (дополнения) по адресу:
- Все приложения, изменения и дополнения к настоящему Регламенту являются его составной и неотъемлемой частью, вступают в силу и становятся обязательными по истечению десяти календарных дней с даты их публикации на сайте удостоверяющего центра, кроме изменений, связанных с изменениями действующего законодательства Российской Федерации, которые вступают в силу одновременно с вступлением в силу соответствующих нормативно-правовых актов, повлекших изменение законодательства.
- Термины, применяемые в настоящем Регламенте, понимаются строго в контексте общего смысла Регламента.
- В случае противоречия и/или расхождения названия какого-либо раздела Регламента со смыслом одного из его пунктов, считается доминирующим смысл и формулировки каждого конкретного пункта.
- В случае противоречия и/или расхождения положений какого-либо приложения к настоящему Регламенту с положениями Регламента, считается доминирующим смысл и формулировки Регламента.

4. УСЛУГИ, ПРЕДОСТАВЛЯЕМЫЕ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

В процессе своей деятельности Удостоверяющий центр ООО «Астрал-М» предоставляет следующие виды услуг:

- Создает квалифицированные сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (Пользователям УЦ);
- Устанавливает сроки действия квалифицированных сертификатов ключей проверки электронных подписей;
- Аннулирует выданные Пользователям УЦ квалифицированные сертификаты ключей проверки электронных подписей;
- Выдает по обращению Пользователей УЦ средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;
- Ведет реестр выданных и аннулированных квалифицированных сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных квалифицированных сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования квалифицированных сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;
- Устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";
- Создает по обращениям Пользователей УЦ ключи электронных подписей и ключи проверки электронных подписей;
- Проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;
- Осуществляет по обращениям Пользователей УЦ проверку электронных подписей;
- Изготавливает по обращениям Пользователей УЦ копии квалифицированных сертификатов ключей проверки электронных подписей Пользователей УЦ на бумажном носителе;
- Предоставляет иные услуги, связанные с использованием электронных подписей.

5. ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ

- Удостоверяющий центр предоставляет Пользователю УЦ по его требованию:

- Копию свидетельства об аккредитации удостоверяющего центра № 54 от 21 августа 2012 года, выданного Минкомсвязи России;

- Копию лицензии УФСБ по Калужской области № 1200Н от 20.08.2014 г. на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

- Удостоверяющий центр вправе запросить, а Пользователь УЦ обязан предоставить Удостоверяющему центру следующие документы:

Для юридического лица:

- Страховое свидетельство обязательного государственного пенсионного страхования (СНИЛС) владельца КСКПЭП (с предъявлением оригинала документа);
- Паспорт владельца КСКПЭП (с предъявлением оригинала документа);
- Заявление на изготовление КСКПЭП (по форме Приложения 1).

Для индивидуальных предпринимателей:

- Страховое свидетельство обязательного государственного пенсионного страхования (СНИЛС) владельца КСКПЭП (с предъявлением оригинала документа);
- Паспорт владельца КСКПЭП (с предъявлением оригинала документа);
- Заявление на изготовление КСКПЭП (по форме Приложения 1).

Для физических лиц:

- Страховое свидетельство обязательного государственного пенсионного страхования (СНИЛС) владельца КСКПЭП (с предъявлением оригинала документа);
- Паспорт владельца КСКПЭП (с предъявлением оригинала документа);
- Заявление на изготовление КСКПЭП (по форме Приложения 1).

6. ПРАВА И ОБЯЗАННОСТИ СТОРОН

Удостоверяющий центр имеет право:

- Отказать пользователю в регистрации в Удостоверяющем центре в случае ненадлежащего оформления необходимых регистрационных документов;

- Отказать в изготовлении квалифицированного сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случаях ненадлежащего оформления заявления на изготовление квалифицированного сертификата ключа проверки электронной подписи и/или непредставления Пользователем УЦ документов, предусмотренных п.5.2 Регламента;

- Отказать в аннулировании (отзыве), приостановлении или возобновлении действия квалифицированного сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления соответствующего заявления на аннулирование (отзыв), приостановление и возобновление действия квалифицированного сертификата ключа проверки электронной подписи;

- Отказать в аннулировании (отзыве), приостановлении или возобновлении действия квалифицированного сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия ключа электронной подписи, соответствующего квалифицированному сертификату ключа проверки электронной подписи;

- Аннулировать (отозвать) квалифицированный сертификат ключа проверки электронной подписи пользователя в случае установленного факта компрометации соответствующего ключа электронной подписи, с уведомлением владельца аннулированного (отозванного) квалифицированного сертификата ключа проверки электронной подписи и указанием обоснованных причин;

- В одностороннем порядке приостановить действие квалифицированного сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра с обязательным уведомлением владельца квалифицированного сертификата ключа проверки электронной подписи, действие которого приостановлено, с указанием обоснованных причин;

- Отказать в предоставлении сведений из Реестра квалифицированных сертификатов ключей проверки электронной подписи, в случае, если объем запрашиваемой информации не соответствует законной цели ее обработки, указанной в заявлении на предоставлении информации.

Пользователь Удостоверяющего центра имеет право:

- Получить квалифицированный сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра;

- Применять квалифицированный сертификат ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра для проверки электронной подписи Уполномоченного лица Удостоверяющего центра в квалифицированных сертификатах ключей проверки электронной подписи, изготовленных Удостоверяющим центром;

- Получать список отозванных (аннулированных) и приостановленных квалифицированных сертификатов ключей проверки электронной подписи, изготовленных Удостоверяющим центром;

- Применять список отозванных квалифицированных сертификатов ключей проверки электронной подписи, изготовленных Удостоверяющим центром, для установления статуса квалифицированных сертификатов ключей проверки электронной подписи, изготовленных Удостоверяющим центром;

• Применять квалифицированный сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в квалифицированном сертификате ключа проверки электронной подписи;

• Получать копию квалифицированного сертификата ключа проверки электронной подписи в электронной форме, находящегося в реестре квалифицированных сертификатов ключей проверки электронной подписи Удостоверяющего центра;

• Обращаться в Удостоверяющий центр с заявлением на изготовление квалифицированного сертификата ключа проверки электронной подписи;

• Обращаться в Удостоверяющий центр с заявлением на аннулирование (отзыв) и приостановление действия квалифицированного сертификата ключа проверки электронной подписи, владельцем которого он является, в течение срока действия соответствующего ключа электронной подписи;

• Обращаться в Удостоверяющий центр с заявлением на возобновление действия квалифицированного сертификата ключа проверки электронной подписи, владельцем которого он является, в течение срока действия соответствующего ключа электронной подписи и срока, на который действие квалифицированного сертификата ключа проверки электронной подписи было приостановлено;

• Обращаться в Удостоверяющий центр за получением информации о статусе квалифицированных сертификатов ключей проверки электронной подписи и их действительности на определенный момент времени;

• Обращаться в Удостоверяющий центр за подтверждением подлинности электронной подписи в электронном документе, сформированной с использованием квалифицированного сертификата ключа проверки электронной подписи, изданного Удостоверяющим центром;

• Получить копию квалифицированного сертификата ключа проверки электронной подписи на бумажном носителе;

• Обращаться в Удостоверяющий Центр за подтверждением подлинности электронной подписи уполномоченного лица Удостоверяющего центра в изготовленных им квалифицированных сертификатах ключа проверки электронной подписи.

Удостоверяющий центр обязан:
В части изготовления и использования ключа ЭП Уполномоченного лица УЦ обязан:
• использовать ключ ЭП Уполномоченного лица УЦ только для подписи издаваемых им сертификатов и списков отозванных сертификатов;
• обеспечивать меры по защите ключа ЭП Уполномоченного лица УЦ.
• В части регистрации Пользователей УЦ обязан:
• обеспечить регистрацию Пользователей по заявлениям в соответствии с порядком регистрации, изложенным в настоящем Регламенте;
• обеспечить уникальность регистрационной информации Пользователей УЦ, заносимой в реестр УЦ и используемой для идентификации владельцев сертификатов;
• не разглашать (не публиковать) регистрационную информацию Пользователей УЦ, за исключением информации, заносимой в изготавливаемые сертификаты.
• В части изготовления ключей ЭП и ключей проверки ЭП УЦ обязан:
• предоставить Пользователю УЦ возможность и соответствующее программное обеспечение для самостоятельной генерации ключа ЭП и ключа проверки ЭП согласно заявления и с использованием СКЗИ, сертифицированных по классу КС2;
• предоставить Пользователю УЦ возможность записать ключ ЭП и ключ проверки ЭП на отчуждаемый ключевой носитель, в соответствии с требованиями по эксплуатации программного и/или аппаратного средства, выполняющего процедуру генерации ключей;
• при отсутствии отчуждаемого ключевого носителя обеспечить возможность создания ключа ЭП и ключа проверки ЭП и их хранение в реестре операционной системы.
• В части изготовления сертификатов УЦ обязан:
• обеспечить изготовление сертификата Пользователю УЦ по заявлению, в соответствии с порядком, определенным в настоящем Регламенте;
• обеспечить уникальность регистрационных (серийных) номеров изготавливаемых сертификатов Пользователей УЦ;

- обеспечить уникальность значений ключей проверки ЭП в изготовленных сертификатах Пользователей УЦ;
- осуществлять выдачу копий сертификатов в бумажной и/или электронной форме по обращениям Пользователей УЦ;
- под расписку ознакомить Пользователя УЦ с информацией, содержащейся в его сертификате;
- выдать владельцу сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

В части аннулирования (отзыва) или приостановки действия сертификатов УЦ обязан аннулировать или приостановить действие сертификата по заявлению его владельца и в течение 12 часов после принятия заявления на аннулирование или приостановление занести сведения об аннулированном или приостановленном сертификате в СОС с указанием даты, времени занесения и причины аннулирования, а так же разместить актуальный СОС в точке публикации на общедоступном сетевом ресурсе.

В части ведения реестра сертификатов УЦ обязан обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования и иных противоправных действий.

УЦ обязан уведомлять владельца сертификата о фактах, которые стали известны УЦ и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата.

Пользователь Удостоверяющего центра обязан:

- предоставить все необходимые и достоверные сведения о себе для формирования заявления на изготовление сертификата;
- ознакомиться и подписать Заявление на изготовление сертификата;
- ознакомиться и соблюдать требования настоящего Регламента, а также руководствоваться им при управлении своими ключами ЭП, ключами проверки ЭП и сертификатами;
- четко знать свои права и обязанности, изложенные в настоящем Регламенте;
- использовать сертификат в соответствии с его назначением;
- хранить ключевой носитель в условиях, исключающих возможность компрометации ключа ЭП;
- немедленно сообщать в УЦ о потере, компрометации или подозрении на компрометацию ключа ЭП;
- немедленно сообщать в УЦ об изменении информации, содержащейся в сертификате.

Пользователь УЦ несет дисциплинарную и административную ответственность за неисполнение или ненадлежащее исполнение своих обязанностей в соответствии с действующим законодательством и взятыми на себя обязательствами.

Перед получением сертификата Пользователь УЦ обязан ознакомиться со своими правами, обязанностями и ответственностью, изложенными в данном пункте настоящего Регламента.

Пользователь УЦ должен знать:

- свои обязанности, связанные с обеспечением безопасности хранения и использованием сертификатов;
- процедуры взаимодействия Пользователей и УЦ;
- порядок действий при компрометации ключа ЭП;
- обязанности, касающиеся использования, проверки и подтверждения подлинности сертификатов.

Персональная информация о Пользователе, хранящаяся в УЦ и не включенная в сертификат, не может быть разглашена без согласия самого Пользователя УЦ, за исключением случаев, предусмотренных действующим законодательством РФ.

Собственноручно подписывая заявление на изготовление, аннулирование или приостановку действия сертификата, Пользователь УЦ подтверждает, что вся информация, содержащаяся в заявлении, является полной и достоверной.

7. ОТВЕТСТВЕННОСТЬ СТОРОН

Стороны несут ответственность за невыполнение либо ненадлежащее выполнение обязательств по настоящему Регламенту в пределах суммы доказанного ущерба, причиненного Стороне невыполнением либо ненадлежащим выполнением обязательств другой Стороной. Ни одна из Сторон не несет ответственность за неполученные доходы (упущенную выгоду), которые могла бы получить другая Сторона.

БСС и УЦ не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если УЦ обоснованно полагался на сведения, указанные в заявлениях Пользователя УЦ.

БСС и/или УЦ несут ответственность за убытки при использовании созданного УЦ ключа ЭП и сертификата, в том случае, если данные убытки возникли по вине БСС и/или УЦ.

Стороны не несут ответственности за полное или частичное неисполнение своих обязательств по настоящему Регламенту, если это явилось следствием форс-мажорных обстоятельств, повлекших невозможность исполнения Стороной (Сторонами) своих обязательств. В таких случаях срок исполнения Сторонами своих обязательств увеличивается соразмерно периоду, в течение которого действуют такие обстоятельства.

Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется законодательством Российской Федерации.

8. РАЗРЕШЕНИЕ СПОРОВ

- Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и Пользователь УЦ.
- При рассмотрении спорных вопросов, связанных с настоящим Регламентом, Стороны будут руководствоваться действующим законодательством Российской Федерации.
- Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.
- Сторона, получившая от другой Стороны претензию, обязана в течение 30 (Тридцати) рабочих дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа.

Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, решаются в Арбитражном суде Калужской области.

9. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ

- Изготовление квалифицированного сертификата ключа проверки электронной подписи.

Клиент БСС (Пользователь УЦ) самостоятельно осуществляет регистрацию в личном кабинете сервиса подготовки документов для регистрации бизнеса (открытия ИП или ООО) на портале БСС, расположенному в сети Интернет по адресу: https://reg.open.ru/ (далее-Сервис).

Выбрав в личном кабинете Сервиса необходимый пункт («Регистрация в качестве индивидуального предпринимателя» или «Регистрация ООО»), клиент, следуя пошаговой инструкции и в соответствии с имеющимися у него документами, указывает в нужных полях Сервиса следующие данные:

- Данные о заявителе (персональные данные);
- Данные паспорта;
- Контактные данные;
- Выражает согласие с условиями пользования Сервисом и согласие на обработку своих персональных данных;
- Данные о месте жительства;
- Номер ИФНС получателя документов на государственную регистрацию ИП\ООО;
- Указывает вид (ы) деятельности;
- Индивидуальный номер налогоплательщика (ИНН);
- Номер страхового свидетельства обязательного государственного пенсионного страхования (СНИЛС);
- Указывает способ получения оригиналов документов после завершения государственной регистрации;
- Выбирает систему налогообложения.

После вода всех данных клиент скачивает пакет автоматически сформированных документов, необходимых для подачи на государственную регистрацию в ИФНС.

Перечень документов:

- Заявление на регистрацию ИП\ООО (Форма Р21001\Р11001);
- Заявление на УСН (если требуется);
- Заявление на изготовление сертификата квалифицированной электронной подписи (Приложение 1);
- Инструкция по онлайн-регистрации;
- Квитанция на оплату госпошлины.

В случае, если клиент выражает желание на подачу заявления на государственную регистрацию в электронном виде, необходимо произвести онлайн-оплату госпошлины (при необходимости) и загрузить в сервис скан-копии следующих должным образом оформленных документов:

- Скан-копию (скриншот) квитанции на оплату госпошлины (при необходимости);
- Скан-копию страхового свидетельства обязательного государственного пенсионного страхования (СНИЛС);
- Скан-копию заявления на УСН (при необходимости), заверенной собственноручной подписью клиента;
- Скан-копию заявления на изготовление сертификата квалифицированной электронной подписи, заверенного собственноручной подписью клиента;
- Скан-копию последней страницы заявления на регистрацию ИП\ООО (Форма Р21001\Р11001), заверенной собственноручной подписью клиента;

УЦ посредством использования системы межведомственного электронного взаимодействия (СМЭВ) осуществляет проверку достоверности документов и сведений, представленных заявителем (клиентом).

В случае, если полученные сведения подтверждают достоверность информации, представленной заявителем для включения в сертификат, Пользователь УЦ в личном кабинете Сервиса скачивает и устанавливает программное

обеспечение, предназначенное для подписания документов ЭП и отправки их в ИФНС (AstralToolBox). В противном случае УЦ отказывает заявителю в создании и выдаче сертификата.

Для формирования на рабочем месте Пользователя УЦ ключа ЭП, ключа проверки ЭП и отправки в УЦ запроса на изготовление сертификата, необходимо наличие на рабочем месте Пользователя УЦ установленного криптопровайдера: «КриптоПро CSP» версии 3.6 и выше или ViPNet CSP версии 4.0 и выше.

Пользователь УЦ, регистрируется на сайте ООО «КРИПТО-ПРО» (www.cryptopro.ru) или ОАО «ИнфоТеКС» (www.infotecs.ru) и осуществляет загрузку дистрибутива криптопровайдера в полном соответствии с лицензионной политикой правообладателя.

Пользователь УЦ производит установку криптопровайдера на своем рабочем месте.

Используя ПО «AstralToolBox» и криптопровайдер, Пользователь УЦ производит генерацию ключевого контейнера (ключа ЭП и ключа проверки ЭП) на отчуждаемый ключевой носитель информации или на раздел жесткого диска (в зависимости от выбора пользователя) и производит отправку запроса в УЦ на изготовление сертификата.

Пользователь УЦ приглашается в УЦ (или к доверенному лицу УЦ, наделенному полномочиями по вручению сертификатов от имени УЦ в соответствии с пунктом 4 статьи 13 Федерального закона от 06.04.2011 г. 63-ФЗ «Об электронной подписи»).

УЦ (доверенное лицо УЦ) устанавливает личность заявителя - физического лица, обратившегося за получением сертификата, посредством проверки оригиналов документов (паспорта и СНИЛС).

После положительного подтверждения личности Пользователя УЦ, Администратор УЦ (доверенное лицо УЦ) под расписку ознакамливает Пользователя УЦ с информацией, содержащейся в его квалифицированном сертификате.

Администратор УЦ (доверенное лицо УЦ) передаёт Пользователю УЦ «Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи в электронном виде или на бумажном носителе (Приложение 3).

Пользователь УЦ производит установку сертификата ключа проверки электронной подписи в сформированный ключевой контейнер посредством криптопровайдера, а затем осуществляет процедуру подписания прикрепленных заявительных документов электронной подписью и их отправку в ИФНС с применением ПО «AstralToolBox».

ИФНС рассмотрит заявку в течение трех рабочих дней с момента ее получения.

- Аннулирование (отзыв) квалифицированного сертификата ключа проверки электронной подписи

Для осуществления аннулирования (отзыва) сертификата ключа проверки электронной подписи Пользователь УЦ подает письменное заявление (Приложение 2) на аннулирование (отзыв) принадлежащего ему сертификата ключа проверки электронной подписи Уполномоченному сотруднику УЦ.

Заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи заверяется собственноручной подписью владельца сертификата ключа проверки электронной подписи (Пользователя УЦ).

Уполномоченное лицо УЦ принимает заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи Пользователя УЦ, визирует его и незамедлительно передает заявление Администратору УЦ.

Оповещение Пользователя УЦ об аннулировании (отзыве) его сертификата ключа проверки электронной подписи производится в течение 12 часов с момента выполнения Администратором УЦ действий по аннулированию (отзыву) сертификата ключа проверки электронной подписи Пользователя УЦ путем публикации актуального Списка отозванных сертификатов в точках распространения Списков отозванных сертификатов.

Временем аннулирования (отзыва) сертификата ключа проверки электронной подписи Пользователя УЦ признается время официального уведомления Пользователя УЦ об аннулировании (отзыве) данного сертификата путем публикации актуального Списка отозванных сертификатов в точках распространения Списков отозванных сертификатов.

10. РАЗБОР КОНФЛИКТНЫХ СИТУАЦИЙ

Удостоверяющий центр осуществляет экспертную проверку электронной подписи:

- В электронных документах, сформированных Пользователями УЦ;
- Уполномоченного лица Удостоверяющего центра, которая использовалась для подписи квалифицированных сертификатов ключей проверки электронной подписи Пользователей УЦ, действующих либо срок действия которых уже истек.

Процедура подтверждения электронной подписи в электронных документах

Подтверждение электронной подписи в электронном документе осуществляется Удостоверяющим Центром по обращению Пользователей УЦ, на основании представленного в письменной форме заявления о подтверждении электронной подписи в электронном документе.

В представленном заявлении должна быть указана информация о дате и времени формирования электронной подписи в электронном документе.

Бремя доказывания достоверности даты и времени формирования электронной подписи в электронном документе возлагается на заинтересованную сторону - владельца электронной подписи.

Обязательным приложением к заявлению о подтверждении электронной подписи в электронном документе является внешний носитель электронной информации, на котором записаны:

- исходный (неподписанный) файл электронного документа, к которому применялась электронная подпись;
- файл электронного документа, подписанный электронной подписью, авторство которого оспаривается;
- файл квалифицированного сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра, являющегося издателем квалифицированного сертификата ключа проверки электронной подписи, соответствующего ключу электронной подписи, с помощью которого была сформирована электронная подпись в электронном документе;
- файл списка отозванных сертификатов, издателем которого является Удостоверяющий центр, использовавшийся для проверки электронной подписи в электронном документе заявителем;
- дистрибутивы средств электронной подписи.

Срок рассмотрения заявления о подтверждении электронной подписи в электронном документе составляет 5 (пять) рабочих дней с момента его представления в Удостоверяющий центр.

По результатам проверки Пользователь УЦ получает на руки протокол (Акт) проверки электронной подписи в котором содержатся:

- результат проверки электронной подписи сертифицированным средством электронной подписи;
- детальный отчет по выполненной проверке (экспертизе).
- Детальный отчет по выполненной проверке (экспертизе) содержит следующие обязательные компоненты:
- время и место проведения проверки (экспертизы);
- основания для проведения проверки (экспертизы);
- сведения об эксперте или комиссии экспертов (фамилия, имя, отчество, занимаемая должность;
- вопросы, поставленные перед экспертом или комиссией экспертов;
- объекты исследований и материалы по заявлению, представленные эксперту для проведения проверки (экспертизы);
- содержание и результаты исследований с указанием примененных методов;
- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;
- иные сведения в соответствии с Федеральным законом.

Детальный отчет составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами комиссии экспертов.

В случае отказа в рассмотрении заявления Пользователя УЦ работник Удостоверяющего центра вносит в его заявление свою резолюцию, раскрывающую причину отказа в рассмотрении поступившей заявки, снимает копию заявления. В оригинале заявления и в его копии Пользователь УЦ ставит свою подпись, подтверждающую факт ознакомления с содержащейся в нем резолюцией работника Удостоверяющего центра.

Процедура подтверждения электронной подписи Уполномоченного лица Удостоверяющего центра

Подтверждение электронной подписи Уполномоченного лица Удостоверяющего центра осуществляется по обращению Клиентов, на основании представленного в письменной форме заявления о подтверждении электронной подписи Уполномоченного лица Удостоверяющего центра в квалифицированном сертификате ключа проверки электронной подписи.

Обязательным приложением к заявлению о подтверждении электронной подписи Уполномоченного лица Удостоверяющего центра является внешний носитель электронной информации, на котором записаны:

- файл квалифицированного сертификата ключа проверки электронной подписи, подвергающийся процедуре проверки;
- файл квалифицированного сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра, являющегося издателем квалифицированного сертификата ключа проверки электронной подписи, в достоверности которого заявитель сомневается и намерен подвергнуть процедуре проверки;
- файл списка отозванных сертификатов, издателем которого является Удостоверяющий центр, использовавшийся заявителем для проверки электронной подписи Уполномоченного лица Удостоверяющего центра.

Срок рассмотрения заявления о подтверждении электронной подписи Уполномоченного лица Удостоверяющего центра в квалифицированном сертификате ключа проверки электронной подписи составляет 5 (пять) рабочих дней с момента его представления в Удостоверяющий центр.

По результатам проверки Пользователь УЦ получает на руки протокол (Акт) проверки электронной подписи в котором содержаться:

- результат проверки электронной подписи сертифицированным средством электронной подписи;
- детальный отчет по выполненной проверке (экспертизе).

Детальный отчет по выполненной проверке (экспертизе) содержит следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);
- основания для проведения проверки (экспертизы);
- сведения об эксперте или комиссии экспертов (фамилия, имя, отчество, занимаемая должность;
- вопросы, поставленные перед экспертом или комиссией экспертов;
- объекты исследований и материалы по заявлению, представленные эксперту для проведения проверки (экспертизы);
- содержание и результаты исследований с указанием примененных методов;
- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;
- иные сведения в соответствии с Федеральным законом.

Детальный отчет составляется в письменной форме на бумажном носителе и заверяется собственноручной подписью эксперта, либо в случае формирования комиссии, подписями членов экспертной комиссии.

В случае отказа в рассмотрении заявления Пользователя УЦ работник Удостоверяющего центра вносит в его заявление свою резолюцию, раскрывающую причину отказа в рассмотрении поступившей заявки, снимает копию заявления. В оригинале заявления и в его копии Пользователь УЦ ставит свою подпись, подтверждающую факт ознакомления с содержащейся в нем резолюцией работника Удостоверяющего центра.

11. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

Типы конфиденциальной информации:

- Пароль, предоставляемый пользователю в процессе прохождения процедуры регистрации;
- Персональная и корпоративная информация пользователей, предоставленная УЦ, не подлежащая непосредственной рассылке в качестве части квалифицированного сертификата ключа проверки электронной подписи и СОС;
- Информация, хранящаяся в журналах аудита УЦ;
- Отчетные материалы по выполненным проверкам деятельности УЦ и аудиту информационной безопасности, за исключением заключений по результатам проверок, публикуемых в соответствии с настоящим Регламентом.

Типы информации, не относящейся к конфиденциальной:

- Информация, не относящаяся к конфиденциальной информации, является открытой информацией;
- Открытая информация может публиковаться по решению УЦ. Место, способ и время публикации определяется решением УЦ;
- Информация, включаемая в квалифицированные сертификаты ключей проверки электронной подписи и СОС, издаваемые УЦ, не считается конфиденциальной;
- Также не считается конфиденциальной информация о настоящем Регламенте.

Предоставление конфиденциальной информации:

УЦ не должен раскрывать информацию, относящуюся к типу конфиденциальной информации, каким бы то ни было третьим лицам за исключением случаев:

- Определенных в настоящем Регламенте;
- Требующих раскрытия в соответствии с действующим законодательством РФ или при наличии судебного постановления.

12. ПРОЧИЕ УСЛОВИЯ

Плановая смена квалифицированного сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра

Плановая смена квалифицированного сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра выполняется в период действия ключа электронной подписи Уполномоченного лица Удостоверяющего центра.

Процедура плановой смены квалифицированного сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра осуществляется в следующем порядке:

- Уполномоченное лицо Удостоверяющего центра генерирует новый ключ электронной подписи;
- Уполномоченное лицо Удостоверяющего центра изготавливает новый квалифицированный сертификат ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра.

Уведомление пользователей о проведении смены ключей Уполномоченного лица Удостоверяющего центра осуществляется посредством размещения информации на официальном сайте Удостоверяющего центра.

Старый ключ электронной подписи Уполномоченного лица Удостоверяющего центра используется в течение своего срока действия для формирования списков отозванных сертификатов, изданных Удостоверяющим центром в период действия старого ключа электронной подписи Уполномоченного лица Удостоверяющего центра.

- Внеплановая смена квалифицированного сертификата ключа проверки электронной подписи Пользователя УЦ

Внеплановая смена квалифицированного сертификата ключа проверки электронной подписи Пользователей УЦ осуществляется в следующих случаях:

- при компрометации ключа электронной подписи Пользователя Удостоверяющего центра и аннулировании квалифицированного сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра;
- при компрометации ключа электронной подписи Уполномоченного лица Удостоверяющего центра;
- в случае, если Пользователь УЦ по каким-либо причинам не смог осуществить плановую смену ключа электронной подписи в установленные для этой процедуры сроки;
- в случае изменения идентификационных данных Пользователя УЦ, заносимых в квалифицированный сертификат ключа проверки электронной подписи;
- в иных случаях, вызванных форс-мажорными обстоятельствами.

Компрометация ключевых документов Уполномоченного лица Удостоверяющего центра, внеплановая смена ключа электронной подписи Уполномоченного лица Удостоверяющего центра

В случае компрометации ключа электронной подписи Уполномоченного лица Удостоверяющего центра квалифицированный сертификат ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра аннулируется (отзывается), Пользователи Удостоверяющего центра уведомляются об указанном факте путем рассылки соответствующего уведомления по электронной почте и публикации информации о компрометации на сайте Удостоверяющего центра.

Все квалифицированные сертификаты ключей проверки электронной подписи, подписанные с использованием скомпрометированного ключа электронной подписи Уполномоченного лица Удостоверяющего центра, считаются аннулированными.

После аннулирования квалифицированного сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра выполняется процедура внеплановой смены квалифицированного сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра. Процедура внеплановой смены сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра (пункт 13.1 настоящего Регламента).

Все действовавшие на момент компрометации ключа электронной подписи Уполномоченного лица Удостоверяющего центра квалифицированные сертификаты ключей проверки электронной подписи, а также квалифицированные сертификаты ключей проверки электронной подписи, действие которых было приостановлено, подлежат внеплановой смене.

Компрометация ключевых документов Пользователя Удостоверяющего центра

Пользователь Удостоверяющего центра самостоятельно принимает решение о факте или угрозе компрометации своего ключа электронной подписи.
Пользователь Удостоверяющего центра осуществляет внеплановую смену ключей в соответствии с пунктом 11.2 настоящего Регламента.

Срок действия ключей Уполномоченного лица Удостоверяющего Центра:

- Срок действия ключа электронной подписи Уполномоченного лица Удостоверяющего Центра составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности Удостоверяющего центра, и для средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.
- Начало периода действия ключа электронной подписи Уполномоченного лица Удостоверяющего Центра исчисляется с даты и времени генерации ключа электронной подписи Удостоверяющего центра.
- Срок действия квалифицированного сертификата ключа проверки электронной подписи, соответствующего ключу электронной подписи Уполномоченного лица Удостоверяющего Центра не превышает 6 (шести) лет.
- Время начала и окончания периода действия квалифицированного сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего Центра заносится в поля квалифицированного сертификата ключа проверки электронной подписи «notBefore» и «notAfter».

Сроки действия ключей электронной подписи Пользователей УЦ - владельцев квалифицированных сертификатов ключей проверки электронной подписи ключей подписи:

- Срок действия ключа электронной подписи Пользователя УЦ составляет не более 1 (Одного) года.
- Срок действия квалифицированного сертификата ключа проверки электронной подписи, соответствующего ключу электронной подписи Пользователя УЦ, составляет не более 1 (Одного) года.
- Время начала и окончания периода действия квалифицированного сертификата ключа проверки электронной подписи Пользователя в поля квалифицированного сертификата ключа проверки электронной подписи «notBefore» и «notAfter».

Хранение квалифицированных сертификатов ключей проверки электронной подписи в Удостоверяющем Центре:

- Хранение в Удостоверяющем Центре квалифицированных сертификатов ключей проверки электронной подписи Пользователей УЦ осуществляется в течение всего периода их действия и 5 (Пять) лет после их аннулирования (отзыва) или истечения срока их действия.
- По истечении указанного срока хранения квалифицированные сертификаты ключей проверки электронной подписи переводятся в режим архивного хранения.

Архивное хранение:

- Документы Удостоверяющего Центра на бумажных носителях хранятся в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

Перечень документов Удостоверяющего Центра, подлежащих архивному хранению:

- Аннулированные (отозванные) квалифицированные сертификаты ключей проверки электронной подписи Уполномоченного лица Удостоверяющего Центра;
- Аннулированные (отозванные) квалифицированные сертификаты ключей проверки электронной подписи Пользователей УЦ;
- Заявления на изготовление квалифицированных сертификатов ключей проверки электронной подписи Пользователей УЦ;
- Копии квалифицированных сертификатов ключей проверки электронной подписи Пользователей УЦ на бумажном носителе;
- Заявления на аннулирование (отзыв) квалифицированных сертификатов ключей проверки электронной подписи Пользователей УЦ;
- Заявления на приостановление действия квалифицированных сертификатов ключей проверки электронной подписи Пользователей УЦ;
- Заявления на возобновление действия квалифицированных сертификатов ключей проверки электронной подписи Пользователей УЦ;
- Служебные документы Удостоверяющего Центра.

Документы Удостоверяющего Центра, подлежащие архивному хранению, являются документами временного хранения. Срок хранения архивных документов - 5 (Пять) лет.

•Выделение архивных документов к уничтожению и их уничтожение осуществляется комиссией, формируемой из числа сотрудников Удостоверяющего Центра.

•Структура квалифицированных сертификатов ключей проверки электронной подписи и Списка отозванных сертификатов:

Форма квалифицированного сертификата ключа проверки электронной подписи, выдаваемого Удостоверяющим центром, соответствует требованиям Приказа ФСБ РФ от 27 декабря 2011 года №795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Дополнительно в выдаваемые сертификаты ключей проверки электронной подписи может быть занесено:

- в поле Subject (идентифицирует владельца сертификата):
  - Поле E (Email) - адрес электронной почты;
  - Поле T (Title) - должность полномочного представителя юридического лица;
- расширение Private Key Validity Period - срок действия ключа электронной подписи, соответствующего квалифицированному сертификату ключа проверки электронной подписи, следующего формата:

Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC;

Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC;

- расширение Extended Key Usage (Улучшенный ключ, Расширенное использование ключа) - набор объектных идентификаторов, устанавливающих ограничения на применение электронной подписи совместно с квалифицированным сертификатом ключа проверки электронной подписи (если такие ограничения указаны Пользователем УЦ);
- расширение CRL Distribution Point (Точка распространения списка отозванных сертификатов) - набор адресов точек распространения списков отозванных сертификатов Удостоверяющего центра;
- расширение Authority Information Access (Доступ к информации о центре) - Адрес обращения к Службе актуальных статусов сертификатов в сети «Интернет», Адрес размещения сертификата Удостоверяющего центра в сети «Интернет»;
- иные поля и расширения по усмотрению Удостоверяющего центра, не противоречащие законодательству Российской Федерации.

Для включения в квалифицированный сертификат ключа проверки электронной подписи иной информации о Пользователе УЦ - владельце квалифицированного сертификата, для которой не предусмотрены соответствующие стандартные атрибуты имени, используется дополнение subjectAlternativeName.

Форма списка отозванных сертификатов, создаваемых Удостоверяющим центром, соответствует структуре:

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	Данные Удостоверяющего центра
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида • Серийный номер сертификата (CertificateSerialNumber) • Время обработки заявления на аннулирование (отзыв) сертификата (Time) • Код причины отзыва сертификата (Reson Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы

signatureAlgorithm Issuer Sign Authority Key Identifier	Алгоритм подписи Подпись издателя СОС Расширения Идентификатор ключа издателя	ГОСТ Р 34.11/34.10-2001 Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 списка отозванных сертификатов Идентификатор ключа электронной подписи уполномоченного лица Удостоверяющего центра, на котором подписан СОС
SzOI D_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата уполномоченного лица Удостоверяющего центра (необязательное поле)
CRLNumber	Номер СОС	Порядковый номер выпущенного СОС

Приложение 1.

В Аккредитованный удостоверяющий центр

О Б Р А ЗЕ Ц

Заявление физического лица

на изготовление квалифицированного сертификата ключа проверки электронной подписи

_____

(фамилия, имя, отчество физического лица)

просит создать ключ электронной подписи, ключ проверки электронной подписи и изготовить квалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении данными:

CommonName (CN)	Фамилия, Имя, Отчество	
Locality (L)	Город	
State (S)	Область	
Contry (C)	RU	
E-Mail (E)	Адрес электронной почты	
INN	ИНН физического лица	
SNILS	СНИЛС физического лица	
Наименование филиала		
UPN (основное имя домена)		

Я,

_____

(фамилия, имя, отчество)

_____

(серия и номер паспорта, кем и кода выдан)

1. даю свое согласие на обработку и использование персональных данных, содержащихся в данном заявлении на время действия сертификата ключа проверки электронной подписи;
2. признаю, что указанные мной в данном заявлении персональные данные относятся к общедоступным персональным данным. Настоящее заявление может быть отозвано мной в письменном виде;
3. подтверждаю, что Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи мной получено.

_____ _____

(подпись) (инициалы, фамилия)

«____» _____ 20___ г.

Приложение 2

Аккредитованный Удостоверяющий центр

О Б Р А З Е Ц

Заявление на аннулирование (отзыв)

сертификата ключа проверки электронной подписи физического лица

_____

(фамилия, имя, отчество)

в связи с

_____

(причина отзыва сертификата)

прошу аннулировать (отозвать) сертификат ключа проверки электронной подписи, содержащий следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа проверки электронной подписи	
Surname(SN)	Фамилия	
GivenName(G)	Имя Отчество	

_____ /_____/

(подпись) (фамилия, инициалы)

«____» _____ 201__ г.

Настоящим подтверждаю, что Заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи получено, личность _____

(фамилия, имя, отчество)

идентифицирована, сведения, указанные в Заявлении проверены.

Уполномоченный сотрудник Соисполнителя _____ /_____/
(подпись) (фамилия, инициалы)

«___» _____ 201___г.

Приложение 3

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

---

1. Введение

Настоящее руководство предназначено для обязательного ознакомления Пользователя УЦ, использующего средства электронной подписи (ЭП).

2. Общие положения и определения

Система - автоматизированная информационная система передачи и приема информации в электронном виде по телекоммуникационным каналам связи в виде юридически значимых электронных документов с использованием средств электронной подписи.

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.

Сертификат ключа проверки электронной подписи - 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.

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган).

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

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

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

Удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом.

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

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

Информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Электронные ключи **– персональное средство аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной подписью.**

3. Работа со средствами электронной подписи (ЭП)

Пользователи УЦ, осуществляющие работу со средствами электронной подписи, получившие и использующие ключи электронной подписи, несут персональную ответственность за:

- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы со средствами ЭП;
- сохранение в тайне содержания средств ЭП;
- сохранность носителей ключевой информации и других документов, выдаваемых с ключевыми носителями;
- сохранение в тайне пин – кодов для доступа к электронным ключам и средствам ЭП;
- самостоятельное удаление информации с электронного ключа;
- самостоятельное проведение повторной инициализации электронного ключа, повлекшее удаление информации с электронного ключа;
- своевременную подачу заявления о приостановлении действия или аннулировании сертификата ключа проверки электронной подписи при наличии оснований полагать, что тайна ключа электронной подписи нарушена (см. п. 5 настоящего Руководства - «Компрометация ключа»);
- своевременное обновление сертификата ключа проверки электронной подписи при истечении его срока действия (плановая смена).

Срок действия сертификата ключа проверки электронной подписи – один год с момента изготовления. Заблаговременно до истечения этого срока владелец сертификата ключа проверки электронной подписи, если же в этом есть необходимость, обязан заменить его, обратившись к уполномоченному сотруднику УЦ (Точки регистрации УЦ).

Пользователями УЦ должны быть обеспечены соответствующие условия хранения электронных ключей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования средств ЭП.

Пользователь УЦ так же несет ответственность за то, чтобы на компьютере, на котором установлены средства ЭП, не были установлены и не эксплуатировались программы (в том числе, - вирусы), которые могут нарушить функционирование программных средств и средств ЭП.

При обнаружении на рабочем месте, оборудованном средствами ЭП, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.

Не допускается:

- разглашать содержимое электронных носителей или передавать сами носители лицам, к ним не допущенным, выводить информацию о средствах ЭП на дисплей и принтер;
- подсоединять электронный носитель при проведении работ, не являющихся штатными процедурами использования средств ЭП (создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи), а также к другим ПК;
- вносить какие – либо изменения в программное обеспечение и средства ЭП;
- осуществлять несанкционированное копирование ключевой информации с электронного ключа.

4. Рекомендуемые организационно – технические меры по обеспечению информационной безопасности в организации

Для хранения электронных ключей и средств ЭП и шифрования в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами с двумя экземплярами ключей (один у исполнителя, другой в подразделении безопасности).

Использовать автоматизированное рабочее место (АРМ) с установленными средствами ЭП необходимо в однопользовательском режиме. В отдельных случаях, при необходимости использования АРМ несколькими лицами, эти лица должны обладать равными правами доступа к информации.

При загрузке операционной системы и при возвращении после временного отсутствия пользователя на рабочем месте должен запрашиваться пароль, состоящий не менее чем из 6 символов. В отдельных случаях при невозможности использования парольной защиты, допускается загрузка операционной системы (ОС) без запроса пароля. При этом должны быть реализованы дополнительные организационно – режимные меры, исключающие несанкционированный доступ к этим АРМ.

Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства АРМ с установленными средствами ЭП.

Должны быть предусмотрены меры, исключающие возможность несанкционированного изменения аппаратной части рабочей станции с установленными средствами ЭП.

Установленное на АРМ программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.

Администрирование должно осуществляться доверенными лицами.

Вхождение пользователей в режим конфигурирования BIOS штатными средствами BIOS должно осуществляться только с использованием парольной защиты при длине пароля не менее 6 символов.

После получения электронного ключа рекомендуется произвести смену стандартного пин – кода электронного ключа на свой собственный. Длина пароля должна быть не менее 6 символов.

В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей сотрудника, имевшего доступ к ключевым носителям, должна быть проведена смена ключей электронной подписи, к которым он имел доступ.

5. Компрометация ключа

Под компрометацией ключей электронной подписи понимается их утрата (в том числе с их последующим обнаружением), хищение, разглашение, несанкционированное копирование, передача их по линии связи в открытом виде, увольнение по любой причине сотрудника, имеющего доступ к ключевым носителям или к ключевой информации на данных носителях, любые другие виды разглашения информации о средствах ЭП, в результате которых средства ЭП могут стать доступными несанкционированным лицам и (или) процессам.

Пользователь УЦ должен самостоятельно определить факт компрометации ключа электронной подписи и оценить значение этого события. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием средств ЭП, организует и осуществляет сам Пользователь УЦ.

В случае компрометации владелец ключа электронной подписи (Пользователь УЦ) обязан незамедлительно обратиться в УЦ (к Уполномоченному сотруднику организации, с заявлением на аннулирование (отзыв) сертификата ключа проверки электронной подписи по факту компрометации ключа электронной подписи.

Аннулирование (отзыв) сертификата ключа проверки электронной подписи производится только при личном прибытии владельца сертификата ключа проверки электронной подписи в точку выдачи и предъявлению документа удостоверяющего личность – паспорта.

6. Заключение

Настоящее Руководство составлено на основании:

- Федерального закона от 06.04.2011 № 63 – ФЗ «Об электронной подписи»;
- Федерального закона от 27.07.2006 № 149 – ФЗ «Об информации, информационных технологиях и о защите информации»;
- Приказа ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказа ФСБ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- средств защиты информации (Положение ПКЗ-2005)».