



Научно-производственное предприятие
“ИЖИНФОРМПРОЕКТ”

УТВЕРЖДЕН
приказом от 17.11.2016 № 17

Регламент
системы защищенного электронного юридически значимого
документооборота «КриптоСвязь-Веб» («КриптоВеб»)

Редакция № 1.3



КРИПТОВЕБ
ЗАЩИЩЕННЫЙ ДОКУМЕНТООБОРОТ

Ижевск 2016

Реферат

Настоящий документ содержит Регламент системы защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») Общества с ограниченной ответственностью научно-производственное предприятие «Ижинформпроект».

Регламент создан в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», Гражданского кодекса Российской Федерации, Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Оператор электронного документооборота использует для оказания услуг программу для ЭВМ «Система защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб»)» (Свидетельство о регистрации программы для ЭВМ № 2013618985 от 24.09.2013), которая соответствует требованиям нормативных документов Российской Федерации (Сертификат соответствия ГОСТ Р № РОСС RU.AB51.H09041 от 13.11.2015).

Содержание

	стр.
1 Определения _____	4
2 Обозначения и сокращения _____	9
3 Введение _____	10
3.1 Сведения об Операторе _____	10
3.2 Идентификация Регламента _____	11
3.3 Статус Регламента _____	11
3.4 Применение Регламента _____	13
3.5 Изменения (дополнения) Регламента _____	13
4 Порядок обработки электронных документов в Системе _____	15
5 Квалифицированные сертификаты _____	17
6 Средства криптографической защиты информации _____	18
7 Условия равнозначности электронной подписи собственноручной _____	20
8 Права и обязанности _____	21
8.1 Обязанности Оператора Системы _____	21
8.2 Обязанности Стороны, присоединившейся к Регламенту _____	21
8.3 Права Оператора Системы _____	22
9 Техническая поддержка _____	24
10 Ответственность сторон _____	26
11 Разрешение споров _____	28
12 Вознаграждение Оператора Системы, сроки и порядок расчетов _____	29
12.1 Вознаграждение Оператора Системы _____	29
12.2 Сроки и порядок расчетов _____	29
13 Конфиденциальность информации _____	30
14 Форс-мажор _____	31
Приложение А Подписной лист к Регламенту системы защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») _____	32
15 Лист регистрации изменений _____	33

1 Определения

Система защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» (КриптоВеб) (Система) — корпоративная информационная система, устройтелем которой является Организатор Системы, основанная на технологии Инфраструктуры открытых ключей (ИОК, РКІ), в которой используются сертификаты, изготовленные Удостоверяющим центром, построенная на базе программных продуктов КриптоВеб, включая программное обеспечение клиентского рабочего места КриптоВеб, и предназначенная для оказания услуг в области использования электронной подписи/шифрования данных и телематических услуг связи пользователям Системы, действующая по правилам, установленным Оператором Системы в соответствии с нормативными правовыми и иными актами, регулирующими защищенный электронный документооборот и применение электронной подписи.

Оператор Системы/Оператор ЭДО — ООО НПП «Ижинформпроект», устройство корпоративной информационной системы для обеспечения электронного документооборота с применением электронной подписи, организующий и обеспечивающий предоставление услуг пользователям Системы.

Доверенный способ передачи информации — способ передачи информации, обеспечивающий требуемую степень ее защищенности.

Сторона, присоединившаяся к Регламенту/ Абонент / Участник Системы — юридическое или физическое лицо, участник информационного обмена электронными документами, зарегистрированный в Системе, и при необходимости имеющий с Организатором Системы договорные отношения о присоединении к Системе, соблюдающий требования и условия пользования Системой (в том числе применения электронной подписи) и признающий настоящий Регламент.

Пользователь Удостоверяющего центра (Пользователь УЦ) — физическое лицо, зарегистрированное в Удостоверяющем центре и являющееся уполномоченным представителем Абонента (Участника) Системы.

Электронный документ — документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

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.

Сертификат средств электронной подписи — документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной подписи установленным требованиям.

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.

Ключ электронной подписи (закрытый ключ) — уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи — уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (проверка электронной подписи).

Сертификат ключа проверки электронной подписи (сертификат) — электронный документ или документ на бумажном носителе, выданные Удостоверяющим центром либо доверенным лицом Удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат) — сертификат ключа проверки электронной подписи, выданный аккредитованным Удостоверяющим центром или доверенным

лицом аккредитованного Удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (уполномоченный федеральный орган).

Сертификат в форме документа на бумажном носителе — документ на бумажном носителе, содержащий информацию из сертификата и заверенный собственноручной подписью уполномоченного лица Удостоверяющего центра и печатью Удостоверяющего центра. Стороны признают возможность использования факсимиле подписи (клише с подписи) уполномоченного лица Удостоверяющего центра для подписи сертификата в качестве аналога собственноручной подписи, равнозначного собственноручной подписи.

Список отозванных (аннулированных) сертификатов (СОС) — электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были отозваны или действие которых было приостановлено.

Владелец сертификата ключа проверки электронной подписи (владелец сертификата) — лицо, которому в установленном Федеральным законом «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

Удостоверяющий центр — удостоверяющий центр InfoTrust ООО НПП «Ижинформпроект», осуществляющий выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи» непосредственно и/или через Регистрационные отделения удостоверяющего центра (перечень публикуется на сайте www.infotrust.ru), а также аккредитованные удостоверяющие центры, входящие в Перечень доверенных удостоверяющих центров Системы (перечень публикуется на сайте www.cryptoweb.ru).

Аккредитация удостоверяющего центра — признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона «Об электронной подписи».

Средства удостоверяющего центра — программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

Реестр Удостоверяющего центра — набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий:

- реестр заявлений на регистрацию в Удостоверяющем центре;
- реестр зарегистрированных пользователей Удостоверяющего центра;
- реестр заявлений на изготовление сертификата;
- реестр заявлений на аннулирование (отзыв) сертификата;
- реестр заявлений на приостановление/возобновление действия сертификата;
- реестр заявлений на подтверждение подлинности электронной подписи в электронном документе;
- реестр заявлений на подтверждение электронной подписи уполномоченного лица Удостоверяющего центра в изданных сертификатах;
- реестр сертификатов;
- реестр изготовленных списков отозванных сертификатов.

Уполномоченное лицо Удостоверяющего центра — физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов и списков отозванных сертификатов.

Регистрационное отделение Удостоверяющего центра (Регистрационное отделение) — подразделение Удостоверяющего центра или юридическое лицо, заключившее с Удостоверяющим центром агентский договор, уполномоченное Удостоверяющим центром осуществлять регистрацию Пользователей УЦ и управление сертификатами Пользователей УЦ, в т.ч.:

- взаимодействие с Пользователем УЦ, информирование и обработка (прием, регистрация, выдача) документов, предусмотренных Регламентом;
- идентификация Пользователей УЦ, проверка атрибутов и полномочий должностных лиц, подготовка и занесение регистрационной информации Пользователя УЦ в Реестр Удостоверяющего центра;

— изготовление ключевых документов по заявлениям Пользователей УЦ.

Инфраструктура открытых ключей (ИОК) / Public Key Infrastructure (PKI) — технологическая инфраструктура и сервисы, гарантирующие безопасность информационных и коммуникационных систем, использующих криптографические алгоритмы с открытыми ключами.

Регламент Удостоверяющего центра (Регламент)/ Certification Practice Statement (CPS) — документ, устанавливающий общий порядок и условия предоставления Удостоверяющим центром услуг по изготовлению и выдаче сертификатов и дополнительных услуг, связанных с управлением сертификатами.

Правила применения сертификатов (ППС)/ Certificate policy (CP) — установленный набор правил, характеризующих возможность применения сертификата определенным сообществом и/или для класса приложений с определенными требованиями безопасности. Правила применения сертификатов позволяет доверяющей стороне оценить надежность использования сертификата для определенного приложения.

Cryptographic Message Syntax (CMS) — стандарт, определяющий формат и синтаксис криптографических сообщений (RFC 5652).

CMS Advanced Electronic Signatures (CAAdES) — формат усовершенствованной электронной подписи типа CAAdES-X Long Type 1 в соответствии ETSI TS 101 733 «Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAAdES)» с учётом использования российских криптографических алгоритмов и RFC 5126.

Online Certificate Status Protocol (OCSP) — протокол установления статуса сертификата открытого ключа (RFC 2560).

Time-Stamp Protocol (TSP) — протокол получения штампа времени (RFC 3161)».

The Transport Layer Security (TLS) Protocol — протокол криптографической защиты на транспортном уровне (RFC 5246).

2 Обозначения и сокращения

CAAdES	CMS Advanced Electronic Signatures (Формат усовершенствованной электронной подписи)
CDP	CRL Distribution Point (Точка распространения СОС)
CMS	Cryptographic Message Syntax (Синтаксис криптографических сообщений)
CP	Certificate Policy (Правила применения сертификатов)
CPS	Certification Practice Statement (Регламент Удостоверяющего центра)
CRL	Certificate Revocation List (Список отозванных сертификатов)
DN	Distinguished Name (Отличительное имя)
OID	Object IDentifier (Объектный идентификатор)
OCSP	Online Certificate Status Protocol (Протокол установления актуального статуса сертификата)
PKI	Public Key Infrastructure (Инфраструктура Открытых Ключей)
RFC	Request For Comments
TLS	Transport Layer Security Protocol (Протокол криптографической защиты на транспортном уровне)
TSP	Time-Stamp Protocol (Протокол получения штампа времени)
URL	Uniform Resource Locator (Единый локатор ресурса)
UTC/GMT	Universal Time Coordinated/Greenwich Mean Time (Универсальное координированное время/Всемирное время «по Гринвичу»)
КСКПЭП	Квалифицированный сертификат ключа проверки электронной подписи (Квалифицированный сертификат)
КС	Квалифицированный сертификат (Квалифицированный сертификат ключа проверки электронной подписи)
КЭП	Квалифицированная электронная подпись
ПО	Программное обеспечение
СОС	Список отозванных сертификатов (Certificate Revocation List)
УЦ	Удостоверяющий центр
ЭДО	Электронный документооборот

3 Введение

3.1 Сведения об Operаторе

Общество с ограниченной ответственностью научно-производственное предприятие «Ижинформпроект» (ООО НПП «Ижинформпроект»), предоставляющее услуги *Operатора Системы* в соответствии с требованиями законодательства Российской Федерации, именуемое в дальнейшем «*Operатор*», зарегистрировано на территории Российской Федерации в городе Ижевске.

Operатор осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий:

1) лицензия Управления ФСБ России по Удмуртской Республике 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 (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) от 11.10.2016 № 110Н;

2) лицензия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) на оказание услуг связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации, от 18.08.2013 № 111185;

3) лицензия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) на оказание телематических услуг связи от 18.08.2013 № 111186.

Реквизиты ООО НПП «Ижинформпроект»:

ИНН 1831014533 КПП 183101001 ОГРН 1021801161140

Юридический адрес: ул. Бородина, 21, офис 207, г. Ижевск, Удмуртская Республика, 426057

Фактическое местонахождение: ул. Бородина, 21, офис 207, г. Ижевск, Удмуртская Республика, 426057

Банковские реквизиты:

Удмуртское отделение № 8618 ПАО СБЕРБАНК г. Ижевск

р/с 40702810768170101530

к/с 30101810400000000601

БИК 049401601

Контактная информация

телефон/факс: +7 (3412) 918-100,

e-mail: info@cryptoweb.ru

www: www.cryptoweb.ru

3.2 Идентификация Регламента

Наименование документа — Регламент системы защищенного юридически значимого электронного документооборота «КриптоСвязь-Веб» («КриптоВеб»).

Версия: 1.3.

Дата: 17.11.2016.

Количество страниц в документе: 33.

3.3 Статус Регламента

Регламент системы защищенного юридически значимого электронного документооборота «КриптоСвязь-Веб» («КриптоВеб») (далее — Регламент)

разработан в соответствии с действующим законодательством Российской Федерации и определяет принципы взаимодействия *Абонентов Системы* защищенного юридически значимого электронного документооборота, порядок применения квалифицированных сертификатов ключей проверки электронной подписи, а также условия, при соблюдении которых электронная подпись в электронном документе признается равнозначной собственноручной.

Регламент является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации. Присоединение к Регламенту производится путем подписания *Абонентом Системы* Подписного листа к настоящему Регламенту, указанного в Приложении А. Подписной лист может быть оформлен и подписан в электронном виде и передан *Оператору* средствами *Системы*.

Факт присоединения лица к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент регистрации Подписного листа. Лицо, присоединившееся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

После присоединения в установленном порядке *Абонента Системы* к Регламенту, Стороны вступают в соответствующие договорные отношения на неопределённый срок.

Действие настоящего Регламента может быть прекращено по инициативе одной из Сторон в следующих случаях:

- по собственному желанию одной из Сторон;
- нарушения одной из Сторон условий настоящего Регламента.

В случае расторжения Регламента инициативная Сторона письменно уведомляет другую Сторону о своих намерениях за тридцать календарных дней до даты расторжения Регламента. Регламент считается расторгнутым после выполнения Сторонами своих обязательств и проведения взаиморасчетов согласно условиям Регламента.

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

Настоящий регламент распространяется:

- в форме электронного документа по адресу: <http://www.cryptoweb.ru>.
- в форме документа на бумажном носителе: при подаче Подписного листа о присоединении к Регламенту (за вознаграждение, установленное настоящим Регламентом).

Любые справки по вопросам, связанным с предоставлением услуг *Оператора*, предоставляются сотрудниками *Оператора* по телефону +7 (3412) 918-100 и info@cryptoweb.ru.

3.4 Применение Регламента

Стороны понимают термины, применяемые в настоящем Регламенте, строго в контексте общего смысла Регламента.

В случае противоречия и/или расхождения названия какой-либо статьи со смыслом какого-либо пункта в ней содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

В случае противоречия и/или расхождения положений какого-либо приложения к настоящему Регламенту с положениями собственно Регламента, Стороны считают доминирующим смысл и формулировки Регламента.

3.5 Изменения (дополнения) Регламента

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

Уведомление *Абонента Системы* о внесении изменений (дополнений) в Регламент осуществляется *Оператором* путем размещения указанных изменений (дополнений) на сайте *Оператора* по адресу <http://www.cryptoweb.ru>.

Все изменения (дополнения), вносимые *Оператором* в Регламент и не связанные с изменением действующего законодательства Российской Федерации,

вступают в силу и становятся обязательными для Сторон по истечении 30 (тридцати) календарных дней с момента размещения указанных изменений и дополнений в Регламенте на сайте *Оператора* <http://www.cryptoweb.ru>.

Все изменения (дополнения), вносимые *Оператором* в Регламент в связи с изменением действующего законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

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

4 Порядок обработки электронных документов в Системе

Абоненты Системы соглашаются при осуществлении взаимоотношений между ними, а также с *Оператором Системы* принимать к обработке электронные документы, подписанные квалифицированной электронной подписью.

Абоненты Системы принимают, что квалифицированная электронная подпись в электронных документах, сформированных владельцем квалифицированного сертификата ключа проверки электронной подписи, является равнозначной собственноручной подписи владельца сертификата и оттиску печати *Абонента Системы* при выполнении условий, определенных настоящим Регламентом.

Использование в рамках настоящего Регламента электронных документов, подписанных электронной подписью, не изменяет содержания прав и обязанностей *Абонентов Системы*, содержания документов и правил заполнения их реквизитов, установленных действующим законодательством Российской Федерации и иными нормативными документами.

Абоненты Системы принимают, что в случае наличия требований к формату и содержанию электронного документа, установленных нормативными актами или *Оператором Системы*, в *Системе* используются электронные документы установленного формата.

Абоненты Системы самостоятельно определяют круг тех участников *Системы*, с которыми будет осуществляться обмен электронными документами.

Абоненты Системы соглашаются, что в соответствии с Федеральным законом от 18.06.2003 № 126-ФЗ «О связи» в *Системе* применяется время *Оператора*, соответствующее Ижевскому времени (3-я часовая зона/МСК+1/Russia Time Zone 3) (UTC+4).

Абоненты Системы соглашаются со следующими принципами электронного документооборота:

— Электронный документ считается отправленным одним *Абонентом Системы* (адресантом) другому *Абоненту Системы* (адресату), если адресантом

получено и подписано Подтверждение *Оператора Системы (Оператора ЭДО)* (далее — Подтверждение), свидетельствующее о получении электронного документа *Оператором Системы*; временем отправки электронного документа является время, зафиксированное *Оператором* в Подтверждении;

— Электронный документ, отправленный адресантом, считается доставленным адресату, если адресантом получена квитанция, подтверждающая получение электронного документа адресатом;

— В случае отправки электронного документа, требующего подписания со стороны адресата: документ считается подписанным адресатом, если адресатом отправлены адресанту квитанция о получении электронного документа и электронный документ с квалифицированной электронной подписью адресата; документ считается неподписанным адресатом, если адресатом отправлен адресанту отказ в подписи полученного электронного документа.

5 Квалифицированные сертификаты

Абоненты Системы обязуются использовать, принимать и признавать квалифицированные сертификаты ключей проверки электронной подписи, созданные Аккредитованным Удостоверяющим центром InfoTrust ООО НПП «Ижинформпроект», а также аккредитованными удостоверяющими центрами, входящими в Перечень доверенных удостоверяющих центров *Системы*.

Для получения в *Удостоверяющем центре* квалифицированного сертификата *Абонент Системы* обращается в *Удостоверяющий центр* в порядке, определенном Регламентом *Удостоверяющего центра*.

Квалифицированный сертификат признается созданным *Удостоверяющим центром*, если подтверждена подлинность электронной подписи издателя квалифицированного сертификата.

Абоненты Системы принимают, что данные, содержащиеся в поле Subject квалифицированного сертификата, соответствуют идентификационным данным владельца квалифицированного сертификата, зарегистрированного в реестре Удостоверяющего центра, и однозначно идентифицируют владельца квалифицированного сертификата и соответствующего ключа электронной подписи.

Абоненты Системы принимают, что для определения действительности квалифицированного сертификата используются квалифицированный сертификат издателя сертификата и список отозванных сертификатов, издаваемый и публикуемый *Удостоверяющим центром* в порядке и с периодичностью, определяемыми Регламентом Удостоверяющего центра.

В качестве места публикации актуального списка отозванных сертификатов принимается адрес информационного ресурса, указанный в поле CRLDistributionPoints квалифицированного сертификата.

6 Средства криптографической защиты информации

Абоненты Системы принимают в качестве средства шифрования и электронной подписи, применяемого для создания и проверки электронной подписи, средство криптографической защиты информации «КриптоПро CSP». Применяемые версии указанных средств криптографической защиты информации должны соответствовать требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

Для обеспечения аутентификации и защиты канала передачи данных по протоколу TLS, шифрования электронных документов и применения электронных подписей в формате CMS применяются:

— алгоритм зашифрования/расшифрования данных и вычисление имитовставки в соответствии с ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая»;

— алгоритм формирования и проверки электронной подписи в соответствии с ГОСТ Р 34.10-2001. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

— алгоритм формирования и проверки цифровой подписи в соответствии с ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

— алгоритм выработки значения хэш-функции в соответствии с ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования»;

— алгоритм выработки значения хэш-функции в соответствии с ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»,

с использованием RFC 4357, RFC 4490 и RFC 4491.

Класс криптографической защиты информации, обеспечиваемый *Оператором Системы*, КС2. Класс криптографической защиты информации *Абонентов Системы* определяется требованиями руководящих документов и моделями угроз

Абонентов Системы. Для обеспечения классов криптографической защиты информации КС2 и выше необходимо использовать сертифицированное ФСБ России средство защиты от несанкционированного доступа типа «электронный замок». Использование средств защиты информации производится в соответствии с технической и эксплуатационной документацией на них.

Оператор Системы не имеет доступа к содержанию электронных документов, передаваемых между *Абонентами Системы*, электронные документы обрабатываются *Оператором Системы* в зашифрованном виде.

7 Условия равнозначности электронной подписи собственноручной

Квалифицированная электронная подпись в электронном документе равнозначна собственноручной подписи владельца квалифицированного сертификата ключа проверки электронной подписи при одновременном соблюдении следующих условий:

— владелец квалифицированного сертификата ключа проверки электронной подписи может быть идентифицирован по содержимому квалифицированного сертификата ключа проверки электронной подписи;

— серийный номер квалифицированного сертификата ключа проверки электронной подписи не содержится в актуальном списке отозванных сертификатов;

— срок действия квалифицированного сертификата ключа проверки электронной подписи наступил и не окончен на момент создания электронной подписи;

— квалифицированная электронная подпись используется в соответствии со сведениями, указанными в квалифицированном сертификате проверки электронной подписи;

— положительный результат проверки с использованием средств электронной подписи отсутствия искажений в подписанном данной квалифицированной электронной подписью электронном документе.

8 Права и обязанности

8.1 Обязанности Оператора Системы

Выполнять требования нормативных документов органов исполнительной власти при обеспечении обмена информацией по телекоммуникационным каналам связи в рамках электронного документооборота, в отношении которого такие требования установлены.

Обеспечивать круглосуточный и бесперебойный обмен информацией по телекоммуникационным каналам связи в рамках электронного документооборота между *Абонентами Системы*, за исключением периодов регламентного технического обслуживания *Системы*.

Обеспечить функционирование программно-аппаратного комплекса Системы в соответствии с требованиями эксплуатационной документации на него.

В случае получения от *Абонента Системы* заявления о внесении изменений в ранее сообщенные учетные данные, не позднее 3 (трех) рабочих дней с момента получения заявления осуществить изменение в *Системе* учетных данных *Абонента Системы*.

Осуществлять техническую поддержку программных средств *Абонентов Системы* в соответствии с настоящим Регламентом.

Осуществлять хранение в течение 5 (пяти) лет всех подтверждений/уведомлений/квитанций и т.п., подтверждающих факт отправки или получения документов *Абонентами Системы*.

8.2 Обязанности Стороны, присоединившейся к Регламенту

Выполнять требования нормативных документов органов исполнительной власти при осуществлении документооборота, в отношении которого такие требования установлены.

Известить *Оператора Системы* об изменениях в документах, представленных *Оператору*, и по требованию *Оператора* предоставить их новые редакции в течение 5 (пяти) рабочих дней с момента регистрации изменений.

Обеспечивать конфиденциальность ключей электронной подписи.

Немедленно информировать Удостоверяющий центр о факте компрометации принадлежащих им ключей электронной подписи.

Немедленно прекратить использование ключей электронной подписи в случае их компрометации.

Использовать средства криптографической защиты информации в соответствии с требованиями, определенными эксплуатационной документацией.

Принимать меры для предотвращения несанкционированного доступа к компьютерам с установленными на них средствами криптографической информации, а также в помещения, в которых они установлены.

С целью обеспечения гарантированного ознакомления Стороны, присоединившейся к Регламенту, с полным текстом изменений и дополнений Регламента до вступления их в силу не реже одного раза в 30 (тридцать) календарных дней обращаться на сайт *Оператора Системы* по адресу <http://cryptoweb.ru> за сведениями об изменениях и дополнениях в Регламент.

8.3 Права Оператора Системы

Проводить регламентные работы по техническому обслуживанию и внесению изменений в *Систему*. Конкретную дату и время проведения регламентных работ *Оператор Системы* определяет самостоятельно, при этом, не менее чем за 3 (три) дня до начала проведения регламентных работ, *Оператор Системы* обязан разместить на своем сайте информацию о проведении таких работ с указанием точной даты и времени их начала и окончания. При соблюдении указанных условий, в период проведения регламентных работ, *Оператор Системы* имеет право приостановить оказание услуг *Абонентам Системы*.

Регламентные работы по техническому обслуживанию *Системы* проводятся *Оператором*, как правило, не чаще 1 (одного) раза в месяц, с уведомлением

Абонентов Системы за 3 (три) рабочих дня о конкретной дате и времени приостановления работы *Системы* в целях технического обслуживания. Продолжительность регламентных технических работ может составлять не более 30 (тридцати) минут.

В отдельных случаях *Оператор* имеет право приостановления работы *Системы* для проведения технического обслуживания на срок до 3 (трех) часов при условии, что такие регламентные работы проводятся с 20:00 до 08:00.

Совершать иные действия, не противоречащие действующему законодательству РФ и настоящему Регламенту.

9 Техническая поддержка

Оператор консультирует Абонента Системы по текущим вопросам, связанным с использованием средств Системы, установленных на стороне Участника, и получением услуг, по телефону или по электронной почте, указанным на сайте *Оператора*. Режим работы службы поддержки *Оператора* — рабочие дни с 9.00 до 18.00 часов по Ижевскому времени.

Реакция *Оператора* на обращение осуществляется в разумные сроки, *Оператор* информирует Абонента Системы о действиях по устранению причин обращения. В случае если *Оператор* не в состоянии оперативно определить и/или устранить причину обращения, Абонент Системы информируется об этом согласованным способом. *Оператор* принимает меры по устранению причины обращения и не позднее 72 часов с момента получения заявки от Абонента Системы сообщает о принятых мерах. В случае невозможности устранения в указанный срок неполадок в работе программных средств, вызвавших обращение Абонента Системы, *Оператор* сообщает план мероприятий по устранению причин неполадок и предполагаемое время, необходимое для его выполнения.

Техническая поддержка не включает в себя:

- исправление ошибок, возникших вследствие действий Абонента Системы, противоречащих эксплуатационной документации на программные средства;
- исправление ошибок, возникших вследствие неавторизованной модификации программных средств (изменение структуры, корректировка баз данных и пр.);
- определение неполадок, не связанных с работой средств Системы;
- разработку технических предложений по изменению и/или развитию конфигурации информационной инфраструктуры Абонента Системы.

Абонент Системы обязан своевременно сообщать *Оператору* обо всех сбоях, отказах и других нештатных ситуациях, связанных с оказанием услуг *Оператором*.

Абонент Системы обязан оперативно предоставлять *Оператору* возможность выполнять свои обязанности по технической поддержке программных средств. В

частности, *Абонент Системы* должен обеспечить *Оператору* возможность удаленного выполнения своих обязанностей по технической поддержке. Под возможностью удаленного выполнения *Оператором* обязанностей по техническому сопровождению программных средств понимается наличие у *Абонента Системы* доступа к сети Интернет, действующего адреса электронной почты (e-mail) и междугородней телефонной связи.

Абонент Системы должен обеспечить соответствие рабочего места требованиям, указанным в эксплуатационной документации на программные средства. При этом на рабочем месте *Абонента Системы* должно быть установлено лицензионное системное программное обеспечение.

При невыполнении *Абонентом Системы* вышеизложенных обязательств *Оператор* не несет ответственность за непредоставление и (или) ненадлежащее предоставление услуг в *Системе*.

10 Ответственность сторон

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

Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной Регламента своих обязательств.

Оператор Системы не несет ответственность за неисполнение, либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если *Оператор Системы* обоснованно полагался на сведения, указанные в документах *Пользователя УЦ* и/или Стороны, присоединившейся к Регламенту.

Оператор Системы не несет ответственности за содержание и достоверность информации, передаваемой *Абонентами Системы*, а также за какой-либо ущерб, потери и прочие убытки, которые понес *Абонент Системы* по причине несоблюдения им требований настоящего Регламента, а также в следующих случаях:

- нарушения и сбои в работе технических средств *Абонента Системы*, в том числе по причине заражения компьютерными вирусами;
- отсутствие у *Абонента Системы* возможностей по обработке информации в требуемом формате;
- нарушение *Абонентом Системы* правил эксплуатации средств криптографической защиты информации, правил хранения и использования ключей электронной подписи;

- невозможность пользоваться услугами *Системы* по причине их неоплаты;
- неизвещение или сделанное ненадлежащим образом извещение *Оператора Системы* об изменении реквизитов *Абонента Системы*;
- в иных, независящих от *Оператора Системы*, обстоятельствах, в частности, наступивших в результате действий или бездействия *Абонентов Системы*.

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

11 Разрешение споров

При рассмотрении спорных вопросов, связанных с настоящим Регламентом, Стороны будут руководствоваться действующим законодательством Российской Федерации.

Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

Сторона, получившая от другой Стороны претензию, обязана в течение 20 (двадцати) рабочих дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа. К ответу должны быть приложены все необходимые документы.

Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, разрешаются в Арбитражном суде Удмуртской Республики.

12 Вознаграждение Оператора Системы, сроки и порядок расчетов

12.1 Вознаграждение Оператора Системы

Вознаграждение *Оператора Системы* по настоящему Регламенту устанавливается в соответствии с Прейскурантом Системы. Действующий Прейскурант можно получить в офисе *Оператора Системы* или загрузить с сайта *Оператора Системы* <http://www.cryptoweb.ru>.

Оплата осуществляется на основании счета на оплату в российских рублях по безналичному расчету с использованием платежных поручений или иным способом, предусмотренным законодательством Российской Федерации.

12.2 Сроки и порядок расчетов

Сторона, присоединившаяся к Регламенту, вносит аванс в размере 100% стоимости услуг, оказываемых *Оператором Системы*, в соответствии размером вознаграждения, установленным настоящим *Регламентом*.

По согласованию с *Оператором Системы* сроки, условия и порядок расчетов могут быть изменены.

13 Конфиденциальность информации

Под конфиденциальной информацией подразумевается любая информация и данные, представляющие собой коммерческую, служебную или иную тайну и персональные данные, доступ к которым ограничивается в соответствии с законодательством Российской Федерации, а также любая иная информация, помеченная как конфиденциальная или в письменном виде явно определенная в качестве таковой.

Оператор или *Абонент Системы*, получившие конфиденциальную информацию при исполнении настоящего Регламента, обязаны использовать ее исключительно в целях выполнения настоящего Регламента, охранять ее конфиденциальность и, если иное прямо не установлено законом, не раскрывать эту информацию, как полностью, так и частично, третьим лицам, за исключением работников или контрагентов, которым эта информация необходима для выполнения возложенных на них обязательств.

К конфиденциальной информации не относится информация, которая: была известна стороне, получившей информацию, до ее предоставления; самостоятельно созданная этой стороной до такого предоставления; стала общеизвестной не по причине действий или бездействия стороны, получившей информацию.

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

Персональные данные, содержащиеся в сертификатах *Пользователей УЦ*, на основании согласия *Пользователя УЦ* относятся к категории общедоступных. В сведениях об учетных записях пользователей *Абонентов Системы*, доступных *Абонентам Системы*, могут быть использованы только общедоступные персональные данные, полученные из сертификатов *Пользователей УЦ*.

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

14 Форс-мажор

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

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

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

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

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

В случае если невозможность полного или частичного исполнения Сторонами какого-либо обязательства по настоящему Регламенту обусловлена действием форс-мажорных обстоятельств и существует свыше одного месяца, то каждая из Сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства, и тогда ни одна из Сторон не вправе требовать возмещения возникших у нее убытков другой Стороной.

Приложение А

Подписной лист к Регламенту системы защищенного электронного юридически значимого документооборота «КристоСвязь-Веб» («КристоВеб»)

_____ (полное наименование организации с указанием организационно-правовой формы в соответствии с учредительными документами или ФИО для индивидуального предпринимателя/физического лица)

ИНН , КПП ,

ОГРН/ОГНИП

зарегистрированного по адресу: _____

(место нахождения, указанное в учредительных документах, или место регистрации для индивидуального предпринимателя/физического лица)

в лице _____

действующего на основании _____,

Полностью и безусловно присоединяется в порядке, предусмотренном статьей 428 Гражданского кодекса Российской Федерации, к Регламенту системы защищенного электронного юридически значимого документооборота «КристоСвязь-Веб» («КристоВеб») Общества с ограниченной ответственностью Научно-производственное предприятие «Ижинформпроект» (ООО НПП «Ижинформпроект») и является Стороной Регламента с момента регистрации настоящего подписного листа в реестре Оператора.

_____/_____/_____
(должность руководителя) (подпись) (Ф.И.О.)

«___» _____ 201__

М.П.

_____ заполняется Оператором Системы _____
Подписной лист получен и зарегистрирован «___» _____ 201__ № _____

М.П.

Представитель Оператора _____/_____/_____

15 Лист регистрации изменений

№ n/n	Дата, №	Редакция документа	Содержание изменения
1	21.10.2014 № 22	1.1	Учтены изменения, связанные с вводом в действие Федерального закона от 21.07.2014 № 248-ФЗ «О внесении изменений в Федеральный закон «Об исчислении времени».
2	08.09.2015 № 23	1.2	Предусмотрена возможность применения квалифицированных сертификатов, изготовленных аккредитованными удостоверяющими центрами, входящими в Перечень доверенных удостоверяющих центров Системы.
3	17.11.2016 № 17	1.3	Переоформлена лицензия ФСБ России