# ПРАВИТЕЛЬСТВО ОРЕНБУРГСКОЙ ОБЛАСТИ

# П О С Т А Н О В Л Е Н И Е

24.11.2017 г. Оренбург № 833-п

Об использовании электронной подписи в органах исполнительной власти и органах местного самоуправления муниципальных образований Оренбургской области

В соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» и в целях обеспечения безопасности при осуществлении электронного документооборота:

1. Возложить функции удостоверяющего центра органов исполнительной власти и органов местного самоуправления муниципальных образований Оренбургской области на государственное казенное учреждение «Центр информационных технологий Оренбургской области».

2. Утвердить:

а) регламент работы удостоверяющего центра государственного казенного учреждения «Центр информационных технологий Оренбургской области» согласно приложению № 1;

б) порядок выдачи и отзыва ключей и сертификатов ключей электронной подписи пользователей удостоверяющего центра государственного казенного учреждения «Центр информационных технологий Оренбургской области» согласно приложению № 2;

в) инструкцию по защите информации при осуществлении электронного документооборота в органах исполнительной власти и органах местного самоуправления муниципальных образований Оренбургской области и подведомственных им учреждениях согласно приложению № 3.

3. Рекомендовать органам местного самоуправления муниципальных образований Оренбургской области использовать электронную подпись при осуществлении электронного документооборота в соответствии с регламентом работы удостоверяющего центра государственного казенного учреждения «Центр информационных технологий Оренбургской области» и порядком выдачи и отзыва ключей и сертификатов ключей электронной подписи пользователей удостоверяющего центра государственного казенного учреждения «Центр информационных технологий Оренбургской области», утвержденными настоящим постановлением.

4. Установить, что органы исполнительной власти Оренбургской области, органы местного самоуправления муниципальных образований Оренбургской области, территориальные органы федеральных органов

государственной власти, организации независимо от их организационно-правовых форм и форм собственности вправе получить усиленную квалифицированную электронную подпись при осуществлении межведомственного электронного взаимодействия в соответствии с регламентом работы удостоверяющего центра государственного казенного учреждения «Центр информационных технологий Оренбургской области» и порядком выдачи и отзыва ключей и сертификатов ключей электронной подписи пользователей удостоверяющего центра государственного казенного учреждения «Центр информационных технологий Оренбургской области», утвержденными настоящим постановлением.

5. Признать утратившими силу постановления Правительства Оренбургской области:

от 27.06.2013 № 525-п «Об использовании электронной подписи в органах исполнительной власти Оренбургской области»;

от 03.10.2014 № 711-п «О внесении изменений в постановление Правительства Оренбургской области от 27.06.2013 № 525-п».

6. Контроль за исполнением настоящего постановления возложить на директора департамента информационных технологий Оренбургской области Засинца И.Д.

7. Постановление вступает в силу после его официального опубликования.

Губернатор

АППАРАТ ГУБЕРНАТОРА И ПРАВИТЕЛЬСТВА ОРЕНБУРГСКОЙ ОБЛАСТИ * АППАРАТ
УПРАВЛЕНИЕ ДОКУМЕНТАЦИОННОГО ОБЕСПЕЧЕНИЯ

Ю.А.Берг

Приложение № 1
к постановлению
Правительства области
от 24.11.2017 № 833-п

# Регламент
## работы удостоверяющего центра государственного казенного учреждения «Центр информационных технологий Оренбургской области»

### I. Термины и определения, используемые в настоящем Регламенте

ViPNet – торговая марка программных продуктов.

Абонентский пункт – автоматизированное рабочее место, на котором установлен ViPNet «Координатор» либо ViPNet «Клиент».

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Внешний пользователь удостоверяющего центра – лицо, обратившееся за услугами удостоверяющего центра, не зарегистрированное в удостоверяющем центре.

Внутренний пользователь удостоверяющего центра – лицо, обратившееся за услугами удостоверяющего центра, зарегистрированное в удостоверяющем центре.

Закрытый ключ электронной подписи – криптографический ключ, хранящийся пользователем удостоверяющего центра в тайне, использующийся для формирования электронной подписи и/или шифрования данных.

Запрос на отзыв сертификата ключа электронной подписи – сообщение, содержащее необходимую информацию для отзыва сертификата ключа электронной подписи.

Запрос на сертификат ключа электронной подписи – сообщение, содержащее необходимую информацию для получения сертификата ключа электронной подписи.

Заявитель – лицо, которому необходимо получить услуги удостоверяющего центра.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Ключевая дискета – файл, содержащий в себе хэш-пароль, действующий персональный ключ, закрытый ключ электронной подписи, сертификат электронной подписи пользователя удостоверяющего центра.

Ключ (криптографический ключ) – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований, ключ электронной подписи, открытый или закрытый ключ электронной подписи.

Ключ электронной подписи – совокупность закрытого и открытого ключей электронной подписи, где закрытый ключ электронной подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронном документе электронной подписи с использованием средств электронной подписи, а открытый ключ электронной подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной подписи подлинности электронной подписи в электронном документе.

Ключевой носитель – носитель, содержащий один или несколько ключей электронной подписи.

Ключевой набор – файл, содержащий в себе ключи связи с центром управления сетью и программным обеспечением программно-аппаратного комплекса ViPNet «Координатор».

Компрометация ключа – недоверие к обеспечению безопасности информации используемыми ключами.

Открытый ключ электронной подписи – криптографический ключ, связанный с закрытым ключом электронной подписи с помощью особого математического соотношения, известный другим пользователям системы и предназначенный для проверки электронной подписи, шифрования, но не позволяющий вычислить закрытый ключ электронной подписи.

Программный комплекс удостоверяющего центра – программный комплекс обеспечения реализации целевых функций удостоверяющего центра. Компонент программы ViPNet «Удостоверяющий и Ключевой центр».

Плановая замена ключей электронной подписи – замена ключей электронной подписи с установленной в системе периодичностью, не вызванная компрометацией ключей электронной подписи.

Пользователь удостоверяющего центра – лицо, обратившееся за услугами удостоверяющего центра.

Пункт регистрации – пункт удостоверяющего центра, предназначенный для приема заявлений, регистрации внешних пользователей удостоверяющего центра, создания ключей электронной подписи и формирования запросов на приостановление, отзыв и возобновление сертификата ключа электронной подписи.

Сертификат ключа электронной подписи – электронный документ или документ на бумажном носителе, содержащий открытый ключ электронной подписи, сведения о владельце открытого ключа подписи, подписанный электронной подписью его издателя.

Список отозванных сертификатов ключей электронной подписи – список сертификатов ключей электронной подписи, созданный удостоверяющим центром, отозванных до окончания срока их действия.

Средства электронной подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций:

создание электронной подписи в электронном документе с использованием закрытого ключа электронной подписи;

подтверждение с использованием открытого ключа электронной подписи подлинности электронной подписи в электронном документе;

создание закрытых и открытых ключей электронной подписи.

Удостоверяющий центр – структурное подразделение государственного казенного учреждения «Центр информационных технологий Оренбургской области», выполняющее функции, предусмотренные Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

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

Электронная подпись – реквизит электронного документа, предназначенный для защиты такого документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в таком документе.

ViPNet «Сервис публикации» – программное обеспечение ViPNet реализующее управление точками публикации сертификатов ключей электронной подписи.

ViPNet «Удостоверяющий и ключевой центр» – программное обеспечение ViPNet, предназначенное для выпуска цифровых сертификатов ключей электронной подписи.

ViPNet «Центр регистрации» – программное обеспечение ViPNet, предназначенное для создания защищенного автоматизированного рабочего места для регистрации внешних пользователей удостоверяющего центра, хранения регистрационных данных, создания запросов на выпуск сертификатов и их обслуживание в программе ViPNet «Удостоверяющий и ключевой центр», а также запросов на формирование дистрибутивов справочно-ключевой информации для узлов сети ViPNet в программе ViPNet «Удостоверяющий и ключевой центр».

## II. Общие положения

1. Настоящий Регламент определяет механизм и условия предоставления услуг удостоверяющего центра государственного казенного учреждения «Центр информационных технологий» (далее – УЦ), включая обязанности пользователей УЦ и администраторов УЦ, содержание протоколов работ УЦ, структуры записей аудита (приложение № 1 к настоящему Регламенту), основные организационно-технические мероприятия, необходимые для безопасной работы УЦ, устанавливает порядок взаимоотношений УЦ и пользователей УЦ в процессе предоставления услуг УЦ.

2. Местонахождение государственного казенного учреждения «Центр информационных технологий» (далее – ГКУ «ЦИТ»): 460046, г. Оренбург, ул. 9 Января, д. 64, каб. 706.

Местонахождение пункта регистрации: г. Оренбург, ул. 9 Января, д. 64, каб. 725.

График работы пункта регистрации: понедельник–четверг с 9:00 до 18:00, пятница – с 9:00 до 17:00, перерыв на обед с 13:00 до 13:48, выходные дни: суббота, воскресенье, а также дни государственных праздников России.

Список услуг, оказываемых УЦ, контактная и справочная информация представлены на официальном сайте ГКУ «ЦИТ» в разделе «Удостоверяющий центр» в сети Интернет (http://uc.orb.ru/).

3. УЦ предназначен для обеспечения участников информационных систем средствами и спецификациями для использования сертификатов ключей электронной подписи (далее – сертификат) в целях обеспечения:

применения электронной подписи (далее – ЭП);

контроля целостности и конфиденциальности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем;

аутентификации участников информационных систем в процессе их взаимодействия.

4. Зарегистрированными пользователями УЦ и владельцами сертификатов могут быть только физические лица.

Пользователями сертификата могут быть физическое лицо, устройство или программное приложение.

Юридических лиц представляют физические лица, имеющие доверенность от имени юридического лица на право пользоваться услугами УЦ.

Сертификаты, требующиеся для работы каких-либо устройств или программных приложений, выдаются на ответственное лицо.

5. Услуга УЦ по предоставлению копий сертификатов в электронной форме, находящихся в реестре сертификатов, предоставляется на безвозмездной основе.

Состав и стоимость дополнительных услуг, предоставляемых УЦ определяются владельцем УЦ.

## III. Услуги, предоставляемые УЦ

6. В процессе своей деятельности УЦ предоставляет пользователям УЦ следующие услуги:

создание и выдача закрытых и открытых ключей ЭП по обращениям пользователей УЦ с записью их на ключевой носитель;

создание сертификатов внутренних пользователей УЦ на бумажном носителе;

установление сроков действия создаваемых сертификатов;

создание сертификатов внутренних пользователей УЦ в электронной форме;

проверка уникальности ключей проверки ЭП в реестре сертификатов;

подтверждение подлинности ЭП в документах, представленных в электронной форме, по обращениям пользователей УЦ;

подтверждение подлинности ЭП уполномоченного лица УЦ в созданных им сертификатах по обращениям пользователей УЦ;

предоставление копий сертификатов в электронной форме, находящихся в реестре сертификатов, по запросам пользователей УЦ;

ведение реестра сертификатов внутренних пользователей УЦ;

аннулирование (отзыв) сертификатов по обращениям владельцев сертификатов;

предоставление пользователям УЦ сведений об аннулированных и приостановленных сертификатах;

приостановление и возобновление действия сертификатов по обращениям владельцев сертификатов;

формирование и обновление справочно-ключевых наборов для организации защищенного обмена информацией;

распространение средств ЭП.

## IV. Права и обязанности УЦ и его пользователей

7. УЦ имеет право:

запрашивать:

у заявителя документы для подтверждения информации, содержащейся в заявлении на создание ключей ЭП, дополнительные документы, подтверждающие достоверность представленных им сведений, в случае наличия противоречий между сведениями, представленными заявителем и сведениями, полученными УЦ в соответствии с частью 2.2 статьи 18 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

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

из государственных информационных ресурсов – выписки из единого государственного реестра юридических лиц (в отношении заявителя – юридического лица), единого государственного реестра индивидуальных предпринимателей (в отношении заявителя – индивидуального предпринимателя), Единого государственного реестра налогоплательщиков (в отношении заявителя – иностранной организации);

отказать в:

регистрации в УЦ лицам, обратившимся по вопросу предоставления копий сертификатов в электронной форме;

приеме документов, не соответствующих требованиям нормативных правовых актов Российской Федерации;

предоставлении услуг по созданию ключей ЭП в случае невыполнения заявителем обязанностей, установленных частью 2 статьи 18 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

предоставлении услуг по созданию ключей ЭП без предоставления информации о причинах отказа;

аннулировании (отзыве) сертификата владельцу сертификата, подавшему заявление на аннулирование (отзыв) сертификата, в случае, если истек установленный срок действия закрытого ключа ЭП, соответствующего ключу ЭП в сертификате;

приостановлении или возобновлении действия сертификата владельцу сертификата, подавшему заявление на приостановление или возобновление действия сертификата, в случае, если истек установленный срок действия закрытого ключа ЭП, соответствующего ключу ЭП в сертификате;

предоставлять копии сертификатов в электронной форме, находящиеся в реестре сертификатов, всем лицам, обратившимся за ними в УЦ;

прекратить действие сертификата без заявления владельца сертификата в случае наличия у УЦ достоверных сведений о нарушении конфиденциальности ключа ЭП владельца сертификата, а также невыполнения владельцем сертификата обязанностей, установленных законодательством Российской Федерации в области ЭП, а также в случае появления у УЦ достоверных сведений о том, что документы, представленные заявителем в целях создания и получения им сертификата не являются подлинными и/или не подтверждают достоверность информации, включенной в данный сертификат, и/или в случае, если услуга по созданию и выдаче данного сертификата не оплачена в надлежащем порядке.

8. Внешние пользователи УЦ имеют право:

получать:

список аннулированных (отозванных) и приостановленных сертификатов, составленный УЦ;

сертификат уполномоченного лица УЦ;

копию сертификата в электронной форме, находящегося в реестре сертификатов;

применять:

сертификат уполномоченного лица УЦ для проверки ЭП уполномоченного лица УЦ в сертификатах, созданных УЦ;

копию сертификата в электронной форме для проверки ЭП в соответствии со сведениями, указанными в сертификате;

список аннулированных (отозванных) и приостановленных сертификатов, созданных УЦ, для проверки статуса сертификатов;

обращаться в УЦ:

за подтверждением подлинности ЭП в документах, представленных в электронной форме;

за подтверждением подлинности ЭП уполномоченного лица УЦ в созданных им сертификатах;

с заявлением на создание ключей ЭП.

9. Внутренние пользователи УЦ имеют права внешних пользователей УЦ, а также право:

пользоваться предоставляемыми УЦ средствами защиты от несанкционированного доступа (в случае предоставления таких средств);

обращаться в УЦ с заявлениями:

на аннулирование (отзыв) сертификата ключа ЭП в течение срока действия соответствующего закрытого ключа ЭП;

на приостановление действия сертификата ключа ЭП в течение срока действия соответствующего закрытого ключа ЭП;

на возобновление действия сертификата ключа ЭП в течение срока действия соответствующего закрытого ключа ЭП.

10. УЦ обязан:

информировать в письменной форме заявителей об условиях и порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и мерах, необходимых для обеспечения безопасности ЭП и их проверки;

вносить в создаваемые сертификаты достоверную и актуальную информацию, подтвержденную соответствующими документами;

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

обеспечивать круглосуточную доступность реестра сертификатов в сети Интернет, за исключением периодов планового или внепланового технического обслуживания;

обеспечивать конфиденциальность созданных ключей ЭП;

не разглашать (не публиковать) информацию о внутренних пользователях УЦ, за исключением информации, используемой для идентификации владельцев сертификатов и заносимой в созданные сертификаты, за исключением случаев, предусмотренных законодательством Российской Федерации;

направлять в соответствии с частью 5 статьи 18 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» в единую систему идентификации и аутентификации сведения о лице, получившем сертификат ключа ЭП (далее – квалифицированный сертификат), в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра);

безвозмездно осуществить регистрацию лица, которому выдан квалифицированный ключ ЭП в единой системе идентификации и аутентификации (по желанию такого лица);

отказать заявителю в создании сертификата в случае:

неподтверждения того, что он владеет ключом ЭП, который соответствует ключу ЭП, указанному в заявлении на создание ключей ЭП;

отрицательного результата проверки в реестре сертификатов уникальности ключа ЭП, указанного в заявлении на создание ключей ЭП;

соблюдать срок действия ключей ЭП, используемых для подписания создаваемых сертификатов, распределяя сроки их действия таким образом, чтобы по окончании таких сроков все сертификаты, подписанные ключами ЭП, прекратили свое действие;

обеспечить регистрацию пользователей УЦ по заявлениям на создание ключа ЭП (приложение № 2 (для юридического лица), приложение № 3 (для физического лица) к настоящему Регламенту);

организовать работу по времени GMT (Greenwich Mean Time) с учетом часового пояса, синхронизировать по времени все программные и технические средства обеспечения деятельности УЦ по назначению;

обеспечить сохранность созданного закрытого ключа ЭП до момента передачи пользователю УЦ;

обеспечить уникальность регистрационной информации внутренних пользователей УЦ, заносимой в реестр сертификатов и используемой для идентификации владельцев сертификатов;

использовать для создания закрытого ключа ЭП уполномоченного лица УЦ и формирования ЭП только средства ЭП, сертифицированные по классу КС2 или выше в соответствии с законодательством Российской Федерации;

использовать закрытый ключ ЭП уполномоченного лица УЦ только для подписи созданных им сертификатов и списков отозванных сертификатов;

принимать меры по защите закрытого ключа ЭП уполномоченного лица УЦ в соответствии с положениями настоящего Регламента;

уведомлять в свободной форме владельца сертификата о фактах, которые стали известны УЦ, влияющих на возможности дальнейшего использования закрытого ключа ЭП и сертификата.

Публикация информации, используемой для идентификации владельцев сертификатов, осуществляется путем включения ее в созданные сертификаты.

11. УЦ обязан вести реестр сертификатов пользователей УЦ.

Реестр сертификатов пользователей УЦ ведется в электронном виде, сертификаты представлены в форме электронных копий.

Реестр сертификатов пользователей УЦ является публичным и размещен в сети Интернет (http://crl.uc.orb.ru/kval/, http://crl2.uc.orb.ru/kval/).

Реестр списков отозванных сертификатов является публичным и размещен в сети Интернет (http://crl.uc.orb.ru/pubservice/, http://crl2.uc.orb.ru/pubservice/).

Созданный сертификат внутреннего пользователя УЦ автоматически записывается в реестр сертификатов пользователей УЦ. Данный процесс

обеспечивается настройками программы ViPNet «Удостоверяющий и ключевой центр» и программы ViPNet «Сервис публикации».

Отозванный сертификат внутреннего пользователя УЦ автоматически заносится в список отозванных сертификатов и записывается в реестр отозванных сертификатов.

УЦ обязан осуществлять выдачу копий сертификатов в электронной форме по заявлениям пользователей УЦ.

Техническое обслуживание серверов, на которых расположены реестры сертификатов пользователей УЦ, происходит поочередно с поддержанием доступа хотя бы к одному из адресов данных реестров.

12. Внутренний пользователь УЦ обязан:

хранить в тайне закрытый ключ ЭП, принимать все возможные меры для предотвращения его потери, раскрытия, модифицирования или несанкционированного использования;

не использовать для ЭП закрытые ключи ЭП в случае, если ему известно об их использовании другими лицами;

использовать закрытый ключ ЭП только для целей, определенных соответствующими областями использования, определенными сертификатом, или в порядке, установленном законодательством Российской Федерации.

Владелец сертификата, пользователь, не являющийся его владельцем, должны удостовериться, что назначение сертификата, определенное соответствующими областями использования, определенными сертификатом согласно настоящему Регламенту, соответствует предполагаемому использованию.

## V. Процедуры и механизмы работы УЦ

13. Перечень документов, необходимых для получения ЭП:

заявление на создание ключа ЭП на бумажном носителе;

документ, удостоверяющий личность заявителя или доверенного лица;

доверенность от заявителя на право доверенного лица предоставлять его интересы в УЦ.

В случае если от имени заявителя – физического лица действует доверенное лицо – физическое лицо на основании доверенности, доверенность должна быть нотариально заверена.

14. Заявление на создание ключа ЭП должно быть заверено подписью заявителя, подается заявителем лично или доверенным лицом по доверенности.

Заявление на создание ключа ЭП должно содержать:

а) для физического лица:

фамилию, имя, отчество;

пол;

дату рождения;

место рождения;

ИНН;

СНИЛС;

адрес электронной почты заявителя;

серию, номер документа, удостоверяющего личность;

кем и когда выдан (включая код подразделения) документ, удостоверяющий личность;

номера контактных телефонов;

б) для физического лица, представляющего юридическое лицо:

наименование юридического лица;

фамилию, имя и отчество;

пол;

дату рождения;

место рождения;

ИНН юридического лица;

ОГРН юридического лица;

СНИЛС;

наименование должности;

серию, номер документа, удостоверяющего личность;

кем и когда выдан (включая код подразделения) документ, удостоверяющий личность;

адрес электронной почты заявителя;

юридический адрес юридического лица.

Дополнительно (определяется заявителем) заявление на создание ключа ЭП может содержать следующую информацию, включаемую в идентификационные данные:

псевдоним;

номер мобильного телефона (для регистрации в единой системе идентификации и аутентификации).

К заявлению на создание ключа ЭП физического лица, представляющего юридическое лицо, прилагаются оригинал доверенности или копии документов, подтверждающих правомочность действий физического лица от имени юридического лица.

15. На основании документов, указанных в пункте 13 настоящего Регламента, сотрудник УЦ устанавливает право заявителя подать данные документы в УЦ. В случае отсутствие такого права сотрудник УЦ обязан отказать в приеме документов.

16. Заявление на создание ключа ЭП рассматривается пунктом регистрации в течение одного рабочего дня со дня его поступления в УЦ.

При подтверждении достоверности информации, содержащейся в документах, указанных в пункте 13 настоящего Регламента, производится процедура идентификации пользователя УЦ.

При выявлении недостоверности информации, содержащейся в документах, указанных в пункте 13 настоящего Регламента производится возврат заявления на создание ключа ЭП заявителю.

17. При соответствии информации, указанной в заявлении на создание ключа ЭП, с записью в реестре пользователей УЦ заявителю присваивается статус идентификации «внутренний пользователь УЦ», при несоответствии – «внешний пользователь УЦ».

18. При наличии заявления на создание ключа ЭП для внешнего пользователя УЦ производится процедура регистрации внешнего пользователя УЦ.

19. Регистрация внешнего пользователя УЦ осуществляется сотрудником пункта регистрации УЦ на основании заявления на создание ключа ЭП.

Сотрудник пункта регистрации УЦ вносит информацию о регистрации внешнего пользователя УЦ в реестр пользователей УЦ.

Регистрация внешнего пользователя УЦ может быть выполнена администратором УЦ непосредственно в программе VipNet «Удостоверяющий и ключевой центр» или по запросу программы VipNet «Центр регистрации».

По окончании процедуры регистрации внешнего пользователя УЦ ему присваивается статус «внутренний пользователь УЦ».

20. Процедура создания ключей ЭП выполняется только для внутренних пользователей УЦ.

Создание ключей ЭП выполняется ответственным сотрудником УЦ на рабочем месте с программой VipNet «Центр регистрации» на основании принятого заявления на создание ключа ЭП.

Созданные ключи ЭП записываются на отчуждаемый носитель, предоставляемый УЦ или заявителем.

Запись созданных ключей ЭП на отчуждаемый носитель производится в соответствии с требованиями по эксплуатации программного и/или аппаратного средства.

Предоставляемый заявителем ключевой носитель должен удовлетворять следующим требованиям:

соответствовать перечню устройств, указанному к документации ViPNet «Информация о внешних устройствах хранения данных» ФРКЕ:00004-04 90 09;

иметь USB-интерфейс, не требующий дополнительных адаптеров;

быть проинициализированным (отформатированным);

содержать исключительно данные инициализации.

Ключевые носители, не удовлетворяющие указанным требованиям, для записи ключевой информации не принимаются.

Ключевой носитель, содержащий созданные ключи ЭП, передается заявителю. Факт выдачи ключей ЭП заносится в журнал учета создания и выдачи ключей ЭП под роспись заявителя.

После создания сертификата заявителю направляется официальное уведомление в соответствии с пунктом 32 настоящего Регламента.

По окончании процедуры создания ключей ЭП внутреннему пользователю УЦ передаются:

ключи ЭП, записанные на отчуждаемый носитель;

копия сертификата на бумажном носителе согласно пункта 54 настоящего Регламента.

Созданный сертификат в электронной форме, заверенный ЭП уполномоченного лица УЦ, предоставляется владельцу при его личном обращении в УЦ либо доверенному лицу, действующему по доверенности.

При необходимости регистрируемый пользователь УЦ должен приобрести (получить) средство ЭП и шифрования, распространяемое УЦ либо свободно распространяемое, совместимое с программным обеспечением УЦ.

21. Аутентификация внутреннего пользователя УЦ по сертификату осуществляется путем выполнения процедуры подтверждения ЭП с использованием сертификата согласно пункту 26 настоящего Регламента.

Данная процедура выполняется при подаче заявлений на аннулирование (отзыв) сертификата, приостановление действия сертификата и в процессе других электронных взаимодействий, не требующих личного присутствия внутреннего пользователя УЦ или его доверенного лица.

22. Владелец сертификата идентифицируется по значениям атрибутов поля Subject сертификата согласно пункту 66 настоящего Регламента.

23. Аннулирование (отзыв) сертификата, созданного УЦ, осуществляется уполномоченным лицом УЦ по заявлению на аннулирование (отзыв) сертификата его владельца или организации.

Заявление на аннулирование (отзыв) сертификата ключа ЭП может быть подано как в электронном, так и письменном виде (приложение № 4 (для юридического лица) или приложение № 5 (для физического лица) к настоящему Регламенту). Заявление на аннулирование (отзыв) сертификата заверяется собственноручной или ЭП заявителя.

Заявление на аннулирование (отзыв) сертификата должно содержать:

фамилию, имя, отчество владельца;

серийный номер отзываемого сертификата;

дату создания сертификата;

ИНН, ОГРН, СНИЛС указанные в сертификате;

причина аннулирования (отзыв) сертификата;

дату, подпись заявителя.

Заявление на аннулирование (отзыв) сертификата подается заявителем администратору УЦ.

Сроки рассмотрения заявления на аннулирование (отзыв) сертификата составляет не более 12 часов с момента его поступления в УЦ.

После аннулирования (отзыва) сертификата его владельцу направляется официальное уведомление согласно пункту 33 настоящего Регламента.

УЦ может по собственной инициативе отозвать сертификат пользователя УЦ в случае установленного факта компрометации соответствующего закрытого ключа ЭП с внесением записи в журнал внештатных ситуаций, уведомлением владельца отозванного сертификата и указанием обоснованных причин отзыва сертификата.

24. Приостановление действия сертификата, созданного УЦ, осуществляется уполномоченным лицом УЦ по заявлению на приостановление действия сертификата. Заявление на приостановление действия сертификата подается пользователем УЦ в УЦ.

Заявление на приостановление действия сертификата ключа ЭП может быть подано как на бумажном носителе, так и в электронном виде (приложение № 6 (для юридического лица), приложение № 7 (для физического лица) к настоящему Регламенту). Заявление на приостановление действия сертификата ключа ЭП заверяется собственноручной или ЭП заявителя.

Заявление на приостановление действия сертификата содержит:

фамилию, имя, отчество заявителя;

серийный номер сертификата, действие которого приостанавливается;

дату создания сертификата;

ИНН, ОГРН, СНИЛС, указанные в сертификате;

срок, на который приостанавливается действие сертификата;

причина приостановки действия сертификата;

дата, подпись заявителя.

Срок рассмотрения заявления на приостановление действия сертификата составляет один рабочий день со дня его поступления в УЦ.

После приостановления действия сертификата его владельцу направляется официальное уведомление согласно пункту 34 настоящего Регламента.

УЦ может по собственной инициативе приостановить действие сертификата с уведомлением его владельца о причинах приостановления действия сертификата.

25. Возобновление действия сертификата, осуществляется уполномоченным лицом УЦ по заявлению на возобновление действия сертификата.

Заявление на возобновление действия сертификата ключа ЭП (приложение № 8 (для юридического лица), приложение № 9 (для физического лица) к настоящему Регламенту) подписывается заявителем собственноручно.

Заявление на возобновление действия сертификата содержит:

фамилию, имя, отчество заявителя;

серийный номер сертификата, действие которого возобновляется;

дату создания сертификата;

ИНН, ОГРН, СНИЛС, указанные в сертификате;

дату, подпись заявителя.

Срок рассмотрения заявления на возобновление действия сертификата составляет до трех рабочих дней со дня его поступления в УЦ.

После возобновления действия сертификата его владельцу направляется официальное уведомление согласно пункту 35 настоящего Регламента.

26. Проверка сертификата осуществляется УЦ согласно обращению пользователя УЦ на основании заявления на проверку подлинности

сертификата, составленного в свободной форме, в письменном или электронном виде (для внутренних пользователей УЦ). При подаче заявления на проверку подлинности сертификата в письменном виде оно должно быть подписано заявителем собственноручно, при подаче заявления на проверку подлинности сертификата в электронной форме – действующим ключом ЭП пользователя УЦ.

Обязательным приложением к заявлению на проверку подлинности сертификата является файл, содержащий сертификат, подлежащий процедуре проверки. При необходимости могут быть запрошены дополнительные данные:

файл, содержащий сертификат уполномоченного лица УЦ, являющегося издателем сертификата, подлежащий процедуре проверки;

файл, содержащий список отозванных сертификатов УЦ, являющегося издателем сертификата, использовавшийся для проверки ЭП уполномоченного лица УЦ заявителем.

Срок рассмотрения заявления на проверку подлинности сертификата составляет до трех рабочих дней со дня его поступления в УЦ. Результаты проверки оформляются в виде отчета, содержащего следующую информацию:

время и место проведения проверки;

сведения о лицах, проводивших проверку;

основание для проведения проверки;

данные, представленные для проверки;

результаты проверки;

оценка результатов проверки.

Отчет оформляется в электронной или письменной форме в зависимости от формы поступившего заявления на проверку подлинности сертификата ключа ЭП и передается пользователю УЦ.

27. Хранение сертификата в реестре сертификатов УЦ осуществляется в течение срока действия сертификата, определенного пунктом 52 настоящего Регламента.

Срок архивного хранения сертификата устанавливается в соответствии со сроком, определенным пунктом 58 настоящего Регламента.

28. Подтверждение ЭП в электронном документе осуществляется УЦ в соответствии с обращением граждан на основании заявления на подтверждение ЭП в электронном документе, составленного в свободной форме, которое подается администратору УЦ лично либо по доверенности.

Заявление на подтверждение ЭП в электронном документе должно содержать информацию о дате и времени формирования ЭП в электронном документе.

Ответственность за достоверность указанных даты и времени формирования ЭП в электронном документе возлагается на заявителя.

Обязательным приложением к заявлению на подтверждение ЭП в электронном документе является отчуждаемый носитель, содержащий:

файл электронного документа, к которому применена ЭП;

файл, содержащий ЭП формата PKCS#7 Cryptographic Message Syntax Standard электронного документа;

файл сертификата уполномоченного лица УЦ, являющегося издателем подтверждаемого сертификата;

файл списка отозванных сертификатов УЦ, являющегося издателем сертификата ключа ЭП электронного документа и использовавшийся для проверки ЭП электронного документа заявителем.

29. Срок рассмотрения заявления на подтверждение ЭП в электронном документе составляет до трех рабочих дней с момента его поступления в УЦ.

В случае отказа подтверждения ЭП в электронном документе заявителю возвращается заявление на подтверждение ЭП в электронном документе с резолюцией администратора УЦ.

В случае подтверждения ЭП в электронном документе заявителю представляется ответ в письменном виде, заверенный собственноручной подписью администратора УЦ и печатью УЦ.

Ответ должен содержать:

результат проверки соответствующим сертифицированным средством ЭП принадлежности ЭП в электронном документе владельцу сертификата и отсутствия искажений в подписанном данной ЭП электронном документе;

детальный отчет о выполненной проверке.

30. Детальный отчет о выполненной проверке включает в себя:

время и место проведения проверки;

основания для проведения проверки;

сведения об эксперте (экспертах) или комиссии экспертов (фамилия(и), имя (имена), отчество(а), образование, специальность(и), стаж работы, ученая степень и/или ученое звание, наименования занимаемых должностей), которому (которым) поручено проведение проверки;

вопросы и их обоснования, поставленные перед экспертом (экспертами);

объекты исследований и материалы, представленные для проведения проверки;

методы проведения, содержание и результаты проверки;

оценка результатов проверки;

иные сведения в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Материалы и документы, подтверждающие заключение(я) эксперта (экспертов), прилагаются к детальному отчету и служат его составной частью.

Детальный отчет составляется в письменной форме и заверяется собственноручной подписью (собственноручными подписями) эксперта (экспертов).

31. Сертификаты и списки отозванных сертификатов издаются УЦ в соответствии с рекомендациями X.509. Контроль корректности сертификатов может осуществляться администратором УЦ или администратором программы VipNet «Центр регистрации» с использованием встроенных

механизмов операционной системы Windows. Для проведения проверки сертификат должен быть экспортирован в файл с расширением *.cer (список отозванных сертификатов – в файл с расширением *.crl).

Критериями корректности сертификатов являются:

отсутствие сообщений об ошибках при экспорте сертификата и при вызове утилиты просмотра сертификата;

корректное отображение сертификата системной утилитой;

соответствие между составами, содержаниями полей при просмотре техническими средствами УЦ и средствами операционной системы.

32. Уведомление о факте создания сертификата его владельца либо доверенного лица производится лично или с помощью электронной почты, указанной в заявлении на создание ключей ЭП.

Срок уведомления о факте создания сертификата – не позднее 24 часов со времени создания сертификата.

33. УЦ официально уведомляет о факте аннулирования (отзыва) сертификата его владельца не позднее 24 часов со времени занесения сведений об аннулированном (отозванном) сертификате в список отозванных сертификатов.

Официальным уведомлением о факте аннулирования сертификата является размещение списка отозванных сертификатов, содержащего сведения об аннулированных (отозванных) сертификатах, в сети Интернет (http://crl.uc.orb.ru/pubservice/, http://crl2.uc.orb.ru/pubservice/).

Временем аннулирования (отзыва) сертификата признается время занесения сведений об аннулированном (отозванном) сертификате в список отозванных сертификатов.

Временем опубликования списка отозванных сертификатов признается включенное в его структуру время создания списка отозванных сертификатов.

УЦ включает полный адрес (URL) списка отозванных сертификатов УЦ в издаваемые сертификаты пользователей УЦ.

34. УЦ официально уведомляет о факте приостановления действия сертификата его владельца не позднее 24 часов с момента занесения сведений об этом сертификате в список отозванных сертификатов.

Официальным уведомлением о факте приостановления действия сертификата является опубликование списка отозванных сертификатов, содержащим сведения о сертификате, действие которого приостановлено, в сети Интернет (http://crl.uc.orb.ru/pubservice/, http://crl2.uc.orb.ru/pubservice/).

Временем приостановления действия сертификата признается время занесения сведений о нем в список отозванных сертификатов.

Временем опубликования списка отозванных сертификатов признается включенное в его структуру время создания списка отозванных сертификатов.

УЦ включает полный адрес (URL) списка отозванных сертификатов в издаваемые сертификаты.

35. УЦ официально уведомляет о факте возобновления действия сертификата его владельца не позднее 24 часов с момента исключения сведений о сертификате, действие которого приостановлено, из списка отозванных сертификатов.

Официальным уведомлением о факте возобновления действия сертификата является опубликование списка отозванных сертификатов, не содержащего сведений об этом сертификате, в сети Интернет (http://crl.uc.orb.ru/pubservice/, http://crl2.uc.orb.ru/pubservice/).

Список отозванных сертификатов должен иметь более позднее время опубликования, чем список отозванных сертификатов, в котором указан сертификат, действие которого приостановлено. Временем возобновления действия сертификата признается время официального уведомления о факте возобновления действия сертификата.

36. Плановая замена ключей ЭП (закрытого и соответствующего ему открытого ключа ЭП) подписи уполномоченного лица УЦ выполняется в соответствии со сроком действия сертификата уполномоченного лица УЦ.

Процедура плановой замены ключей ЭП уполномоченного лица УЦ осуществляется в следующем порядке:

уполномоченное лицо УЦ формирует новый закрытый и соответствующий ему открытый ключи ЭП или запрос в вышестоящий УЦ в формате *.p12;

уполномоченное лицо УЦ или вышестоящий УЦ изготавливает новый сертификат уполномоченного лица УЦ и подписывает его ЭП;

администратор УЦ настраивает УКЦ для создания ключей ЭП на новом ключе ЭП уполномоченного лица УЦ.

37. Внеплановая замена ключей ЭП выполняется в случае компрометации или угрозы компрометации закрытого ключа ЭП уполномоченного лица УЦ.

Процедура внеплановой замены ключей ЭП уполномоченного лица УЦ выполняется в порядке, определенном процедурой плановой замены ключей ЭП уполномоченного лица УЦ.

После выполнения процедуры внеплановой замены ключей ЭП уполномоченного лица УЦ:

прекращается действие всех сертификатов, подписанных таким ключом ЭП;

заносятся сведения об отозванных сертификатах в список отозванных сертификатов;

скомпрометированный сертификат уполномоченного лица УЦ аннулируется (отзывается) путем занесения в список отозванных сертификатов;

УЦ безвозмездно создает сертификаты для всех владельцев сертификатов, чьи сертификаты прекращают действие в связи с внеплановой сменой.

38. Внеплановая смена ключа ЭП по причине, отличной от компрометации, выполняется в порядке, определенном процедурой плановой

замены ключей ЭП уполномоченного лица УЦ.

39. Срок действия закрытого ключа ЭП уполномоченного лица УЦ составляет один год.

Начало действия закрытого ключа ЭП уполномоченного лица УЦ исчисляется с даты и времени начала действия соответствующего сертификата.

Максимальный срок, устанавливаемый в качестве срока действия сертификатов уполномоченного лица УЦ, составляет шесть лет.

40. Процедура смены ключа ЭП владельца сертификата идентична процедура создания ключей ЭП.

## VI. Политика конфиденциальности

41. Ключевая информация администратора УЦ:

предназначена для защиты ключевой информации, формируемой и хранимой в УЦ;

хранится в УЦ, архивации не подлежит;

объем – не более 3 Кб;

зашифрована на парольном ключе защиты.

42. Ключевая информация УЦ, необходимая для выполнения его функций как ключевого центра:

формируется и хранится в УЦ в течение срока действия ключей ЭП (но не более 1 года);

защищается ключами администратора УЦ;

объем – не более 1 Мб;

подлежит архивации.

43. Ключевая информация внутренних пользователей УЦ:

формируется и депонируется в УЦ до момента передачи;

архивации не подлежит;

защищается ключами ЭП администратора УЦ;

объем – не более 10 Кб на одного пользователя УЦ.

Программное обеспечение ViPNet надежно удаляет ключевую информацию после передачи внутреннему пользователю УЦ или доверенному лицу.

44. Под конфиденциальной информацией подразумевают:

пароли (ПИН-коды) внутренних пользователей УЦ;

персональная и корпоративная информация пользователей УЦ, содержащаяся в УЦ, не подлежащая непосредственной рассылке в качестве части сертификата или списка отозванных сертификатов;

информация, содержащаяся в журналах аудита УЦ;

отчетные материалы о выполненных проверках деятельности УЦ, не публикуемые в соответствии с настоящим Регламентом.

45. К открытой информации относится информация, включаемая в сертификаты и списки отозванных сертификатов.

Открытая информация может публиковаться по решению УЦ, место, способ и время публикации также определяются решением УЦ.

46. УЦ не должен раскрывать информацию, относящуюся к типу конфиденциальной, третьим лицам, за исключением случаев:

определенных настоящим Регламентом;

требующих раскрытия в соответствии с законодательством Российской Федерации или при наличии судебного акта.

## VII. Дополнительные положения

47. Срок предоставления любой услуги УЦ не должен превышать 3 рабочих дней при наличии всех условий для ее предоставления.

48. Сертификат прекращает свое действие:

по истечении срока его действия;

на основании заявления владельца сертификата об аннулировании (отзыве) сертификата ключа ЭП, подаваемого в письменной или электронной форме;

в случае прекращения деятельности УЦ без передачи его функций другим лицам;

в иных случаях, предусмотренных законодательством Российской Федерации в области ЭП.

УЦ признает сертификат аннулированным в случаях, если:

не подтверждено, что владелец сертификата владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в сертификате;

установлено, что содержащийся в сертификате ключ проверки ЭП уже содержится в ином ранее созданном сертификате;

вступило в силу решение суда, которым установлено, что сертификат содержит недостоверную информацию.

49. Уполномоченное лицо УЦ идентифицируется по следующим данным:

фамилия, имя, отчество;

организация: ГКУ «ЦИТ»;

подразделение;

адрес электронной почты;

субъект Российской Федерации: Оренбургская область.

50. Средство ЭП должно соответствовать требованиям к средствам ЭП класса не ниже КС1 согласно приказу Федеральной службы безопасности Российской Федерации от 27 декабря 2011 года № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

51. Средства УЦ должны соответствовать требованиям к средствам УЦ класса не ниже КС2 согласно приказу Федеральной службы безопасности Российской Федерации от 27 декабря 2011 года № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

52. Срок действия закрытого ключа ЭП пользователя УЦ, соответствующего сертификату, владельцем которого он является, составляет один год.

Начало действия закрытого ключа ЭП пользователя УЦ исчисляется с даты и времени начала действия соответствующего сертификата.

Максимальный срок, устанавливаемый в качестве срока действия сертификата, составляет пять лет.

Срок действия сертификата устанавливается УЦ в момент его создания.

53. Закрытые ключи ЭП при их генерации должны записываться на отчуждаемые носители.

Закрытые ключи ЭП на отчуждаемом носителе защищаются паролем (ПИН-кодом). Пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей ЭП, учитывая следующие требования:

длина пароля (ПИН-кода) не меньше 8 символов;

срок действия пароля (ПИН-кода) – не более 12 месяцев;

пароль (ПИН-код) должен содержать символы цифр и/или букв латинского алфавита.

В случае если процедуру генерации ключей ЭП выполняет сотрудник УЦ, он должен сообщить сформированный пароль (ПИН-код) владельцу закрытых ключей ЭП.

Ответственность за сохранение пароля (ПИН-кода) возлагается на владельца закрытых ключей ЭП.

Не допускается использование одинакового значения пароля (ПИН-кода) для защиты нескольких закрытых ключей ЭП.

Сотрудники УЦ, являющиеся владельцами закрытых ключей ЭП, также выполняют указанные в настоящем разделе меры защиты закрытых ключей ЭП.

54. Копия сертификата в электронной форме представляет собой электронный документ, имеющий структуру, соответствующую стандарту Международного союза телекоммуникаций ITU-T X.509 версии 3 и рекомендациям IETF (Internet Engineering Task Force) RFC 2459, представленный в кодировке Der или Base64.

55. Копия сертификата на бумажном носителе представляет собой документ, содержащий:

серийный номер сертификата;

идентификационные данные владельца сертификата;

идентификационные данные издателя сертификата (идентификационные данные из сертификата уполномоченного лица УЦ);

сведения о средстве ЭП уполномоченного лица УЦ;

сведения о ключе ЭП владельца сертификата и алгоритме его формирования;

сведения об областях использования закрытого ключа ЭП и сертификата;

собственноручную подпись уполномоченного лица УЦ;

печать УЦ.

Копия сертификата печатается на белой бумаге, листе формата А4, не содержащем средств защиты от копирования и подделки.

56. Источником комплектования архивного фонда УЦ является пункт регистрации УЦ, обеспечивающий документирование. Архивированию подлежат:

реестр сертификатов пользователей УЦ;

сертификаты уполномоченного лица УЦ;

журналы аудита программно-аппаратных средств обеспечения деятельности УЦ;

реестр зарегистрированных пользователей УЦ;

заявления на создание ключей ЭП;

заявления на аннулирование (отзыв) сертификата;

заявления на приостановление действия сертификата;

заявления на возобновление действия сертификата;

служебные документы УЦ.

57. Архивные документы хранятся в специально оборудованном помещении – архивохранилище, в котором обеспечивается режим хранения архивных документов, установленный законодательством Российской Федерации.

58. Срок хранения архивных документов – 11 лет.

59. Выделение архивных документов к уничтожению и их уничтожение осуществляется постоянно действующей комиссией, формируемой из числа сотрудников УЦ и назначаемой приказом руководителя УЦ.

60. Количество программ VipNet «Центр регистрации», сетевых узлов и пользователей, которые могут быть зарегистрированы в программе ViPNet «Центр управления сетью», и сертификатов, которые могут быть созданы в УЦ, ограничивается лицензией производителя при поставке программного обеспечения. Распределение квот на регистрацию пользователей УЦ и число создаваемых запросов на сертификаты производится администратором УЦ в программе ViPNet «Центр управления сетью» для каждого из пунктов регистрации.

При распределении лицензий администратор должен учитывать:

суммарное количество лицензий;

количество обслуживаемых центров регистрации;

распределение нагрузки по количеству обслуживаемых пользователей УЦ между пунктами регистрации.

61. Суммарное число лицензий на сертификаты не должно превышать общего числа свободных лицензий для внутренних пользователей УЦ в данной сети.

62. При возникновении споров УЦ и пользователи УЦ (далее – стороны) предпринимают необходимые меры для их урегулирования путем переговоров.

Споры между сторонами, не урегулированные в процессе переговоров, должны рассматриваться в соответствии с законодательством Российской Федерации.

63. УЦ не несет ответственности за негативные последствия, наступившие в результате нарушения пользователями УЦ положений настоящего Регламента.

Претензии к УЦ ограничиваются указанием на несоответствие его действий настоящему Регламенту.

64. Деятельность УЦ может быть прекращена в порядке, установленном законодательством Российской Федерации.

## VIII. Структура сертификата и списков отозванных сертификатов

65. УЦ создает сертификаты пользователей УЦ и уполномоченного лица УЦ в электронной форме формата X.509 версии 3.

66. Сертификаты содержат следующие базовые поля X.509:

| | |
|---|---|
| Signature: | ЭП уполномоченного лица УЦ |
| Issuer: | идентифицирующие данные уполномоченного лица УЦ |
| Validity: | даты начала и окончания срока действия сертификата |
| Subject: | идентифицирующие данные владельца сертификата |
| SubjectPublicKey-Information: | идентификатор алгоритма средства ЭП, с которым используется данный открытый ключ ЭП, значение открытого ключа ЭП |
| Version: | версия сертификата формата X.509 версия 3 |
| SerialNumber: | уникальный серийный (регистрационный) номер сертификата в реестре сертификатов УЦ |

67. Сертификаты содержат следующие дополнения:

| | |
|---|---|
| AuthorityKeyIdentifier: | идентификатор открытого ключа ЭП уполномоченного лица УЦ |
| SubjectKeyIdentifier: | идентификатор ключа ЭП владельца сертификата |
| ExtendedKeyUsage: | область (области) использования ключа ЭП, при котором электронный документ с ЭП будет иметь юридическое значение |
| CRLDistributionPoint: | точка распространения списка аннулированных (отозванных) сертификатов, созданных УЦ (может включаться или не включаться в соответствии с настройками УЦ) |
| KeyUsage: | назначение ключа ЭП |
| Basic Constraints: | определяет принадлежность сертификата УЦ и ограничение длины цепочки сертификатов для подчиненного УЦ |

68. УЦ обеспечивает формирование ключей ЭП пользователей в соответствии с параметрами:

| Алгоритм подписи | Описание | Параметры ключа ЭП | Описание OID ISO | Длина ключа ЭП |
|---|---|---|---|---|
| ГОСТ Р 34.10-2012 | стандарт ЭП, основанный на арифметике эллиптических кривых. OID «1.2.643.2.2.19» | ГОСТ Р 34.10-2012 параметры по умолчанию | набор параметров по умолчанию (рекомендуется). OID «1.2.643.2.2. 35.1» | 512 |
| | | ГОСТ Р 34.10-2012 «Оскар» | набор параметров «КриптоПРО» (Параметры 2) OID «1.2.643.2.2. 35.2» | |
| | | ГОСТ Р 34.10-2012 параметры подписи 3 | набор параметров «КриптоПРО» (Параметры 3) OID «1.2.643.2.2. 35.3» | |

69. В сертификате поля идентификационных данных уполномоченного лица УЦ и владельца сертификата содержат атрибуты имени формата X.500.

70. Обязательными атрибутами поля идентификационных данных уполномоченного лица УЦ являются:

| | |
|---|---|
| commonName | наименование удостоверяющего центра |
| Organization-Name | наименование юридического лица, являющейся владельцем УЦ |
| organizationUnit-Name | наименование подразделения, сотрудником которого является уполномоченное лицо УЦ |
| e-mail | адрес электронной почты |
| countryName | RU |
| stateOrProvince-Name | субъект Российской Федерации, где зарегистрирована организация, являющаяся владельцем УЦ |
| localityName | наименование населенного пункта |
| INN | ИНН УЦ |
| OGRN | ОГРН УЦ |
| streetAddress | Юридический адрес УЦ |

71. Обязательными атрибутами поля идентификационных данных владельца сертификата, являющегося физическим лицом, являются:

| | |
|---|---|
| commonName | фамилия, имя, отчество |
| surname | Фамилия |
| givenName | имя, отчество |
| e-mail | адрес электронной почты |
| countryName | RU |

| | |
|---|---|
| stateOrProvince-Name | субъект Российской Федерации, где зарегистрировано физическое лицо |
| localityName | наименование населенного пункта, где зарегистрировано физическое лицо |
| streetAddress | название улицы, номер дома, где зарегистрировано физическое лицо |
| INN | ИНН физического лица |
| SNILS | СНИЛС физического лица |

72. Обязательными атрибутами поля идентификационных данных владельца сертификата, являющегося физическим лицом и представляющего юридическое лицо, являются:

| | |
|---|---|
| commonName | наименование юридического лица |
| surname | Фамилия |
| givenName | имя, отчество |
| countryName | RU |
| stateOrProvince-Name | субъект Российской Федерации, где зарегистрировано юридическое лицо |
| localityName | наименование населенного пункта, где зарегистрировано юридическое лицо |
| streetAddress | название улицы, номер дома, где зарегистрировано юридическое лицо |
| title | Должность |
| OGRN | ОГРН юридического лица |
| SNILS | СНИЛС |
| INN | ИНН юридического лица |

73. УЦ издает список отозванных сертификатов пользователей УЦ и уполномоченного лица УЦ в электронной форме формата X.509 версии 2.

74. УЦ использует следующие дополнения:

| | |
|---|---|
| AuthorityKey-Identifier | идентификатор открытого ключа ЭП уполномоченного лица УЦ |
| ReasonCode | код причины отзыва сертификата |

## IX. Программные и технические средства обеспечения деятельности УЦ

75. Для реализации своих услуг и обеспечения жизнедеятельности УЦ использует следующие программные и технические средства:

программный комплекс обеспечения реализации целевых функций УЦ;

технические средства обеспечения работы программного комплекса УЦ;

программные и программно-аппаратные средства защиты информации.

76. Программный комплекс обеспечения реализации целевых функций УЦ включает в себя следующие программные компоненты:

ViPNet «Администратор»;

ViPNet «Центр управления сетью»;

ViPNet «Удостоверяющий и ключевой центр»;

ViPNet CSP;

ViPNet «Сервис публикации»;

ViPNet «Центр регистрации»;

ViPNet «Администратор».

77. ViPNet «Администратор» является базовым компонентом программного комплекса УЦ, включает в себя программы ViPNet «Центр управления сетью» и ViPNet «Удостоверяющий и ключевой центр».

Программа ViPNet «Центр управления сетью» предназначена для формирования и изменения структуры корпоративной сети, обеспечивает реализацию следующих функций УЦ:

регистрация сетевого узла;

распределение задач для сетевого узла («Координатор», «Клиент», «Центр регистрации»);

регистрация клиентов (абонентов) в сети на сетевом узле;

задание и изменение разрешенных связей для сетевого узла;

формирование и рассылка адресных справочников для сетевого узла;

формирование справочников для программы ViPNet «Удостоверяющий и ключевой центр»;

рассылка для сетевого узла обновлений справочно-ключевой информации, формируемой программой ViPNet «Удостоверяющий и ключевой центр»;

рассылка для сетевого узла списков отозванных сертификатов и списков сертификатов уполномоченных лиц УЦ своей и смежных сетей;

прием и передача в программу ViPNet «Удостоверяющий и ключевой центр» запросов на сертификаты, на обновление сертификатов от пользователей корпоративной сети и центров регистрации, рассылка созданных сертификатов на сетевые узлы.

78. Программу ViPNet «Удостоверяющий и ключевой центр» с учетом выполнения функций можно условно разделить на две программы: «Ключевой центр» и «Удостоверяющий центр».

Программа «Ключевой центр» предназначена для формирования пользовательской ключевой информации на основе информации, поступающей из центра управления сетью. Созданные программой «Ключевой центр» ключи ЭП передаются пользователям, после чего при наличии соответствующего программного обеспечения ViPNet пользователи сети смогут безопасно обмениваться конфиденциальной информацией.

Программа «Ключевой центр» обеспечивает реализацию следующих функций УЦ:

формирование ключевых дискет для пользователей сети ViPNet;

формирование ключевых наборов для сетевых узлов;

формирование паролей;

обновление ключевых дискет и ключевых наборов.

79. Программа «Удостоверяющий центр» предназначена для обслуживания следующих запросов на:

создание сертификатов;

отзыв, приостановление и возобновление приостановленного действия сертификатов, сформированных на сетевых узлах сети ViPNet (пользователями корпоративной сети) или в центрах регистрации для внешних пользователей.

Программа «Удостоверяющий центр» обеспечивает реализацию следующих функций:

создание ключей ЭП и создание сертификатов уполномоченных лиц УЦ;

формирование запросов в головной удостоверяющий центр на создание сертификата уполномоченного лица УЦ;

импорт сертификатов уполномоченных лиц УЦ смежных сетей и головного УЦ;

ведение эталонной копии реестра справочников сертификатов уполномоченных лиц УЦ, формирование и отправка в программу VipNet «Центр управления сетью» обновлений справочников сетевых узлов;

создание ключей ЭП пользователей и создание сертификатов корпоративной сети по запросам программы VipNet «Центр управления сетью»;

рассмотрение запросов на создание сертификатов от пользователей корпоративной сети;

рассмотрение запросов на создание сертификатов внешних пользователей от программы VipNet «Центр регистрации»;

хранение информации о запросах на создание сертификатов и ведение эталонной копии реестра справочников созданных сертификатов от программы VipNet «Центр регистрации»;

рассмотрение запросов на отзыв, приостановление и возобновление сертификатов;

отправка в программу VipNet «Центр управления сетью» обновлений списков отозванных сертификатов;

ведение эталонной копии списка аннулированных (отозванных) и приостановленных сертификатов пользователей УЦ.

Программа «Удостоверяющий центр» обеспечивает возможность формирования и сертификации ключей ЭП для алгоритма ГОСТ Р 34.10-2012.

Ответственность за эксплуатацию программы ViPNet «Администратор» возлагается на уполномоченное лицо УЦ.

80. Программа ViPNet CSP – средство ЭП УЦ. Данное средство (криптопровайдер) пользователь УЦ самостоятельно приобретает или получает через официальный сайт производителя безвозмездно.

81. Программа ViPNet «Центр регистрации» обеспечивает реализацию следующих функций УЦ:

регистрация персональных данных внешних пользователей УЦ;

ведение реестра зарегистрированных внешних пользователей УЦ;

генерация секретного ключа ЭП и сохранение его на персональном ключевом носителе внешнего пользователя УЦ;

формирование запроса на сертификат;

отправка запроса в программу ViPNet «Удостоверяющий и ключевой центр» (через программу ViPNet «Центр управления сетью»);

прием и ввод в действие созданных сертификатов;

ведение реестра справочников запросов и созданных сертификатов;

формирование запросов на отзыв, приостановление или возобновление сертификатов;

ведение журнала событий и действий абонентов центра регистрации.

Ответственность за эксплуатацию программы ViPNet «Центр регистрации» возлагается на УЦ.

82. Техническими средствами обеспечения работы программного комплекса УЦ являются:

выделенный сервер с программой ViPNet «Администратор» (ViPNet «Центр управления сетью» и ViPNet «Удостоверяющий и ключевой центр» могут быть установлены на разных компьютерах);

компьютер с программой ViPNet «Центр регистрации»;

выделенный сервер с программой ViPNet «Координатор»;

программно-аппаратные комплексы защиты от несанкционированного доступа типа «электронный замок»;

телекоммуникационное оборудование;

автоматизированные рабочие места сотрудников УЦ;

устройства печати (принтеры).

Ответственность за эксплуатацию технических средств и общесистемного программного обеспечения возлагается на сотрудников УЦ.

83. Программными и программно-аппаратными средствами защиты информации являются:

средство криптографической защиты информации ViPNet CSP;

средство криптографической защиты информации ViPNet «Координатор»;

средство криптографической защиты информации ViPNet «Клиент»;

устройства обеспечения температурно-влажностного режима и кондиционирования служебных и рабочих помещений УЦ;

устройства обеспечения противопожарной безопасности помещений УЦ.

Ответственность за эксплуатацию программных и программно-аппаратных средств защиты информации возлагается на администратора УЦ.

84. Программы ViPNet «Удостоверяющий и ключевой центр» и ViPNet «Центр регистрации» обеспечивает реализацию следующих функций УЦ:

вход администратора в программу ViPNet «Удостоверяющий и ключевой центр»;

регистрация администратора программы ViPNet «Удостоверяющий и ключевой центр»;

создание сертификата администратора программы ViPNet «Удостоверяющий и ключевой центр»;

формирование списка отозванных сертификатов;

принятие запроса на создание ключа ЭП;

отклонение запроса на создание ключа ЭП;

создание ключей ЭП;

принятие запроса на отзыв сертификата;

удовлетворение запроса на отзыв сертификата;

отклонение запроса на отзыв сертификата;

невыполнение внутренней операции программной компоненты;

системные события общесистемного программного обеспечения.

85. При эксплуатации программного комплекса обеспечения реализации целевых функций УЦ выполняется резервное копирование данных компонент программного комплекса УЦ. Периодичность создания резервных копий определяется настройками программы ViPNet «Удостоверяющий и ключевой центр» и может варьироваться в зависимости от числа выполненных операций.

Перечень данных программного комплекса УЦ, подлежащих резервному копированию, включает в себя:

списки сертификатов уполномоченных лиц программы ViPNet «Удостоверяющий и ключевой центр» и УЦ смежных сетей в электронном виде;

базу данных пользователей УЦ;

базу данных созданных сертификатов, включая очередь входящих запросов и историю запросов на сертификаты;

журналы программы ViPNet «Удостоверяющий и ключевой центр».

## X. Обеспечение безопасности, инженерно-технические меры защиты информации

86. Серверы и телекоммуникационное оборудование размещаются в выделенном помещении в шкафу-стойке.

Остальные технические средства УЦ размещаются в рабочих помещениях УЦ согласно схеме организации рабочих мест сотрудников ГКУ «ЦИТ».

87. Помещение УЦ оборудовано системой сигнализации, выведенной на пульт охраны.

Рабочие и служебные помещения УЦ не подключены к системе контроля доступа и оборудованы механическими замками.

Ключи механических замков рабочих помещений УЦ выдаются сотрудникам УЦ по распоряжению руководителя УЦ в соответствии со

схемой организации рабочих мест сотрудников ГКУ «ЦИТ». Ключи также имеют руководитель и заместитель руководителя ГКУ «ЦИТ».

88. Технические средства УЦ подключены к общегородской сети электроснабжения.

Серверы, телекоммуникационное оборудование УЦ подключены к источникам бесперебойного питания, обеспечивающим их работу в течение часа после прекращения основного электроснабжения.

Технические средства, используемые на рабочих местах сотрудников УЦ, также обеспечены источниками бесперебойного питания.

Служебные помещения УЦ, используемые для архивного хранения документов на бумажных, магнитных и оптических носителях, серверное помещение оборудованы средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

89. Помещение УЦ оборудовано пожарной сигнализацией. Пожарная безопасность помещений УЦ обеспечивается в соответствии с нормами и требованиями, установленными законодательством Российской Федерации.

90. Документальный фонд УЦ как фондообразователя подлежит хранению в соответствии с законодательством Российской Федерации по делопроизводству и архивному делу.

91. Выделение к уничтожению и уничтожение документов УЦ, не подлежащих архивному хранению, осуществляется сотрудниками УЦ, обеспечивающими документирование.

## XI. Структура УЦ, обязанности и функции администратора и оператора УЦ

92. Структура УЦ:

администратор УЦ;

оператор центра регистрации УЦ.

93. Администратором УЦ может являться только уполномоченное лицо УЦ.

Администратор УЦ выполняет следующие функции:

управление деятельностью УЦ;

координация деятельности центра регистрации УЦ;

взаимодействие с пользователями УЦ в части разрешения вопросов, связанных с применением средств ЭП, распространяемых УЦ, с подтверждением ЭП уполномоченного лица УЦ в сертификатах, созданных УЦ в электронной форме, или подтверждения собственноручной подписи уполномоченного лица УЦ в копиях сертификатов, созданных УЦ на бумажном носителе.

администрирование программы ViPNet «Удостоверяющий и ключевой центр»;

администрирование программы ViPNet «Центр управления сетью»;

обеспечение соблюдения правил безопасной эксплуатации программного и аппаратного комплекса УЦ в целом;

осуществление настройки операционной системы и прикладного программного обеспечения;

обеспечение синхронизации времени на серверах времени и контроль за синхронизацией времени на компьютерах пользователей УЦ;

осуществление контроля за соблюдением правил эксплуатации и соблюдением мер защиты от несанкционированного доступа;

осуществление проверки целостности программного обеспечения и данных компонент УЦ;

осуществление аудита событий по журналам программных компонент УЦ, журналам операционной системы и аппаратных средств защиты от несанкционированного доступа;

контроль целостности журналов и архивов журналов;

осуществление регистрации абонентских пунктов и пользователей сети ViPNet;

назначение связи между объектами сети;

формирование и рассылка справочников для абонентских пунктов и программы ViPNet «Удостоверяющий и ключевой центр», а также обновления ключевой и справочной информации;

обеспечение взаимодействия программы ViPNet «Центр управления сетью» с другими сетями ViPNet.

94. Для выполнения своих функций администратору УЦ необходимо:

обладать паролями входа в операционную систему с правами, достаточными для выполнения своих функций. Иметь полный доступ к программе ViPNet «Администратор» и ее рабочим каталогам;

осуществлять первичную генерацию ключевой информации в программе ViPNet «Удостоверяющий и ключевой центр» и абонентских пунктов сети;

осуществлять формирование симметричных ключей шифрования для абонентских пунктов сети;

осуществлять формирование и своевременную смену мастер-ключей своей сети и для межсетевого взаимодействия;

обеспечивать своевременной передачи в программу ViPNet «Центр управления сетью» сформированной ключевой и справочной информации.

95. Администратор УЦ при администрировании программы ViPNet «Удостоверяющий и ключевой центр» выполняет следующие функции:

формирует ключ ЭП уполномоченного лица, издает корневой сертификат УЦ и запросы на сертификаты уполномоченного лица к вышестоящему УЦ

издает сертификаты по запросам центра регистрации УЦ и запросам на обновление сертификатов;

отзывает, приостанавливает и возобновляет сертификаты по запросам пользователей УЦ или по запросам программы ViPNet «Центр регистрации»;

осуществляет экспорт и отправку в программу ViPNet «Центр управления сетью» справочников сертификатов УЦ, пользователей УЦ, списков отозванных сертификатов.

96. В обязанности администратора УЦ входят:

своевременное создание архивов баз данных и их восстановление при сбоях;

настройка и ведение журналов программа ViPNet «Удостоверяющий и ключевой центр»;

ведение документации программы ViPNet «Удостоверяющий и ключевой центр» в соответствии с настоящим Регламентом и должностными инструкциями.

97. Оператор центра регистрации УЦ выполняет следующие функции:

осуществляет регистрацию внешних пользователей УЦ и ведение реестра внешних пользователей УЦ;

создает запросы на создание обновления и отзыв сертификатов внешних пользователей УЦ;

осуществляет (при необходимости) проверку сертификатов внешних пользователей УЦ.

98. Администратор совместно с оператором программы ViPNet «Центр регистрации» выполняют следующие функции:

организация и выполнение мероприятий по защите ресурсов УЦ;

формирование и обновление справочно-ключевых наборов для организации защищенного обмена информацией;

обеспечение взаимодействия с другими УЦ на основе кросс-сертификации;

создание и предоставление ключей ЭП согласно заявлениям пользователей УЦ;

создание и предоставление сертификатов в электронной форме по заявлениям пользователей УЦ;

создание и предоставление копий сертификатов на бумажном носителе по заявлениям их владельцев;

аннулирование (отзыв) сертификатов по заявлениям пользователей УЦ, являющихся владельцами сертификатов;

приостановление и возобновление действия сертификатов по заявлениям пользователей УЦ, являющихся владельцами сертификатов;

предоставление пользователям УЦ сведений об аннулированных и приостановленных сертификатах;

предоставление копий сертификатов, находящихся в реестре созданных сертификатов, по запросам пользователей УЦ;

техническое обеспечение процедуры подтверждения ЭП в документах, представленных в электронной форме, подлинности ЭП уполномоченного лица УЦ в созданных сертификатах по заявлениям пользователей УЦ;

организация и выполнение мероприятий по эксплуатации программных и технических средств обеспечения деятельности УЦ;

организация и выполнение мероприятий по техническому сопровождению распространяемых средств ЭП;

направление в единую систему идентификации и аутентификации сведений о лице, получившем квалифицированный сертификат, в объеме,

необходимом для регистрации в единой системе идентификации и аутентификации, и полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра).

99. Для выполнения своих функций оператору программы VipNet «Центр регистрации» необходимо:

иметь действительный ключ ЭП и сертификат для подписи запросов к УЦ;

обладать паролями входа в операционную систему с правами, достаточными для выполнения своих обязанностей;

иметь полный доступ к программе ViPNet «Администратор» (ViPNet «Центр регистрации») и ее рабочим каталогам.

100. Организацию доступа к техническим средствам УЦ, размещенных на рабочих местах сотрудников УЦ, обеспечивают сотрудники УЦ, ответственные за эксплуатацию технических средств.

Доступ к техническим средствам УЦ осуществляется администраторами УЦ при:

регистрации пользователей УЦ, сетевых объектов, управлении сетью в центре управления сетью;

создании ключевой информации для зарегистрированных пользователей УЦ;

создании сертификатов по запросам пользователей УЦ;

отзыве сертификатов пользователей УЦ;

регистрации пользователей УЦ в программе VipNet «Центр регистрации», создание запросов на регистрацию пользователей УЦ в программе VipNet «Центр управления сети»;

формировании ключей ЭП в программе VipNet «Центр регистрации», создание запросов на создание сертификатов ключа ЭП в программе ViPNet «Удостоверяющий и ключевой центр»;

создании и отзыве сертификатов по запросам программы VipNet «Центр регистрации».

101. Все рабочие места сотрудников УЦ, на которых установлены программы ViPNet «Администратор» (ViPNet «Центр управления сетью», ViPNet «Удостоверяющий и ключевой центр», ViPNet «Центр регистрации», ViPNet «Сервис публикации»), оснащены программно-аппаратными комплексами защиты от несанкционированного доступа согласно паспорту автоматизированного рабочего места. Доступ системных администраторов общесистемного программного обеспечения серверов для выполнения регламентных работ осуществляется в присутствии администратора УЦ.

102. Аутентификация администратора УЦ предусматривает:

аутентификацию пользователя компьютера и операционной системы с использованием устройств аутентификации к аппаратным средствам защиты от несанкционированного доступа;

аутентификацию пользователя программы ViPNet «Клиент» (или CSP) на узле ViPNet, зарегистрированном в прикладных задачах, отвечающих за роли администратора (в программах ViPNet «Центр регистрации», ViPNet «Центр управления сетью», ViPNet «Удостоверяющий и ключевой центр» или ViPNet «Сервис публикации»);

аутентификацию пользователя программ ViPNet, соответствующего выполняемой роли администратора УЦ.

103. В перечень объектов доступа, предоставляемых администратору УЦ при взаимодействии с программно-аппаратными средствами УЦ, входят:

устройства аутентификации к аппаратным средствам защиты от несанкционированного доступа («электронный замок») с правами администратора УЦ;

учетные записи и пароли пользователей операционной системы на подконтрольных технических средствах с правами, необходимыми для выполнения своих обязанностей;

ключевая информация пользователя программы ViPNet «Клиент» (или CSP) для аутентификации на подконтрольных компьютерах;

пароли администратора сетевых узлов ViPNet для аутентификации с правами администратора УЦ на подконтрольных компьютерах;

журналы аудита операционной системы и программно-аппаратных средств УЦ и их настройки на подконтрольных технических средствах;

программа ViPNet «Администратор» (программы ViPNet «Центр управление сетью») или программа ViPNet «Центр регистрации» в зависимости от полномочий;

журналы аудита программного обеспечение ViPNet;

программа ViPNet «Администратор», аутентификационная информация администратора программы ViPNet «Удостоверяющий и ключевой центр»;

секретный ключ ЭП уполномоченного лица УЦ для администраторов, выполняющих данную роль;

журналы аудита программы ViPNet «Администратор».

104. Контролю целостности подлежат следующие компоненты программного обеспечения, эксплуатируемого УЦ:

программное обеспечение средств ЭП и криптографической защиты информации;

программа ViPNet «Администратор»;

программа ViPNet «Центр регистрации»;

программа ViPNet «Сервис публикации».

Состав программ и справочно-ключевой информации, подлежащих контролю целостности, определяется документацией программного обеспечения ViPNet «Правила пользования» ФРКЕ:00106-03 99 01 ПП, «Правила пользования» ФРКЕ:00109-07 99 01 ПП, «Правила пользования» ФРКЕ.00116-03 99 01 ПП.

Система контроля целостности основывается на аппаратном контроле целостности общесистемного программного обеспечения до загрузки операционной системы.

Данная система обеспечивается использованием сертифицированного устройства типа «электронный замок».

Программная составляющая системы контроля целостности осуществляет проверку контрольных сумм, подлежащих контролю программ и справочно-ключевой информации, при каждом запуске программ или в процессе работы по требованию администратора УЦ.

Контроль целостности программного обеспечения средств ЭП и криптографической защиты информации, а также справочно-ключевой информации УЦ осуществляется средствами ЭП и криптографической защиты информации.

Периодичность выполнения мероприятий по контролю целостности – при каждом перезапуске программного обеспечения УЦ, но не реже одного раза в сутки.

Ответственность за выполнение мероприятий по контролю целостности программных средств возлагается на группу администраторов безопасности УЦ.

105. Контролю целостности подлежат средства просмотра, файлы конфигурации и данных журналов (содержимое подкаталогов log каталогов установки программных средств УЦ).

Компоненты подсистемы ведения журналов, не изменяющиеся в процессе работы программного обеспечения, подлежат контролю целостности с использованием устройств типа «электронный замок».

Программная составляющая подсистемы контроля целостности осуществляет проверку контрольных сумм файлов конфигурации и данных журналов при каждом запуске программного обеспечения и при каждом вызове функций просмотра или настроек журнала событий. При обнаружении искажений журналов факт обнаружения фиксируется в служебном журнале, доступ к программному обеспечению возможен только с правами администратора УЦ.

Настройки операционной системы должны предоставлять права на доступ к подкаталогам log в каталогах установки программных компонент УЦ только для пользователей, обеспечивающих эксплуатацию данной компоненты программного обеспечения.

Периодичность выполнения мероприятий по контролю целостности – при каждом перезапуске программного обеспечения УЦ, но не реже чем раз в сутки.

Ответственность за выполнение мероприятий по контролю целостности журналов возлагается на группу администраторов безопасности и аудита УЦ.

106. Контроль целостности технических средств УЦ обеспечивается опечатыванием корпусов устройств, препятствующих их неконтролируемому вскрытию.

Опечатывание устройств выполняется перед вводом технических средств в эксплуатацию и после выполнения регламентных работ.

Контроль целостности технических средств УЦ осуществляется в начале каждой рабочей смены.

Ответственность за выполнение мероприятий по контролю целостности технических средств УЦ возлагается на администратора УЦ.

107. Защита конфиденциальной информации, передаваемой между программно-техническими средствами обеспечения деятельности УЦ и программными средствами, предоставляемыми УЦ пользователям УЦ в процессе обмена документами в электронной форме, осуществляется путем шифрования информации с использованием шифровальных (криптографических) средств, сертифицированных в соответствии с законодательством Российской Федерации.

В качестве шифровальных (криптографических) средств, используемых для защиты конфиденциальной информации пользователями УЦ, используется программа ViPNet «Клиент».

Требуемый уровень безопасности (класс 1В) обеспечивается использованием программного обеспечения ViPNet, сертифицированного Федеральной службой по техническому и экспортному контролю Российской Федерации и Федеральной службой безопасности Российской Федерации.

108. Поступающая в УЦ информация:

запросы на создание сертификата;

запросы на отзыв, приостановление и возобновление сертификатов;

заявления на аннулирование (отзыв), приостановление и возобновление действия сертификата в электронной форме;

списки сертификатов уполномоченного лица других УЦ.

109. Передаваемая из УЦ информация:

бланки копий сертификатов для вывода на бумажный носитель;

списки сертификатов уполномоченного лица;

списки сертификатов пользователей УЦ и их статусы;

список запросов на сертификаты пользователей УЦ и их статус;

список запросов на аннулирование (отзыв), приостановление и возобновление действия сертификатов пользователей УЦ и их статус.

110. Уполномоченное лицо УЦ должно иметь высшее профессиональное образование и профессиональную подготовку в области информационной безопасности.

Сотрудники УЦ должны иметь высшее профессиональное образование или пройти курсы повышения квалификации в области информационной безопасности.

Профессиональная переподготовка персонала УЦ не осуществляется.

111. Доступ сотрудников УЦ к документальному фонду организации организован в соответствии с их должностными инструкциями и функциональными обязанностями.

112. УЦ должен иметь разрешения (лицензии) на все виды деятельности, связанные с предоставлением услуг, указанных в разделе III настоящего Регламента.

Системы безопасности УЦ и защиты информации УЦ создаются и поддерживаются совместно с юридическими лицами, осуществляющими свою деятельность на основании лицензий, полученных в соответствии с законодательством Российской Федерации на договорной основе.

Все меры по защите информации в УЦ должны применяться в соответствии с приказами руководителя УЦ.

Для обеспечения своей деятельности УЦ должен использовать средства ЭП и криптографической защиты информации, сертифицированные в соответствии с законодательством Российской Федерации.

Исключительные имущественные права на информационные ресурсы УЦ находятся в собственности УЦ.

Пользователям УЦ предоставляются неисключительные имущественные права на копии сертификатов и списков отозванных сертификатов, создаваемые УЦ соответствии с настоящим Регламентом.

Приложение № 1
к регламенту работы
удостоверяющего центра
государственного казенного
учреждения «Центр
информационных технологий
Оренбургской области»

## Структуры записей аудита

1. Структура записи аудита программного обеспечения удостоверяющего и ключевого центра

| Поле | Описание |
|---|---|
| Тип события | информация, предупреждение, ошибка |
| Время события (по Гринвичу, UTC) | дата и время, когда произошло событие |
| Источник события | имя источника события |
| Идентификатор события | идентификатор события |
| Сообщение | детализирующая информация |

2. Структура записи события по степени детализации информации

| Уровень детализации | Событие | Поле |
|---|---|---|
| Минимальный | вход администратора | дата, идентификатор, имя |
| | завершение работы | дата, код завершения |
| | зарегистрирован новый администратор | дата, идентификатор, имя |
| | создан мастер-ключ своей сети | дата, тип ключа: основной, персональный ключ, ключ защиты |
| | создан сертификат администратора | дата, серийный номер, имя сертификата владельца, тип объекта: корневой сертификат, запрос PKCS#10 к внешнему удостоверяющему центру |
| Средний | создан сертификат абонента | дата, серийный номер, имя сертификата владельца, основание для создания: запрос центра регистрации, запрос абонента на обновление сертификата, формирование ключевой дискеты абонента |

| Уровень детализации | Событие | Поле |
|---|---|---|
| | принят запрос на сертификат абонента | дата, серийный номер, имя сертификата объекта, основания: запрос центра регистрации, запрос абонента на обновление сертификата |
| | отклонен запрос на создание сертификата | дата, серийный номер, имя сертификата администратора |
| | принят запрос на отзыв сертификата | дата, серийный номер запроса, имя сертификата издателя запроса, серийный номер сертификата, основания для отзыва, приостановления, возобновления |
| | отклонен запрос на отзыв сертификата | дата, серийный номер запроса, имя сертификата издателя запроса, серийный номер сертификата |
| | создан список отозванных сертификатов | дата, серийный номер списка отозванных сертификатов, имя сертификата издателя списка отозванных сертификатов, основание: инициатива администратора, запрос на отзыв |
| Максимальный | создана ключевая дискета абонента | дата, идентификатор, тип генерации: индивидуальная, автоматическая, компрометация, код завершения операции |
| | создан ключевой набор сетевого узла | дата, идентификатор, тип ключевого набора (полный, обновление), тип генерации: индивидуальная, автоматическая, компрометация, код завершения операции |
| | создан межсетевой мастер-ключ | дата, тип ключа, номер сети, серийный номер ключа, код завершения операции |
| | импортирован межсетевой мастер-ключ | дата, тип ключа, номер сети, серийный номер ключа, код завершения операции |
| | импортирован сертификат администратора смежной сети | дата, серийный номер, имя сертификата владельца, код завершения операции |

| Уровень детализации | Событие | Поле |
|---|---|---|
| | импортирован список отозванных сертификатов смежной сети | дата, серийный номер, имя сертификата издателя, код завершения операции |
| | экспортирован ключевой набор | дата, идентификатор, тип набора (ключевая дискета; ключевой набор; дистрибутив, резервный набор персональных ключей, код завершения операции) |

3. Структура записи аудита программы ViPNet «Клиент», «Координатор» (события IP-трафика, проходящего через компьютер)

| Поле | Описание |
|---|---|
| Начало интервала | дата и время создания новой записи при регистрации пакета с определенными характеристиками |
| Конец интервала | дата и время последней регистрации IP-пакета с данной характеристикой |
| IP-адрес | значение IP-адреса, с которого (по которому) произошло обращение |
| Имя адресата | имя адресата, от которого (к которому) произошло обращение |
| Местный порт | номер местного порта |
| Внешний порт | номер внешнего порта |
| Протокол | протокол обмена, по которому происходил обмен IP-пакетами |
| Событие | событие, присвоенное записи |
| Счетчик | количество IP-пакетов с одинаковой характеристикой в заданный интервал времени |
| Атрибуты | исходящий пакет, входящий пакет, зашифрованный пакет, открытый пакет, широковещательный пакет, обычный пакет |

4. Дополнительная информация в структуре записи события

| Поле | Значение |
|---|---|
| Направление | входящий, исходящий |
| Крипто-признак | зашифрованный, открытый |
| Широковещательный признак | широковещательный, обычный |
| Начало интервала | дата и время создания новой записи при регистрации пакета с данной характеристикой |

| Поле | Значение |
|---|---|
| Конец интервала | дата и время последней регистрации IP-пакета с данной характеристикой |
| Местный IP-адрес | значение местного IP-адреса |
| Внешний IP-адрес | значение внешнего IP-адреса |
| Идентификатор местного абонентского пункта | идентификатор местного абонентского пункта |
| Идентификатор внешнего абонентского пункта | идентификатор внешнего абонентского пункта |
| Имя адресата | имя адресата, от которого (к которому) поступило обращение |
| Местный порт | номер местного порта |
| Внешний порт | номер внешнего порта |
| Протокол | протокол обмена, по которому происходил обмен IP-пакетами |
| Ethernet-протокол | Ethernet-протокол |
| Событие | событие, присвоенное записи |
| Счетчик | количество IP-пакетов с данной характеристикой в заданный интервал времени |
| Сетевой адаптер | имя сетевого адаптера, с которого (на который) отправлен (поступил) пакет |
| Номера ключей | номера асимметричных ключей |

5. Регистрация действий пользователей и администратора, произведенных в программе «Монитор»

| Поле | Описание |
|---|---|
| Дата и время | дата и время, когда произошло данное событие |
| Имя пользователя | имя пользователя, производившего действие |
| Событие | название события |
| Режим | номер установленного режима безопасности программы |
| Сетевой интерфейс | IP-адрес сетевого интерфейса, для которого производились регистрируемые действия (только для ViPNet «Координатора») |

6. Регистрация событий, связанных с проявлением сетевой активности приложений, работающих на компьютере

| Поле | Описание |
|---|---|
| Начало интервала | дата и время первой регистрации события данного типа |
| Конец интервала | дата и время последней регистрации события данного типа |
| Исполняемый файл | полный путь к исполняемому приложению |

| Событие | описание произошедшего события |
|---|---|
| Местный адрес | значение местного IP-адреса, от которого произошло обращение |
| Местный порт | номер местного порта, от которого произошло обращение |
| Удаленный адрес | IP-адрес, к которому произошло обращение |
| Удаленный порт | номер внешнего порта, к которому произошло обращение |
| Протокол | название протокола обмена, по которому происходил обмен IP-пакетами |
| Код | номер события |
| Счетчик | количество запросов, производимых приложением |

Приложение № 2
к регламенту работы
удостоверяющего центра
государственного казенного
учреждения «Центр
информационных технологий
Оренбургской области»

В удостоверяющий центр
государственного
казенного учреждения
«Центр информационных
технологий»

Заявление

на создание ключа электронной подписи

_____,
(полное наименование организации согласно ЕГРЮЛ)

в лице_____,
(наименование должности согласно ЕГРЮЛ, фамилия, имя, отчество)

действующего на основании _____, просит создать закрытый и открытый ключ электронной подписи и создать сертификат ключа электронной подписи уполномоченного(ых) представителя(ей) в соответствии с указанными в настоящем заявлении данными, передать в единую систему идентификации и аутентификации сведения о лице(ах), получившем(их) квалифицированный сертификат.

Подпись каждого из заявителей свидетельствует об обязательстве выполнения положений регламента работы удостоверяющего центра ГКУ «ЦИТ» со дня поступления настоящего заявления в ГКУ «ЦИТ».

| № п/п | Фамилия, имя, отчество, пол, дата, место рождения | Наименование должности | Серия, номер документа, удостоверяющего личность, код подразделения, дата выдачи | Наименование подразделения организации | Адрес электронной почты, номер мобильного телефона | ИНН, ОГРН, СНИЛС | Подпись |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1. | | | | | | | |
| 2. | | | | | | | |
| 3. | | | | | | | |

Юридический адрес организации согласно ЕГРЮЛ _____

Наименование должности
руководителя согласно ЕГРЮЛ _____ _____
(подпись) (инициалы, фамилия)

«____» _____ 20___ г. М.П.
(при наличии)

Примечание. Номер мобильного телефона заполняется по желанию заявителя и необходим для его регистрации в единой системе идентификации и аутентификации.

Приложение № 3
к регламенту работы
удостоверяющего центра
государственного казенного
учреждения «Центр
информационных технологий
Оренбургской области»

В удостоверяющий центр
государственного
казенного учреждения
«Центр информационных
технологий»

Заявление

на создание ключа электронной подписи

Я, _____
_____,
(фамилия, имя, отчество)

прошу создать закрытый и открытый ключи электронной подписи, сертификат ключа электронной подписи в соответствии с указанными в настоящем заявлении данными, передать в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат ключа электронной подписи.

Своей подпись свидетельствую об обязательстве выполнения положений регламента работы удостоверяющего центра ГКУ «ЦИТ» со дня поступления настоящего заявления в ГКУ «ЦИТ».

| Фамилия, имя, отчество, пол, дата, место рождения | Серия, номер документа, удостоверяющего личность, код подразделения, дата выдачи | Адрес электронной почты, номер мобильного телефона | ИНН, СНИЛС | Подпись |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |

_____ _____
(подпись) (инициалы, фамилия)

«____» _____ 20___ г.

Приложение № 4
к регламенту работы
удостоверяющего центра
государственного казенного
учреждения «Центр
информационных технологий
Оренбургской области»

В удостоверяющий центр
государственного
казенного учреждения
«Центр информационных
технологий»

Заявление

на аннулирование (отзыв) сертификата ключа электронной подписи

_____,
(полное наименование организации согласно ЕГРЮЛ)

в лице _____,
(наименование должности согласно ЕГРЮЛ, фамилия, имя, отчество)

действующего на основании _____, в связи с

_____
(причина отзыва сертификата (некорректные данные сертификата, увольнение, другое)

просит аннулировать (отозвать) сертификат ключа электронной подписи своего уполномоченного представителя:

| | |
|---|---|
| Серийный номер (32 символа) | |
| Фамилия, имя, отчество | |
| Дата создания сертификата электронной подписи | |
| ИНН | |
| ОГРН | |
| СНИЛС | |

Наименование должности
руководителя согласно ЕГРЮЛ _____ _____
(подпись) (инициалы, фамилия)

«____» _____ 20___ г. М.П.
(при наличии)

Приложение № 5
к регламенту работы
удостоверяющего центра
государственного казенного
учреждения «Центр
информационных технологий
Оренбургской области»

В удостоверяющий центр
государственного
казенного учреждения
«Центр информационных
технологий»

Заявление
на аннулирование (отзыв) сертификата ключа электронной подписи

Я, _____,
(фамилия, имя, отчество)

в связи с _____
(причина отзыва сертификата)

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

| | |
|---|---|
| Серийный номер (32 символа) | |
| Фамилия, имя, отчество | |
| Дата создания сертификата электронной подписи | |
| ИНН | |
| СНИЛС | |

_____ _____
(подпись) (инициалы, фамилия)

«____» _____ 20___ г.

Приложение № 6
к регламенту работы
удостоверяющего центра
государственного казенного
учреждения «Центр
информационных технологий
Оренбургской области»

В удостоверяющий центр
государственного
казенного учреждения
«Центр информационных
технологий»

Заявление
на приостановление действия сертификата ключа электронной подписи

_____,
(полное наименование организации согласно ЕГРЮЛ)

в лице _____,
(наименование должности согласно ЕГРЮЛ, фамилия, имя, отчество)

действующего на основании _____, в связи с _____

_____
(причина приостановки действия сертификата)

просит приостановить действие сертификата ключа электронной подписи своего уполномоченного представителя:

| | |
|---|---|
| Серийный номер (32 символа) | |
| Фамилия, имя, отчество | |
| Дата создания сертификата электронной подписи | |
| ИНН | |
| ОГРН | |
| СНИЛС | |

Срок приостановления действия сертификата _____ дней.
(количество дней прописью или «бессрочно»)

Наименование должности
руководителя согласно ЕГРЮЛ _____ _____
(подпись) (инициалы, фамилия)

«____» _____ 20___ г. М.П.
(при наличии)

Приложение № 7
к регламенту работы
удостоверяющего центра
государственного казенного
учреждения «Центр
информационных технологий
Оренбургской области»

В удостоверяющий центр
государственного
казенного учреждения
«Центр информационных
технологий»

Заявление
на приостановление действия сертификата ключа электронной подписи

Я, _____,
(фамилия, имя, отчество)

в связи с _____
(причина приостановки действия сертификата)

прошу приостановить действие сертификата ключа электронной подписи, содержащий следующие данные:

| | |
|---|---|
| Серийный номер (32 символа) | |
| Фамилия, имя, отчество | |
| Дата создания сертификата электронной подписи | |
| ИНН | |
| СНИЛС | |

Срок приостановления действия сертификата _____ дней.
(количество дней прописью или «бессрочно»)

_____ _____
(подпись) (инициалы, фамилия)

«____» _____ 20___ г.

Приложение № 8
к регламенту работы
удостоверяющего центра
государственного казенного
учреждения «Центр
информационных технологий
Оренбургской области»

В удостоверяющий центр
государственного
казенного учреждения
«Центр информационных
технологий»

Заявление
на возобновление действия сертификата ключа электронной подписи

_____,
(полное наименование организации согласно ЕГРЮЛ)
в лице _____,
(наименование должности согласно ЕГРЮЛ, фамилия, имя, отчество)

действующего на основании _____, просит возобновить действие сертификата ключа электронной подписи своего уполномоченного представителя:

| | |
|---|---|
| Серийный номер (32 символа) | |
| Фамилия, имя, отчество | |
| Дата создания сертификата электронной подписи | |
| ИНН | |
| ОГРН | |
| СНИЛС | |

Наименование должности
руководителя согласно ЕГРЮЛ _____ _____
(подпись) (инициалы, фамилия)

«_____» _____ 20___ г. М.П.
(при наличии)

Приложение № 9
к регламенту работы
удостоверяющего центра
государственного казенного
учреждения «Центр
информационных технологий
Оренбургской области»

В удостоверяющий центр
государственного
казенного учреждения
«Центр информационных
технологий»

Заявление
на возобновление действия сертификата ключа электронной подписи

Я, _____,
прошу возобновить действие сертификата ключа электронной подписи, содержащего следующие данные:

| | |
|---|---|
| Серийный номер (32 символа) | |
| Фамилия, имя, отчество | |
| Дата создания сертификата электронной подписи | |
| ИНН | |
| СНИЛС | |

_____ _____
(подпись) (инициалы, фамилия)

«____» _____ 20___ г.

_____

Приложение № 2
к постановлению
Правительства области
от 24.11.2017 № 833-п

# Порядок
выдачи и отзыва ключей и сертификатов ключей электронной подписи пользователей удостоверяющего центра государственного казенного учреждения «Центр информационных технологий Оренбургской области»

## I. Общие положения

1. Настоящий Порядок определяет механизм выдачи и отзыва сертификатов ключей электронной подписи пользователей удостоверяющего центра государственного казенного учреждения «Центр информационных технологий Оренбургской области», использующих электронную подпись.

### Термины и определения, используемые в настоящем Порядке

Внешний пользователь удостоверяющего центра – лицо, не зарегистрированное в удостоверяющем центре.

Внутренний пользователь удостоверяющего центра – лицо, зарегистрированное в удостоверяющем центре.

Заявитель – лицо, которому необходимо получить услуги удостоверяющего центра.

Ключевой носитель – информационный носитель, на который записаны криптографические ключи.

Ключ электронной подписи – совокупность закрытого и открытого ключей электронной подписи, где закрытый ключ электронной подписи – уникальная последовательность символов, известная владельцу сертификата ключа электронной подписи и предназначенная для создания в электронном документе электронной подписи с использованием средств электронной подписи, а открытый ключ электронной подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной подписи подлинности электронной подписи в электронном документе.

Компрометация ключа – констатация владельцем ключа электронной подписи обстоятельств, при которых возможно несанкционированное использование секретного ключа неуполномоченными лицами.

Конфликтная ситуация – ситуация, при которой у участников электронного документооборота возникает необходимость разрешить вопросы признания или непризнания авторства и/или целостности

электронных документов системы документооборота, обработанных средствами криптографической защиты информации.

Криптографическая защита – защита данных с помощью их криптографического преобразования.

Пользователь удостоверяющего центра – лицо, обратившееся за услугами удостоверяющего центра.

Реестр пользователей удостоверяющего центра – список пользователей удостоверяющего центра или организаций, которым выданы ключи электронной подписи.

Сертификат ключа электронной подписи – электронный документ или документ на бумажном носителе, содержащий открытый ключ электронной подписи субъекта, сведения о владельце открытого ключа электронной подписи, подписанный электронной подписью его издателя.

Удостоверяющий центр – структурное подразделение государственного казенного учреждения «Центр информационных технологий Оренбургской области», выполняющее функции, предусмотренные Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

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

Электронная подпись – реквизит электронного документа, предназначенный для защиты такого документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата ключа электронной подписи, а также установить отсутствие искажения информации в данном документе.

## II. Организация регистрации пользователей удостоверяющего центра

2. Для регистрации пользователей удостоверяющего центра государственного казенного учреждения «Центр информационных технологий Оренбургской области» (далее – УЦ) в реестре пользователей УЦ (далее – реестр) заявитель представляет в УЦ заявление, (приложение № 2 (для юридического лица), приложение № 3 (для физического лица) к регламенту работы удостоверяющего центра государственного казенного учреждения «Центр информационных технологий Оренбургской области»), содержащее информацию о пользователях УЦ (далее – заявление).

3. УЦ в течение 24 часов со времени получения заявления осуществляет его рассмотрение и информирование заявителя о его регистрации в реестре.

4. УЦ имеет право отказать в регистрации заявителю в случаях несоответствия заявления требованиям настоящего Порядка и(или) недостоверности представленной информации, о чем заявителю направляется письменное уведомление в срок не позднее одного рабочего дня со дня приема заявления.

## III. Организация выдачи сертификатов пользователям УЦ

5. УЦ на основании заявления изготавливает ключи электронной подписи (далее – ЭП) и сертификаты ключей ЭП (далее – сертификат) в электронном виде и в форме документа на бумажном носителе в двух экземплярах. Для межведомственного электронного взаимодействия изготавливаются усиленные квалифицированные ключи ЭП. Сертификат оформляется на бланке УЦ, заверяется собственноручной подписью сотрудника УЦ и печатью УЦ. Все экземпляры сертификата собственноручно подписываются владельцем сертификата – пользователем УЦ. Один экземпляр сертификата выдается пользователю УЦ, второй – хранится в УЦ.

6. Получение ключей ЭП и сертификата осуществляется:

пользователем УЦ лично при предъявлении документа, удостоверяющего личность;

уполномоченным лицом пользователя УЦ при предъявлении доверенности на получение ключей и сертификата ЭП, составленной по форме, согласно приложению к настоящему Порядку.

7. Пользователь УЦ или доверенное лицо расписывается в соответствующих журналах выдачи ключей ЭП и сертификатов о получении:

отчуждаемого носителя с ключами ЭП;

сертификата.

8. УЦ в установленный срок производит необходимые работы по изготовлению ключей ЭП и сертификатов.

9. Срок действия ключей ЭП составляет один год. Замена ключей ЭП и сертификата с истекшим сроком действия производится в порядке, определенном настоящим Положением. УЦ имеет право отозвать ключ ЭП в течение действия сертификата, уведомив об этом пользователя УЦ в электронном виде за 24 часа.

10. Предоставление ключей ЭП и сертификатов органам исполнительной власти Оренбургской области, Законодательному Собранию Оренбургской области, органам местного самоуправления муниципальных образований Оренбургской области, а также подведомственным им учреждениям осуществляется на безвозмездной основе, территориальным органам федеральных органов государственной власти, организациям независимо от их организационно-правовых форм и форм собственности – на основании соглашений.

## IV. Отзыв сертификатов

11. В случае исключения пользователя УЦ из реестра пользователей УЦ, УЦ приостанавливает действие его сертификата в течение одного рабочего дня.

После получения заявления на аннулирование (отзыв) сертификата ключа ЭП, УЦ в течение 12 часов помещает сертификат в список аннулированных (отозванных) сертификатов.

12. В случае компрометации ключа ЭП владелец сертификата немедленно извещает УЦ о возникшей ситуации. УЦ после получения такого извещения немедленно приостанавливает действие сертификата. Владелец сертификата в течение одного рабочего дня со дня наступления компрометации ключа ЭП направляет заявление об аннулировании (отзыве) сертификата ключа ЭП в УЦ (приложение № 4 (для юридического лица), приложение № 5 (для физического лица) к регламенту работы удостоверяющего центра государственного казенного учреждения «Центр информационных технологий Оренбургской области»).

13. К событиям, связанным с компрометацией ключей ЭП, относятся:

утрата ключевого носителя;

утрата ключевого носителя с последующим обнаружением;

увольнение сотрудников, имевших доступ к ключевой информации;

возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;

нарушение целостности печатей на сейфах с ключевыми носителями (в случае, если используется процедура опечатывания сейфов);

утрата ключей от сейфов в момент нахождения в них ключевых носителей;

утрата ключей от сейфов в момент нахождения в них ключевых носителей с последующим обнаружением;

доступ посторонних лиц к ключевым носителям.

## V. Права и обязанности организаций, использующих ключи ЭП и пользователей УЦ

14. Организации, сотрудники которых используют ключи ЭП, обязаны провести мероприятия по подготовке к эксплуатации средств криптографической защиты информации в соответствии с законодательством Российской Федерации в сфере криптографической защиты и информационной безопасности.

15. Пользователи УЦ обязаны:

обеспечивать сохранность, неразглашение и нераспространение ключа ЭП во время его использования и хранения;

не использовать для ЭП ключи ЭП в случае, если пользователям УЦ известно, что они скомпрометированы;

немедленно требовать от УЦ отзыва сертификата в случае, если тайна закрытого ключа ЭП подписи нарушена.

16. Пользователи УЦ несут персональную ответственность за безопасность собственных закрытых ключей ЭП.

Приложение
к порядку выдачи и отзыва
сертификатов ключей электронных
подписей пользователей
удостоверяющего центра органов
исполнительной власти
Оренбургской области

Доверенность
на получение ключей и сертификата электронной подписи

г. Оренбург «__»_____ 20__ г.

Я, _____,
(фамилия, имя, отчество)
_____,
(серия, номер документа, удостоверяющего личность, кем и когда выдан)
_____,

доверяю _____,
(фамилия, имя, отчество)
_____,
(серия, номер документа, удостоверяющего личность, кем и когда выдан)
_____,
подать заявление на регистрацию пользователя(ей) удостоверяющего центра и создание сертификата ключа(ей) электронной подписи, получить изготовленные ключи электронной подписи в соответствии с заявлением, расписаться в получении ключа электронной подписи и копии сертификата ключа электронной подписи на бумажном носителе.

Доверенность выдана сроком на 1 (один) месяц без права передоверия.

Подпись уполномоченного
представителя _____ _____
(подпись) (инициалы, фамилия)

подтверждаю _____ _____.
(подпись) (инициалы, фамилия)

Пользователь удостоверяющего
центра _____ _____
(подпись) (инициалы, фамилия)

«___»_____ 20___ г.
М.П. (при наличии)

_____

Приложение № 3
к постановлению
Правительства области
от 24.11.2017 № 833-п

# Инструкция
# по защите информации при осуществлении электронного документооборота в органах исполнительной власти, органах местного самоуправления муниципальных образований Оренбургской области и в подведомственных им учреждениях

## I. Общие положения

1. Настоящая Инструкция определяет организационно-технические мероприятия по защите информации в системе электронного документооборота в органах исполнительной власти, органах местного самоуправления муниципальных образований Оренбургской области и в подведомственных им учреждениях (далее – организации).

2. Организационно-технические мероприятия по защите информации при осуществлении обмена электронными документами, заверенными электронной подписью, эксплуатации средств защиты информации, в том числе средств электронной подписи, а также при обращении с ключевой информацией, используемой для криптографической защиты электронных документов выполняются должностным лицом участника электронного документооборота, ответственным за информационную безопасность.

3. Организационно-технические мероприятия по защите информации при обмене электронными документами позволяют обеспечить:

конфиденциальность электронных документов;

подлинность электронных документов – подтверждение авторства и целостности электронных документов;

разграничение и контроль доступа к средствам обмена электронными документами;

сохранность в тайне содержания закрытых ключей электронной подписи;

ведение журнала учета ключевых документов и средств криптографической защиты информации в соответствии с приказом Федерального агентства правительственной связи от 13 июня 2001 года № 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».

4. Настоящая Инструкция обязательна для исполнения всеми лицами, осуществляющими подготовку, обработку, отправку/получение, хранение и учет электронных документов, заверенных электронной подписью.

## II. Управление ключевой системой обмена электронными документами

5. Ключевая система обмена электронными документами представляет собой ключи электронной подписи пользователей удостоверяющего центра государственного казенного учреждения «Центр информационных технологий Оренбургской области» (далее – УЦ).

Для каждого типа ключей электронной подписи формируются рабочий и резервный комплекты.

6. Пользователи ключей электронной подписи обеспечивают хранение, передачу, использование, уничтожение, учет ключевой информации и ее носителей в соответствии с требованиями технической и эксплуатационной документации на используемые средства криптографической защиты информации. Пользователи УЦ обязаны неукоснительно соблюдать и выполнять требования следующих документов:

регламент работы УЦ;

порядок выдачи и отзыва ключей и сертификатов ключей электронной подписи пользователей УЦ;

регламент по организации электронного документооборота в органах исполнительной власти Оренбургской области, утвержденный постановлением Правительства Оренбургской области от 3 марта 2013 года № 174-п;

настоящая Инструкция;

техническая и эксплуатационная документация на средства криптографической защиты информации.

## III. Компрометация ключевой информации

7. При подозрении на компрометацию рабочего комплекта закрытого ключа электронной подписи пользователь УЦ немедленно прекращает использование соответствующего закрытого ключа электронной подписи и незамедлительно сообщает об этом в УЦ или специалисту по технической защите информации организации.

8. В зависимости от обстоятельств компрометации рабочего комплекта закрытого ключа электронной подписи руководителем организации может быть назначено служебное расследование с участием в нем представителей УЦ и специалиста по технической защите информации организации.

## IV. Защита информации при обработке электронных документов

9. Формирование, подготовка, обработка, хранение электронных документов, заверение электронных документов электронной подписью, проверка подлинности электронной подписи электронных документов должны производиться на специально подготовленных рабочих местах пользователей УЦ, оборудованных необходимыми программно-техническими средствами, в том числе средствами электронной подписи, при необходимости и средствами защиты информации.

10. Для выполнения функций, указанных в пункте 9 настоящей Инструкции, в организации могут назначаться операторы, обеспечивающие непосредственную эксплуатацию средств обмена электронными документами.

11. Доступ к указанным рабочим местам должен ограничиваться пользователями или операторами электронной подписи и ответственным за техническую защиту информации. Для обеспечения защиты от несанкционированного доступа посторонних лиц необходимо принимать организационные или организационно-технические меры.

12. Контроль за соблюдением требований по защите информации возлагается на специалиста по технической защите информации организации.