

Общество с ограниченной ответственностью
Научно-производственное предприятие «Ижинформпроект»

«СОГЛАСОВАНО»

Директор ООО «РИТ»
Кладуков И.А. /
«30» 08 2013 2.



«УТВЕРЖДАЮ»

Генеральный директор
ООО НПД «Ижинформпроект»
В.Н. Цыркин /
«30» 08 2013 2.



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

Технические условия
ТУ 5061-002-16908055-2013

Введены впервые
Срок действия: с 30.08.2013

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дудл.	Подп. дата
ТУ 5061-002-16908055-2013				
Изм	Лист	№ докум.	Подп.	Дата
Разраб.	Канторович			30.08.13
Пров.	Вагин			30.08.13
Т. контр.	Майшев			30.08.13
Н. контр.	Канторович			30.08.13
Утв.	Цыркин			
Система документооборота «КриптоСвязь-Веб»				
ООО Научно-производственное предприятие «Ижинформпроект»				
Лист	Лист	Листов		
Т	1	41		

Настоящие технические условия (далее — ТУ) распространяются на Систему защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» (далее — система «КриптоВеб» или Система).

Система «КриптоВеб» предназначена для организации электронного документооборота между предприятиями и организациями (далее — Абонентами) с использованием средств криптографической защиты информации (СКЗИ) для подписи и зашифрования передаваемых документов в адрес отправителя и получателя.

Особенностью системы «КриптоВеб» является наличие в маршруте документооборота третьей, гарантирующей стороны — Специализированного оператора связи (СОС), который регистрирует все переданные в системе документы, а также изменение их статуса (отправлен, доставлен, получен, подписан и т.д.)

Составной частью системы «КриптоВеб» является подсистема электронной отчетности, выполняющая доставку сведений установленного образца (отчетов) от абонентов системы в организации, осуществляющие прием отчетности на основании заключенных договоров или согласно действующему законодательству (т.н. Контролирующие органы).

Система «КриптоВеб» предназначена для передачи между абонентами, в том числе, персональных и конфиденциальных данных, за исключением сведений, составляющих государственную тайну.

Согласно ГОСТ Р ИСО/МЭК ТО 12182-2002 программная система (ПС) «КриптоВеб» относится к нижеследующим классам.

Таблица 1. Классификация ПС «КриптоВеб»

Наименование раздела	Наименование класса
Функция ПС	Электронный документооборот
Прикладная область информационной системы	Делопроизводство
Режим эксплуатации	Обработка данных в режиме реального времени
Масштаб ПС	Средний
Представление данных	Реляционный (для БД), объектный (для Web-кода), неструктурированный (для файлов пользователя)

Подп. дата		Система «КриптоВеб» предназначена для передачи между абонентами, в том числе, персональных и конфиденциальных данных, за исключением сведений, составляющих государственную тайну. Согласно ГОСТ Р ИСО/МЭК ТО 12182-2002 программная система (ПС) «КриптоВеб» относится к нижеследующим классам. Таблица 1. Классификация ПС «КриптоВеб» <table><tr><th>Наименование раздела</th><th>Наименование класса</th></tr><tr><td>Функция ПС</td><td>Электронный документооборот</td></tr><tr><td>Прикладная область информационной системы</td><td>Делопроизводство</td></tr><tr><td>Режим эксплуатации</td><td>Обработка данных в режиме реального времени</td></tr><tr><td>Масштаб ПС</td><td>Средний</td></tr><tr><td>Представление данных</td><td>Реляционный (для БД), объектный (для Web-кода), неструктурированный (для файлов пользователя)</td></tr></table>					Наименование раздела	Наименование класса	Функция ПС	Электронный документооборот	Прикладная область информационной системы	Делопроизводство	Режим эксплуатации	Обработка данных в режиме реального времени	Масштаб ПС	Средний	Представление данных	Реляционный (для БД), объектный (для Web-кода), неструктурированный (для файлов пользователя)
Наименование раздела	Наименование класса																	
Функция ПС	Электронный документооборот																	
Прикладная область информационной системы	Делопроизводство																	
Режим эксплуатации	Обработка данных в режиме реального времени																	
Масштаб ПС	Средний																	
Представление данных	Реляционный (для БД), объектный (для Web-кода), неструктурированный (для файлов пользователя)																	
Инв. № дубл.																		
Взам. инв. №																		
Подп. и дата																		
Инв. № подл.																		
Изм.	Лист	№ докум.	Подп.	Дата	ТУ 5061-002-16908055-2013													
					Лист 2													

Наименование раздела	Наименование класса
Исходный язык	Объектно-ориентированные: C#, PHP, JavaScript
Критичность	Защита конфиденциальной информации, защита персональных данных
Класс пользователя	Обычный (уровень подготовки делопроизводителя)
Стабильность ПС	Постоянное внесение изменений
Готовность программно-го продукта	Готовый коммерческий
Использование программных данных	Для множества пользователей
Требуемые рабочие характеристики	Емкость данных: высокая Время отклика: среднее Производительность: высокая
Требование защиты:	Защита от НСД: сильная Контрольный след: средняя Защита программ и данных: сильная
Требование надежности:	Завершенность: высокая Отказоустойчивость: высокая Восстанавливаемость: средняя
Вычислительная система и среда:	см. разделы 1.7, 1.8 настоящих ТУ
Требование к вычислительным ресурсам:	см. разделы 1.7, 1.8 настоящих ТУ

Наименования «КриптоСвязь-Веб» и «КриптоВеб» являются синонимами.

Пример записи Системы в технической документации:

Система документооборота «КриптоВеб», ТУ 5061-002-16908055-2013

Подп. дата			Контрольный след:	средняя						
		Требование надежности:	Завершенность:	высокая						
			Отказоустойчивость:	высокая						
			Восстанавливаемость:	средняя						
Инв. № дубл.	Инв. №	Вычислительная система и среда:	см. разделы 1.7, 1.8 настоящих ТУ							
		Требование к вычислительным ресурсам:	см. разделы 1.7, 1.8 настоящих ТУ							
Наименования «КриптоСвязь-Веб» и «КриптоВеб» являются синонимами.										
Пример записи Системы в технической документации:										
Система документооборота «КриптоВеб», ТУ 5061-002-16908055-2013										
Инв. № подл.		Изм	Лист	№ докум	Подп.					
						Дата	ТУ 5061-002-16908055-2013	Лист		
	3									

СОДЕРЖАНИЕ

1	Технические требования.....	5
1.1	Требования к субъектам системы документооборота	5
1.2	Требования к отправленным в системе документооборота	7
1.3	Требования к автоматизируемым транзакциям документооборота	10
1.4	Требования к функционалу рабочего места пользователя	11
1.5	Требования к последовательности отправки документов	13
1.6	Требования к функционалу рабочего места спецоператора	14
1.7	Технические требования к рабочему месту пользователя	15
1.8	Технические требования к серверу системы.....	16
2	Требования безопасности	18
2.1	Требования к информационной безопасности	18
3	Требования охраны окружающей среды	21
4	Правила приемки.....	22
5	Методы контроля.....	23
6	Транспортирование и хранение.....	24
7	Указания по эксплуатации.....	25
8	Гарантии изготовителя.....	26
ПРИЛОЖЕНИЕ А (обязательное) Термины и определения		27
A.1	Информационно-телекоммуникационная система и ее участники.....	27
A.2	Удостоверяющий центр	27
A.3	Электронные подписи (ЭП)	29
A.4	Сертификаты ключей проверки электронной подписи	30
ПРИЛОЖЕНИЕ Б (обязательное) Схемы транзакций документооборота		32
B.1	Транзакция №1 «Абонент — Контролирующий орган»	32
B.2	Транзакция №2 «Абонент А — Абонент Б» (без требования подписи получателя).....	35
B.3	Транзакция №3 «Абонент А — Абонент Б» (с требованием подписи получателя).....	37
ПРИЛОЖЕНИЕ В (справочное) Нормативные ссылки		40

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата	6	Транспортирование и хранение.....	24
					7	Указания по эксплуатации.....	25
					8	Гарантии изготовителя.....	26
					ПРИЛОЖЕНИЕ А (обязательное) Термины и определения		27
					A.1	Информационно-телекоммуникационная система и ее участники.....	27
					A.2	Удостоверяющий центр	27
					A.3	Электронные подписи (ЭП)	29
					A.4	Сертификаты ключей проверки электронной подписи	30
					ПРИЛОЖЕНИЕ Б (обязательное) Схемы транзакций документооборота		32
					B.1	Транзакция №1 «Абонент — Контролирующий орган».....	32
					B.2	Транзакция №2 «Абонент А — Абонент Б» (без требования подписи получателя).....	35
					B.3	Транзакция №3 «Абонент А — Абонент Б» (с требованием подписи получателя).....	37
					ПРИЛОЖЕНИЕ В (справочное) Нормативные ссылки		40

Система защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») должна соответствовать требованиям настоящих технических условий.

Информационная система «КриптоВеб» должна быть предназначена для организации защищенного, юридически значимого электронного документооборота с участием следующих субъектов: абонент, контролирующий орган, специализированный оператор связи (далее — «Участники»). Каждый участник документооборота должен быть представлен набором физических лиц — пользователей системы.

а) *Пользователь* — физическое лицо, зарегистрированное в системе в установленном порядке с определенным набором полномочий, имеющее действующий сертификат ключа проверки электронной подписи, по которому оно аутентифицируется системой. Каждый пользователь принадлежит ровно одному участнику электронного документооборота. Незарегистрированные в системе лица доступ к Системе не имеют. В случае, если физическое лицо действует в интересах нескольких участников документооборота, оно регистрируется в Системе несколько раз и получает несколько сертификатов ключа проверки электронной подписи.

Пользователи системы имеют доступ к входящей, исходящей и отправленной корреспонденции только своего почтового ящика, т.к. отправления системы являются зашифрованными. При необходимости создания отправок для нескольких участников (пользователей участников) корреспонденция шифруется в адрес каждого из участников (пользователей участников).

б) *Абонент* — типовой участник электронного документооборота, представляет собой организацию, индивидуального предпринимателя или физическое лицо. Каждый абонент может получать один или несколько сертификатов ключа проверки электронной подписи по количеству пользователей (сотрудников), вовлеченных в процесс электронного документооборота. Работа

абонента в системе ограничивается правами доступа к потокам документов и направлению документооборота (входящий документ, исходящий документ);

в) *Контролирующий орган* (далее — КО) — особый участник документооборота, являющийся субъектом приема документов установленного образца (далее — Отчетов) на основании заключенных договоров либо согласно действующему законодательству, а также выполняющий обработку, контроль представленных Абонентами сведений и уведомление их о статусе переданных Отчетов;

г) *Специализированный оператор связи* (далее — СОС, Оператор системы или Оператор) — оператор электронного документооборота, функциями которого являются:

- регистрация участников документооборота в системе;
- регистрация пользователей участников документооборота, а также их сертификатов ключа проверки электронной подписи;
- назначение прав доступа и тарифных планов для участников документооборота;
- обеспечение транспорта писем между участниками системы;
- подтверждение даты и времени передачи писем между участниками;
- автоматическое формирование уведомлений, фиксирующих перемещение писем, квитанций и других отправок между участниками, выдача текущего статуса письма;
- разрешение спорных ситуаций между участниками документооборота.

д) *Группа пользователей* — именованное множество пользователей одного участника документооборота (например, «общий отдел», «бухгалтерия», «руководители отделов», «рабочая группа по проекту», «механизированный цех», «Первомайский филиал банка» и др.)

Группы пользователей могут содержать другие группы пользователей. Один и тот же пользователь может входить в одну или несколько групп либо не входить ни в одну из них.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата	– подтверждение даты и времени передачи писем между участниками; – автоматическое формирование уведомлений, фиксирующих перемещение писем, квитанций и других отправок между участниками, выдача текущего статуса письма; – разрешение спорных ситуаций между участниками документооборота.
					д) <i>Группа пользователей</i> — именованное множество пользователей одного участника документооборота (например, «общий отдел», «бухгалтерия», «руководители отделов», «рабочая группа по проекту», «механизированный цех», «Первомайский филиал банка» и др.)
					Группы пользователей могут содержать другие группы пользователей. Один и тот же пользователь может входить в одну или несколько групп либо не входить ни в одну из них.

					ТУ 5061-002-16908055-2013	Лист
						6
Изм.	Лист	№ докум.	Подп.	Дата		

Группы пользователей используются:

- при указании получателя письма, например, «ООО «Знамя», общий отдел»; в этом случае перед отправкой группа разыменовывается системой и преобразуется в поименный список получателей;
- при указании полномочий на просмотр отправок участника документооборота; в этом случае пользователь может просматривать список не только входящих (исходящих) отправок, адресованных ему лично, но и список отправок группы пользователей, с указанием лиц, в адрес которых зашифрованы сами отправления. Например, пользователь имеет доступ к папкам «Входящие», «Исходящие» и «Входящие (бухгалтерия)»; следовательно, он может просматривать, какие документы поступили в бухгалтерию, однако доступ к самому документу он сможет получить только при наличии соответствующего сертификата ключа проверки электронной подписи.

1.2 Требования к отправлениям в системе документооборота

Система «КриптоВеб» в схемах документооборота должна оперировать следующими типами отправлений:

а) *Письмо* — подписанный, зашифрованный исходящий документ с вложениями (количество вложений ограничено и определяется СОС) от любого из участников документооборота. Схемы прохождения писем описываются транзакциями, которые определяют порядок взаимодействия участников документооборота при движении письма. Письмом, в том числе, может являться и отчет, передаваемый абонентом в контролирующий орган (так называемый неформализованный обмен с контролирующим органом). Количество документов во вложениях при подсчете трафика системой во внимание не принимается; действует правило «одно письмо — одно отправление». Письмо является основным отправлением в системе документооборота.

Письмо подписывается отправителем и зашифровывается в адреса отправителя и получателя (получателей). Письмо состоит из следующих информационных блоков (см. Приложение Б):

- Открытые поля письма (включая заголовок письма);
- Текст письма;
- Вложения письма.

Каждый из блоков письма подписывается каждой стороной документооборота в отдельности: заголовок и открытые поля подписываются напрямую, остальные информационные блоки могут быть подписаны участником документооборота только после расшифрования. Механизм «подпись на подпись» (заверяющая подпись) в системе не применяется. Механизм «совмещенная подпись с информационным блоком» также не применяется.

Все блоки, кроме заголовка и открытых полей, зашифровываются в адрес отправителя и одного или нескольких получателей. Если в качестве получателя указана группа пользователей, она разыменовывается перед отправкой и преобразуется в поименный список получателей, после чего выполняется зашифрование и отправка.

С точки зрения пользователя системы подпись и шифрование всех информационных блоков осуществляется одной технологической операцией («подписать и зашифровать»/«подписать и отправить»).

б) *Форма* — особый вид письма, отличающийся наличием автоматически создаваемого вложения с закрытыми, т.е. зашифрованными, полями (заранее описанного подмножества XML). Вложение формы может прикрепляться из внешнего файла или генерироваться автоматически на основе информации, введенной пользователем непосредственно во время работы системы. Наличие автоматического вложения не исключает возможности присоединять другие вложения к письму.

Форма предназначена для обмена формализованными документами с контролирующими органами. Каждый ҚО имеет свой набор отчетности, которая, в свою очередь, описывается одной или несколькими формами.

Правила подписания и зашифрования формы те же, что и для письма.

в) *Протокол* — подписанный, зашифрованный исходящий документ с вложениями (количество вложений ограничено и определяется СОС) от контролирующего органа абоненту, отправившему письмо с отчетом. Протокол может быть как положительный (отчет принят контролирующим органом), так и отрицательный (отчет не принят контролирующим органом). Статус протокола отражается в его открытых полях.

Правила подписания и зашифрования те же, что и для письма.

г) *Отказ* — подписанный, зашифрованный исходящий документ с вложениями от любого из участников документооборота; высылается только

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата	ляться из внешнего файла или генерироваться автоматически на основе информации, введенной пользователем непосредственно во время работы системы. Наличие автоматического вложения не исключает возможности присоединять другие вложения к письму. Форма предназначена для обмена формализованными документами с контролирующими органами. Каждый КО имеет свой набор отчетности, которая, в свою очередь, описывается одной или несколькими формами. Правила подписания и зашифрования формы те же, что и для письма. в) <i>Протокол</i> — подписанный, зашифрованный исходящий документ с вложениями (количество вложений ограничено и определяется СОС) от контролирующего органа абоненту, отправившему письмо с отчетом. Протокол может быть как положительный (отчет принят контролирующим органом), так и отрицательный (отчет не принят контролирующим органом). Статус протокола отражается в его открытых полях. Правила подписания и зашифрования те же, что и для письма. г) <i>Отказ</i> — подписанный, зашифрованный исходящий документ с вложениями от любого из участников документооборота; высылается только																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																											

Правила подписания и зашифрования отказа те же, что и для письма.

Квитанция подписывается ключом отправителя и является открытым документом (без шифрования). Все поля квитанции являются открытыми и описаны в схемах транзакций.

ж) *Уведомление* — открытый подписанный документ, автоматически создаваемый специализированным оператором связи в процессе движения вторичных отправок: протоколов, отказов, квитанций. Уведомление подтверждает дату и время прохождения отправления через сервер и хранится на сервере спецоператора до востребования его любым из участников документооборота, который относится к данной транзакции. Уведомление подписывается только специализированным оператором связи.

з) *Отправленная электронная подпись* — дополнительный файл, содержащий электронную подпись на ранее сформированное отправление (на пример, подпись второй стороны на договоре, подпись контролирующего органа на письме, содержащем отчет). Данное действие не предусматривает повторную отправку и повторное сохранение исходного отправления на сервере, ЭП лишь прикрепляется к тому отправлению, на которое она сформирована. Как таковым отправлением (с присвоением кода отправления) не является.

1.3 Требования к автоматизируемым транзакциям документооборота

В системе «КриптоВеб» должны присутствовать следующие автоматизированные транзакции электронного документооборота:

Таблица 2. Перечень транзакций документооборота.

№	Наименование	Описание транзакции
1	Абонент – Контролирующий орган	Документооборот совершается между абонентом и контролирующим органом. Абонент-отправитель письма выбирает систему документооборота контролирующего органа, в который он сдает отчетность (например, отчетность в Энергосбыт). Функционально отправка происходит через третью сторону – спецоператора, который является гарантом передачи сообщения от Отправителя Получателю. Контролирующий орган, со своей стороны, в установленные сроки обязан отправить Отправителю Протокол результата проверки содержимого письма. Протокол результата также проходит через спецоператора связи.
2	Абонент А – Абонент Б (без требования подписи получателя)	Документооборот совершается между абонентами. Абонент А (Отправитель письма) выбирает из справочника абонента Б (Получателя). Функционально отправка происходит через третью сторону – спецоператора, который является гарантом передачи сообщения от Отправителя Получателю. После завершения отправки письма документооборот завершается.
3	Абонент А – Абонент Б (с требованием подписи получателя)	Документооборот совершается между абонентами. Абонент А (Отправитель письма) выбирает из справочника абонента Б (Получателя). Функционально отправка происходит через третью сторону – спецоператора, который является гарантом передачи сообщения от Отправителя Получателю. После завершения отправки письма абонент Б обязан подписать исходное письмо либо направить абоненту А мотивированный отказ. Документ, свидетельствующий об отказе, направляется через спецоператора связи.

Подп. дата	Инв. № дубл.	Взам. инв. №	Подп. и дата	Инв. № подл.
Изм.	Лист	№ докум.	Подп.	Дата
ТУ 5061-002-16908055-2013				Лист
				10

При работе с системой «КриптоСвязь» любой из участников документооборота получает возможность работать с адресной книгой и отправлениями в системе, а также просматривать структуру абонента (то есть видеть список пользователей абонента, назначенные группы пользователей и т.д.) Базовая конфигурация рабочего места назначается спецоператором связи на основании тарифного плана, после этого каждый пользователь системы (т.е. владелец сертификата ключа проверки электронной подписи) может настраивать рабочее место по своему усмотрению.

1.4.1 *Адресная книга* содержит перечень зарегистрированных участников документооборота, в том числе временно или постоянно отключенных от системы спецоператором (на основании окончания действия тарифного плана, задолженности абонента или официального письма абонента спецоператору). Каждый участник адресной книги должен быть помечен статусом (действующий, временно недоступен, доступен только на прием писем, отключен и т.д.)

Абоненты и контролирующие органы должны визуально находиться в различных категориях адресной книги. В случае контролирующего органа статус также может означать, что данный контролирующий орган недоступен, поскольку услуга сдачи отчетности в этот контролирующий орган не подключена (не оплачена).

Каждый пользователь участника системы на своем рабочем месте может настроить папки для автоматической и/или ручной сортировки (раскладывания по папкам) записей о других участниках системы. Автоматическая сортировка осуществляется на основании значений открытых полей, например, в папку «Воткинск» автоматически попадут все абоненты, которые в открытом поле «Город» выставили соответствующее значение; эта папка будет автоматически пополняться вновь зарегистрированными абонентами. Ручная сортировка производится самим пользователем, скажем, папка «Мои контрагенты», как правило, заполняется вручную путем «перетаскивания» ярлыков абонентов адресной книги.

Один и тот же участник (также и пользователь) документооборота может одновременно входить в несколько папок. Папки могут быть вложены друг в друга. Условия для автоматической сортировки могут определяться

специализированным оператором связи при присвоении конфигурации абонента, доопределяться внутренними приказами участника документооборота и модифицироваться самим конечным пользователем. Пользователь при работе с конфигурацией не может превышать те права доступа, которые были установлены спецоператором связи на основании тарифного плана.

1.4.2 *Папка отправлений* состоит из разделов «Отчеты», «Письма». Раздел «Отчеты» содержит стандартные папки: «Отправленные», «Доставленные», «Проверенные», «Принятые отчеты», «Непринятые отчеты», «Архив отчетов». Раздел «Письма» содержит стандартные папки: «Входящие», «Отправленные», «Подписанные», «На подпись», «Все письма», «Архив писем».

Каждое письмо содержит заголовок, открытые поля, тело письма, перечень вложений и электронную подпись отправителя. Перечень открытых полей для писем по транзакциям №№1 – 3 определяет спецоператор связи. Особым открытым полем является поле «Статус», значение которого изменяется в зависимости от пункта транзакции, где письмо находится в настоящий момент. Помимо этого, для каждого вложения имеется поле «Примечание», которое заполняет отправитель.

Так же, как и в адресной книге, пользователь на своем рабочем месте может создавать папки для автоматической и/или ручной сортировки (раскладывания) писем в них на основании открытых полей писем, например «Договора», «Документы, требующие подписания», «Отчеты Можгинского филиала», «Важные документы» и др.

Один и тот же документ может одновременно находиться в нескольких папках. Папки могут быть вложены друг в друга. Условия для автоматической сортировки могут определяться специализированным оператором связи при присвоении конфигурации абонента, доопределяться внутренними приказами участника документооборота и модифицироваться самим конечным пользователем. Пользователь при работе с конфигурацией не может превышать те права доступа, которые были установлены спецоператором связи на основании тарифного плана.

Письмо должно визуально отображать свой статус на основании определенном спецоператором перечня статусов (письмо отправлено, письмо получено, содержимое письма проверено, передача завершена и т.д.) Текстовый статус письма должен дублироваться соответствующей пиктограммой. Дополнительно, при выборе соответствующего режима, пользователь должен

Инв. № подл.	Подп. и дата				Взам. инв. №	Инв. № дубл.				Подп. дата														
Так же, как и в адресной книге, пользователь на своем рабочем месте может создавать папки для автоматической и/или ручной сортировки (раскладывания) писем в них на основании открытых полей писем, например «Договора», «Документы, требующие подписания», «Отчеты Можгинского филиала», «Важные документы» и др. Один и тот же документ может одновременно находиться в нескольких папках. Папки могут быть вложены друг в друга. Условия для автоматической сортировки могут определяться специализированным оператором связи при присвоении конфигурации абонента, доопределяться внутренними приказами участника документооборота и модифицироваться самим конечным пользователем. Пользователь при работе с конфигурацией не может превышать те права доступа, которые были установлены спецоператором связи на основании тарифного плана. Письмо должно визуально отображать свой статус на основании определенном спецоператором перечня статусов (письмо отправлено, письмо получено, содержимое письма проверено, передача завершена и т.д.) Текстовый статус письма должен дублироваться соответствующей пиктограммой. Дополнительно, при выборе соответствующего режима, пользователь должен																								
Изм.					Лист					№ докум.					Подп.					Дата				
ТУ 5061-002-16908055-2013												Лист												
												12												

1.4.3 Структура абонента относится к абоненту в целом и для всех рабочих мест конечных пользователей одинакова. Она позволяет:

- 1.4.4 Рабочее место пользователя должно позволять осуществлять поиск контрагента или письма по любым его полям с возможностью комбинировать условия поиска. При поиске пользователь может выбрать, в какой папке (папках) его осуществлять (либо выполнять поиск по всем папкам).

Для того, чтобы отправить письмо через систему «КриптоВеб», пользователь системы обязан выполнить следующую последовательность действий:

- | | | | | | | |
|------|------|----------|-------|------|---------------------------|------|
| | | | | | ТУ 5061-002-16908055-2013 | Лист |
| Изм. | Лист | № докум. | Подп. | Дата | | 13 |

- указать конкретные ФИО получателей либо групп получателей, в случае, если участник документооборота имеет несколько пользователей;
- заполнить поля письма (возможно наличие необязательных полей);
- написать текст тела письма;
- присоединить вложения, возможно, с комментариями;
- указать, требуется ли обязательное подписание документа получателем (для транзакций №№2 – 3);
- выполнить одним действием подписание и шифрование документа в адрес получателей.

С момента прохождения письма через сервер специализированного оператора связи письмо считается созданным и имеющим дату/время, о чем СОС отправляет соответствующее подтверждение согласно схемам транзакций.

Получателем письма не может являться временно или постоянно отключенный пользователь. Получателем отчета по Транзакции №1 не может являться контролирующий орган, услуги взаимодействия с которым пользователем не оплачены согласно действующему тарифному плану.

Перед подписанием и шифрованием документа во избежание ошибок система должна в явном виде указать пользователю, каким именно сертификатом ключа проверки электронной подписи будет выполнено подписание (указать полностью ФИО и название организации, а также предоставить ссылку на просмотр сертификата).

Для отправки счетов-фактур система «КриптоВеб» должна быть интегрирована с общероссийской системой электронного документооборота «Диадок» (разработчик ЗАО ПФ «СКБ Контур», г. Екатеринбург). Интеграция осуществляется с использованием открытого API системы «Диадок».

1.6 Требования к функционалу рабочего места спецоператора

Сервер специализированного оператора связи должен обеспечивать работу системы в автоматическом режиме, а также иметь возможность настройки системы.

Подп. дата					система должна в явном виде указать пользователю, каким именно сертификатом ключа проверки электронной подписи будет выполнено подписание (указать полностью ФИО и название организации, а также предоставить ссылку на просмотр сертификата).
Инв. № дубл.					Для отправки счетов-фактур система «КриптоВеб» должна быть интегрирована с общероссийской системой электронного документооборота «Диадок» (разработчик ЗАО ПФ «СКБ Контур», г. Екатеринбург). Интеграция осуществляется с использованием открытого API системы «Диадок».
Взам. инв. №					1.6 Требования к функционалу рабочего места спецоператора Сервер специализированного оператора связи должен обеспечивать работу системы в автоматическом режиме, а также иметь возможность настройки системы.
Подп. и дата					
Инв. № подл.					

Изм.	Лист	№ докум.	Подп.	Дата	ТУ 5061-002-16908055-2013	Лист
						14

- регистрацию абонентов в системе с заполнением части обязательных полей (недоступную для редактирования клиентом, например, ИНН);
- регистрацию пользователей по сертификату ключа проверки электронной подписи в системе с заполнением части обязательных полей из сертификата;
- просмотр активности абонентов системы (вход в систему, отправленные письма в системе за период);
- изменение статуса подключения абонентов с фиксацией даты изменения статуса абонента.

- просмотр журнала всех отправок системы вне зависимости от отправителя и получателя;
- просмотр открытых полей всех отправок системы;
- поиск, фильтрацию и сортировку журнала отправок системы, по некоторым полям журнала;
- просмотр и печать любых подтверждений, уведомлений, квитанций, передаваемых в открытом виде.

1.6.3 *Журнал работы* выполняет учет всех выполненных операций пользователями спецоператора. Система должна вести протокол, какой пользователь в какое время выполнил какие операции в любом из вышеприведенных модулей.

1.7 Технические требования к рабочему месту пользователя

Для развертывания системы «КриптоВеб» на рабочем месте конечного пользователя требуются следующие технические и программные компоненты.

1.7.1 Техническая конфигурация рабочего места:

- Архитектура компьютера: IBM-совместимая;
- Процессор: 32-х или 64-х разрядный Intel-совместимый процессор тактовой частотой не ниже рекомендуемых требований используемой операционной системы (ОС);

- Оперативная память: не ниже рекомендуемых требований ОС;
- Свободное дисковое пространство: не ниже 1 ГБ;
- Сеть: наличие проводного или беспроводного сетевого соединения с выходом в сеть Интернет на скорости не менее 256 Кб/с;
- Дисплей: цветной, разрешение не менее 1024x768 пикселей, глубина цвета не менее 24 бит;
- Порты ввода/вывода: свободный порт USB;
- Периферия: рекомендуется наличие принтера для печати передаваемых документов пользователей и служебных документов системы.

1.7.2 Программная конфигурация рабочего места:

- Операционная система: Microsoft Windows XP SP3, Vista, 7, 8;
- Исполняемая среда: Microsoft .Net Framework версии 3.5;
- Интернет-обозреватель (браузер) Microsoft Internet Explorer версии не ниже 7.0;
- Средство криптографической защиты информации (СКЗИ): КриптоПро CSP 3.6;
- Драйверы электронного идентификатора (eToken, Рутокен) в случае, если ключи электронной подписи выпущены на USB-токене.

1.8 Технические требования к серверу системы

Для развертывания сервера документооборота системы «КриптоВеб» требуются следующие технические и программные компоненты.

1.8.1 Техническая конфигурация сервера

- Архитектура компьютера: IBM-совместимая;
- Процессор: 64-х разрядный Intel-совместимый процессор тактовой частотой не ниже 3 ГГц;
- Количество ядер процессора: не менее четырех;
- Оперативная память: не менее 8 Гб;
- Дисковое пространство: не ниже 2 ТБ с расширением по мере накопления документов в системе документооборота;
- Сеть: наличие выделенного проводного канала связи на скорости не менее 20 Мб/с;
- Дисплей: не требуется;

Подп. дата		чае, если ключи электронной подписи выпущены на USB-токене.				
Инв. № дубл.		1.8 Технические требования к серверу системы				
Взам. инв. №		Для развертывания сервера документооборота системы «КриптоВеб» требуются следующие технические и программные компоненты.				
Подп. и дата		1.8.1 Техническая конфигурация сервера				
Инв. № подл.		– Архитектура компьютера: IBM-совместимая; – Процессор: 64-х разрядный Intel-совместимый процессор тактовой частотой не ниже 3 ГГц; – Количество ядер процессора: не менее четырех; – Оперативная память: не менее 8 Гб; – Дисковое пространство: не ниже 2 ТБ с расширением по мере накопления документов в системе документооборота; – Сеть: наличие выделенного проводного канала связи на скорости не менее 20 Мб/с; – Дисплей: не требуется;				
		ТУ 5061-002-16908055-2013				
		Лист				
		16				
		Изм.	Лист	№ докум.	Подп.	Дата

- Порты ввода-вывода: не требуются;
- Периферия: не требуется.

1.8.2 Программная конфигурация сервера

- Операционная система Windows Server 2008 R2;
- Исполняемая среда веб-компонентов сервера системы «КриптоВеб»: Microsoft .Net Framework версии 3.5;
- Исполняемая среда ядра сервера системы «КриптоВеб»: PHP версии 5.3;
- Web-сервер: Microsoft Internet Information Services версии 7.0;
- СУБД: MySQL Server версии 5.5;
- Средство криптографической защиты информации (СКЗИ): КриптоПро CSP 3.6.

[illegible]

2.1 Требования к информационной безопасности

Сертификат ключа проверки электронной подписи признается изданным УЦ, если подтверждена подлинность электронной подписи (ЭП) издателя сертификата ключа подписи с использованием сертификата уполномоченного лица УЦ.

- формирование электронной подписи электронного документа осуществляется с использованием средств электронной подписи;
- формирование электронной подписи должно осуществляться только с использованием действующего закрытого ключа подписи;
- подтверждение подлинности электронной подписи электронного документа осуществляется с использованием средств электронной подписи;
- при подтверждении подлинности электронной подписи должна осуществляться проверка, что электронная подпись в электронном документе равнозначна собственноручной (должно осуществляться выполнение условий равнозначности электронной подписи собственноручной), и только после признания электронной подписи равнозначной собственноручной, может быть осуществлено исполнение данного электронного документа.

- создание электронных документов осуществляется надлежаще уполномоченными лицами;
- сертификат ключа проверки электронной подписи уполномоченного на совершение указанного действия лица должен содержать сведения, ус-

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата	существляется с использованием средств электронной подписи; – формирование электронной подписи должно осуществляться только с использованием действующего закрытого ключа подписи; – подтверждение подлинности электронной подписи электронного документа осуществляется с использованием средств электронной подписи; – при подтверждении подлинности электронной подписи должна осуществляться проверка, что электронная подпись в электронном документе равнозначна собственноручной (должно осуществляться выполнение условий равнозначности электронной подписи собственноручной), и только после признания электронной подписи равнозначной собственноручной, может быть осуществлено исполнение данного электронного документа. 2.1.2 Формирование электронного документа осуществляется с учетом следующих требований: – создание электронных документов осуществляется надлежаще уполномоченными лицами; – сертификат ключа проверки электронной подписи уполномоченного на совершение указанного действия лица должен содержать сведения, ус-
Изм.	Лист	№ докум.	Подп.	Дата	ТУ 5061-002-16908055-2013
					Лист 18

- порядок применения участниками электронной подписи в электронных документах определяется Оператором системы.

а) ключа проверки электронной подписи (открытый ключ) действует на определенный момент времени (действительный сертификат), если:

- сертификат изготовлен доверенным Удостоверяющим центром;
- подтверждена подлинность электронной подписи уполномоченного лица доверенного Удостоверяющего центра;
- наступил момент времени начала действия сертификата;
- срок действия сертификата не истек;
- сертификат отсутствует в актуальном списке отозванных сертификатов доверенного Удостоверяющего центра;

- наступил момент времени начала действия закрытого ключа;
- срок действия закрытого ключа не истек;
- сертификат ключа проверки электронной подписи, соответствующий данному закрытому ключу, действует на данный момент времени (является действительным);

1) на момент формирования электронной подписи электронного документа:

- ключа проверки электронной подписи (открытый ключ), относящийся к электронной подписи, являлся действительным;
- ключ электронной подписи (закрытый ключ), соответствующий указанному сертификату, являлся действительным;

Изм.	Лист	№ докум.	Подп.	Дата	Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата
– наступил момент времени начала действия закрытого ключа; – срок действия закрытого ключа не истек; – сертификат ключа проверки электронной подписи, соответствующий данному закрытому ключу, действует на данный момент времени (является действительным); в) Электронная подпись в электронном документе действительна при одновременном соблюдении следующих условий: 1) на момент формирования электронной подписи электронного документа: – ключа проверки электронной подписи (открытый ключ), относящийся к электронной подписи, являлся действительным; – ключ электронной подписи (закрытый ключ), соответствующий указанному сертификату, являлся действительным;									
					ТУ 5061-002-16908055-2013				
Изм.	Лист	№ докум.	Подп.	Дата	Лист 19				

- 2) подтверждена подлинность электронной подписи электронного документа на сертификате, относящемся к данной электронной подписи;
- 3) электронная подпись электронного документа сформирована в соответствии со сведениями, указанными в сертификате ключа подписи: сертификат ключа проверки электронной подписи в расширениях Extended Key Usage, Certificate Policies содержит области использования сертификата и ключа электронной подписи, устанавливающие право владельца данного сертификата подписывать соответствующие электронные документы.

[illegible]

3 ТРЕБОВАНИЯ ОХРАНЫ ОКРУЖАЮЩЕЙ СРЕДЫ

Требования охраны окружающей среды к программному продукту Система защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») не предъявляются.

[illegible]

4 ПРАВИЛА ПРИЕМКИ

Система защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») при производстве должна проходить контроль согласно требованиям раздела 1 настоящего ТУ, а также на соответствие следующим стандартам:

- ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование.
- ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.
- ГОСТ Р 53898-2010. Системы электронного документооборота. Взаимодействие систем управления документами. Требования к электронному сообщению.

По окончании приемо-сдаточных испытаний сервер Системы вводится в эксплуатацию Специализированным оператором связи.

Установочные комплекты рабочих мест пользователей по окончании приемо-сдаточных испытаний размещаются на общедоступном Интернет-ресурсе. Дополнительная проверка цифровых копий установочных комплектов для программы для ЭВМ не требуется.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата	установочные комплекты рабочих мест пользователей по окончании приемо-сдаточных испытаний размещаются на общедоступном Интернет- ресурсе. Дополнительная проверка цифровых копий установочных комплектов для программы для ЭВМ не требуется.	
Изм.	Лист	№ докум.	Подп.	Дата	ТУ 5061-002-16908055-2013	Лист
						22

5 МЕТОДЫ КОНТРОЛЯ

Контроль выпуска системы защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») проводится при проведении приемо-сдаточных испытаний продукта.

Дальнейший контроль над соответствием требованиям настоящего ТУ производится во время дальнейших обновлений системы и развития ее функциональных возможностей.

Специальных методов контроля для данного программного продукта не предусмотрено.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата
Изм.	Лист	№ докум.	Подп.	Дата
ТУ 5061-002-16908055-2013				Лист
				23

6 ТРАНСПОРТИРОВАНИЕ И ХРАНЕНИЕ

Система защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») с точки зрения транспортирования и хранения состоит из двух основных компонентов:

а) *Серверный компонент системы* находится исключительно у Специализированного оператора связи, транспортировке и распространению не подлежит;

б) *Встраиваемый компонент системы* (рабочее место пользователя) распространяется путем публикации в вычислительной сети Интернет согласно ГОСТ 15971-90, ГОСТ 19781-90, ГОСТ 29099-91 (стандарты RFC 1122, RFC 2616).

Хранение компонентов системы «КриптоВеб» осуществляется согласно ГОСТ Р ИСО/МЭК 14764-2002.

[illegible]

7 УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

Для эксплуатации Системы защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») требуется соблюдение технических требований к рабочему месту, изложенных в разделе 1.7 настоящих ТУ.

Подключение к Системе осуществляется путем:

- заключения договора присоединения к Регламенту Удостоверяющего центра InfoTrust ООО НПП «Ижинформпроект»;
- получения в установленном порядке сертификата ключа проверки электронной подписи в УЦ InfoTrust ООО НПП «Ижинформпроект» либо в доверенном УЦ;
- заключения Лицензионного договора со специализированным оператором связи по организации защищенного электронного документооборота через Интернет в системе «КриптоСвязь», с выбором тарифного плана, включающего документооборот в системе «КриптоВеб».

Эксплуатация Системы «КриптоВеб» осуществляется согласно Руководству по эксплуатации 5061-002-16908055-2013 РЭ.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата					
Изм.	Лист	№ докум.	Подп.	Дата					
					ТУ 5061-002-16908055-2013				
					Лист				
					25				

8 ГАРАНТИИ ИЗГОТОВИТЕЛЯ

Изготовитель гарантирует соответствие Системы защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») требованиям настоящих технических условий при соблюдении условий эксплуатации.

Гарантийный срок эксплуатации составляет 24 месяца с момента ввода в эксплуатацию рабочего места конечного пользователя.

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата
Изм.	Лист	№ докум.	Подп.	Дата
ТУ 5061-002-16908055-2013				Лист
				26

Термины и определения

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.

A.1 Информационно-телекоммуникационная система и ее участники

Информационно-телекоммуникационная система (Система) — корпоративная информационная система, устройтелем которой является Организатор Системы, основанная на технологии Инфраструктуры открытых ключей (ИОК, PKI), в которой используются сертификаты ключей проверки электронной подписи, изготовленные Удостоверяющим центром, и предназначенная для оказания услуг в области использования электронной подписи/шифрования данных и телематических услуг связи пользователям Системы.

Организатор Системы (Оператор, Владелец) — устроитель корпоративной информационной системы с применением электронной подписи, организующий и обеспечивающий предоставление услуг пользователям Системы.

Участники электронного взаимодействия — осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане.

А.2 Удостоверяющий центр

Удостоверяющий центр — удостоверяющий центр InfoTrust ООО НПП «Ижинформпроект», осуществляющий выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом «Об элек-

тронной подписи» непосредственно и/или через регистрационные отделения удостоверяющего центра.

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 следующую информацию:

- 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 удостоверяющее 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 ключей проверки электронной подписи 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.

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

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.

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.

А.3 Электронные подписи (ЭП)

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

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата	ТУ 5061-002-16908055-2013					Лист 29
Изм.	Лист	№ докум.	Подп.	Дата						

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

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

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.

А.4 Сертификаты ключей проверки 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

	Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата
Сертификат ключа проверки электронной подписи (<i>сертификат</i>) — 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. <i>Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат)</i> — 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). <i>Сертификат в форме документа на бумажном носителе</i> — 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					
Изм.	Лист	№ докум.	Подп.	Дата	
					ТУ 5061-002-16908055-2013
					Лист 30

удостоверяющего центра для подписи сертификата в качестве аналога собственноручной подписи, равнозначного собственноручной подписи.

Список отозванных (аннулированных) сертификатов — 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.

Псевдоним владельца сертификата — вымышленное имя владельца сертификата, которое он сознательно и легально принимает для регистрации в удостоверяющем центре.

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

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.

					ТУ 5061-002-16908055-2013	Лист
Изм	Лист	№ докум.	Подп.	Дата		31

ПРИЛОЖЕНИЕ Б

(обязательное)

Схемы транзакций документооборота

Б.1 Транзакция №1 «Абонент — Контролирующий орган»

Документооборот совершается между абонентом и контролирующим органом. Абонент-отправитель письма выбирает систему документооборота контролирующего органа, в который он сдает отчетность (например, отчетность в Энергосбыт). Функционально отправка происходит через третью сторону — спецоператора, который является гарантом передачи сообщения от Отправителя Получателю. Контролирующий орган, со своей стороны, в установленные сроки обязан отправить Отправителю Протокол результата проверки содержимого письма. Протокол результата также проходит через спецоператора связи.

Таблица Б-1. Описание транзакции №1

№ оп.	Наименование операции	Содержание	Подписано	Зашифровано	Статус исходного письма
1	Отправка отчета	Открытые поля	Абонент	—	Отправка
		Текст отчета, вложения		Абонент, КО	
2	Отправка Подтверждения СОС в адрес Абонента	Открытые поля Отчета, дата и время, наименования и коды отправителя и получателя, хэш*	СОС	—	Обработка СОС
3	Отправка Подтверждения СОС в адрес КО				
4	Подписание Подтверждения СОС со стороны Абонента	ЭП Абонента к Подтверждению СОС	—	—	Отправлено

№ оп.	Наименование операции	Содержание	Подпи- сано	Защи- фровано	Статус исходного письма
5	Подписание Под- тверждения СОС со стороны КО	ЭП КО к Подтвер- ждению СОС	—	—	Доставлено
6	Отправка Кви- танции о получе- нии Отчета	Открытые поля От- чета, наименования и коды отправителя и получателя, хэш*	КО	—	Получено
7	Формирование Уведомления об отправке Квитанции (п. 6)	Открытые поля От- чета, наименования и коды отправителя и получателя, хэш*	СОС	—	
8	Отправка Прото- кола входного контроля	ЭП КО к Отчету и его вложениям	—	—	Проверено
		Протокол входного контроля, вложения к Протоколу	КО	КО, Абонент	
9	Формирование Уведомления об отправке Протокола вход- ного контроля	Открытые поля От- чета, дата и время, наименования и ко- ды отправителя и получателя, хэш*	СОС	—	Завершено
10	Отправка Кви- танции о получе- нии Протокола	ЭП Абонента к Протоколу	—	—	
		Открытые поля От- чета, наименования и коды отправителя и получателя, хэш*	Абонент	—	
11	Формирование Уведомления об отправке Квитанции (п. 10)	Открытые поля От- чета, наименования и коды отправителя и получателя, хэш*	СОС	—	

* Хэш текста отчета и его вложений вычисляется по ГОСТ Р 34.11-94.

Подп. дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

Изм.	Лист	№ докум.	Подп.	Дата

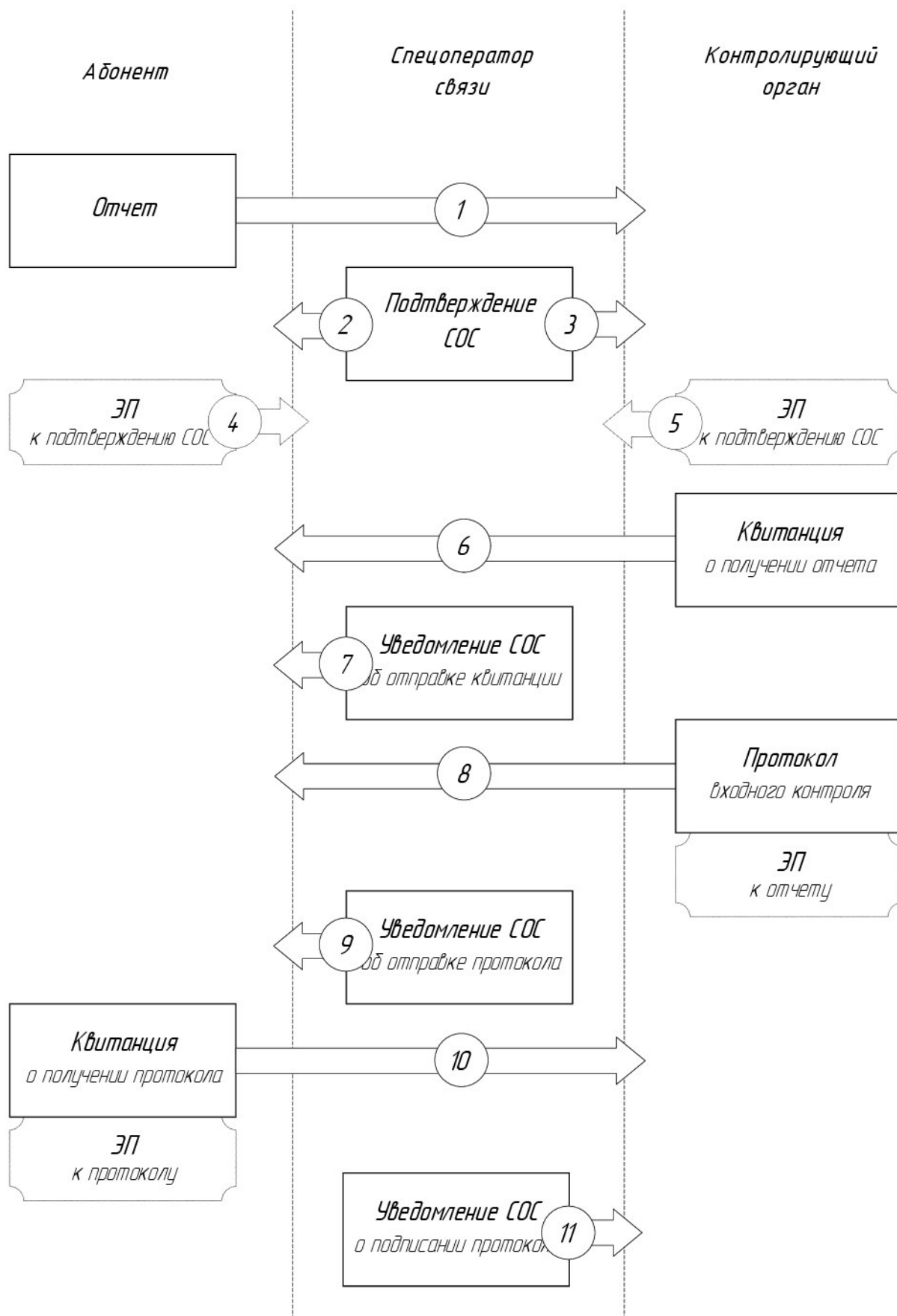


Рисунок Б-1. Графическое изображение транзакции №1

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата

The flowchart illustrates the process of document handling across three vertical lanes representing different departments. The process begins in the rightmost lane with a box labeled 'Протокол входного контроля' (Protocol of incoming control), which includes a stamp 'ЭП к отчету' (Electronic signature for report). An arrow labeled '8' points left to the middle lane. In the middle lane, an arrow labeled '9' points left to the leftmost lane, accompanied by a box 'Уведомление СОС об отправке протокола' (Notification of the SOC about sending the protocol). In the leftmost lane, a box 'Квитанция о получении протокола' (Receipt of protocol) includes a stamp 'ЭП к протоколу' (Electronic signature for protocol). An arrow labeled '10' points right from this box to the middle lane. In the middle lane, a box 'Уведомление СОС о подписании протокола' (Notification of the SOC about signing the protocol) has an arrow labeled '11' pointing right to the rightmost lane.

Рисунок Б-1. Графическое изображение транзакции №1

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата

Изм.	Лист	№ докум.	Подп.	Дата

ТУ 5061-002-16908055-2013

Лист
34

Б.2 Транзакция №2 «Абонент А — Абонент Б» (без требования подписи получателя)

Документооборот совершается между абонентами. Абонент А (Отправитель письма) выбирает из справочника абонента Б (Получателя). Функционально отправка происходит через третью сторону — спецоператора, который является гарантом передачи сообщения от Отправителя Получателю. После завершения отправки письма документооборот завершается.

Таблица Б-2. Описание транзакции №2

№ оп.	Наименование операции	Содержание	Подписано	Зашифровано	Статус исходного письма
1	Отправка письма	Открытые поля	Абонент А	—	Отправка
		Текст письма, вложения		Абоненты А, Б	
2	Отправка Подтверждения СОС Абоненту А	Открытые поля Письма, дата и время, наименования и коды отправителя и получателя, хэш*	СОС	—	Обработка СОС
3	Отправка Подтверждения СОС Абоненту Б				
4	Подписание Подтверждения СОС (Абонент А)	ЭП Абонента А к Подтверждению СОС	—	—	Отправлено
5	Подписание Подтверждения СОС (Абонент Б)	ЭП Абонента Б к Подтверждению СОС	—	—	Доставлено
6	Отправка Квитанции о получении Письма	Открытые поля Письма, наименования и коды отправителя и получателя, хэш*	Абонент Б	—	Завершено

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата

№ оп.	Наименование операции	Содержание	Подпи- сано	Заши- фровано	Статус исходного письма
7	Формирование Уведомления об отправке Квитанции (п. 6)	Открытые поля Письма, наимено- вания и коды от- правителя и полу- чателя, хэш*	СОС	—	

* Хэш текста письма и его вложений вычисляется по ГОСТ Р 34.11-94.

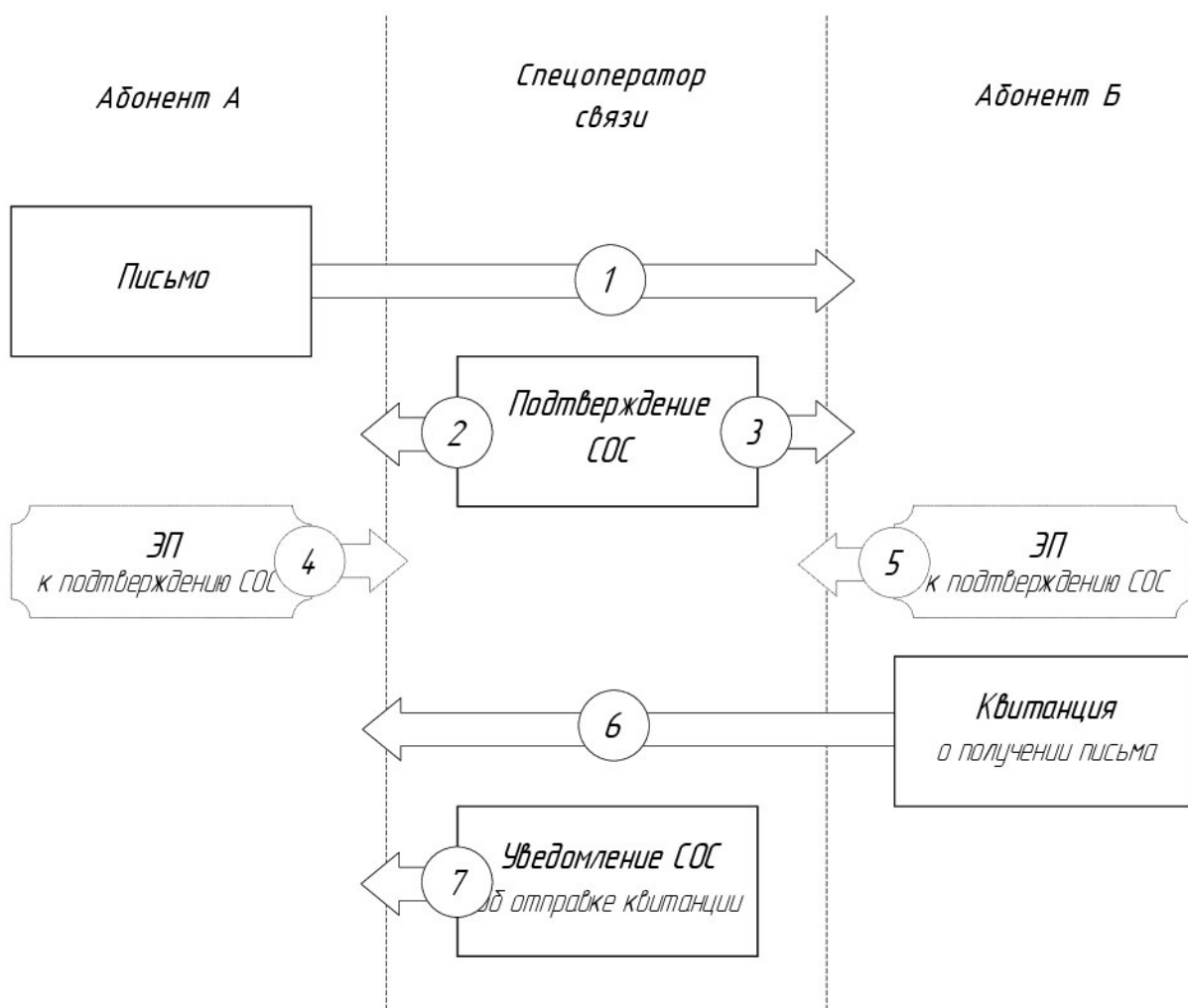


Рисунок Б-2. Графическое изображение транзакции №2

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата
Изм.	Лист	№ докум.	Подп.	Дата
ТУ 5061-002-16908055-2013				
Лист				
36				

Б.3 Транзакция №3 «Абонент А — Абонент Б» (с требованием подписи получателя)

Документооборот совершается между абонентами. Абонент А (Отправитель письма) выбирает из справочника абонента Б (Получателя). Функционально отправка происходит через третью сторону — спецоператора, который является гарантом передачи сообщения от Отправителя Получателю. После завершения отправки письма абонент Б обязан подписать исходное письмо либо направить абоненту А мотивированный отказ. Документ, свидетельствующий об отказе, направляется через спецоператора связи.

Таблица Б-3. Описание транзакции №3

№ оп.	Наименование операции	Содержание	Подписано	Зашифровано	Статус исходного письма
1	Отправка письма	Открытые поля Текст письма, вложения	Абонент А	— Абоненты А, Б	Отправка
2	Отправка Подтверждения СОС Абоненту А	Открытые поля Письма, дата и время, наименования и коды отправителя и получателя, хэш*	СОС	—	Обработка СОС
3	Отправка Подтверждения СОС Абоненту Б				
4	Подписание Подтверждения СОС (Абонент А)	ЭП Абонента А к Подтверждению СОС	—	—	Отправлено
5	Подписание Подтверждения СОС (Абонент Б)	ЭП Абонента Б к Подтверждению СОС	—	—	Доставлено
6	Отправка Квитанции о получении Письма	Открытые поля Письма, наименования и коды отправителя и получателя, хэш*	Абонент Б	—	Получено

Подп. дата	Инв. № докл.	Взам. инв. №	Подп. и дата	Инв. № подл.

Изм.	Лист	№ докум.	Подп.	Дата

№ оп.	Наименование операции	Содержание	Подпи- сано	Защи- фровано	Статус исходного письма
7	Формирование Уведомления об отправке Квитанции (п. 6)	Открытые поля Письма, наимено- вания и коды от- правителя и полу- чателя, хэш*	СОС	—	
8А	Подписание Письма со сторо- ны Абонента Б	ЭП Абонента Б к Письму	—	—	Подписано
9А	Формирование Уведомления о подписании Письма (п. 8А)	Открытые поля Письма, наимено- вания и коды от- правителя и полу- чателя, хэш*	СОС	—	
8Б	Отправка Отказа на подписание Письма	Текст отказа, вложения	Абонент Б	Абонен- ты Б, А	Отказ в подписи
9Б	Формирование Уведомления об отправке Отказа (п. 8Б)	Открытые поля Письма, наимено- вания и коды от- правителя и полу- чателя, хэш*	СОС	—	
10	Формирование Квитанции о по- лучении ответа	Открытые поля Письма, наимено- вания и коды от- правителя и полу- чателя, хэш*	Абонент А	—	Завершено
11	Формирование Уведомления об отправке Квитанции (п. 10)	Открытые поля Письма, наимено- вания и коды от- правителя и полу- чателя, хэш*	СОС	—	

* Хэш текста письма и его вложений вычисляется по ГОСТ Р 34.11-94.

Подп. дата	Инв. № докл.	Взам. инв. №	Подп. и дата	Инв. № подл.

Изм.	Лист	№ докум.	Подп.	Дата	ТУ 5061-002-16908055-2013	Лист
						38

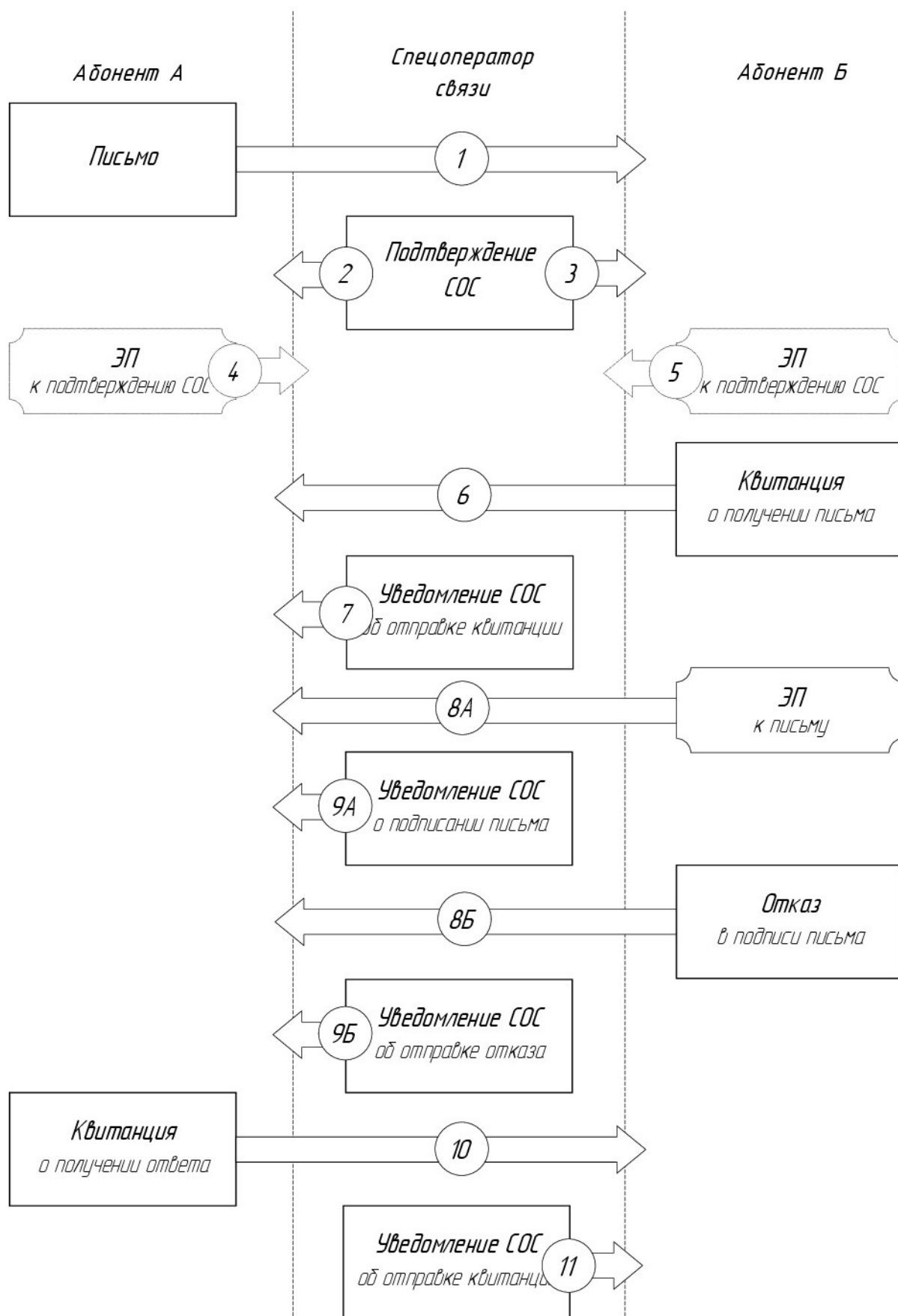


Рисунок Б-3. Графическое изображение транзакции №3:
ветвь «А» — подписание письма, ветвь «Б» — отказ в подписи

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата	
Изм.	Лист	№ докум.	Подп.	Дата	ТУ 5061-002-16908055-2013
					Лист 39

ПРИЛОЖЕНИЕ В

(справочное)

Нормативные ссылки

В настоящих технических условиях использованы ссылки на нижеследующие стандарты и нормативные документы.

Таблица В-1. Перечень ссылок на использованные нормативные документы

Обозначение документа	Наименование нормативного документа	Номера разделов, подразделов, пунктов, приложений, где дана ссылка на документ
ГОСТ 15971-90	Системы обработки информации. Термины и определения	Раздел 6
ГОСТ 19781-90	Обеспечение систем обработки информации программное. Термины и определения	Раздел 6
ГОСТ 29099-91	Сети вычислительные локальные. Термины и определения	Раздел 6
ГОСТ Р 34.11-94	Информационная технология. Криптографическая защита информации. Функция хэширования	Приложение Б
ГОСТ Р ИСО/МЭК 12119-2000	Информационная технология. Пакеты программ. Требования к качеству и тестирование	Раздел 4
ГОСТ Р ИСО/МЭК ТО 12182-2002	Информационная технология. Классификация программных средств	Введение
ГОСТ Р ИСО/МЭК 14764-2002	Информационная технология. сопровождение программных средств	Раздел 6

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата

Изм.	Лист	№ докум.	Подп.	Дата

<i>Обозначение документа</i>	<i>Наименование нормативного документа</i>	<i>Номера разделов, подразделов, пунктов, приложений, где дана ссылка на документ</i>
ГОСТ Р ИСО/МЭК ТО 19791-2008	Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем	Раздел 4
ГОСТ Р 53898-2010	Системы электронного документооборота. Взаимодействие систем управления документами. Требования к электронному сообщению	Раздел 4
RFC 1122	Requirements for Internet Hosts. Communication Layers	Раздел 6
RFC 2616	Hypertext Transfer Protocol — HTTP/1.1	Раздел 6

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. дата		
Изм.	Лист	№ докум.	Подп.	Дата	ТУ 5061-002-16908055-2013	Лист 41