

УТВЕРЖДАЮ
Генеральный директор
АО «Реестр»

_____ Ю.Э. Тарановский

«16» июня 2023 г.

РЕГЛАМЕНТ
электронного взаимодействия

(Приложение № 5 к Правилам ведения реестров владельцев ценных бумаг)

Оглавление

1. Термины и определения	3
2. Общие положения	7
3. Порядок доступа к Информационным сервисам	9
4. Обработка персональных данных Оператором ИС	10
5. Электронные подписи	10
6. Признание Электронного документа подлинником (оригиналом), копия Электронного документа	11
7. Порядок проверки электронной подписи, установление подлинности Электронного документа	11
8. Обязанности, ответственность и гарантии Оператора ИС	12
9. Обязанности, ответственность и гарантии Пользователя	13
10. Система обеспечения информационной безопасности	15
11. Порядок действий при Компрометации	15
12. Электронный архив	15
13. Обстоятельства непреодолимой силы	15
14. Ограничение ответственности	16
15. Разрешение спорных ситуаций	17
16. Техническая поддержка Пользователей	17

1. Термины и определения

В настоящем Регламенте используются следующие термины и определения:

Абонентский номер – телефонный номер подвижной радиотелефонной связи, выделяемый физическому или юридическому лицу, заключившему с оператором связи соответствующий договор об оказании услуг.

Авторизация – санкционирование доступа Пользователя Информационных сервисов к их функциям и данным в объеме имеющихся у Пользователя прав и полномочий после успешного прохождения Аутентификации.

Аутентификационные данные (Регистрационные данные) - совокупность Логинов, Паролей, Ключей, УКЭП и иных известных только пользователю идентификаторов, необходимых для входа в Информационный сервис.

Аутентификация – процедура проверки подлинности Пользователя, осуществляемая с использованием Аутентификационных данных, осуществляемая при входе Пользователя в Информационный сервис.

Владелец сертификата ключа проверки электронной подписи – Пользователь Информационного сервиса, которому в установленном настоящим Регламентом порядке выдан сертификат ключа проверки электронной подписи.

Доставка электронного сообщения/ документа – процесс перемещения электронного сообщения или документа от отправителя к получателю.

Единый профиль Пользователя (Единый профиль) – совокупность Аутентификационных и персональных данных Пользователя, используемая для входа в любой Информационный сервис.

ЕСИА, Единая система идентификации и аутентификации — государственная информационная система Российской Федерации, обеспечивающая санкционированный доступ участников информационного взаимодействия (граждан-заявителей и должностных лиц органов исполнительной власти) к информации, содержащейся в государственных информационных сервисах и иных информационных сервисах (подробности по ссылке <https://esia.gosuslugi.ru>).

Заявитель - лицо, желающее стать Пользователем.

Заявление – волеизъявление Заявителя о подключении или внесении изменений в параметры подключения к Информационному сервису, совершенное в установленной Оператором ИС форме и/или с использованием функциональных возможностей соответствующего Информационного сервиса.

Идентификация – определение Пользователя Информационного сервиса по присвоенному ему персональному идентификатору, который присваивается Пользователю при его регистрации в соответствующем Информационном сервисе.

Информационный сервис (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, владельцем которых является АО «Реестр», в том числе упоминаемые совместно или по отдельности Личный кабинет Эмитента (ЛКЭ), Личный кабинет клиента «Реестр-Онлайн» (ЛКК), Инвестиционная платформа АО «Реестр» (ИнвестПлатформа), Сервис дистанционного принятия решения единственным акционером (Сервис РЕА) и другие.

Ключ электронной подписи – уникальная последовательность символов, известная только Владелцу сертификата ключа и предназначенная для создания усиленной электронной подписи.

Ключ проверки электронной подписи - уникальная последовательность символов,

однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Код подтверждения – одноразовый цифровой или цифробуквенный код, формируемый с помощью программного обеспечения на оборудовании Пользователя или присылаемый на номер телефона и/или Контактный e-mail Пользователя в целях дополнительного подтверждения действий Пользователя в соответствующем Информационном сервисе.

Компрометация Аутентификационных данных (Компрометация) - констатация Пользователем Информационного сервиса обстоятельств, при которых возможно несанкционированное использование неуполномоченными лицами Аутентификационных данных, предоставляющих доступ и/или использование ИС.

Конфиденциальная информация – документированная информация, имеющая действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, при отсутствии к ней свободного доступа на законном основании и/или если обладатель информации принимает меры к ее охране.

Конфликтная ситуация - ситуация, при которой у Сторон возникает необходимость разрешить вопросы признания или непризнания авторства и/или целостности электронного запроса и/или сообщения, подписанных электронной подписью.

Контактный e-mail – адрес электронной почты Пользователя, указанный в Заявлении о подключении к электронному сервису ЛКК, ЛКЭ.

Криптографическая защита - защита данных при помощи их криптографического преобразования.

Криптографический ключ (Ключ) - общее название ключа усиленной электронной подписи и ключа проверки электронной подписи.

Личный кабинет - общее название Информационных сервисов, обеспечивающих единый интерфейс для взаимодействия между Пользователем и Информационным сервисом, доступный в виде веб-интерфейса, размещенного на Сайте или в виде приложения для мобильных устройств.

Логин – часть Аутентификационных данных, предоставляющих доступ к ИС; уникальная последовательность символов, позволяющая однозначно идентифицировать Пользователя Информационного сервиса. В Едином Профиле Пользователя Логин является номер мобильного телефона, указанный при Регистрации Пользователя.

Обработка информации – создание, хранение, прием, передача, преобразование и отображение информации.

Оператор Информационного сервиса (Оператор ИС) – Акционерное общество «Реестр» (АО «Реестр»).

Отправитель – лицо, которое направляет Электронное сообщение и/или Электронный документ посредством функциональных возможностей Информационных сервисов.

Пароль – часть регистрационных данных, предоставляющих доступ; известная только Пользователю Информационного сервиса последовательность символов, связанная с Логин, используемая для аутентификации и авторизации Пользователя.

Получатель – лицо, которому адресовано Электронное сообщение и/или Электронный документ, отправленные Отправителем или от имени и по поручению Отправителя.

Пользователь (Пользователи) – физическое лицо, прошедшее процедуру Регистрации пользователя и авторизовавшееся в Информационном сервисе, включая, но не ограничиваясь владельцы ценных бумаг; лица, осуществляющие права по ценным бумагам; лица, которым принадлежат все голосующие акции Эмитента (далее – Единственный акционер); Эмитенты;

Инвесторы; Уполномоченные представители.

Правила использования ИС – документ Оператора ИС, опубликованный на официальном сайте и доступный в соответствующей ИС, описывающий порядок и особенности работы в соответствующей ИС.

Простая электронная подпись (ПЭП) - электронная подпись, которая посредством использования логинов, паролей и/или иных средств подтверждает факт формирования электронной подписи Пользователем.

Расшифровка - процесс криптографического преобразования зашифрованных данных в расшифрованные.

Реестр ID (Reestr ID) – уникальный идентификатор Единого профиля Пользователя Личного кабинета.

Реестр Пользователей – список записей о Пользователях (в том числе о Единых профилях), ведение которого осуществляется в целях учета и предоставления Пользователям доступа к Информационным сервисам, в том числе формируемый для внесения сведений о Пользователях в порядке, предусмотренном Федеральным законом от 31.07.2020 №259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

Роль Пользователя – совокупность разрешений и ограничений по использованию функциональных возможностей Информационного сервиса в соответствии с полномочиями, предоставленными Пользователю, сведения о которых содержатся в Учетной системе.

Регистрация Пользователя, Регистрация – процедура создания Единого профиля Пользователя, в том числе создание записи о Пользователе Информационного сервиса.

Регламент – настоящий Регламент электронного взаимодействия, определяющий порядок и условия электронного взаимодействия Оператора ИС с Пользователями посредством Информационных сервисов.

Сайт - официальный сайт АО «Реестр» в информационно – телекоммуникационной сети Интернет <https://www.aoreestr.ru>.

Сервис идентификации – сторонний сервис идентификации и/или аутентификации Пользователя, оператором которого не является АО «Реестр», предоставляющий с согласия Пользователя Оператору ИС информацию о персональных данных Пользователя.

Секретный ключ шифрования – уникальная последовательность данных, используемая для формирования электронной подписи и расшифровки электронного документа (см. также Ключ электронной подписи).

Сертификат ключа проверки электронной подписи (Сертификат ключа) – электронный документ и/или документ на бумажном носителе, выданные УНЭП или УКЭП Удостоверяющим центром или Администратором безопасности Оператора ИС, и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа.

Системный журнал – электронный журнал Информационного сервиса, автоматически формируемый соответствующим Информационным сервисом Оператора ИС, в котором содержится информация о действиях и лицах, выполнивших эти действия (Пользователях) в Информационном сервисе.

СКЗИ, Средства криптографической защиты информации - совокупность программно-технических средств, обеспечивающих применение шифрования при взаимодействии в рамках СЭД.

Средства усиленной 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.

Стороны электронного обмена информацией и документами (Стороны) – упоминаемые совместно Отправитель и Получатель.

Уполномоченный представитель – физическое лицо, выполняющее функции единоличного исполнительного органа юридического лица, в том числе его управляющей организации, и/или физическое лицо, действующее от имени юридического лица или иного физического лица на основании доверенности или иного документа, подтверждающего полномочия на совершение определенных действий.

Усиленная квалифицированная электронная подпись (УКЭП) – электронная подпись, которая удовлетворяет всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом 63-ФЗ от 06.04.2011 «Об электронной подписи».

Усиленная неквалифицированная электронная подпись (УНЭП) – электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

Учетная система – программное обеспечение и базы данных Оператора ИС, не предназначенное для распространения среди Пользователей, не являющихся сотрудниками Оператора ИС.

Шифрование - процесс криптографического преобразования данных, позволяющий предотвратить доступ неуполномоченных лиц к зашифрованному содержимому электронного документа.

Электронное сообщение – сообщение (информация) в электронном виде, отправляемое и получаемое Сторонами посредством функциональных возможностей Информационных сервисов, в целях взаимодействия при оказании коротких консультаций, использования «чата», направления информационных сообщений и т.д., исключая обмен Электронными документами, для которых предусмотрены специальные разделы соответствующих Информационных сервисов.

Электронный документ – документ, информация которого представлена в электронной форме (файл, запись в базе данных) и подписана электронной подписью, предусмотренной настоящим Регламентом, Правилами использования ИС и функциональными возможностями соответствующего Информационного сервиса, равнозначный документу на бумажном носителе, подписанному собственноручной подписью.

Эмитент (Эмитенты) – юридическое лицо, держателем реестра владельцев ценных бумаг которого является Акционерное общество «Реестр» (Регистратор) и/или которому Акционерное общество «Реестр» оказывает услуги по привлечению инвестиций (Оператор инвестиционной платформы).

Одинаковые по наименованию термины, определенные в настоящем Регламенте и используемые в законодательстве РФ, понимаются в значении, указанном в настоящем Регламенте.

Термины и определения, используемые в Регламенте и не перечисленные в настоящем разделе, понимаются в значении, определенном действующим законодательством Российской Федерации, Правилами ведения реестров владельцев ценных бумаг АО «Реестр», Правилами инвестиционной платформы АО «Реестр».

2. Общие положения

- 2.1.** Настоящий Регламент определяет порядок и условия электронного взаимодействия Оператора ИС с Заявителями и Пользователями посредством Информационных сервисов.
- 2.2.** Регламент является приложением к Правилам ведения реестров владельцев ценных бумаг, размещенным на сайте Регистратора <http://www.aoreestr.ru>, и их неотъемлемой частью.
- 2.3.** Оператор ИС вправе вносить изменения и дополнения в Регламент в одностороннем порядке. Изменения и дополнения, внесенные в настоящий Регламент, не имеют обратной силы.
- 2.4.** Авторизация Пользователя в соответствующем Информационном сервисе означает согласие Пользователя с действующей на момент Авторизации редакцией Регламента.
- 2.5.** Настоящий Регламент в соответствии со ст. 428 Гражданского кодекса Российской Федерации является договором присоединения. Договор присоединения считается заключенным с Пользователем с момента, когда Пользователь первый раз успешно авторизуется в Информационном сервисе.
- 2.6.** Присоединяясь к настоящему Регламенту в порядке, установленном ст. 437 и ст. 438 Гражданского кодекса Российской Федерации, Заявители и Пользователи Информационных сервисов соглашаются, что положения настоящего Регламента являются для них обязательными, а успешная Авторизация в Информационном сервисе является достаточным условием для Идентификации и Аутентификации Пользователя, и подтверждает его право пользоваться Информационным сервисом в соответствии с условиями, установленными настоящим Регламентом.
- 2.7.** Настоящий Регламент не является публичным договором, публичной офертой и не обязывает Оператора ИС предоставить доступ к ИС каждому обратившемуся лицу.
- 2.8.** Пользователь Информационного сервиса обязуется не разглашать третьим лицам Аутентификационные данные для доступа к Информационному сервису или подтверждения действий в Информационном сервисе, и принимает на себя все риски, связанные с их разглашением или утратой.
- 2.9.** Стороны соглашаются, что используемые ими организационные и технические средства осуществления электронного документооборота обеспечивают необходимый уровень конфиденциальности и защиты информации от неправомерных действий третьих лиц. Заявитель и Пользователь при использовании Информационных сервисов осознают и принимают риски, связанные с возможным нарушением конфиденциальности, в том числе в результате неправомерных действий третьих лиц, направленных на причинение вреда (убытков) Заявителям, Пользователям, Оператору ИС.
- 2.10.** Пользователь использует функционал ИС на свой собственный риск. Оператор ИС не принимает на себя никакой ответственности за соответствие ИС ожиданиям Заявителей и Пользователей.
- 2.11.** Стороны осознают и соглашаются, что никакое программное обеспечение не свободно от ошибок. Оператор ИС не предоставляет какую-либо явную или подразумеваемую

гарантию безусловной и безошибочной работоспособности ИС или пригодности их для определенной цели. Оператор ИС подтверждает, что любая ИС позволит Пользователю использовать ее для целей реализации действий Пользователя в соответствии с ее функциональными возможностями.

2.12. Действия, осуществляемые в Информационных сервисах, дата и время поступления документов в Информационный сервис определяются по московскому времени (системное время) и фиксируются автоматически.

С целью снижения вероятности ошибочного толкования времени, указываемого в отчетных документах и в Информационных сервисах Оператора ИС, при указании времени могут использоваться следующие уточняющие термины:

- Время в месте события (локальное время события) – локальное время, определенное с учетом часового пояса места наступления события. Используется в Информационных сервисах.
- Местное время (локальное время Пользователя) – время наступления события, определенное с учетом часового пояса географического нахождения Пользователя, с учетом разницы во времени с часовым поясом места наступления события. Используется в Информационных сервисах.
- Московское время – время наступления события в часовом поясе города Москвы с учетом разницы во времени с часовым поясом места события. Используется в Информационных сервисах и отчетах.

2.13. Электронный документ считается предоставленным Получателю:

- если Электронный документ направлен Оператором ИС, то с момента его размещения в соответствующем Информационном сервисе. С этого момента обязанности Оператора ИС по предоставлению Электронного документа считаются исполненными.
- если Электронный документ направлен Пользователем, то с момента изменения статуса на «Принято в обработку», и/или присвоения входящего номера в Учетной системе, и/или с даты и времени, указанных в уведомлении, подтверждающем его получение Оператором ИС и направленном в виде Электронного сообщения в ИС и/или на электронную почту Пользователя.

2.14. Электронный документ считается полученным Получателем по истечении 24 часов с момента его предоставления в порядке указанном в п. 2.12. В случае, если момент получения электронного документа приходится на нерабочее время по Местному времени Получателя, электронный документ считается полученным в 10 часов 00 минут (по местному времени Получателя) следующего рабочего дня.

2.15. Услуги Оператора ИС, оказываемые с помощью Информационных сервисов, тарифицируются в соответствии с заключенными соглашениями с Оператором ИС, а при их отсутствии – в соответствии с действующими тарифами на услуги Акционерного общества «Реестр», размещенными на Сайте.

2.16. Электронные документы, созданные/пересылаемые Сторонами с использованием Информационных сервисов и подписанные ПЭП или УНЭП, в соответствии с п. 2 ст. 6 Федерального закона от. 06.04.2011 г. № 63-ФЗ «Об электронной подписи» признаются юридически значимыми и равнозначными документам на бумажном носителе, подписанным собственноручной подписью подписанта. Оператор ИС вправе не принимать к исполнению Электронные документы, направленные Пользователем, если такая отправка производится с использованием разделов Информационных сервисов, предназначенных для обмена Электронными сообщениями и не предназначенных для обмена Электронными документами.

- 2.17.** Стороны не вправе оспаривать признание электронной подписи и (или) подписанного ею Электронного документа как не имеющего юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств автоматического создания и (или) автоматической проверки электронных подписей.
- 2.18.** Одной электронной подписью могут быть подписаны несколько связанных между собой Электронных документов (Пакет Электронных документов).
- 2.19.** Замена Ключей электронной подписи не влияет на юридическую силу Электронного документа, если он был подписан электронной подписью, действительной на момент подписания.
- 2.20.** Пользователь информирован и соглашается с тем, что при обращении по телефону к Оператору ИС по вопросам, связанным с работой ИС, Оператор ИС вправе осуществлять запись телефонных разговоров.

3. Порядок доступа к Информационным сервисам

- 3.1.** Оператор ИС предоставляет доступ к Информационным сервисам с использованием Сайта.
- 3.2.** Доступ к соответствующей ИС предоставляется Пользователям, успешно прошедшим процедуру Регистрации, Аутентификации и Авторизации Пользователя, в том числе с использованием Сервисов идентификации.
- 3.3.** Регистрация Пользователя в Личном кабинете осуществляется:
- дистанционно, включая, но не ограничиваясь, посредством Сервисов идентификации, сертификата УКЭП;
 - путем предоставления Заявления Оператору ИС (лично, Уполномоченным представителем, почтовым отправлением) на бумажном носителе.
- 3.4.** Функциональные возможности конкретной ИС предоставляются Пользователю в результате проверки совпадения данных из Единого профиля с данными, содержащимися в Учетной системе, в том числе фамилии, имени, отчества (при наличии), серии и номера документа, удостоверяющего личность, номера мобильного телефона, ИНН, СНИЛС, а также с учетом Роли Пользователя. В случае несовпадения данных и/или отсутствия необходимых полномочий (в том числе в связи с истечением их срока) все или некоторые функциональные возможности ИС могут быть ограничены или недоступны.
- 3.5.** Документы, подтверждающие полномочия Пользователя, являющегося Уполномоченным представителем, должны быть оформлены и предоставлены Оператору ИС в соответствии с Правилами ведения реестров и Правилами использования ИС.
- 3.6.** Оператор ИС имеет право ограничить доступ Пользователя к отдельным функциям ИС в случае:
- нарушения Правил использования ИС;
 - нарушения обязанностей по оплате услуг Оператора ИС;
 - при наличии информации о прекращении правоспособности и/или полномочий Пользователя.
 - в иных случаях, предусмотренных Правилами использования ИС.
- 3.7.** Доступ к Информационным сервисам предоставляется Пользователям круглосуточно. Ограничение доступа Пользователям к ИС может осуществляться Оператором ИС в одностороннем порядке для проведения технических работ, а также в случае действия форс-мажорных обстоятельств, которые Оператор ИС не мог предусмотреть или предотвратить разумными средствами. Информация об ограничении доступа размещается на Сайте и/или интернет-странице соответствующего Информационного сервиса.

- 3.8.** Оператор ИС вправе использовать Абонентский номер, указанный в Едином профиле, для целей однозначной идентификации Пользователя и совершенных им действий в ИС. Оператор ИС расценивает все действия, совершенные в ИС с использованием Абонентского номера, указанного в Едином профиле, действиями, совершенными Пользователем, или по указанию Пользователя, или с разрешения Пользователя. В разумный срок Пользователь обязан уведомить Оператора ИС о расторжении договора с оператором связи об использовании Абонентского номера.
- 3.9.** Изменение параметров Единого профиля Пользователя осуществляется Оператором ИС на основании Заявления Пользователя, в том числе с использованием функциональных возможностей Личного кабинета.
- 3.10.** Авторизуясь в Информационном сервисе для его использования в соответствии с функциональными возможностями, Пользователь соглашается с порядком предоставления услуг Акционерного общества «Реестр» с использованием Информационного сервиса, обязуется соблюдать Правила использования ИС и инструкции по работе с данными сервисами, а также руководствоваться указаниями Оператора ИС.

4. Обработка персональных данных Оператором ИС

- 4.1.** Регистрируясь в Личном кабинете, Пользователь подтверждает, что он ознакомлен и согласен с локальным нормативным актом Оператора ИС «Политика обработки персональных данных в информационных системах персональных данных АО «Реестр»¹, и дает Оператору ИС согласие на автоматизированную и неавтоматизированную обработку своих персональных данных для совершения Оператором ИС следующих действий: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. Настоящее согласие дается Пользователем Оператору ИС на срок 10 лет. Персональные данные, которые Пользователь предоставляет Оператору ИС, включают в себя: фамилия, имя, отчество; данные документа, удостоверяющего личность; ИНН; СНИЛС; номер мобильного телефона; адрес электронной почты, адрес места жительства (и/или регистрации); сведения, содержащиеся в доверенности или ином документе, подтверждающем полномочия Пользователя как Уполномоченного представителя.
- 4.2.** Обработка персональных данных Пользователя прекращается на основании его письменного заявления, подпись Пользователя на котором удостоверена сотрудником Регистратора или нотариально, или Электронного документа, направленного Пользователем в Информационном сервисе при наличии в ней соответствующего функционала.
- 4.3.** После получения заявления, указанного в п.4.2. настоящего Регламента, Оператор ИС прекращает обработку персональных данных Пользователя путем удаления Единого профиля Пользователя и/или путем обезличивания данных Пользователя в Едином профиле, за исключением персональных данных, обработка которых осуществляется для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора ИС функций, полномочий и обязанностей.

5. Электронные подписи

- 5.1.** В Информационных сервисах могут использоваться следующие виды электронных подписей: ПЭП, УНЭП, УКЭП.
- 5.2.** Оператор ИС самостоятельно устанавливает функциональные возможности, а также

¹ Размещена на Сайте по адресу <https://www.aoreestr.ru/upload/politics.pdf>

необходимость и возможность применения определенного вида электронной подписи при подписании Электронных документов, обмен которыми осуществляется в соответствующей ИС.

- 5.3. Электронные документы, исходящие от Оператора ИС, подписываются УКЭП.
- 5.4. При автоматическом создании и (или) автоматической проверке электронных подписей в соответствующем Информационном сервисе, Оператор ИС вправе использовать УКЭП, для которой не указывается в качестве владельца сертификата ключа проверки электронной подписи физическое лицо, действующее от имени Оператора ИС.
- 5.5. Электронные документы, сформированные Пользователем, авторизованным в Информационном сервисе с помощью его Логина и Пароля и/или дополнительно подтвержденные Кодом, являются Электронными документами, подписанными ПЭП.

6. Признание Электронного документа подлинником (оригиналом), копия Электронного документа

- 6.1. Все экземпляры Электронного документа, представленного в Информационном сервисе или на электронном носителе, имеющиеся у Оператора ИС, Получателя и Отправителя, являются подлинниками (оригиналами) данного Электронного документа.
- 6.2. Подлинник Электронного документа не существует, если:
 - нет ни одного учтенного в ИС и/или Учетной системе экземпляра данного Электронного документа;
 - получение или восстановление экземпляра данного Электронного документа в первоначальном виде невозможно;
 - невозможно установить подлинность электронной подписи на Электронном документе.
- 6.3. Подлинник (оригинал) электронного документа существует только в электронном виде. Содержимое электронного документа, визуализированное на бумажном носителе, является копией электронного документа на бумажном носителе.
- 6.4. Воспроизведенный на бумажном носителе Электронный документ является копией Электронного документа и не является подлинником. Копия Электронного документа может содержать графические изображения подписи уполномоченного лица и печати Отправителя.
- 6.5. В зависимости от целей использования копия Электронного документа может быть представлена в виде распечатки машинных кодов, содержащихся в Электронном документе, либо в иной форме, доступной для восприятия третьими лицами, с учетом выполненных преобразований машинных кодов без изменения их смысла и содержания. Информация, содержащаяся в копии Электронного документа на бумажном носителе, должна соответствовать информации, содержащейся в подлиннике Электронного документа, в том числе с учетом преобразования машинных кодов в значения, понятные третьим лицам.

7. Порядок проверки электронной подписи, установление подлинности Электронного документа

- 7.1. Все электронные документы, подписанные УКЭП или УНЭП, отправляемые и получаемые Сторонами в ИС, проверяются на целостность (доставку в неискаженном виде по отношению к первоначальному) и неизменность электронной подписи.
- 7.2. Полученный Электронный документ проверяется на соответствие установленному для него формату в случае, если использование установленного формата обязательно или предусмотрено функционалом соответствующего Информационного сервиса.

- 7.3.** Электронный документ подлежит дальнейшей обработке и исполнению только в случае положительного результата проверки целостности Электронного документа, его соответствия установленному формату и подлинности электронной подписи.
- 7.4.** В случае невозможности расшифровки Электронного документа, а также при отрицательном результате проверки целостности Электронного документа и/или соответствия установленному формату и/или подлинности электронной подписи документ считается не полученным Получателем и не подлежит дальнейшей обработке и исполнению.
- 7.5.** Электронные документы, подписанные УКЭП, помимо программного обеспечения, интегрированного в Информационные сервисы Оператора ИС, могут быть проверены с использованием публичных сервисов проверки электронной подписи, в том числе в сети Интернет² и/или с использованием программного обеспечения «КриптоАрм»³ или иного специализированного программного обеспечения.
- 7.6.** В случае возникновения конфликтных ситуаций между Сторонами о признании подлинности Электронного документа, подписанного УКЭП, криптографические ключи которой выдает Удостоверяющий центр, любая Сторона имеет право обратиться в Удостоверяющий центр для проверки электронной подписи Отправителя и установления подлинности Электронного документа.
- 7.7.** В случае необходимости получения доказательств фактов осуществления каких-либо действий в Информационном сервисе, включая действия с Электронными документами, а также установления Пользователей, осуществивших такие действия, необходимым и достаточным доказательством будет являться заверенная Оператором ИС выписка из Системного журнала Информационного сервиса Оператора ИС. Данным способом подтверждаются такие действия как: создание, модификация, уничтожение и подписание электронной подписью Электронных документов в Информационных сервисах Оператора ИС, а также могут подтверждаться иные действия Пользователей.

8. Обязанности, ответственность и гарантии Оператора ИС

8.1. Оператор ИС обязан:

- предпринимать необходимые и достаточные меры для поддержания бесперебойной работы Информационных сервисов и обеспечивать Пользователям возможность выполнения всей совокупности доступных действий в соответствии с настоящим Регламентом и Правилами использования ИС;
- соблюдать режим конфиденциальности, предпринимать необходимые и достаточные организационно-технические меры по защите информации, которая становится доступной Оператору ИС в связи с выполнением им своих функций и которая содержится в Информационных сервисах, а также касается паролей, идентификаторов и Криптографических ключей;
- предпринимать организационные и технические меры в целях предотвращения конфликта интересов при совмещении различных видов деятельности.
- незамедлительно предпринять организационные и технические меры в целях защиты интересов Пользователя после получения от него информации о компрометации Аутентификационных данных.

8.2. Оператор ИС несет ответственность:

² <https://www.gosuslugi.ru>, <https://crypto.kontur.ru/>, <https://dss.cryptopro.ru/verify/#!/signature> и другие

³ <https://www.cryptopro.ru/products/partner/crypto-arm>

- за соблюдение требований законодательства в области защиты персональных данных Пользователей, а также иного применимого к Оператору ИС законодательства РФ;
- за соблюдение требований настоящего Регламента в отношении обязанностей Оператора ИС;

8.3. Оператор ИС гарантирует, что:

- будет использовать его персональные данные Пользователя, предоставленные для использования в ИС исключительно в целях, необходимых для обеспечения возможности Пользователя пользования ИС;
- не будет осуществлять действий, нарушающих конфиденциальность информации о самом Пользователе и о совершаемых им действиях в ИС, кроме как для обеспечения возможности пользования ИС и исполнения Оператором ИС указаний Пользователя, осуществленных с использованием функциональных возможностей ИС, за исключением случаев, если предоставление таких сведений уполномоченным государственным органам осуществляется в соответствии с требованиями действующего законодательства РФ;
- если законодательством РФ на Оператора ИС возлагаются обязанности по передаче информации от Пользователя иным лицам, то Оператор ИС осуществит все необходимые действия по обработке и/или передаче информации и документов, которые будут подготовлены Пользователем с помощью ИС.
- вся информация, представленная в ИС, получена Оператором ИС на законных основаниях и соответствует информации, содержащейся в Учетной системе;
- приложит максимум усилий для обеспечения бесперебойной работы Сервиса, а в случаях, когда такая бесперебойность находится в сфере влияния Оператора ИС, то предпримет все возможные меры для оперативного устранения возникших проблем.

9. Обязанности, ответственность и гарантии Пользователя

9.1. Пользователь обязан:

- 9.1.1. обеспечивать сохранность и конфиденциальность своих Аутентификационных данных, Кодов подтверждения, иных идентификационных данных. Запрещается передавать указанную информацию третьим лицам по любым каналам связи, даже в случае получения таких указаний от сотрудников Оператора ИС;
- 9.1.2. не совершать действий, которые могут привести к событиям, в результате которых доступ к соответствующей Информационной системе окажется невозможен и/или такой доступ будет предоставлен неуполномоченным лицам;
- 9.1.3. не предпринимать действий, направленных на нарушение работоспособности Информационной системы, а также действий, направленных на нарушение авторских и лицензионных прав Оператора ИС;
- 9.1.4. незамедлительно известить Оператора ИС по телефону и/или электронной почте о ставших ему известными действиях третьих лиц, способных привести к компрометации Аутентификационных данных и/или нарушению системы информационной безопасности Оператора ИС;
- 9.1.5. предпринять действия, указанные в разделе 11 настоящего Регламента в случае компрометации Аутентификационных данных;
- 9.1.6. не реже одного раза в год самостоятельно производить смену пароля для доступа к соответствующей Информационной системе;

- 9.1.7. принимать следующие меры для обеспечения безопасного использования Информационных систем для предотвращения похищения и искажения информации, вводимой в целях авторизации в Информационной системе на оборудовании (компьютере, мобильном устройстве), с которого производится доступ к Информационной системе
- регулярно проводить обновление операционной системы, устанавливая выпускаемые разработчиками пакеты обновлений, устраняющих или направленных на снижение уязвимостей в системе безопасности операционной системы при ее эксплуатации;
 - регулярно проводить обновление мобильных версий Информационных систем на платформах iOS и Android;
 - регулярно проводить антивирусную проверку с актуальными антивирусными базами;
 - не использовать программное обеспечение, полученное из сомнительных или ненадежных источников;
 - не открывать письма электронной почты и вложения электронной почты, если такие письма получены из сомнительных источников или от неизвестных отправителей;
 - при пользовании информационно-телекоммуникационной сетью Интернет не переходить по ссылкам сомнительного содержания;
- 9.1.8. регулярно осуществлять проверку электронного почтового ящика, адрес которого указан Пользователем для работы в Информационной системе, и, в случае получения сообщения от Оператора ИС (с адресов электронной почты в домене aoreestr.ru), выполнить указанные им действия;
- 9.1.9. не использовать для доступа к Информационным системам небезопасные сети и компьютеры общего пользования.
- 9.2.** Пользователь несет ответственность за все риски несанкционированного распространения информации, полученной посредством доступа к Информационным системам, в связи с передачей неуполномоченным лицам своих Аутентификационных данных.
- 9.3.** Пользователь заверяет и гарантирует Оператору ИС, что в случае использования УКЭП, квалифицированный Сертификат ключа действителен, не содержит ограничений его использования, выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата и такой удостоверяющий центр уполномочен для выдачи Пользователю квалифицированного Сертификата ключа, Пользователь при получении квалифицированного Сертификата ключа в удостоверяющем центре выполнил все требования удостоверяющего центра об ознакомлении с информацией, содержащейся в квалифицированном Сертификате ключа.
- 9.4.** Пользователь заверяет и гарантирует Оператору ИС, что Абонентский номер мобильного телефона, указанный им при регистрации в Едином профиле, принадлежит Пользователю на законных основаниях и/или Пользователь имеет необходимые разрешения и полномочия на его использование от владельца такого Абонентского номера.
- 9.5.** При несоблюдении требований, изложенных в настоящем разделе Регламента, ответственность за убытки, причиненные вследствие использования скомпрометированных данных, возлагается на Пользователя.
- 9.6.** До момента, пока Пользователь не заявит Оператору ИС о Компрометации, все действия, совершенные в ИС с использованием его Аутентификационных данных, признаются совершенными Пользователем.
- 9.7.** Пользователь не вправе совершать любые действия в ИС в случае прекращения и/или отмены его полномочий как Уполномоченного представителя.

10. Система обеспечения информационной безопасности

10.1.Соблюдение требований информационной безопасности при работе с Информационными сервисами призвано обеспечить:

- защиту информации от несанкционированного доступа;
- целостность, достоверность и криптографическую защиту информации;
- однозначную аутентификацию Отправителя электронного документа.

10.2.Система обеспечения информационной безопасности реализуется посредством применения аппаратно-программных средств и организационных мер.

10.3.К аппаратно-программным средствам относятся:

- встроенные в Информационные сервисы программные средства, обеспечивающие реализацию системы защищенного обмена Электронными документами между Оператором ИС и Пользователями;
- система комплексного резервирования и архивирования данных.

10.4. К организационным мерам относятся:

- безопасное хранение Пользователем простой электронной подписи, предотвращающее компрометацию, в том числе потерю или несанкционированное использование Аутентификационных данных;
- размещение аппаратно-программных средств Информационных сервисов в защищенном помещении Оператора ИС с контролируемым доступом;
- административное ограничение доступа сотрудников и уполномоченных лиц Оператора ИС к аппаратно-программным средствам.

11. Порядок действий при Компрометации

11.1.Пользователь не должен применять скомпрометированные Аутентификационные данные с момента, когда ему стало известно об их компрометации.

11.2.Пользователь скомпрометированных Аутентификационных данных обязан незамедлительно проинформировать Оператора ИС о факте Компрометации доступными для Пользователя и Оператора ИС средствами связи, включая, но не ограничиваясь, по телефону, электронной почте. При этом Оператор ИС вправе запросить дополнительную информацию об обратившемся лице с целью его идентификации как Пользователя или Уполномоченного представителя.

11.3.Оператор ИС, получив информацию о Компрометации, приостанавливает доступ Пользователя к Единому профилю.

11.4.Для восстановления доступа к Единому профилю Пользователь должен обратиться лично к Оператору ИС и предоставить заявление на восстановление доступа.

12. Электронный архив

12.1.Доступ к архиву Электронных документов обеспечивается функционалом соответствующего Информационного сервиса.

12.2.Оператор ИС осуществляет регулярное резервное копирование Электронных документов и служебной информации ИС в соответствии с внутренними документами Оператора ИС.

13. Обстоятельства непреодолимой силы

13.1.Стороны не несут ответственности за убытки, причиненные одной Стороной

противоположной Стороне по причине несвоевременного или ненадлежащего выполнения обязательств, если такое невыполнение было обусловлено обстоятельствами непреодолимой силы (в том числе, действия органов государственной власти и управления, военные действия, стихийные бедствия, эпидемии, сбои, неисправности и отказы систем связи, энергоснабжения и жизнеобеспечения), которые Стороны не могли предвидеть и предотвратить.

13.2. Сторона, надлежащее исполнение обязательств которой оказалось невозможным в силу влияния обстоятельств непреодолимой силы, в течение 2 (двух) рабочих дней после их наступления в письменной форме информирует другую Сторону о наступлении этих обстоятельств и об их последствиях одним из перечисленных способов: через ЛКЭ или ЛКК, курьерской связью, заказным письмом с уведомлением о получении сообщения, по электронной почте с уведомлением о прочтении сообщения и др. Организатор СЭД вправе размещать информацию о действии форс-мажорных обстоятельств на Сайте. Стороны обязаны принимать все возможные меры с целью максимально ограничить отрицательные последствия, вызванные указанными обстоятельствами.

13.3. Незвещение или несвоевременное извещение об обстоятельствах непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства как обстоятельства, освобождающие от ответственности.

14. Ограничение ответственности

14.1. Оператор ИС не несет ответственности за любые причины, по которым Пользователь не будет иметь возможности воспользоваться ИС, если такие причины лежат вне разумного контроля и влияния со стороны Оператора ИС, например:

- стихийные бедствия, аварии, техногенные катастрофы, отключение электроэнергии;
- техническое состояние компьютерного оборудования и мобильного телефона Пользователя, возможные помехи на линии связи, плохое соединение или невозможность установить соединение и другие, не зависящие от Оператора ИС причины, делающие невозможным использование ИС;
- неработоспособность или ограничения на доступ к ИС с оборудования Пользователя (включая ограничения, установленные службой информационной безопасности организации, если доступ к ИС осуществляется через компьютерную сеть организации);
- неоплата Пользователем услуг оператора связи или интернет-провайдера;
- неработоспособность портала «Госуслуг» (www.gosuslugi.ru) или Сервисов идентификации, в результате которой Пользователь не будет иметь возможность зарегистрироваться или авторизоваться в ИС;
- воздействия вредоносного программного обеспечения на оборудование Пользователя;
- неполучения Пользователем Кода подтверждения в связи с техническими проблемами, в том числе по вине оператора сотовой связи, в связи ограничениями, налагаемыми оператором сотовой связи и/или при нахождении Пользователя в роуминге, а также в случае, если это обусловлено причинами, не зависящими от Оператора ИС;
- использование Пользователем оборудования с нелегальным (или «взломанным») программным обеспечением;
- нарушение системы защиты информации ИС не по вине Оператора ИС;

14.2. Оператор ИС не несет ответственности за нарушение Пользователем правил конфиденциальности информации при использовании ИС и, если Оператором ИС предварительно не будет получено уведомление о компрометации учетных данных в порядке, предусмотренном настоящим Регламентом, то Оператор будет расценивать

любые действия, совершенные с использованием учетных данных Пользователя как действия, совершенные самим Пользователем.

14.3. Оператор ИС не гарантирует работу ИС в виде web-приложения, доступного через интернет браузер, если:

- разработчиком прекращена поддержка такого браузера и/или операционной системы, под управлением которой он используется;
- установленная версия браузера или операционной системы устарела и при этом имеются более актуальные версии браузера или операционной системы соответственно, и со времени выпуска таких версии прошло не более 6 месяцев.

14.4. Оператор ИС не гарантирует работу мобильных версий ИС на платформах iOS и Android ниже версий, указанных при установке на мобильное устройство Пользователя, или к моменту пользования ИС имеется его более новая версия, чем установленная на мобильном устройстве Пользователя;

14.5. В случае возникновения у Оператора ИС технических неисправностей или других обстоятельств, препятствующих использованию Сервиса или обеспечению требуемого уровня безопасности, в том числе изменение действующего законодательства РФ, Оператор ИС вправе в одностороннем порядке приостановить на неопределенный срок доступ к ИС и/или использование отдельных функций ИС без предварительного уведомления Пользователя.

15. Разрешение спорных ситуаций

15.1. В случае возникновения споров или разногласий между Сторонами, вытекающих из настоящего Регламента или связанных с ним, Стороны принимают все меры к разрешению их путем переговоров.

15.2. В случае невозможности разрешения споров путем переговоров они подлежат рассмотрению по месту нахождения Регистратора в соответствии с действующим процессуальным законодательством РФ.

16. Техническая поддержка Пользователей

16.1. Поддержка Пользователей по работе с Информационными сервисами осуществляется:

- в разделе Сайта «Часто задаваемые вопросы» (<https://www.aoreestr.ru/faq/>)
- в соответствующем разделе Информационного сервиса;
- посредством чата в Информационном сервисе (при наличии соответствующего функционала);
- по единому телефону Оператора ИС: +7 (495) 617-01-01;
- персональными менеджерами (при наличии) по контактам, указанным в Информационном сервисе.