УЦ ГАЗИНФОРМ СЕРВИС

# РЕГЛАМЕНТ

использования средств криптографической защиты информации в автоматизированных информационных системах

**Утвержден приказом №3 от 03 февраля 2016 г.**

***СОДЕРЖАНИЕ***

# 1 Введение

1.1 Настоящий Регламент разработан на основании действующего законодательства Российской Федерации и определяет:

- порядок эксплуатации средств криптографической защиты информации;
- порядок организации криптографической защиты информации при обмене электронными документами в автоматизированной информационной системе обмена информацией по телекоммуникационным каналам связи в виде юридически значимых электронных документов с использованием электронной цифровой подписи (далее – Система);
- порядок организации защиты информации при обмене электронными документами с использованием электронной подписи (ЭП).
- Порядок регистрации и подключения пользователей к Системе;
- Порядок действий при возникновении внештатных ситуаций, связанных с применением средств криптографической защиты информации (далее СКЗИ)

1.2 ООО «УЦ ГИС» имеет в соответствии с законодательством Российской Федерации лицензии, дающие право оказывать услуги по изготовлению и выдаче сертификатов ключей проверки электронных подписей и распространению средств криптографической защиты информации, осуществляет свою деятельность на территории Российской Федерации и выполняет функции Удостоверяющего Центра.

1.3 Пользователи используют для защиты информации сертифицированные, в порядке, установленном законодательством Российской Федерации, средства электронной подписи (далее – средства ЭП), позволяющие идентифицировать владельца сертификата ключа проверки электронной подписи, а также установить отсутствие искажения информации, в электронном виде.

1.4 Пользователи используют для защиты информации, при передаче ее по открытым каналам связи сертифицированные, в порядке, установленном законодательством Российской Федерации, средства криптографической защиты информации (далее – СКЗИ).

1.5 Используемые во взаимоотношениях между Пользователями электронные документы, подписанные ЭП, являются оригиналами, имеют юридическую силу, подлежат хранению в хранилище юридически значимых документов и могут использоваться в качестве доказательств в суде, а также при рассмотрении споров в досудебном порядке.

1.6 Пользователь признает, что использование сертифицированных СКЗИ, которые реализуют функции по формированию и проверке ЭП и шифрование, достаточно для обеспечения конфиденциальности информационного взаимодействия Пользователей, а также подтверждения того, что электронный документ:

- исходит от Пользователя (подтверждение авторства документа);
- не претерпел изменений при информационном взаимодействии Пользователя (подтверждение целостности и подлинности документа).

1.7 При обмене электронными документами Пользователи должны руководствоваться положениями настоящего Регламента и Регламентом Удостоверяющего центра ООО «УЦ ГИС».

# 2 Термины и сокращения, используемые в регламенте

***Аутентификация информации*** - подтверждение подлинности и целостности информации, содержащейся в документе. Аутентификация может осуществляться как на основе структуры и содержания документа или его реквизитов, так и путем реализации криптографических алгоритмов преобразования информации. Доказательная аутентификация информации осуществляется анализом (экспертизой) подписей должностных лиц и печатей на бумажных документах или проверкой корректности ЭП.

***Автоматизированное рабочее место (АРМ) Пользователя УЦ*** – web-приложение, предназначенное для регистрации и управления сертификатами ключей проверки ЭП

Пользователя УЦ.

***Владелец сертификата ключа проверки ЭП*** - лицо, которому в установленном Федеральным законом «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

***Договор*** – договор, заключенный между пользователем Системы и Удостоверяющим центром. Договор определяет состав, порядок исполнения и стоимость услуг, оказываемых пользователю Системы

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

***Пользователь*** –физическое лицо (физическое лицо, действующее от имени юридического лица), прошедшее регистрацию в Удостоверяющем Центре, участник информационного обмена электронными документами и признающий данный Регламент.

***Ключевой носитель*** – отчуждаемый носитель (дискета, eToken, и т.п.), содержащий один или несколько ключей ЭП.

***Компрометация ключа ЭП*** - утрата доверия к тому, что используемый ключ ЭП недоступен посторонним лицам. К событиям, связанным с компрометацией ключей ЭП, относятся, включая, но, не ограничиваясь, следующие:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевым носителям;
- возникновение подозрений на утечку информации или ее искажение в Системе;
- нарушение целостности печатей на сейфах с ключевыми носителями, если используется процедура опечатывания;
- утрата ключей от сейфов (помещений) в момент нахождения в них ключевых носителей;
- утрата ключей от сейфов (помещений) в момент нахождения в них ключевых носителей с последующим обнаружением;
- доступ посторонних лиц к ключу ЭП;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе, когда ключевой носитель вышел из строя и не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

***Конфиденциальная информация*** - информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ, а также настоящим Регламентом и требующая защиты.

***Конфликтная ситуация*** - ситуация, при которой у Пользователя возникает необходимость разрешить вопросы признания или непризнания авторства и/или подлинности электронных документов, обработанных средствами криптографической защиты информации.

***Ключ (криптографический ключ)*** – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразования.

***Некорректный электронный документ*** - электронный документ, не прошедший процедуры проверки ЭП или имеющий искажения в тексте сообщения, не позволяющие понять его смысл.

***Несанкционированный доступ (НСД) к информации*** - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

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

***Ответственное лицо за обеспечение безопасности использования СКЗИ*** - назначенный решением руководителя организации специалист подразделения информатизации, ответственный за обеспечение условий безопасного использования электронной подписи с

использованием СКЗИ.

***Подтверждение подлинности электронной подписи в электронном документе*** - положительный результат проверки соответствующим сертифицированным средством ЭП принадлежности электронной подписи в электронном документе владельцу сертификата ключа проверки ЭП с использованием сертификата ключа проверки ЭП и отсутствия искажений в подписанном данной электронной подписью электронном документе.

***Сертификат ключа проверки электронной подписи*** - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

***СОС (Список отозванных сертификатов, Certificate Revocation List, CRL)*** – список отозванных сертификатов.

***Средства криптографической защиты информации*** **–** программные или аппаратные средства вычислительной техники, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности.

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

***Удостоверяющий центр (УЦ)*** – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом № 63-ФЗ «Об электронной подписи».

***Уполномоченное лицо Удостоверяющего центра*** – физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов ключей проверки ЭП и списков отозванных сертификатов.

***Управление ключами*** - создание (генерация) ключей, их хранение, распространение, удаление (уничтожение), учет и применение, а также выдача и отзыв сертификатов ключей проверки ЭП в соответствии с политикой безопасности Удостоверяющего центра.

***Целостность информации*** – способность автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

***Электронный документ*** – документ, в котором информация представлена в электронно-цифровой форме.

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

## 3 Общие положения

3.1 Пользователи УЦ соблюдают установленную настоящим Регламентом последовательность действий при обмене электронными документами и проверке их подлинности.

3.2 УЦ осуществляет работы по управлению ключами ЭП и сертификатами ключей проверки ЭП в соответствии с положениями настоящего Регламента и Регламента работы УЦ, на основании Заявления Пользователя.

3.3 В случае нарушения правил использования СКЗИ и/или возникновения конфликтных ситуаций, связанных с подтверждением авторства и/или подлинности электронных документов, подписанных ЭП, или иных конфликтных ситуаций, связанных с использованием ЭП, Стороны руководствуются Порядком разрешения конфликтных ситуаций, изложенным в Регламенте оказания услуг УЦ.

## 4 Общие вопросы организации защиты информации

4.1 Пользователь предоставляет УЦ право изготовить ключи ЭП и ключи проверки ЭП Пользователя на Автоматизированном рабочем месте оператора УЦ (АРМ УЦ). АРМ УЦ расположен на территории УЦ.

4.2 УЦ предоставляет Пользователю возможность самостоятельной выработки ключей ЭП и проверки ЭП в присутствии оператора УЦ и под его непосредственным контролем с использованием программно-аппаратных средств УЦ.

4.3 УЦ изготавливает сертификаты ключей проверки ЭП Пользователя в электронном виде и вместе с ключевым носителем передает их ему. При изготовлении сертификатов ключей проверки ЭП УЦ оформляет два экземпляра сертификата в форме документов на бумажных носителях, которые заверяются собственноручными подписями владельца сертификата ключа проверки ЭП и сотрудника УЦ, а также печатью УЦ. Один экземпляр сертификата ключа на бумажном носителе выдается владельцу сертификата ключа проверки ЭП, второй – остается в УЦ. УЦ использует программные и технические средства генерации ключевой информации в неизменном виде по отношению к сертифицированному эталону. УЦ гарантирует отсутствие привнесенных нерегламентированных процедур скрытого копирования индивидуальной ключевой информации в используемых программных и технических средствах.

4.4 Пользователь получает доступ к реестру выданных сертификатов УЦ и списку отозванных сертификатов (реестр сертификатов и СОС публикуется на сайте УЦ в Интернете по адресу http://ca.gisca.ru/).

4.5 Срок действия ключей ЭП Пользователя УЦ, составляет 1 (Один) год. Начало периода действия ключей ЭП Пользователя УЦ исчисляется с даты и времени начала действия соответствующих им сертификатов ключей проверки ЭП.

## 5 Правила использования средств ЭП

5.1 Работы по первоначальной установке (инсталляции) и настройке СКЗИ на рабочем месте Пользователя должны выполняться представителями организации, имеющей лицензию ФСБ России на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств с указанием данного вида работ.

5.2 На технических средствах, предназначенных для работы со средствами ЭП должно использоваться только лицензионное программное обеспечение.

5.3 На ЭВМ с установленными средствами ЭП должны отсутствовать средства разработки ПО и отладчики.

5.4 Средства ЭП должны использоваться со средствами антивирусной защиты, сертифицированными ФСБ России.

5.5 Использование средств ЭП для обработки информации, содержащей сведения, составляющие государственную тайну **НЕ ДОПУСКАЕТСЯ!**

5.6 Средства ЭП должны использоваться в соответствии с эксплуатационной документацией на данные средства.

## 6 Функции и задачи УЦ

5.1 УЦ предоставляет услуги, а именно:

- создает криптографические ключи по обращению Пользователя, с гарантией сохранения в тайне ключей ЭП. Ключ ЭП передается владельцу сертификата ключа проверки ЭП на ключевом носителе;
- изготавливает сертификаты ключей проверки ЭП на основании надлежащим образом оформленного Заявления и всех необходимых документов, согласно Регламенту оказания услуг УЦ;
- выдает сертификаты ключей проверки ЭП в форме документа на бумажном носителе и в электронном виде;
- обеспечивает уникальность ключей проверки ЭП в реестре сертификатов ключей проверки ЭП и архиве УЦ;
- вносит сертификаты ключей проверки ЭП в реестр сертификатов ключей проверки ЭП не позднее даты начала их действия;
- предоставляет Пользователю доступ к реестру сертификатов ключей проверки ЭП и списку отозванных сертификатов;
- обеспечивает выпуск и обновление списка отозванных сертификатов с включением в него всех сертификатов скомпрометированных ключей ЭП, с указанием даты и времени аннулирования сертификата ключа проверки ЭП.

5.2 УЦ уведомляет Пользователей о фактах, которые стали ему известны и которые существенным образом могут сказаться на возможности дальнейшего использования СКЗИ и сертификата ключа проверки ЭП.

5.3 УЦ обязан аннулировать сертификат ключа проверки ЭП:

- по заявлению в письменной форме владельца сертификата ключа проверки ЭП;
- если УЦ стало достоверно известно о прекращении действия документа, на основании которого оформлен сертификат ключа проверки ЭП.

5.4 УЦ обеспечивает хранение сертификата ключа проверки ЭП Пользователя в форме электронного документа после аннулирования сертификата ключа проверки ЭП не менее трех лет. По истечении указанного срока хранения, сертификат ключа подписи исключается из реестра сертификатов ключей проверки ЭП и переводится в режим архивного хранения. Сертификат ключа проверки ЭП в форме документа на бумажном носителе хранится в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

5.5 УЦ участвует в работе Экспертной комиссии при рассмотрении спорных вопросов (конфликтных ситуаций).

## 7 Права и обязанности Пользователя

6.1 Пользователь обязан предоставить достоверную регистрационную и идентифицирующую его информацию в объеме, определенном положениями настоящего Регламента и Регламента оказания услуг УЦ.

6.2 Пользователь, в соответствии с лицензионным соглашением и эксплуатационной документацией на СКЗИ, подготавливает и содержит в рабочем состоянии компьютер и программное обеспечение, предназначенные для работы в автоматизированных информационных системах.

6.3 Пользователь обязан организовать режим функционирования рабочих мест таким образом, чтобы исключить возможность доступа к СКЗИ, несанкционированной модификации или использования СКЗИ лицами, не имеющими допуска к работе с СКЗИ, а также исключить возможность использования криптографических ключей не уполномоченными на то лицами.

6.4 Пользователь обязан при обработке электронных документов осуществлять их архивирование и хранить эти архивы в течение срока, установленного соответствующими законами и нормативными актами, для хранения бумажных документов.

6.5 Пользователь обязан при разрешении конфликтных ситуаций, связанных с установлением подлинности и/или авторства спорного документа или иных конфликтных ситуаций, связанных с использованием ЭП, предоставлять Экспертной комиссии, создаваемой и действующей в соответствии с Регламентом оказания услуг УЦ, все документы и материалы, относящиеся к предмету конфликтной ситуации.

6.6 Замена криптографических ключей производится по инициативе Пользователя на возмездной основе, но не реже одного раза в год (отдельным решением могут быть установлены другие сроки) в следующем порядке:

- Пользователь направляет УЦ заявление на замену ключей (рекомендуется за месяц до истечения срока действия сертификата старого ключа проверки ЭП);
- УЦ согласовывает с Пользователем время проведения работ;
- Пользователь оплачивает работы по изготовлению и выдаче новых сертификатов ключей проверки ЭП;
- Работы по изготовлению новых ключей ЭП и выдаче сертификатов ключей проверки ЭП производит УЦ в соответствии с разделом 6 настоящего Регламента;
- Пользователь после получения новых ключей ЭП и сертификатов ключей проверки ЭП проверяет их работоспособность;
- Пользователь принимает решение о сроках и порядке архивного хранения или об уничтожении старых ключей, так как все риски, связанные с несанкционированным использованием старых ключей, ложатся на Пользователя;
- Факт уничтожения или возвращение старого ключа ЭП оформляется документом, который заверяется подписями владельца старого ключа ЭП, руководителя организации и печатью организации. 2-й экземпляр данного документа передается УЦ;
- В случае уничтожения старых ключей ЭП – перед уничтожением необходимо расшифровать все электронные документы, зашифрованные с их использованием, иначе в дальнейшем прочитать эти документы будет невозможно!
- Пользователь обеспечивает хранение расшифрованных документов в электронном виде в соответствии с требованиями, установленными законодательством и настоящим Регламентом;

6.7 Пользователь имеет право:

- не принимать к исполнению электронные документы, заверенные ЭП, если:
  - сертификат ключа проверки ЭП отправителя утратил силу (не действует, находится в СОС) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
  - не подтверждена подлинность ЭП в электронном документе;
  - ЭП используется не в соответствии со сведениями, указанными в сертификате ключа проверки ЭП.
- запрашивать подтверждение по полученным им электронным документам в случае возникновения сомнений;
- требовать от УЦ аннулирования своего сертификата ключа проверки ЭП в случае наступления событий, трактуемых как компрометация ключевой информации;
- в случае возникновения конфликтной ситуации, связанной с установлением подлинности и/или авторства спорного документа, требовать разрешения указанных вопросов Экспертной комиссией в соответствии с согласованным порядком.

## 8 Действия Сторон при компрометации ключей

7.1 УЦ в момент генерации ключей и выпуска сертификата ключа проверки ЭП передает Пользователю пароль для экстренной связи в случае компрометации ключей ЭП. Пользователь обеспечивает сохранение конфиденциальности пароля.

7.2 Пользователь в случае принятия решения о компрометации собственных ключей ЭП, обязан немедленно информировать УЦ по телефонным каналам связи с использованием устного пароля о наступлении события, трактуемого как компрометация.

7.3 При компрометации ключа ЭП, Пользователь должен прекратить обмен электронными документами с другими Пользователями.

7.4 УЦ, получивший сообщение о компрометации ключей ЭП Пользователя, должен убедиться в достоверности сообщения о компрометации (запросить пароль или факсимильное сообщение, заверенное подписью и печатью Пользователя) и после этого обязан немедленно аннулировать скомпрометированные ключи (занести соответствующие сертификаты в СОС).

7.5 Пользователь, объявивший о компрометации собственных ключей ЭП, в течение одного рабочего дня документально оформляет уведомление и направляет его в УЦ.

7.6 Пользователь, допустивший компрометацию собственных ключей ЭП, несет все издержки, связанные с генерацией новых ключей ЭП, выпуском сертификата ключа проверки ЭП и вводом в действие.

## 9 Конфиденциальность информации

8.1 УЦ и Пользователи в процессе взаимодействия обязаны обеспечить сохранность конфиденциальной информации, полученной друг от друга, в соответствии с действующим законодательством Российской Федерации.

8.2 УЦ обязан не разглашать (публиковать) информацию, полученную от Пользователей, за исключением регистрационной информации, включенной в изготовленные сертификаты Пользователей.

8.3 Порядок предоставления конфиденциальной информации правоохранительным, судебным органам и органам государственной власти осуществляется в соответствии с действующим законодательством Российской Федерации.

## 10 Ответственность участников взаимодействия

9.1. Пользователь несет ответственность за достоверность сведений, указанных им в Заявлении, а также при внесении изменений в указанные сведения.

9.2. Пользователь несет ответственность за сохранность и правильность эксплуатации СКЗИ и своих ключей ЭП.

9.3. В случае несвоевременного сообщения о факте компрометации ключей ЭП Пользователь, допустивший компрометацию ключей, несет ответственность в полном объеме за ущерб, причиненный им другим Пользователям автоматизированных информационных систем.

9.4. УЦ не несет ответственности в случае нарушения Пользователями положений настоящего Регламента.

9.5. УЦ не несёт ответственности перед владельцами сертификатов ключей проверки ЭП и лицами, использующими сертификаты ключей проверки ЭП для проверки подписи и шифрования сообщений, а также перед третьими лицами за любые убытки, потери, иной ущерб, связанный с использованием сертификатов ключей проверки ЭП, независимо от суммы, заключенных с использованием сертификатов ключей проверки ЭП сделок и совершения ими иных действий, за исключением случаев нарушения УЦ обязательств, предусмотренных Регламентом и/или действующим законодательством Российской Федерации.

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

9.7. За неисполнение или ненадлежащее исполнение обязательств по настоящему Регламенту участники взаимодействия несут ответственность в соответствии с договором и действующим законодательством Российской Федерации.

9.8. Пользователь несет ответственность за сохранность СКЗИ, своих ключей ЭП.

## 10. Порядок взаимодействия Сторон при нештатных ситуациях, связанных с эксплуатацией СКЗИ

10.1. При возникновении нештатных ситуаций, таких как выход из строя ключевого носителя, сбои и отказы в работе СКЗИ, сбои и отказы в работе средств электронной подписи и др. Пользователь обязан:

- руководствоваться эксплуатационной документацией на используемые средства ЭП;
- сообщить о возникшей ситуации в УЦ;
- выполнить указания УЦ, касающиеся выхода из данной внештатной ситуации.

## 11. Прочие условия

11.1. Изменения и дополнения в настоящий Регламент вносятся УЦ с обязательным уведомлением всех Пользователей.

11.2. Все приложения, изменения и дополнения являются неотъемлемой частью настоящего Регламента.