

**Регламент  
Удостоверяющего центра  
Территориального фонда обязательного  
медицинского страхования Оренбургской  
области**

*Редакция №3*

г. Оренбург  
2016 год

## Оглавление

1.	Общие положения.....	6
1.1.	Термины и определения.....	7
1.2.	Статус Регламента .....	10
1.3.	Порядок присоединение к Регламенту.....	10
1.4.	Порядок расторжения Регламента .....	11
1.5.	Порядок изменения (дополнения) Регламента .....	11
1.6.	Идентификация Регламента .....	12
1.7.	Реквизиты удостоверяющего центра.....	12
2.	Предоставление информации .....	12
3.	Права и обязанности Сторон .....	13
3.1.	Обязательства УЦ.....	13
3.2.	Обязательства Стороны, присоединившейся к Регламенту .....	15
3.3.	Обязательства Пользователя УЦ.....	15
3.4.	Права ТФОМС Оренбургской области .....	16
3.5.	Права Пользователя УЦ.....	16
4.	Ответственность Сторон.....	17
5.	Решение споров.....	17
6.	Порядок предоставления и пользования услугами .....	17
6.1.1.	Регистрация Пользователя в УЦ и изготовление первого сертификата.....	17
6.2.	Изготовление сертификата Пользователя УЦ при плановой смене ключей .....	19
6.3.	Изготовление сертификата Пользователя УЦ при внеплановой смене ключей .....	20
6.4.	Аннулирование (отзыв) сертификата Пользователя УЦ .....	21
6.5.	Приостановление действия сертификата Пользователя УЦ.....	22
6.5.1.	Приостановление действия сертификата по заявлению в устной форме .....	23
6.5.2.	Приостановления действия сертификата по заявлению в бумажной форме .....	23
6.5.3.	Приостановление действия сертификата по решению УЦ .....	23
6.6.	Возобновление действия сертификата Пользователя УЦ .....	24
6.7.	Получение информации о статусе сертификата, изданного УЦ.....	24
6.8.	Подтверждение подлинности ЭП в электронном документе.....	25
6.9.	Прочие условия .....	25
7.	Структура сертификатов ключей ЭП.....	26
7.1.	Структура сертификата Пользователя УЦ.....	26
7.2.	Структура данных поля Issuer (идентификационных данных УЦ).....	27
7.3.	Структура данных поля Subject (идентификационных данных владельца сертификата) .....	28
7.3.1.	Для юридических лиц: .....	28
7.3.2.	Для физических лиц: .....	28
7.3.3.	Для индивидуальных предпринимателей: .....	29
7.4.	Структура сертификата ключа ЭП Уполномоченного лица УЦ .....	29
7.5.	Структура списка отозванных сертификатов УЦ.....	30
7.6.	Сроки действия ключевых документов.....	31
7.6.1.	Сроки действия ключевых документов уполномоченного лица УЦ.....	31
7.6.2.	Сроки действия ключевых документов Пользователей УЦ .....	32
7.7.	Плановая смена ключей ЭП Администратора УКЦ УЦ.....	32
7.8.	Компрометация и внеплановая смена ключей ЭП Администратора УКЦ .....	32
8.	Компрометация ключевых документов Пользователя УЦ .....	33
8.1.	Конфиденциальность информации .....	33
8.2.	Хранение сертификатов в УЦ .....	33
8.3.	Прекращение оказания услуг .....	33
8.4.	Форс-мажор.....	34
	Приложение № 1 .....	35

Приложение № 2 .....	37
Приложение № 3 .....	39
Приложение № 4 .....	41
Приложение № 5 .....	43
Приложение № 6 .....	44
Приложение № 7 .....	46
Приложение № 8 .....	49
Приложение № 9 .....	51
Приложение № 10 .....	53
Приложение № 11 .....	60



## 1. ОБЩИЕ ПОЛОЖЕНИЯ

Территориальный фонд обязательного медицинского страхования Оренбургской области (далее – ТФОМС Оренбургской области) является организатором и администратором защищенной сети ViPNet №672 (далее - защищенная сеть). ТФОМС обеспечивает деятельность по выполнению функций Удостоверяющего центра корпоративного уровня Территориального фонда обязательного медицинского страхования Оренбургской области (далее — Удостоверяющий центр (УЦ)), совокупностью штатных единиц, организационных мероприятий, программных и технических средств и мероприятий, в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Регламент Удостоверяющего Центра корпоративного уровня Территориального фонда обязательного медицинского страхования Оренбургской области (далее - Регламент), разработан в соответствии с:

- Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федеральным законом от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи»;
- Гражданским кодексом Российской Федерации;
- Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Общими принципами построения и функционирования информационных систем и порядок информационного взаимодействия в сфере обязательного медицинского страхования, утв. приказом Федерального фонда обязательного медицинского страхования от 7 апреля 2011 г. № 79 (с изм. и доп.);
- Приказом Министерства здравоохранения и социального развития РФ от 25 января 2011 г. №29н «Об утверждении Порядка ведения персонифицированного учета в сфере обязательного медицинского страхования»;
- Приказом Министерства здравоохранения и социального развития РФ от 28 февраля 2011 г. № 158н «Об утверждении Правил обязательного медицинского страхования»;
- Приказом ФСБ РФ от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;
- Приказом ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказом ФАПСИ от 13 июня 2001 г. №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».
- Приказ ТФОМС Оренбургской области от 03.10.2012 г. «О вводе в



действие Положения об организации криптографической защиты информации в системе обязательного медицинского страхования Оренбургской области».

УЦ выполняет свои функции на основании лицензии ФСБ России (ЛСЗ №004973 Рег. № 137Н от 11.08.2014г.) 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).

Целью настоящего Регламента является создание условий для организации защищенного обмена электронными документами и взаимодействия информационных систем, правовых условий использования электронной подписи в электронных документах, при соблюдении которых электронная подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе в соответствии с Федеральным законом РФ от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Настоящий Регламент устанавливает общий порядок и условия предоставления УЦ участникам защищенной сети возможность участвовать в обмене электронными документами, в том числе юридически значимыми, с применением электронной подписи.

Политика УЦ определяет создание, управление и использование усиленных неквалифицированных сертификатов формата X.509 для обеспечения идентификации владельца сертификата и целостности электронной информации. Для юридически значимого электронного взаимодействия Участники Защищенной сети используют электронную подпись, выпущенную УЦ, если требование об использовании усиленной неквалифицированной подписи в соответствии с целями ее использования не противоречит требованиям федеральных законов или принимаемым в соответствии с ними нормативными правовыми актами.

Для обеспечения деятельности УЦ использует средства УЦ, включая средства ЭП, сертифицированные в соответствии с действующим законодательством РФ (разработчик ОАО «Инфотекс» г.Москва, продуктовая линейка ViPNet Custom,).

УЦ предоставляет услуги для:

- участников автоматизированных информационных систем информационного пространства системы обязательного медицинского страхования (далее — Система ОМС) на территории Оренбургской области;
- прочих организаций, с которыми ТФОМС осуществляет электронный информационный обмен в силу закона.

ТФОМС Оренбургской области является зарегистрированным пользователем УЦ.

### **1.1. Термины и определения**

В настоящем Регламенте используются термины и определения, установленные



Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», а также термины и определения их дополняющие и конкретизирующие, а именно:

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

*Электронный документ* – 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.

*Владелец сертификата ключа проверки электронной подписи* (владелец сертификата) – лицо, которому в соответствии с настоящим Регламентом выдан сертификат ключа проверки электронной подписи;

*Заявитель* — юридическое или физическое лицо, обратившееся в УЦ с заявлением на получение электронной подписи;

*Ключ электронной подписи (ключ ЭП)* - уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ электронной подписи действует на определенный момент времени (действующий ключ электронной подписи) если:

- наступил момент времени начала действия ключа электронной подписи;
- срок действия ключа электронной подписи не истек;
- сертификат ключа проверки электронной подписи, соответствующий данному ключу электронной подписи, действует на указанный момент времени.

*Ключ электронной подписи УЦ* - ключ электронной подписи, соответствующий сертификату ключа проверки электронной подписи (корневому сертификату) УЦ.

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

*Ключевая информация* – ключи электронной подписи и проверки электронной подписи, предназначенные для создания/проверки электронной подписи, действующие в течение определенного срока.

*Сертификат ключа проверки электронной подписи (сертификат)* - электронный документ, выданный Удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификат ключа проверки электронной подписи действует на определенный момент времени (действующий сертификат) если:

- наступил момент времени начала действия сертификата ключа проверки электронной подписи;
- срок действия сертификата ключа проверки электронной подписи не истек;
- сертификат ключа проверки электронной подписи не аннулирован, не прекратил действие и действие его не приостановлено;

*Неквалифицированная электронная подпись* - электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;



- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

- создается с использованием средств электронной подписи

*Оператор Удостоверяющего центра (Оператор УЦ)* – ответственный сотрудник ТФОМС Оренбургской области уполномоченный устанавливать личность заявителя - физического лица, обратившегося к нему за получением сертификата, получать от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением сертификата проверять полноту и достоверность информации, предоставленной заявителем/владельцем для включения в сертификат, принимать решения по заявлениям, которые подают заявители и/или владельцы сертификатов, вести реестр Оператора УЦ.

*Администратор Удостоверяющего ключевого центра (Администратор УКЦ)* — уполномоченное лицо Удостоверяющего центра, выполняющий следующие функции:

- управление ключевым центром (УКЦ) УЦ;
- создание и обновление справочно-ключевой информации сетевых узлов ViPNet;
- создание и отзыв сертификатов ключей проверки электронных подписей Пользователей Удостоверяющего центра;
- подпись выпущенных сертификатов, списков отозванных сертификатов своей ЭП уполномоченного лица УЦ;
- заверение собственноручной подписью и своей печатью сертификатов ключей проверки электронных подписей на бумажном носителе.

*Пользователь Удостоверяющего центра (Пользователь УЦ)* – физическое лицо или выступающее в лице своего уполномоченного представителя, юридическое лицо, внесенное в реестр удостоверяющего центра.

*Рабочий день Удостоверяющего центра (далее – рабочий день)* – промежуток времени с 9:00 по 18:00 (время местное) каждого дня недели за исключением выходных и праздничных дней.

*Реестр Оператора УЦ* – набор документов УЦ в электронной и/или бумажной форме, включающий следующую информацию:

- реестр заявлений о присоединении к Регламенту УЦ центра;
- реестр заявлений на регистрацию в УЦ;
- реестр заявлений на создание и выдачу сертификатов ключей проверки электронных подписей;
- реестр заявлений на прекращение действия (аннулирование) 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 УЦ* – набор документов УЦ в электронной и/или бумажной форме, включающий, в том числе, следующую информацию:

- реестр зарегистрированных пользователей УЦ;
- реестр сертификатов ключей проверки электронных подписей;
- реестр изготовленных списков отозванных сертификатов.

*Корневой сертификат УЦ* - сертификат Уполномоченного лица УЦ



(Администратор Удостоверяющего ключевого центра), которым подписаны сертификаты Пользователей УЦ и списки отозванных сертификатов УЦ.

*Список отозванных сертификатов (COC)* – электронный документ с электронной подписью Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, которые на определенный момент времени были аннулированы или действие которых было приостановлено.

*Средство криптографической защиты информации (СКЗИ)* – средство вычислительной техники, осуществляющее криптографические преобразования информации для обеспечения ее безопасности.

*Средство электронной подписи* – средство криптографической защиты информации (СКЗИ), используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

*Cryptographic Message Syntax (CMS)* – стандарт, определяющий формат и синтаксис криптографических сообщений.

*Public Key Cryptography Standards (PKCS)* – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. Удостоверяющий центр осуществляет свою работу в соответствии со следующими стандартами PKCS:

- PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений. Удостоверяющий центр использует описанный в PKCS#7 тип данных PKCS#7 Signed – подписанные данные;
- PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат ключа подписи.

*Ответственный пользователь криптосредств* — сотрудник, назначенный приказом заявителя — юридического лица, на которого возлагается функции по передаче документов других Пользователей УЦ в Удостоверяющий центр, получению ключевой информации для других Пользователей УЦ в соответствии с настоящим Регламентом и Положением об организации криптографической защиты информации в системе обязательного медицинского страхования Оренбургской области.

## **1.2. Статус Регламента**

Настоящий Регламент является договором присоединения к Регламенту участников системы обязательного медицинского страхования Оренбургской области, граждан Российской Федерации, прочих организаций, в соответствии со статьёй 428 Гражданского кодекса Российской Федерации.

## **1.3. Порядок присоединение к Регламенту**

Организация защищенного обмена электронными документами и взаимодействия информационных систем, признание юридической значимости электронных документов в рамках Защищенной сети между ее участниками производится путём подписания и предоставления заинтересованным лицом в УЦ Заявления о присоединении к Регламенту по форме настоящего Регламента.

С момента регистрации в УЦ Заявления о присоединении к Регламенту лицо, подавшее заявление, считается присоединившимся к Регламенту и является Стороной Регламента.

УЦ вправе отказать любому лицу в приёме и регистрации Заявления о присоединении к Регламенту.



Факт присоединения Стороны к Регламенту подтверждается полным принятием ею условий настоящего Регламента и всех его приложений в редакции, действующей на момент присоединения, и Сторона принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

Заявления о присоединении к Регламенту, подписанные в рамках предыдущих редакций Регламента Удостоверяющего центра ТФОМС Оренбургской области распространяют свое действие на настоящую редакцию Регламента и не требуют перезаключения договора присоединения к Регламенту участников системы обязательного медицинского страхования Оренбургской области.

#### **1.4. Порядок расторжения Регламента**

Сторона имеет право в одностороннем порядке расторгнуть договор присоединения к Регламенту, письменно уведомив об этом УЦ за один месяц до дня расторжения. Уведомление о расторжении договора присоединения к Регламенту, полученное УЦ от Стороны, является основанием для обязательного аннулирования сертификатов ключей проверки электронных подписей Пользователей УЦ, уполномоченных данной Стороной. Датой аннулирования указанных сертификатов ключей подписей Пользователей УЦ будет дата расторжения Регламента.

Регламент считается расторгнутым после выполнения Сторонами своих обязательств согласно условиям Регламента.

Расторжение Регламента не освобождает Стороны от исполнения обязательств, возникших до указанного прекращения, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

#### **1.5. Порядок изменения (дополнения) Регламента**

Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится УЦ в одностороннем порядке.

Уведомление о внесении изменений (дополнений) в Регламент осуществляется УЦ путём обязательного размещения указанных изменений (дополнений) на сайте ТФОМС Оренбургской области.

Все изменения (дополнения, новые редакции Регламента), вносимые УЦ в Регламент, не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными по истечении 30 календарных дней с даты размещения указанных изменений и дополнений в Регламент на сайте ТФОМС Оренбургской области.

Все изменения (дополнения), вносимые ТФОМС в Регламент в связи с изменениями действующего законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных нормативных правовых актах.

В случае изменения законодательства Российской Федерации настоящий Регламент применяется в части, не противоречащей действующему законодательству.

Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу. В случае несогласия с изменениями (дополнениями) Сторона Регламента имеет право до вступления в силу таких изменений (дополнений) на расторжение Регламента в порядке, предусмотренном пунктом настоящего Регламента.



Исходя из общих принципов норм права по действию во времени, изданные в установленном порядке нормативные правовые акты не имеют обратной силы и применяются к отношениям, возникшим после вступления актов в силу (если иное не установлено федеральными законами). Учитывая изложенное, сертификаты проверки электронной подписи, выпущенные по требованиям предыдущей версии Регламента, действуют до истечения сроков их действия.

#### **1.6. Идентификация Регламента**

Наименование документа: «Регламент Удостоверяющего центра Территориального фонда обязательного медицинского страхования Оренбургской области».

Регламент Удостоверяющего центра ТФОМС Оренбургской области является Регламентом корпоративного уровня.

Объектный идентификатор УЦ: 1.2.643.3.218.

#### **1.7. Реквизиты удостоверяющего центра**

- Полное наименование юридического лица УЦ: Территориальный фонд обязательного медицинского страхования Оренбургской области

- ИНН 5610032620

- КПП 561001001

- Юридический адрес: 460014, Оренбургская область, город Оренбург, переулок Фабричный, дом 19

- Почтовый адрес: 460014, Оренбургская область, город Оренбург, переулок Фабричный, дом 19

- Получатель: УФК по Оренбургской области (ТФОМС Оренбургской области л/с 03535035060)

- р/с 40404810253540000001 в ГРКЦ ГУ Банка России по Оренбургской области г. Оренбург

- БИК 045354001

- ОКПО 23920766

- ОКАТО 53401364000.

Контактная информация:

- Телефон: (3532)98-15-00;

- Факс: (3532)77-50-83;

- Адрес электронной почты: office@orenfoms.ru

- Адрес сайта: <http://www.orenfoms.ru>

## **2. ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ**

УЦ вправе запросить, а Сторона, присоединившаяся к Регламенту, обязана представить в УЦ документы, подтверждающие достоверность информации предоставленной заявителем для включения в сертификат.

При представлении оригиналов документов Оператор УЦ делает копии документов, заверяет их своей подписью и оттиском своей печати.

Копии документов, предоставляемые Стороной, присоединившейся к Регламенту, должны быть надлежащего качества, заверены подписью руководителя и оттиском гербовой печати или нотариально.

Представлять, предоставлять и получать документы в УЦ для осуществления



действий в рамках настоящего Регламента, владелец сертификата может лично или через ответственного пользователя криптосредств (для юридических лиц).

Оригиналы (нотариально заверенные копии документов) представляются в УЦ для идентификации личности и подтверждения информации, включаемой в сертификат, в случае необходимости Оператор УЦ делает копии документов и возвращает оригиналы документов. Копии документов, заверенные надлежащим образом предоставляемые в УЦ (не возвращаются).

### **Перечень документов необходимых при получении сертификата**

#### ***для заявителей - юридических лиц:***

- 1) учредительные документы или копии, заверенные надлежащим образом;
- 2) свидетельство о государственной регистрации или копия, заверенная надлежащим образом;
- 3) свидетельство о постановке на учет в налоговом органе или копия, заверенная надлежащим образом;
- 4) копия документа, заверенная надлежащим образом, подтверждающая право руководителя действовать от имени юридического лица;
- 5) копии документов, заверенные надлежащим образом, подтверждающие правомочность лица, выступающего от имени заявителя - юридического лица, обращаться за получением сертификата с указанием полномочий и/или надлежащим образом оформленные доверенности (Приложение № 11);
- 6) копия приказа, заверенная надлежащим образом, о назначении ответственного пользователя криптосредств в случае, если документы предоставляются не владельцем сертификата.

Документы, перечисленные в пунктах 1 - 4 могут не предоставляться в УЦ, если они предоставлены и зарегистрированы в ТФОМС Оренбургской области в рамках иных нормативно-правовых актов и требований.

#### ***для физических лиц:***

- 1) документы, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность заявителя — физического лица;
- 2) страховое свидетельство государственного пенсионного страхования заявителя — физического лица;
- 3) идентификационный номер налогоплательщика.
- 4) согласие на обработку персональных данных, подписанное собственноручной подписью физического лица;
- 5) доверенность или иной документ, подтверждающий право заявителя действовать от имени других лиц;

Заявитель в заявлении на изготовление сертификата указывает ограничения использования квалифицированного сертификата (если такие ограничения имеются).

## **3. ПРАВА И ОБЯЗАННОСТИ СТОРОН**

### **3.1. Обязательства УЦ**

Предоставить Пользователю УЦ сертификат уполномоченного лица Удостоверяющего центра.



Обеспечить регистрацию пользователей в Удостоверяющем центре по заявлениям на регистрацию в Удостоверяющем центре, в соответствии с порядком, определённым в настоящем Регламенте.

Обеспечить занесение регистрационной информации Пользователя УЦ в Реестр Удостоверяющего центра.

Обеспечить изготовление сертификата, зарегистрированного в Удостоверяющем центре Пользователя УЦ, по заявлению на изготовление сертификата ключа проверки подписи Пользователя Удостоверяющего центра (Приложение № 3), в соответствии с порядком, определённым в настоящем Регламенте.

Аннулировать (отозвать), приостановить и возобновить действие сертификата пользователя УЦ по соответствующему заявлению на аннулирование (отзыв), приостановление и возобновление действия сертификата, в соответствии с порядком, определённым в настоящем Регламенте.

Аннулировать (отозвать) сертификат Пользователя УЦ, если истёк установленный срок, на который действие сертификата было приостановлено.

Аннулировать (отозвать) сертификат Пользователя УЦ в случае компрометации ключа ЭП уполномоченного лица Удостоверяющего центра, с использованием которого был издан сертификат.

Официально уведомить об аннулировании (отзыве), приостановлении и возобновлении действия сертификата всех лиц, зарегистрированных в Удостоверяющем центре.

Публиковать актуальный список отозванных сертификатов на своём сайте. Период публикации списка отозванных сертификатов в рабочее время Удостоверяющего центра — один час.

Предоставлять безвозмездно любому лицу по его письменному обращению информацию, содержащуюся в реестре сертификатов.

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

Обеспечивать конфиденциальность созданных удостоверяющим центром ключей электронных подписей.

Хранить информацию, внесенную в реестр сертификатов в течении всего срока деятельности УЦ.

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

Использовать для создания и проверки усиленных неквалифицированных электронных подписей, создания ключей усиленных неквалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с федеральным законодательством.

Для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи использовать средства электронной подписи которые:

- позволяют установить факт изменения подписанного электронного документа после момента его подписания;



- обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки.

### **3.2. Обязательства Стороны, присоединившейся к Регламенту**

Письменно известить ТФОМС Оренбургской области о внесенных изменениях в документы, приведённых в пункте 2 и предоставить документы в течении пяти рабочих дней с момента регистрации данных изменений.

С целью обеспечения гарантированного ознакомления Стороны, присоединившейся к Регламенту, с полным текстом изменений и дополнений Регламента до вступления их в силу, не реже одного раза в тридцать календарных дней должны обращаться на сайт ТФОМС Оренбургской области за сведениями об изменениях и дополнениях в Регламент.

### **3.3. Обязательства Пользователя УЦ**

Обязанности Пользователя УЦ:

#### **3.3.1 Обязанности лиц, проходящих процедуру регистрации:**

- Лица, проходящие процедуру регистрации в УЦ, обязаны представить регистрационную информацию в требуемом для создания сертификата объеме;
- Лица, проходящие процедуру регистрации в УЦ, несут ответственность за достоверность предоставленной регистрационной информации.

#### **3.3.2 Обязанности владельца электронной подписи:**

- Использовать для создания и проверки усиленных неквалифицированных электронных подписей, создания ключей усиленных неквалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральными законами, совместимых со средствами УЦ;
- Обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;
- Пользователь УЦ обязан применять для формирования ЭП только действующий ключ ЭП;
- Применять ключ ЭП только в соответствии с областями применения, определенными в полях сертификата: KeyUsage, ExtendedKeyUsage и CertificatePolicies;
- Уведомлять УЦ, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- Не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
- Не использовать ключ ЭП и связанный с ним сертификат, заявление на аннулирование (отзыв) которого подано в УЦ;
- Использовать электронную подпись в соответствии с «Руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи» (далее - Руководство), которое является информационным документом, описывающим условия и порядок использования электронных подписей и средств электронной подписи, риски, связанные с использованием электронных



подписей, меры, необходимые для обеспечения безопасности электронных подписей (Приложение № 10). Руководство публикуется на сайте ТФОМС Оренбургской области (<http://www.orenfoms.ru>).

### **3.4. Права УЦ**

Отказать Пользователю в регистрации в УЦ в случае ненадлежащего оформления необходимых регистрационных документов.

Отказать в изготовлении сертификата Пользователя УЦ в случае ненадлежащего оформления заявления на изготовление сертификата.

Отказать в аннулировании (отзыве) сертификата Пользователя УЦ в случае ненадлежащего оформления заявления на аннулирование (отзыв) сертификата.

Отказать в приостановлении/возобновлении действия сертификата Пользователя УЦ в случае ненадлежащего оформления заявления на приостановлении/возобновление действия сертификата.

Отказать в аннулировании (отзыве) сертификата Пользователя УЦ в случае, если истек установленный срок действия ключа ЭП, соответствующего этому сертификату.

Отказать в приостановлении действия сертификата Пользователя УЦ в случае, если истек установленный срок действия ключа ЭП, соответствующего этому сертификату.

Отказать в возобновлении действия сертификата Пользователя УЦ в случае, если истек установленный срок действия ключа ЭП, соответствующего этому сертификату.

Отказать в изготовлении сертификата Пользователя УЦ в случае, если использованное Пользователем УЦ для формирования запроса на сертификат средство криптографической защиты информации (средство ЭП) не поддерживается Удостоверяющим центром.

В одностороннем порядке приостановить действие сертификата Пользователя УЦ с обязательным уведомлением владельца сертификата, действие которого приостановлено, и указанием обоснованных причин.

### **3.5. Права Пользователя УЦ**

Применять сертификат уполномоченного лица УЦ для проверки ЭП уполномоченного лица УЦ в сертификатах, изготовленных УЦ.

Применять список отозванных сертификатов, изготовленный УЦ, для установления статуса сертификатов, изготовленных УЦ.

Применять сертификат Пользователя УЦ для проверки ЭП электронных документов в соответствии со сведениями, указанными в сертификате.

Для хранения личного ключа ЭП применять носитель, поддерживаемый средством ЭП.

Обратиться в УЦ с заявлением на изготовление сертификата.

Обратиться в УЦ с заявлением на аннулирование (отзыв) и приостановление действия сертификата, владельцем которого он является, в течение срока действия соответствующего ключа ЭП.

Обратиться в УЦ с заявлением на возобновление действия сертификата, владельцем которого он является, в течение срока действия соответствующего ключа ЭП и срока, на который действие сертификата было приостановлено.

Обратиться в УЦ области за получением информации о статусе сертификатов и



их действительности на определенный момент времени.

Обратиться в УЦ области за подтверждением подлинности ЭП в электронном документе, сформированной с использованием сертификата, изданного УЦ.

#### **4. ОТВЕТСТВЕННОСТЬ СТОРОН**

Ответственность Сторон регулируется действующим законодательством Российской Федерации,

УЦ не несёт ответственности за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, если УЦ обоснованно полагался на сведения, указанные в заявлениях Пользователя УЦ.

Вся ответственность по регистрации Пользователя УЦ, занесению данных в сертификаты, принятию решений по изготовлению и управлению сертификатами, формированию копий сертификатов Пользователя УЦ полностью возлагается на Оператора УЦ, являющегося полномочным лицом УЦ.

Сторона, присоединившаяся к Регламенту, несёт ответственность за достоверность сведений о владельцах сертификатов, указанных в сертификатах, изготавливаемых УЦ по заявлениям Пользователя УЦ.

#### **5. РЕШЕНИЕ СПОРОВ**

Сторонами в споре, в случае его возникновения, считаются ТФОМС Оренбургской области и Сторона, присоединившаяся к Регламенту.

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 20 (двадцати) календарных дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа. К ответу должны быть приложены все необходимые документы.

Спорные вопросы между Сторонами, не урегулированные в претензионном порядке, решаются в Арбитражном суде по месту регистрации ТФОМС Оренбургской области.

#### **6. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ПОЛЬЗОВАНИЯ УСЛУГАМИ**

##### **6.1.1. Регистрация Пользователя в УЦ и изготовление первого сертификата**

УЦ осуществляет регистрацию физических лиц и уполномоченных представителей юридических лиц только в том случае, если указанное лицо присоединилось к Регламенту в соответствии с пунктом 10 настоящего Регламента.

Регистрация Пользователя в УЦ осуществляется на основании заявления на регистрацию по форме Приложение № 2 настоящего Регламента. Пользователь УЦ с заявлением на регистрацию предоставляет документы, подтверждающие достоверность информации, предоставленной заявителем для включения в сертификат. Перечень необходимых документов приведен в пункте 2 настоящего Регламента.

В случае, если Пользователем УЦ представляются оригиналы документа удостоверяющего личность, страхового свидетельства государственного пенсионного



страхования или других документов уполномоченное лицо УЦ или Оператор УЦ по необходимости делают копии документов и заверяют их собственноручно.

Заявление на регистрацию, документы, могут предоставляются в ТФОМС Оренбургской области:

- лично;
- через ответственного пользователя криптосредств (при себе иметь, паспорт, копию приказа о назначении ответственного пользователя криптосредств);
- посредством почтовой либо курьерской связи, с описью вложений.

После получения необходимых регистрационных документов Оператор УЦ принимает решение о регистрации и об изготовлении первого сертификата.

В случае отказа в регистрации Пользователь уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, Оператор УЦ регистрирует Пользователя УЦ.

Регистрация Пользователя УЦ должна быть осуществлена не позднее 5 (пяти) рабочих дней, следующих за днем, и течение которого был предоставлен полный комплект регистрационных документов.

Средства Электронной подписи (криптографической средства), предназначенные для работы с ЭП, приобретаются Сторонами самостоятельно. Это необходимо сделать до подачи заявлений о регистрации пользователя в УЦ.

Изготовление первого усиленного неквалифицированного сертификата осуществляется на основании заявления на изготовление сертификата по форме Приложение № 3 настоящего Регламента.

Способ предоставления файла запроса (необходимость использования файла определяется Оператором УЦ) на сертификат (файл формата PKCS#10 в кодировке Base64) определяется Пользователем УЦ по согласованию с Оператором УЦ.

Заявление на изготовление сертификата и документы физическими лицами предоставляются в УЦ лично. Оператор УЦ устанавливает личность заявителя - физического лица, обратившегося к нему за получением сертификата.

После предоставления необходимых документов и данных Оператор УЦ осуществляет проверку корректности данных, указанных в заявлении на изготовление сертификата и принимает решение об изготовлении первого сертификата. А так же Оператор УЦ осуществляет проверку средств электронной подписи с помощью которых, формировался файл запроса на предмет соответствия обязательным требованиям по защите сведений соответствующей степени секретности в соответствии с законодательством Российской Федерации.

В случае отказа в изготовлении сертификата Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, Администратор Удостоверяющего ключевого центра изготавливает сертификат Пользователю УЦ. Оператор УЦ предоставляет сертификат Пользователю УЦ, способ предоставления сертификата определяется Пользователем УЦ по согласованию с Оператором УЦ.

Изготовление сертификата должно быть осуществлено не позднее 5 (пяти) рабочих дней следующих за днем, в течение которого был предоставлен полный комплект документов (заявление на изготовление сертификата, файл запроса на сертификат).

После изготовления сертификата Администратор Удостоверяющего ключевого центра формирует, визирует и заверяет печатью УЦ два экземпляра сертификата на



бумажном носителе, которые предоставляются Пользователю УЦ.

## **6.2. Изготовление сертификата Пользователя УЦ при плановой смене ключей**

Изготовление сертификата юридического лица при плановой смене ключей осуществляется на основании запроса на сертификат (Приложение № 3) и документов, подтверждающих достоверность информации предоставленной заявителем для включения в сертификат.

Документы, предоставляются юридическим лицом в УЦ посредством:

- лично;
- через ответственного пользователя криптосредств;
- почтовой либо курьерской связью, с описью вложений.

Файлы, содержащие сканкопии документов (формат PDF/A), подтверждающих достоверность информации, предоставленной в файле запросе, должны быть подписаны ЭП руководителя заявителя - юридического лица. ЭП руководителя заявителя - юридического лица, может быть либо квалифицированная ЭП, либо неквалифицированная усиленная ЭП, выпущенная УЦ. Запрос на сертификат подписывается действующей ЭП Пользователя УЦ.

Изготовление сертификата физического лица при плановой смене ключей осуществляется на основании запроса на сертификат и следующих документов, подтверждающих достоверность информации предоставленной заявителем для включения в сертификат:

- паспорт гражданина Российской Федерации или иного документа, удостоверяющего личность лица, выступающего от имени заявителя - юридического лица или копия (2-я, 3-я страницы паспорта и место регистрации);
- страховое свидетельство государственного пенсионного страхования физического лица, или копия, заверенная в установленном порядке;
- идентификационный номер налогоплательщика физического лица или копия, заверенная в установленном порядке;
- заявление на изготовление сертификата и документы физическими лицами предоставляются в Удостоверяющий центр лично. Оператор УЦ устанавливает личность заявителя - физического лица, обратившегося к нему за получением квалифицированного сертификата.

В случае, если к моменту формирования файла запроса на сертификат, ключ ЭП прекратил своё действие, то обновить сертификат в автоматическом режиме будет невозможно.

В случае использования СКЗИ VipNet CSP, сформированный запрос на сертификат можно передать Оператору УЦ лично, либо почтовой или курьерской связью с описью вложений. Способ передачи предварительно должен согласовываться с Оператором УЦ.

После предоставления заявления и документов для выпуска сертификата в УЦ, Оператор УЦ проверяет достоверность информации предоставленной заявителем для включения в сертификат и принимает решение по заявлению. А так же Оператор УЦ осуществляет проверку средств электронной подписи, с помощью которых формировался файл запроса на предмет соответствия обязательным требованиям по защите сведений соответствующей степени секретности в соответствии с законодательством Российской Федерации.

В случае отказа в изготовлении сертификата Пользователь УЦ уведомляется об



этом с указанием причины отклонения заявления. При использовании СКЗИ VipNet Client статус запроса пользователь может узнать при помощи средств СКЗИ.

При принятии положительного решения, Администратора Удостоверяющего ключевого центра изготавливает сертификат Пользователю УЦ. Оператор УЦ предоставляет сертификат Пользователю УЦ, способ предоставления сертификата определяется Пользователем УЦ по согласованию с Оператором УЦ.

Изготовление сертификата и уведомление Пользователя УЦ об изготовлении сертификата должны быть осуществлены не позднее 5 (пяти) рабочих дней, следующих за днём, в течении которого было получено и зарегистрировано в УЦ заявление на изготовление сертификата.

По запросу Пользователя УЦ, после изготовления сертификата Администратора Удостоверяющего ключевого центра формирует, визирует и заверяет печатью УЦ экземпляр сертификата на бумажном носителе.

### **6.3. Изготовление сертификата Пользователя УЦ при внеплановой смене ключей**

Внеплановая смена ключей осуществляется Пользователем УЦ в следующих случаях:

- при компрометации ключа ЭП Пользователя УЦ;
- при компрометации ключа ЭП Администратора УКЦ Удостоверяющего центра;
- в случае, если Пользователь УЦ по каким-то причинам не смог осуществить плановую смену ключей в установленные для этой процедуры сроки;
- в иных случаях, вызванных форс-мажорными обстоятельствами.

При внеплановой смене ключей ЭП документы и заявление в бумажной форме предоставляется юридическим лицом в УЦ по форме (Приложение № 3) к настоящему Регламенту посредством почтовой либо курьерской связью, с описью вложений.

Изготовление сертификата для физического лица при внеплановой смене ключей осуществляется на основании заявления на изготовление в бумажной форме (Приложение № 3), запроса на сертификат и следующих документов, подтверждающих достоверность информации предоставленной заявителем для включения в сертификат в соответствии с разделом 2 данного Регламента.

Заявление на изготовление сертификата и документы физическими лицами предоставляются в УЦ лично. Оператор УЦ устанавливает личность заявителя - физического лица, обратившегося к нему за получением сертификата.

Изготовление неквалифицированного сертификата при внеплановой смене ключей осуществляется на основании заявления на изготовление сертификата в бумажной форме и запроса на сертификат.

После предоставления необходимых документов и данных Оператор УЦ осуществляет сравнение содержимого файла запроса на сертификат с данными, указанными в заявлении на изготовление сертификата и с данными указанными в документах, подтверждающих достоверность информации предоставленной заявителем для включения в сертификат, принимает решение об изготовлении сертификата.

В случае отказа в изготовлении сертификата Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, Администратор УКЦ изготавливает



сертификат.

Изготовление сертификата и уведомление Пользователя УЦ об изготовлении сертификата должны быть осуществлены не позднее 5 (пяти) рабочих дней, следующих за днем, в течение которого был предоставлен полный комплект документов.

После изготовления сертификата Администратор УКЦ по запросу пользователя формирует, визирует и заверяет печатью УЦ два экземпляра сертификата на бумажном носителе, которые предоставляются Пользователю УЦ.

#### **6.4. Аннулирование (отзыв) сертификата Пользователя УЦ**

УЦ аннулирует сертификат Пользователя УЦ в следующих случаях:

- в случае прекращения действия настоящего Регламента в отношении Стороны, присоединившейся к Регламенту;
- в случае прекращения полномочий Пользователя УЦ;
- при компрометации ключа ЭП Пользователя УЦ.
- при компрометации ключа ЭП уполномоченного лица УЦ.

В случае прекращения действия настоящего Регламента, прекращения полномочий Пользователя УЦ, истечения срока, на который было приостановлено действие сертификата, отзыва сертификата Пользователя УЦ по его заявлению или заявлению заявителя — юридического лица УЦ должен официально уведомить Пользователя УЦ и всех лиц, зарегистрированных в УЦ, об аннулировании (отзыве) сертификата не позднее одного рабочего дня с момента наступления описанного события.

Сторона, присоединившаяся к Регламенту, являющаяся юридическим лицом, вправе аннулировать (отозвать) сертификаты своих полномочных представителей, зарегистрированных в УЦ.

Официальным уведомлением о факте отзыва сертификата является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения об отозванном сертификате, и изданного не ранее времени наступления произошедшего случая. Временем отзыва сертификата признается время издания указанного списка отозванных сертификатов, хранящееся в поле `thisUpdate` списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты в расширение CRL Distribution Point сертификата.

В случае аннулирования сертификата Пользователя УЦ по истечении срока его действия временем аннулирования сертификата Пользователя УЦ признается время, хранящееся в поле `notAfter` поля `Validity` сертификата. В данном случае информация об аннулированном сертификате Пользователя УЦ в список отозванных сертификатов не заносится.

В случае компрометации ключа электронной подписи УЦ временем аннулирования сертификата Пользователя УЦ признается время компрометации ключа электронной подписи УЦ, фиксирующееся в реестре УЦ. В случае компрометации ключа электронной подписи УЦ информация о сертификате Пользователя УЦ в список отозванных сертификатов не заносится.

Аннулирование (отзыв) сертификата осуществляется по заявлению его владельца, в бумажной форме, либо по заявлению заявителя-юридического лица, присоединившегося к Регламенту.



Заявление в бумажной форме предоставляется в УЦ по форме (Приложение № 4) к настоящему Регламенту посредством почтовой либо курьерской связи.

После предоставления заявления Оператор УЦ принимает решение об аннулировании (отзыве) сертификата.

В случае отказа в аннулировании (отзыве) сертификата Пользователь УЦ или заявитель-юридическое лицо уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, Оператор УЦ осуществляет аннулирование (отзыв) сертификата.

Аннулирование (отзыв) сертификата и официальное уведомление Пользователя УЦ об аннулировании (отзыве) сертификата должны быть осуществлены не позднее одного рабочего дня, следующего за днём, в течение которого было зарегистрировано заявление в Удостоверяющем центре.

Аннулирование (отзыв) сертификатов Пользователей УЦ, являющихся полномочными представителями Стороны, присоединившейся к Регламенту, осуществляется путем отзыва полномочий (доверенность/приказ) сотрудника, на основании которой Пользователю УЦ предоставлялись услуги Удостоверяющего центра. Форма заявления на отзыв полномочий сотрудника Приложение № 5.

Аннулирование (отзыв) сертификата и официальное уведомление Пользователя УЦ об аннулировании (отзыве) сертификата должны быть осуществлены не позднее одного рабочего дня, следующего за днем, в течение которого было зарегистрировано заявление на отзыв доверенности в УЦ.

#### **6.5. Приостановление действия сертификата Пользователя УЦ**

УЦ приостанавливает действие сертификата Пользователя УЦ в следующих случаях:

- по заявлению Пользователя УЦ в бумажной форме;
- по заявлению Пользователя УЦ в устной форме в случае компрометации или подозрения в компрометации ключа ЭП Пользователя УЦ;
- в иных случаях, предусмотренных положениями настоящего Регламента, по решению УЦ.

Действие сертификата приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата составляет десять дней.

Если в течение срока приостановления действия сертификата действие этого сертификата не будет возобновлено, то сертификат аннулируется (отзывается) УЦ.

Приостановление действия сертификата и официальное уведомление Пользователя УЦ о приостановлении действия сертификата должны быть осуществлены не позднее одного рабочего дня, следующего за рабочим днем, в течение которого УЦ было принято заявление.

Официальным уведомлением о факте приостановления действия сертификата является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено, и изданного не ранее времени наступления произошедшего случая. Временем приостановления действия сертификата признается время издания указанного списка отозванных сертификатов, хранящееся в поле `thisUpdate` списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные УЦ сертификаты в расширение CRL Distribution Point сертификата.



Приостановление действия сертификата осуществляется по заявлению его владельца, поданному в Удостоверяющий центр в устной, электронной или бумажной форме, а также по решению Удостоверяющего центра в случаях, определенных настоящим Регламентом.

#### **6.5.1. Приостановление действия сертификата по заявлению в устной форме**

Приостановление действия сертификата по заявлению Пользователя УЦ в устной форме осуществляется исключительно при компрометации ключа ЭП или подозрении и компрометации ключа ЭП Пользователя УЦ.

Заявление в устной форме подается в УЦ по телефону.

Заявитель должен сообщить Оператору УЦ следующую информацию:

- идентификационные данные владельца сертификата;
- серийный номер сертификата, действие которого требуется приостановить;
- срок, на который приостанавливается действие сертификата.

Заявление принимается только в случае положительной аутентификации Пользователя УЦ.

Приняв заявление Оператор УЦ принимает решение о приостановлении действия сертификата. В случае, если Оператор УЦ не смог достоверно идентифицировать заявителя, то он вправе отказать в приостановлении действия сертификата.

В случае отказа в приостановлении действия сертификата Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При положительном решении, Оператор УЦ приостанавливает действие сертификата.

#### **6.5.2. Приостановления действия сертификата по заявлению в бумажной форме**

Заявление на приостановление сертификата предоставляется в Удостоверяющий центр в бумажной форме, посредством почтовой либо курьерской связи.

После предоставления заявления Оператор УЦ принимает решение о приостановлении действия сертификата.

В случае отказа в приостановлении действия сертификата Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При положительном решении, Оператор УЦ приостанавливает действие сертификата.

#### **6.5.3. Приостановление действия сертификата по решению УЦ**

УЦ вправе приостановить действие сертификата Пользователя УЦ в случаях компрометации или подозрения в компрометации ключа ЭП Пользователя УЦ в том случае, если Пользователю УЦ не было известно о возможном факте компрометации ключей, а также в случаях неисполнения обязательств Пользователя УЦ по настоящему Регламенту.

После приостановления действия сертификата Оператор УЦ сообщает Пользователю УЦ о наступлении события, повлекшего приостановление действие сертификата, и уведомляет его о том, что действие сертификата Пользователя УЦ



приостановлено.

#### **6.6. Возобновление действия сертификата Пользователя УЦ**

Возобновление действия сертификата может быть осуществлено исключительно в период приостановления действия сертификата.

Возобновление действия сертификата и официальное уведомление Пользователя УЦ о возобновлении действия сертификата должны быть осуществлены не позднее одного рабочего дня, следующего за днем, в течение которого УЦ было принято заявление.

Официальным уведомлением о факте возобновления действия сертификата является опубликование первого (наиболее раннего) списка отозванных сертификатов, не содержащего сведения о сертификате, действие которого было возобновлено, и изданного не ранее времени предоставления заявления на возобновление действия сертификата. Временем возобновления действия сертификата признается время издания указанного списка отозванных сертификатов, хранящееся в поле `thisUpdate` списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты в расширение CRL Distribution Point.

Возобновление действия сертификата осуществляется на основании заявления в бумажной форме (Приложение № 7). Заявление предоставляется в ТФОМС почтовой либо курьерской связью.

После получения заявления Оператор УЦ принимает решение о возобновлении действия сертификата.

В случае отказа в возобновлении действия сертификата Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, Оператор УЦ возобновляет действие сертификата.

#### **6.7. Получение информации о статусе сертификата, изданного УЦ**

Получение информации о статусе сертификата, изданного УЦ осуществляется на основании заявления Пользователя УЦ. Данное заявление оформляется по форме (Приложение № 8) и предоставляется в УЦ посредством почтовой либо курьерской связи.

Заявление должно содержать следующую информацию:

- время и дата подачи заявления;
- время и дата (либо период времени), на момент наступления которых требуется установить статус сертификата;
- идентификационные данные Пользователя УЦ, статус сертификата которого требуется установить;
- серийный номер сертификата, статус которого требуется установить.

По результатам проведения работ по заявлению оформляется ответ, содержащая информацию о статусе сертификата, который предоставляется Пользователю УЦ.

Предоставление Пользователю УЦ ответа о статусе сертификата должно быть осуществлено не позднее десяти рабочих дней с момента получения ТФОМС соответствующего заявления.



### **6.8. Подтверждение подлинности ЭП в электронном документе**

По желанию Стороны, присоединившейся к Регламенту, УЦ осуществляет проведение экспертных работ по подтверждению подлинности ЭП в электронном документе.

В данном случае для подтверждения подлинности ЭП в электронных документах Пользователь УЦ подает заявление в УЦ (Приложение № 9).

Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные Пользователя УЦ, 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.

Обязательным приложением к заявлению на подтверждение подлинности ЭП и электронном документе является электронный носитель, содержащий:

- сертификат, 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 нескольких файлов: один из которых содержит данные, а другой значение ЭП этих данных.

Проведение работ по подтверждению подлинности ЭП в электронном документе осуществляет комиссия, сформированная из числа сотрудников Удостоверяющего центра.

Результатом проведения работ по подтверждению подлинности ЭП в электронном документе является заключение Удостоверяющего центра.

Заключение содержит:

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

Отчет по выполненной проверке содержит:

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

Заключение УЦ по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

Срок проведения работ по подтверждению подлинности ЭП в одном электронном документе и предоставлению Пользователю заключения по выполненной проверке определяется УЦ.

### **6.9. Прочие условия**

Период времени действия ключа ЭП, соответствующего выданному сертификату Пользователя УЦ должен находиться в пределах периода времени, на который Стороной, присоединившейся к Регламенту (для юридических лиц) выдана соответствующая доверенность на совершение действий, определённых положениями



настоящего Регламента.

Стороны признают равную юридическую силу собственноручной подписи и ЭП в электронных документах.

## 7. СТРУКТУРА СЕРТИФИКАТОВ КЛЮЧЕЙ ЭП

### 7.1. Структура сертификата Пользователя УЦ

Название	Описание	Содержание
<b>Базовые поля сертификата</b>		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	идентификатор криптографического алгоритма с помощью которого УЦ сформировал ЭП данного сертификата (ГОСТ Р 34.10/34.11-2001)
Encrypted	ЭП	ЭП сформированная УЦ, под структурированной совокупностью полей сертификата
Issuer	Сведения об издателе сертификата	См. п. настоящего Регламента
Validity Period	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм:сс GMT Действителен по: дд.мм.гггг чч:мм:сс GMT
Subject	Сведения о владельце сертификата	См. п. настоящего Регламента
Subject Alternative Name	Дополнительные сведения о владельце сертификата	Информации о владельце сертификата, для которой не предусмотрены соответствующие стандартные атрибуты имени, в том числе информации о полномочиях владельца сертификата и сроке их действия
Subject Public Key Info	Ключ проверки ЭП	алгоритм подписи (ГОСТ Р 34.10/34.11-2001), значение ключа проверки ЭП владельца сертификата
<b>Дополнения сертификата</b>		
Key Usage (critical)	Область использования ключа проверки ЭП	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Электронная подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшенный ключ ЭП	Набор идентификаторов (OID),



		определяющий отношения, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение)
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор ключа ЭП уполномоченного лица Удостоверяющего Центра, на котором подписан данный сертификат
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор ключа ЭП владельца сертификата
Certificate Policies	Политики сертификации	Политики в соответствие с которыми должен использоваться сертификат
Subject Sign Tool	Средства ЭП владельца	Наименование средств ЭП, владельца сертификата
Issuer Sign Tool	Средства ЭП издателя	Средства ЭП и средства УЦ, которые использованы для создания ключа ЭП, ключа проверки ЭП, сертификата, реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с Федеральным законодательством
CRL Distribution Points	Точки распространения списка отозванных сертификатов (CRL)	

## 7.2. Структура данных поля Issuer (идентификационных данных УЦ)

Название	Описание	Содержание
CommonName, CN	Общее имя	Наименование (псевдоним)УЦ
CountryName, C	Страна	RU
LocalityName, L	Город, населенный пункт	г. Оренбург
StateOrProvinceName, S	Наименование субъекта РФ	Оренбургская обл.
StreetAdress, Street	Название улицы, номер дома, квартира, строение	пер. Фабричный, д. 19
OrganizationName, O	Наименование организации	ТФОМС Оренбургской обл.
OrganizationUnit, OU	Подразделение	Отдел информационной безопасности
Title, T	Должность	
Email, E	Адрес электронной почты	



### 7.3. Структура данных поля Subject (идентификационных данных владельца сертификата)

#### 7.3.1. Для юридических лиц:

Название	Описание	Содержание
CommonName, CN	Общее имя	Наименование юридического лица
SureName	Фамилия	Фамилия уполномоченного представителя юридического лица(владельца сертификата)
GivenName	Приобретенное имя	Имя отчество уполномоченного представителя юридического лица(владельца сертификата)
CountryName, C	Страна	RU
LocalityName, L	Город, населенный пункт	Город или населенный пункт места нахождения юридического лица
StateOrProvinceName, S	Наименование субъекта РФ	Субъект РФ места нахождения юридического лица
StreetAdress, Street	Название улицы, номер дома, квартира, строение	Часть адреса места регистрации юридического лица
OrganizationName, O	Наименование организации	Наименование юридического лица
OrganizationUnit, OU	Подразделение	Наименование подразделения, сотрудником которого является уполномоченный представитель юридического лица (владельца сертификата)
Title, T	Должность	Должность уполномоченного представителя юридического лица (владельца сертификатами)
Email, E	Адрес электронной почты	
OGRN	Основной государственный регистрационный номер (ОГРН)	ОГРН юридического лица (владельца сертификата)
INN	Идентификационный номер налогоплательщика	ИНН юридического лица (владельца сертификата)
SNILS	Страховой номер индивидуального лицевого счета	СНИЛС должностного лица, являющегося уполномоченным представителем юридического лица (владельца сертификата)

#### 7.3.2. Для физических лиц:

Название	Описание	Содержание
CommonName, CN	Общее имя	Фамилия, имя, отчество владельца сертификата
CountryName, C	Страна	RU



LocalityName, L	Город, населенный пункт	Город или населенный пункт места регистрации владельца сертификата
StateOrProvinceName, S	Наименование субъекта РФ	Субъект РФ места регистрации владельца сертификата
StreetAdress, Street	Название улицы, номер дома, квартира, строение	Часть адреса места регистрации владельца сертификата
Email, E	Адрес электронной почты	
SNILS	Страховой номер индивидуального лицевого счета	СНИЛС владельца сертификата

### 7.3.3. Для индивидуальных предпринимателей:

Название	Описание	Содержание
CommonName, CN	Общее имя	Фамилия, имя, отчество владельца сертификата
CountryName, C	Страна	RU
LocalityName, L	Город, населенный пункт	Город или населенный пункт места регистрации владельца сертификата
StateOrProvinceName, S	Наименование субъекта РФ	Субъект РФ места регистрации владельца сертификата
StreetAdress, Street	Название улицы, номер дома, квартира, строение	Часть адреса места регистрации владельца сертификата
Email, E	Адрес электронной почты	
SNILS	Страховой номер индивидуального лицевого счета	СНИЛС владельца сертификата
OGRNIP	Основной государственный регистрационный номер индивидуального предпринимателя	ОГРНИП индивидуального предпринимателя (владельца сертификата)
INN	Идентификационный номер налогоплательщика	ИНН индивидуального предпринимателя (владельца сертификата)

### 7.4. Структура сертификата ключа ЭП Уполномоченного лица УЦ

Название	Описание	Содержание
<b>Базовые поля сертификата</b>		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001



Issuer	Издатель сертификата	Данные УЦ. См. п. настоящего Регламента
Validity Period	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм:сс GMT Действителен по: дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	Данные Уполномоченного лица УЦ
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
<b>Дополнения сертификата</b>		
Key Usage (critical)	Использование ключа	Неотрекаемость – невозможность осуществления отказа от совершенных действий; Цифровая подпись; Подписание сертификатов; Автономное подписание списка отзыва (CRL); Подписание списка отзыва (CRL)
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор ключа ЭП уполномоченного лица Удостоверяющего Центра, данному сертификату
CRL Distribution Point	Точка распространения списка отозванных сертификатов	
CA_Version	Объектный идентификатор сертификата	Версия сертификата Уполномоченного лица УЦ

#### 7.5. Структура списка отозванных сертификатов УЦ

Название	Описание	Содержание
<b>Базовые поля списка отозванных сертификатов</b>		
Version	Версия	V2
Issuer	Издатель сертификата	Данные Уполномоченного лица УЦ
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: <ul style="list-style-type: none"> <li>Серийный номер сертификата (CertificateSerialNumber);</li> <li>Время обработки заявления на</li> </ul>



		аннулирование (отзыв) и приостановление действия сертификата (Time).
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
<b>Расширения списка отозванных сертификатов</b>		
Reason Code	Код причины отзыва сертификата	<ul style="list-style-type: none"> <li>• "0" Не указана</li> <li>• "1" Компрометация ключа</li> <li>• "2" Компрометация ключа ЭП уполномоченного лица Удостоверяющего Центра</li> <li>• "3" Изменение принадлежности</li> <li>• "4" Сертификат заменен</li> <li>• "5" Прекращение работы</li> <li>• "6" Приостановление действия</li> </ul>
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа ЭП уполномоченного лица Удостоверяющего Центра, на котором подписан СОС
CA Version	Объектный идентификатор сертификата издателя	Версия сертификата Уполномоченного лица УЦ

## 7.6. Сроки действия ключевых документов

Сертификат действует на определённый момент времени (действующий сертификат), если:

- наступил момент времени начала действия сертификата;
- срок действия сертификата не истёк;
- сертификат не аннулирован (отозван) и действие его не приостановлено;
- сертификат УЦ не аннулирован (отозван);
- срок действия сертификата УЦ не истёк;
- срок аккредитации УЦ не истек (для квалифицированных сертификатов);

Ключ электронной подписи действует на определённый момент времени (действующий ключ ЭП) если:

- наступил момент времени начала действия ключа ЭП;
- срок действия ключа ЭП электронной подписи не истёк;
- сертификат, соответствующий данному ключу ЭП, действует на указанный момент времени (не аннулирован).

### 7.6.1. Сроки действия ключевых документов уполномоченного лица УЦ

Срок действия ключа ЭП уполномоченного лица УЦ составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности УЦ, и для средства ЭП, с использованием которого данный ключ был сформирован.



Начало действия периода ключа ЭП уполномоченного лица УЦ исчисляется с даты и времени генерации ключа ЭП уполномоченного лица УЦ.

Срок действия сертификата уполномоченного лица УЦ не превышает тридцать лет. Время начала периода действия сертификата уполномоченного лица УЦ и его окончания заносится в поля «notBefore» и «notAfter» поля «Validity Period» соответственно.

#### **7.6.2. Сроки действия ключевых документов Пользователей УЦ**

Срок действия ключа ЭП Пользователя УЦ один год.

Начало периода действия ключа ЭП Пользователя УЦ исчисляется с даты и времени начала действия соответствующего сертификата.

Срок действия сертификата пользователя УЦ не превышает тридцать лет. Время начала периода действия сертификата Пользователя УЦ и его окончания заносится в поля «notBefore» и «notAfter» поля «Validity Period» соответственно.

#### **7.7. Плановая смена ключей ЭП Администратора УКЦ УЦ**

Плановая смена ключей (ключа ЭП и соответствующего ему ключа проверки ЭП) уполномоченного лица УЦ выполняется не ранее, чем через один год и не позднее, чем через один год и три месяца после начала действия ключа ЭП уполномоченного лица УЦ.

Процедура плановой смены ключей ЭП Администратора УКЦ УЦ осуществляется в следующем порядке:

- уполномоченное лицо УЦ генерирует новый ключ ЭП и соответствующий ему ключ проверки ЭП;
- уполномоченного лица УЦ изготавливает новый сертификат уполномоченного лица УЦ.

Уведомление Пользователей УЦ о проведении смены ключей ЭП Администратора УКЦ осуществляется посредством публикации информации на сайте ТФОМС Оренбургской области.

Старый ключ ЭП Администратора УКЦ используется в течение своего срока действия для формирования списков отозванных сертификатов, изданных УЦ в период действия старого ключа ЭП Администратора УКЦ УЦ.

#### **7.8. Компрометация и внеплановая смена ключей ЭП Администратора УКЦ**

В случае компрометации ключа ЭП Администратора УКЦ сертификат уполномоченного лица УЦ аннулируется (отзывается). Все сертификаты, подписанные с использованием скомпрометированного ключа ЭП Администратора УКЦ УЦ, считаются аннулированными.

Уведомление Пользователей УЦ о компрометации ключа ЭП Администратора УКЦ УЦ осуществляется посредством размещения данной информации на сайте УЦ.

После аннулирования сертификата Администратора УКЦ УЦ выполняется процедура внеплановой смены ключей ЭП Администратора УКЦ УЦ. Процедура внеплановой смены ключей ЭП Администратора УКЦ УЦ выполняется в порядке, определенном процедурой плановой смены ключей ЭП Администратора УКЦ УЦ (п. 7.7 настоящего Регламента).

При компрометации ключа ЭП Администратора УКЦ УЦ все сертификаты Пользователей УЦ, подписанные этим ключом подлежат внеплановой смене.



## **8. КОМПРОМЕТАЦИЯ КЛЮЧЕВЫХ ДОКУМЕНТОВ ПОЛЬЗОВАТЕЛЯ УЦ**

Пользователь УЦ самостоятельно принимает решение о факте или угрозе компрометации своего ключа ЭП.

В случае компрометации или угрозы компрометации ключа ЭП Пользователь связывается с УЦ по телефону и приостанавливает действие сертификата, соответствующего скомпрометированному ключу, посредством подачи заявления на приостановление действия сертификата на основании заявления в устной форме (п. 6.5.1 настоящего Регламента).

Если в течение срока приостановления действия сертификата Пользователь УЦ не направит в УЦ заявление на возобновление действия сертификата, то УЦ автоматически аннулирует (отзовет) данный сертификат.

Пользователь УЦ осуществляет внеплановую смену ключей в соответствии с п. 6.3 настоящего Регламента.

### **8.1. Конфиденциальность информации**

Типы конфиденциальной информации:

- Ключ ЭП, соответствующий сертификату является конфиденциальной информацией лица, зарегистрированного в УЦ. УЦ не осуществляют хранение ключей ЭП Пользователей УЦ;
- персональная и корпоративная информация о лицах, зарегистрированных в УЦ, содержащаяся в Реестре УЦ и Реестре Оператора УЦ, не подлежащая непосредственной рассылке в качестве части сертификата, считается конфиденциальной.

Типы информации, не являющейся конфиденциальной:

- информация, не являющаяся конфиденциальной информацией, считается открытой информацией;
- открытая информация может публиковаться по решению УЦ. Место, способ и время публикации открытой информации определяется Удостоверяющим центром;
- информация, включаемая в сертификаты и списки отозванных сертификатов, издаваемые УЦ, не считается конфиденциальной;
- персональные данные, включаемые в сертификаты, издаваемые УЦ, относятся к общедоступным персональным данным;
- информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.

УЦ имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Российской Федерации.

### **8.2. Хранение сертификатов в УЦ**

Срок хранения сертификата в УЦ осуществляется в течение всего периода его действия и пять лет после его аннулирования (отзыва). По истечении указанного срока хранения сертификаты переводятся в режим архивного хранения.

### **8.3. Прекращение оказания услуг**

В случае расторжения Регламента одной из Сторон все сертификаты, владельцами которых являются Пользователь УЦ — Сторона Регламента (если



Сторона регламента — физическое лицо) и Пользователи УЦ — полномочные представители Стороны Регламента (если Сторона Регламента — юридическое лицо), аннулируются (отзываются) УЦ.

#### **8.4. Форс-мажор**

Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Регламенту, если это неисполнение явилось следствием форс-мажорных обстоятельств, возникших после присоединения к настоящему Регламенту.

Форс-мажорными обстоятельствами признаются чрезвычайные (т.е. находящиеся вне разумного контроля Сторон) и непредотвратимые при данных условиях обстоятельства включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования аппаратно-программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по настоящему Регламенту.

В случае возникновения форс-мажорных обстоятельств, срок исполнения Сторонами своих обязательств по настоящему Регламенту отодвигается соразмерно времени, в течение которого действуют такие обстоятельства.

Сторона, для которой создалась невозможность исполнения своих обязательств по настоящему Регламенту, должна немедленно известить в письменной форме другую Сторону о наступлении, предполагаемом сроке действия и прекращении форс-мажорных обстоятельств, а также представить доказательства существования названных обстоятельств.

Неизвещение или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства.

В случае, если невозможность полного или частичного исполнения Сторонами какого-либо обязательства по настоящему Регламенту обусловлена действием форс-мажорных обстоятельств и существует свыше одного месяца, то каждая из Сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства.



Приложение № 1

к Регламенту Удостоверяющего центра

(Форма заявления о присоединении к Регламенту для юридических лиц)

**Заявление**  
**о присоединении к Регламенту УЦ ТФОМС Оренбургской области**

\_\_\_\_\_

(полное наименование организации, включая организационно-правовую форму)

В лице \_\_\_\_\_

\_\_\_\_\_

(должность)

\_\_\_\_\_

(фамилия, имя, отчество)

действующего на основании \_\_\_\_\_

в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяется к Регламенту Удостоверяющего центра Территориального фонда обязательного медицинского страхования Оренбургской области (далее — ТФОМС Оренбургской области), условия которого определены ТФОМС Оренбургской области.

С Регламентом предоставления услуг Удостоверяющего центра и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

Руководитель \_\_\_\_\_

должность

ФИО

«

»

20

г.

подпись

М.П.

\_\_\_\_\_

(заполняется Уполномоченным лицом Удостоверяющего центра)

Данное Заявление о присоединении к Регламенту Удостоверяющего центра ТФОМС Оренбургской области зарегистрировано в реестре Оператора Удостоверяющего центра.

Регистрационный № \_\_\_\_\_ от «\_\_\_\_\_» \_\_\_\_\_ 20\_\_\_\_ г.

Оператор УЦ \_\_\_\_\_

М.П.



Продолжение приложения № 1  
к Регламенту Удостоверяющего центра  
(Форма заявления о присоединении к Регламенту для физических лиц)

**Заявление  
о присоединении к Регламенту УЦ ТФОМС Оренбургской области**

Я,

\_\_\_\_\_

(фамилия, имя, отчество)

\_\_\_\_\_

(серия и номер паспорта)

\_\_\_\_\_

(кем и когда выдан паспорт)

в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Регламенту Удостоверяющего центра Территориального фонда обязательного медицинского страхования Оренбургской области (далее — ТФОМС Оренбургской области), условия которого определены ТФОМС Оренбургской области.

С Регламентом предоставления услуг Удостоверяющего центра и приложениями к нему ознакомлен(а) и обязуюсь соблюдать все положения указанного документа.

Пользователь УЦ

\_\_\_\_\_ /

ФИО

\_\_\_\_\_

подпись

«    »

20    г.

\_\_\_\_\_

(заполняется Уполномоченным лицом Удостоверяющего центра)

Данное Заявление о присоединении к Регламенту Удостоверяющего центра ТФОМС Оренбургской области зарегистрировано в реестре Оператора Удостоверяющего центра.

Регистрационный № \_\_\_\_\_ от «\_\_\_\_\_» \_\_\_\_\_ 20\_\_\_\_ г.

Оператор УЦ

\_\_\_\_\_

М.П.



Приложение № 2  
к Регламенту Удостоверяющего центра  
(Форма заявления для юридических лиц на регистрацию Пользователя УЦ)

**Заявление  
на регистрацию Пользователя Удостоверяющего центра**

(наименование организации, включая организационно-правовую форму)

в лице

(должность)

(фамилия, имя, отчество)

действующего на основании

Просит зарегистрировать уполномоченного представителя

(фамилия, имя, отчество)

в Реестре Удостоверяющего центра, наделить полномочиями Пользователя Удостоверяющего центра, установленные Регламентом Удостоверяющего центра Территориального фонда обязательного медицинского страхования Оренбургской области в соответствии с указанными в настоящем заявлении идентификационными данными:

Title (T)	Должность	
CommonName (CN)	ФИО или псевдоним	
OrganizationUnit (OU)	Подразделение	
Organization (O)	Организация	
Locality (L)	Город	
State (S)	Область	Оренбургская область
Country (C)	Страна	RU
E-mail (E)	Электронная почта	

Настоящим

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

соглашается с обработкой своих персональных данных Удостоверяющим центром и признаёт, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Пользователь УЦ

«      »      20      г.      подпись  
«      »      20      г.

Должность      руководителя

ФИО

М.П.      подпись



Продолжение приложения №  
к Регламенту Удостоверяющего центра  
(Форма заявления для физических лиц на регистрацию Пользователя УЦ)

**Заявление  
на регистрацию Пользователя Удостоверяющего центра**

Я,

\_\_\_\_\_

(фамилия, имя, отчество)

\_\_\_\_\_

(серия и номер паспорта)

\_\_\_\_\_

(кем и когда выдан паспорт)

прошу зарегистрировать меня в Реестре Удостоверяющего центра, наделить полномочиями Пользователя Удостоверяющего центра, установленные Регламентом Удостоверяющего центра Территориального фонда обязательного медицинского страхования Оренбургской области в соответствии с указанными в настоящем заявлении идентификационными данными:

CommonName (CN)	ФИО	
Locality (L)	Город	
State (S)	Область	Оренбургская область
Country (C)	Страна	RU
E-mail (E)	Электронная почта	

Настоящим

\_\_\_\_\_

(фамилия, имя, отчество)

соглашается с обработкой своих персональных данных Удостоверяющим центром и признаёт, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Пользователь УЦ \_\_\_\_\_

«    »    20    г.



Приложение № 3  
к Регламенту Удостоверяющего центра  
(Форма заявления для юридических лиц  
на изготовление ключа подписи Пользователя УЦ)

**Заявление  
на изготовление сертификата ключа проверки подписи Пользователя  
Удостоверяющего центра**

\_\_\_\_\_ (полное наименование организации, включая организационно-правовую форму)

в лице \_\_\_\_\_

\_\_\_\_\_ (должность)

\_\_\_\_\_ (фамилия, имя, отчество)

действующего на основании \_\_\_\_\_

Просит изготовить сертификат ключа подписи уполномоченного представителя \_\_\_\_\_

\_\_\_\_\_ (фамилия, имя, отчество)

в соответствии со следующими данными:

Вид сертификата ключа проверки подписи Пользователя УЦ:

Название	Описание	Содержание
CommonName, CN	Общее имя	
SureName	Фамилия	
GivenName	Приобретенное имя	
CountryName, C	Страна	RU
LocalityName, L	Город, населенный пункт	
StateOrProvinceName, S	Наименование субъекта РФ	Оренбургская область
StreetAdress, Street	Название улицы, номер дома, квартира, строение	
OrganizationName, O	Наименование организации	
OrganizationUnit, OU	Подразделение	
Title, T	Должность	
Email, E	Адрес электронной почты	
OGRN	Основной государственный регистрационный номер (ОГРН)	
INN	Идентификационный номер налогоплательщика	
SNILS	Страховой номер индивидуального лицевого счета	

Уполномоченный представитель

«                      »                      20                      подпись

Должность  
руководителя

ФИО                      М.П.                      подпись

«                      »



Продолжение приложения № 3  
к Регламенту Удостоверяющего центра  
(Форма заявления для физических лиц  
на изготовление ключа подписи Пользователя УЦ)

**Заявление  
на изготовление сертификата ключа проверки подписи Пользователя  
Удостоверяющего центра**

Я,

\_\_\_\_\_

(фамилия, имя, отчество)

\_\_\_\_\_

(серия и номер паспорта)

\_\_\_\_\_

(кем и когда выдан паспорт)

прошу изготовить сертификат ключа подписи в соответствии со следующими данными:

Название	Описание	Содержание
CommonName, CN	Общее имя	
CountryName, C	Страна	RU
LocalityName, L	Город, населенный пункт	
StateOrProvinceName, S	Наименование субъекта РФ	Оренбургская обл.
StreetAddress, Street	Название улицы, номер дома, квартира, строение	
Email, E	Адрес электронной почты	
SNILS	Страховой номер индивидуального лицевого счета	
INN	Идентификационный номер налогоплательщика	

Пользователь удостоверяющего центра

« »

20



Приложение № 4  
к Регламенту Удостоверяющего центра  
(Форма заявления для юридических лиц  
на отзыв сертификата ключа подписи Пользователя УЦ)

**Заявление  
на аннулирование (отзыв) сертификата ключа подписи  
Пользователя Удостоверяющего центра**

\_\_\_\_\_  
(полное наименование организации, включая организационно-правовую форму)

в лице \_\_\_\_\_

\_\_\_\_\_  
(должность)

\_\_\_\_\_  
(фамилия, имя, отчество)

действующего на основании \_\_\_\_\_

в связи с \_\_\_\_\_

\_\_\_\_\_  
(причина отзыва сертификата)

Просит аннулировать (отозвать) сертификат ключа подписи своего уполномоченного  
представителя — Пользователя Удостоверяющего центра:

\_\_\_\_\_  
(фамилия, имя, отчество)

содержащий следующие данные:

SerialNumber (SN)	Номер сертификата	
Title (T)	Должность	
CommonName (CN)	ФИО или псевдоним	
OrganizationUnit (OU)	Подразделение	
Organization (O)	Организация	
Locality (L)	Город	
State (S)	Область	Оренбургская область
Country (C)	Страна	RU
E-mail (E)	Электронная почта	

Пользователь удостоверяющего центра

\_\_\_\_\_  
ФИО

\_\_\_\_\_  
подпись

Руководитель организации

\_\_\_\_\_  
должность

\_\_\_\_\_  
ФИО

\_\_\_\_\_  
Дата подписания

\_\_\_\_\_  
подпись

\_\_\_\_\_  
. М.П.



Продолжение приложения № 4  
к Регламенту Удостоверяющего центра  
(Форма заявления для физических лиц  
на отзыв сертификата ключа подписи Пользователя УЦ)

**Заявление  
на аннулирование (отзыв) сертификата ключа подписи  
Пользователя Удостоверяющего центра**

Я,

\_\_\_\_\_

(фамилия, имя, отчество)

\_\_\_\_\_

(серия и номер паспорта)

\_\_\_\_\_

(кем и когда выдан паспорт)

В СВЯЗИ С

\_\_\_\_\_

(причина аннулирования сертификата)

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

SerialNumber (SN)	Номер сертификата	
CommonName (CN)	ФИО или псевдоним	
Locality (L)	Город	
State (S)	Область	Оренбургская область
Country (C)	Страна	RU
E-mail (E)	Электронная почта	

Пользователь удостоверяющего центра

\_\_\_\_\_

«      »

20



**Заявление  
на отзыв полномочий Пользователя Удостоверяющего центра на право  
пользования ЭП**

\_\_\_\_\_  
(полное наименование организации, включая организационно-правовую форму)

в лице \_\_\_\_\_

\_\_\_\_\_  
(должность)

\_\_\_\_\_  
(фамилия, имя, отчество)

действующего на основании \_\_\_\_\_  
заявляет, что отзывает Приказ/Доверенность № \_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ года,  
выданную для представления в Уполномоченную организацию Удостоверяющего центра  
своему полномочному представителю

\_\_\_\_\_  
(фамилия, имя, отчество)

и просит аннулировать (отозвать) все действующие сертификаты ключей подписей и  
сертификаты ключей подписей, действие которых приостановлено, владельцем которых  
является

\_\_\_\_\_  
(фамилия, имя, отчество)

\_\_\_\_\_  
должность

\_\_\_\_\_  
ФИО

\_\_\_\_\_  
подпись «      »

\_\_\_\_\_  
20      г.

\_\_\_\_\_  
М.П.



Приложение № 6  
к Регламенту Удостоверяющего центра  
(Форма заявления для юридических лиц  
на приостановление действия сертификата ключа подписи Пользователя УЦ)

**Заявление  
на приостановление действия сертификата ключа подписи  
Пользователя Удостоверяющего центра**

(полное наименование организации, включая организационно-правовую форму)
в лице
(должность)
(фамилия, имя, отчество)
действующего на основании

Просит приостановить действие сертификата ключа подписи своего уполномоченного представителя — Пользователя Удостоверяющего центра:

(фамилия, имя, отчество)
--------------------------

содержащего следующие данные:

SerialNumber (SN)	Номер сертификата	
Title (T)	Должность	
CommonName (CN)	ФИО или псевдоним	
OrganizationUnit (OU)	Подразделение	
Organization (O)	Организация	
Locality (L)	Город	
State (S)	Область	Оренбургская область
Country (C)	Страна	RU
E-mail (E)	Электронная почта	

Срок приостановления действия сертификата \_\_\_\_\_ дней  
(количество дней прописью)

Пользователь удостоверяющего центра  
«      »      20      подпись

Руководитель организации  
\_\_\_\_\_ Г.  
должность      ФИО      «      »      20      подпись  
М.П.



Продолжение приложения № 6  
к Регламенту Удостоверяющего центра  
(Форма заявления для физических лиц  
на приостановление действия сертификата ключа подписи Пользователя УЦ)

**Заявление  
на приостановление действия сертификата ключа подписи  
Пользователя Удостоверяющего центра**

Я,

\_\_\_\_\_  
(фамилия, имя, отчество)

\_\_\_\_\_  
(серия и номер паспорта)

\_\_\_\_\_  
(кем и когда выдан паспорт)

прошу приостановить действие сертификата ключа подписи, содержащего следующие данные:

SerialNumber (SN)	Номер сертификата	
CommonName (CN)	ФИО или псевдоним	
Locality (L)	Город	
State (S)	Область	Оренбургская область
Country (C)	Страна	RU
E-mail (E)	Электронная почта	

Срок приостановления действия сертификата \_\_\_\_\_ дней

(количество дней прописью)

Пользователь удостоверяющего центра

\_\_\_\_\_  
/ «      » 20      г.



Приложение № 7  
к Регламенту Удостоверяющего центра  
(Форма заявления для юридических лиц  
на возобновление действия сертификата ключа подписи Пользователя УЦ)

**Заявление  
на возобновление действия сертификата ключа подписи  
Пользователя Удостоверяющего центра**

(полное наименование организации, включая организационно-правовую форму)
в лице
(должность)
(фамилия, имя, отчество)
действующего на основании
Просит возобновить действие сертификата ключа подписи своего уполномоченного представителя — Пользователя Удостоверяющего центра:

(фамилия, имя, отчество)		
содержащего следующие данные:		
SerialNumber (SN)	Номер сертификата	
Title (T)	Должность	
CommonName (CN)	ФИО или псевдоним	
OrganizationUnit (OU)	Подразделение	
Organization (O)	Организация	
Locality (L)	Город	
State (S)	Область	Оренбургская область
Country (C)	Страна	RU
E-mail (E)	Электронная почта	

Пользователь удостоверяющего центра

«    »	20	подпись
--------	----	---------

Руководитель организации

должность	ФИО	«    »	20	подпись
М.П.				



Продолжение приложения № 7  
к Регламенту Удостоверяющего центра  
(Форма заявления для физических лиц  
на возобновление действия сертификата ключа подписи Пользователя УЦ)

**Заявление  
на возобновление действия сертификата ключа подписи  
Пользователя Удостоверяющего центра**

Я,

\_\_\_\_\_  
(фамилия, имя, отчество)

\_\_\_\_\_  
(серия и номер паспорта)

\_\_\_\_\_  
(кем и когда выдан паспорт)

прошу возобновить действие сертификата ключа подписи, содержащего следующие данные:

SerialNumber (SN)	Номер сертификата	
CommonName (CN)	ФИО или псевдоним	
Locality (L)	Город	
State (S)	Область	Оренбургская область
Country (C)	Страна	RU
E-mail (E)	Электронная почта	

Пользователь удостоверяющего центра

«        »                      20        г.



Продолжение приложения № 7  
к Регламенту Удостоверяющего центра  
(Форма заявления для сотрудников  
ТФОМС- Пользователей УЦ)

**Заявление  
на возобновление действия сертификата ключа подписи  
Пользователя Удостоверяющего центра**

Прошу возобновить действие следующих сертификатов ключей подписи сотрудников

\_\_\_\_\_  
(наименование подразделения)

\_\_\_\_\_  
(наименование подразделения)

№ п/п	Серийный номер сертификата	ФИО	Должность	Подпись сотрудника
1.				
2.				
3.				
4.				
5.				
6.				
7.				

\_\_\_\_\_  
Должность руководителя подразделения

\_\_\_\_\_  
ФИО руководителя подразделения

«

»

20

г.

\_\_\_\_\_  
Подпись руководителя подразделения



**Заявление**  
**на получение информации о статусе сертификата ключа подписи,**  
**изданного Удостоверяющим центром**

действующего на основании

SerialNumber (SN)	Номер сертификата	
Title (T)	Должность	
CommonName (CN)	ФИО или псевдоним	
OrganizationUnit (OU)	Подразделение	
Organization (O)	Организация	
Locality (L)	Город	
State (S)	Область	Оренбургская область
Country (C)	Страна	RU
E-mail (E)	Электронная почта	

С « » ПО « ».

✻

Продолжение приложения № 8  
к Регламенту Удостоверяющего центра  
(Форма заявления для физических лиц  
на получение информации о статусе сертификата ЭП)

**Заявление**  
**на получение информации о статусе сертификата ключа подписи,**  
**изданного Удостоверяющим центром**

Я,

\_\_\_\_\_

(фамилия, имя, отчество)

\_\_\_\_\_

(серия и номер паспорта)

\_\_\_\_\_

(кем и когда выдан паспорт)

прошу предоставить информацию о статусе следующего сертификата ключа подписи:

SerialNumber (SN)	Номер сертификата	
CommonName (CN)	ФИО или псевдоним	
Locality (L)	Город	
State (S)	Область	Оренбургская область
Country (C)	Страна	RU
E-mail (E)	Электронная почта	

Период времени \* на который требуется установить статус сертификата:

с « \_\_\_\_\_ » по « \_\_\_\_\_ ».

Пользователь удостоверяющего центра \_\_\_\_\_

« \_\_\_\_\_ » 20 \_\_\_\_ г.

\* Время и дата должны быть указаны с учётом часового пояса Оренбургской области. Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром



**Заявление**  
**на подтверждение подлинности электронной цифровой подписи**  
**в электронном документе**

\_\_\_\_\_

(полное наименование организации, включая организационно-правовую форму)

в лице \_\_\_\_\_

\_\_\_\_\_

(должность)

\_\_\_\_\_

(фамилия, имя, отчество)

действующего на основании \_\_\_\_\_

Просит подтвердить подлинность ЭП в электронном документе на основании следующих данных:

1. Файл, содержащий сертификат ключа подписи, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе на прилагаемом к заявлению носителе — регистрационный № \_\_\_\_\_;
2. Файл, содержащий подписанный ЭП данные и значение ЭП, либо несколько файлов (ЭП отдельно от подписанного файла с данными) на прилагаемом к заявлению носителе — регистрационный № \_\_\_\_\_;
3. Время\*, на момент наступления которых требуется подтвердить подлинность ЭП:

« \_\_\_\_\_ : \_\_\_\_\_ » « \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_ »

час                      минута                      день                      месяц                      год

Руководитель организации

\_\_\_\_\_

должность

\_\_\_\_\_

ФИО

\_\_\_\_\_

подпись

«    »

20

г.

М.П.

\* Время и дата должны быть указаны с учётом часового пояса Оренбургской области. Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

**Заявление  
на подтверждение подлинности электронной цифровой подписи  
в электронном документе**

Я,

\_\_\_\_\_  
(фамилия, имя, отчество)

прошу подтвердить подлинность ЭП в электронном документе на основании следующих данных:

1. Файл, содержащий сертификат ключа подписи, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе на прилагаемом к заявлению носителе — регистрационный № \_\_\_\_\_;
2. Файл, содержащий подписанный ЭП данные и значение ЭП, либо несколько файлов (ЭП отдельно от подписанного файла с данными) на прилагаемом к заявлению носителе — регистрационный № \_\_\_\_\_;
3. Время\*, на момент наступления которых требуется подтвердить подлинность ЭП:

« \_\_\_\_\_ : \_\_\_\_\_ » « \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_ »  
час минута день месяц год

Пользователь удостоверяющего центра

« \_\_\_\_\_ » \_\_\_\_\_ 20\_\_\_\_

\* Время и дата должны быть указаны с учётом часового пояса Оренбургской области. Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром



Территориальный фонд обязательного медицинского страхования Оренбургской области

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

*Настоящее руководство является информационным документом, описывающим условия и порядок использования электронных подписей и средств электронной подписи, риски, связанные с использованием электронных подписей, меры, необходимые для обеспечения безопасности электронных подписей*

## Оглавление

1. Общие положения .....	54
2. Требования по размещению .....	54
3. Меры по обеспечению защиты от несанкционированного доступа .....	54
4. Требования по обеспечению информационной безопасности при работе в системах обмена электронными документами .....	57
4.1 Меры защиты ключей электронной подписи .....	57
4.2 Обращение с ключевой информацией и ключевыми носителями .....	57
4.3 Обеспечение безопасности АРМ, с установленными СКЗИ .....	57
5. Требования по установке средств электронной подписи и средств криптографической защиты, общесистемного и специального программного обеспечения .....	58
6. Дополнительные требования .....	59

### 1. Общие положения

Настоящее руководство составлено в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» является средством официального информирования лиц, заинтересованных в получении или владеющих сертификатом ключа проверки электронной подписи, об условиях, рисках и порядке использования электронных подписей и средств электронной подписи, а так же о мерах, необходимых для обеспечения безопасности при использовании электронных подписей.

Применение электронных подписей в системах юридически значимого электронного документооборота и иных системах, сопровождаются рисками финансовых убытков и иного рода потерь, связанных с признанием недействительности сделок, совершенных с использованием электронной подписи при несанкционированном получении злоумышленником ключа 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.

### 2. Требования по размещению

При размещении средств электронной подписи и средств криптографической защиты:

- должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства электронной подписи и средства криптографической защиты, посторонним лицам, не имеющим допуск к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства криптографической защиты и передаваемую информацию;

- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

### 3. Меры по обеспечению защиты от несанкционированного доступа

При использовании средств электронной подписи и средств криптографической защиты должны выполняться следующие меры по защите информации от несанкционированного доступа:

Необходимо разработать и применить политику назначения и смены паролей (для



входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 6 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, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- личный пароль пользователь не имеет права никому сообщать;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 дней.

Запрещается:

- оставлять технические средства с установленными средствами электронной подписи и средствами криптографической защиты без контроля, после ввода ключевой информации;
- вносить какие-либо изменения в программное обеспечение средств электронной подписи и средств криптографической защиты;
- осуществлять несанкционированное Администратором безопасности копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием средств электронной подписи и средств криптографической защиты;
- записывать на ключевые носители постороннюю информацию.

Администратор безопасности должен сконфигурировать операционную систему и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- не использовать нестандартные, измененные или отладочные версии операционных систем;
- исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;
- исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;
- на технических средствах с установленными средствами электронной подписи и средствами криптографической защиты должна быть установлена только одна операционная система;
- правом установки и настройки операционной системы, а также средств электронной подписи и средств криптографической защиты должен обладать только Администратор безопасности;
- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);
- режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;
- необходимо предусмотреть меры, максимально ограничивающие доступ к ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):



- системному реестру;
- файлам и каталогам;
- временным файлам;
- журналам системы;
- файлам подкачки;
- кэшируемой информации (пароли и т.п.);
- отладочной информации.

Кроме того необходимо организовать стирание (по окончании сеанса работы средств электронной подписи и средств криптографической защиты) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это не выполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

Должно быть исключено попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий.

Необходимо регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а так же исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий.

В случае подключения технических средств с установленными средствами электронной подписи и средствами криптографической защиты к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети. С целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем к программному обеспечению, в окружении которого функционируют средства электронной подписи и средства криптографической защиты и к компонентам средств электронной подписи и средств криптографической защиты со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN-сетей и т.п.). Все средства защиты, должны иметь сертификат уполномоченного органа по сертификации средств защиты.

Организовать и использовать систему аудита, организовать регулярный анализ результатов аудита.

Организовать и использовать комплекс мероприятий по антивирусной защите.

#### **ЗАПРЕЩАЕТСЯ:**

- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер (за исключением случаев, предусмотренных данными требованиями);
- вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя;
- подключать к техническим средствам с установленными средствами электронной подписи и средствами криптографической защиты дополнительные устройства и соединители, не предусмотренные штатной комплектацией;
- работать на технических средствах с установленными средствами электронной подписи и средствами криптографической защиты, если во время его начальной загрузки не проходит встроенный тест ОЗУ;
- вносить какие-либо изменения в программное обеспечение средств электронной подписи и средств криптографической защиты;
- изменять настройки, выставленные программой установки средств электронной подписи и средств криптографической защиты или Администратором



безопасности;

- обрабатывать на технических средствах с установленными средствами электронной подписи и средствами криптографической защиты информацию, содержащую государственную тайну;
- осуществлять несанкционированное вскрытие корпуса технического средства с установленными средствами электронной подписи и средствами криптографической защиты;
- работать со средствами электронной подписи и средствами криптографической защиты при включенных в техническое средство штатных средствах выхода в радиоканал;
- приносить и использовать в помещении, где размещены средства электронной подписи и средства криптографической защиты, радиотелефоны и другую радиопередающую аппаратуру (требование носит рекомендательный характер).

#### **4. Требования по обеспечению информационной безопасности при работе в системах обмена электронными документами**

##### **4.1 Меры защиты ключей электронной подписи**

Ключи электронной подписи при их создании должны записываться на типы ключевых носителей, которые поддерживаются используемым средством электронной подписи согласно технической и эксплуатационной документации к ним.

Ключи электронной подписи на ключевом носителе защищаются паролем (ПИН-кодом). Пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство электронной подписи.

Если процедуру генерации ключей выполняет сотрудник Удостоверяющего центра, то он должен сообщить сформированный пароль (ПИН-код) владельцу ключа электронной подписи.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа электронной подписи.

##### **4.2 Обращение с ключевой информацией и ключевыми носителями**

Недопустимо пересылать файлы с ключевой информацией для работы в системах обмена электронными документами по электронной почте сети Интернет или по внутренней электронной почте (кроме запросов на сертификат и открытых ключей).

Ключевая информация должна размещаться на сменном носителе информации (floppy-диск, USB-flash накопитель, e-Token, ru-Token и др.). Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами электронной подписи и средствами криптографической защиты, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем либо уполномоченным лицом на использование данного носителя, и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами электронной подписи и средствами криптографической защиты операций формирования и проверки электронной подписи, зашифрования и расшифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

##### **4.3 Обеспечение безопасности АРМ, с установленными СКЗИ**

С целью контроля исходящего и входящего подозрительного трафика, технические средства с установленными средствами электронной подписи и средствами криптографической защиты должны быть защищены от внешнего доступа программными



или аппаратными средствами межсетевого экранирования. Эти средства должны пресекать отправку в Интернет информации, инициированную программами, не имеющими соответствующих полномочий.

На технических средствах, используемых для работы в системах обмена электронными документами:

- на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям, приведенным в разделе 3;
- должно быть установлено только лицензионное программное обеспечение;
- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;
- должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски C\$ и т.д.);
- должны регулярно устанавливаться обновления операционной системы;
- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами электронной подписи и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в системе обмена электронными документами;
- должна быть активирована подсистема регистрации событий информационной безопасности;
- должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

В качестве автоматизированного рабочего места для работы в системах обмена электронными документами крайне не рекомендуется выбирать переносной компьютер (ноутбук). Если выбран ноутбук, недопустимо его подключение к сетям общего доступа в местах свободного доступа в Интернет (Интернет-кафе, гостиницы, офисные центры и т.д.), при этом для хранения ключевой информации должен использоваться сменный носитель информации.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств на которых были установлены средства электронной подписи и средства криптографической защиты, необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред организации, в том числе средства электронной подписи и средства криптографической защиты, журналы работы систем обмена электронными документами и т.д.).

## **5. Требования по установке средств электронной подписи и средств криптографической защиты, общесистемного и специального программного обеспечения**

К установке общесистемного и специального программного обеспечения, а также программного обеспечения средств электронной подписи и средств криптографической защиты, допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее программное обеспечение.

При установке программного обеспечения средств электронной подписи и средств криптографической защиты следует:

- на технических средствах, на которые устанавливаются средства электронной подписи и средства криптографической защиты, использовать только лицензионное программное обеспечение фирм-изготовителей;
- установка программного обеспечения средств электронной подписи и средств криптографической защиты должна производиться только с дистрибутива, полученного от лицензиата ФСБ России, имеющего лицензию на распространение криптографических средств и должны быть обеспечены организационно-технические меры по исключению подмены дистрибутива, внесения изменений в средства электронной подписи



и средства криптографической защиты после установки;

- на технических средствах с установленными средствами электронной подписи и средствами криптографической защиты не должны устанавливаться средства разработки программного обеспечения и отладчики. Если средства отладки приложений нужны для технологических потребностей пользователя, то их использование должно быть санкционировано Администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода и памяти программного обеспечения средств электронной подписи и средств криптографической защиты в процессе обработки защищаемой информации и/или при загруженной ключевой информации;

- предусмотреть меры исключающие возможность несанкционированного изменения аппаратной части технических средств, на которых установлены средства электронной подписи и средства криптографической защиты (например, путем опечатывания системного блока и разъемов);

Программное обеспечение используемое на технических средствах с установленными средствами электронной подписи и средствами криптографической защиты, 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 области собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки операционной системы;
- использовать недокументированные фирмой-разработчиком функции операционной системы.

## **6. Дополнительные требования**

Дополнительные требования по обеспечению информационной безопасности при работе в системах обмена электронными документами могут дополнительно устанавливаться правилами систем ЭДО, требованиями по эксплуатации и безопасности средств электронной подписи и средств криптографической защиты.





## Доверенность

г. \_\_\_\_\_ « \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

\_\_\_\_\_

(полное наименование организации, включая организационно-правовую форму)

в лице \_\_\_\_\_,

(должность) (фамилия, имя, отчество)

действующего на основании \_\_\_\_\_ уполномочивает

\_\_\_\_\_

(фамилия, имя, отчество)

\_\_\_\_\_

(серия и номер паспорта, кем и когда выдан)

выступать в роли Пользователя Удостоверяющего центра и осуществлять действия в рамках Регламента предоставления услуг Уполномоченной организации Удостоверяющего центра, установленные для Пользователя Удостоверяющего центра.

Представитель наделяется правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей Доверенностью.

Подписывать электронные документы своей электронной подписью с полномочиями:

\_\_\_\_\_  
(Руководитель, Главный бухгалтер, Исполнитель, Специалист, Иные)

Настоящая доверенность действительна по « \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

Подпись уполномоченного представителя \_\_\_\_\_ подтверждаю.

(Фамилия И.О.) (Подпись)

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания

Печать организации

