

**УТВЕРЖДАЮ**

Генеральный директор  
ЗАО «Сервер-Центр»

  
В.В. Решетников  
«12» марта 2008 г.



## РЕГЛАМЕНТ

### работы в системе «ОТЧЕТНОСТЬ» для обмена электронными документами по каналам связи

#### 1. ОБЩИЕ ПОЛОЖЕНИЯ.

Настоящий документ определяет регламент работы и функционирования системы обмена юридически значимыми электронными документами по каналам связи «ОТЧЕТНОСТЬ».

Настоящий регламент основывается на следующих документах:

- Федеральный закон «О связи»;
- Федеральный закон «Об электронной цифровой подписи»;
- Федеральный закон «Об информации, информационных технологиях и защите информации»;
- Федеральный закон «О персональных данных».

Настоящий регламент обязателен для всех участников Системы «ОТЧЕТНОСТЬ».

#### 2. ОПРЕДЕЛЕНИЕ ТЕРМИНОВ.

Для целей правильного понимания текста регламента термины, применяемые в нем, используются в следующем значении:

Документ – это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. Например ДЕКЛАРАЦИЯ – это документ, реквизиты которого оформлены в соответствии с утвержденными правилами;

Электронный документ - это документ, в котором реквизиты представлены в электронно-цифровой форме;

ЭЦП документа (электронная цифровая подпись) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

Формат представления документа в электронном виде (электронный формат) - формализованное описание состава и структуры показателей документов, представляемых в электронном виде, а также требований к их формированию;

СЭОД – система электронной обработки данных. Термин СЭОД понимается в широком смысле. Это созданные и вновь создаваемые информационные системы обработки данных, системы декларирования, любые информационные системы обработки документов представленных в электронном виде;

Система «Отчетность» (Система) - организационно упорядоченная совокупность правил и информационных технологий с использованием вычислительной техники и систем связи, реализующая автоматизированные процессы передачи электронных документов между Абонентами системы;

Абоненты системы – участники обмена электронными документами, подключенные к системе «ОТЧЕТНОСТЬ». В системе обмена электронными документами определены три вида Абонентов:

Абонент - учреждение, организация, индивидуальный предприниматель, физическое лицо, которые подключены к системе «Отчетность» на основании клиентского договора;

Пункт коллективного доступа (ПКД) – Абонент Системы, уполномоченный (в соответствии с действующим законодательством РФ) использовать Систему от имени и по поручению юридического или физического лица на основании доверенности.

Ведомство – юридические лица, организации, учреждения, подключенные к системе «Отчетность» на основании договора «О совместных действиях по организации и функционированию системы доставки электронных документов от Абонентов в системы электронной обработки данных Ведомства». Ведомство принимает электронные документы от широкого круга Абонентов по правилам, определенным в настоящем регламенте. Электронный формат документов определяется Ведомством;

Специализированный оператор связи (СОС или Оператор) – организация ЗАО "Сервер-Центр", действующая на основании своих лицензий: «Телематические услуги связи» № 35807 от 31.10.2005 года, «Услуги связи в сети передачи данных, за исключением передачи голосовой информации» № 35808 от 31.10.2005, "Деятельность по распространению шифровальных криптографических средств" №564Р от 09.04.2008, "Деятельность по техническому обслуживанию шифровальных (криптографических) средств" №565Х от 09.04.2008, "Деятельность по предоставлению услуг в области шифрования информации" №566У от 09.04.2008, которая предоставляет услуги доставки электронных документов по каналам связи между Абонентами;

Интернет — открытые телекоммуникационные каналы связи;

ЭЦП Ведомства - электронная цифровая подпись, владельцем сертификата открытого ключа которой является должностное лицо Ведомства, уполномоченное использовать средства электронной цифровой подписи в рамках системы «Отчетность»;

ЭЦП Абонента - электронная цифровая подпись, владельцем сертификата открытого ключа которой является должностное лицо Абонента или Пункта коллективного доступа, уполномоченное использовать средства электронной цифровой подписи в рамках системы представления деклараций в электронном виде по телекоммуникационным каналам связи;

ЭЦП специализированного оператора связи (ЭЦП Оператора) - электронная цифровая подпись, владельцем сертификата открытого ключа которой является должностное лицо специализированного оператора связи, уполномоченное использовать средства электронной цифровой подписи в рамках системы «Отчетность»;

Подтверждение специализированного оператора связи (Подтверждение Оператора) - электронный документ, формируемый специализированным оператором связи, в котором указана дата представления Абонентом электронного документа. Подтверждение подписывается ЭЦП оператора связи;

Протокол входного контроля - электронный документ, подписанный ЭЦП должностного лица ведомства, в котором указаны результаты проверки электронного документа Абонента на соответствие требованиям утвержденному электронному формату. Протокол входного контроля формируется в СЭОД ведомства автоматически;

Квитанция о получении электронного документа - электронный документ, содержащий ЭЦП абонента отправителя и абонента получателя для электронного документа, предоставленного абонентом отправителем. Формируется абонентом-получателем при получении электронного документа. Например, абонентом получателем может быть Ведомство;

Квитанция о получении протокола входного контроля - электронный документ, содержащий ЭЦП Абонента и Ведомства, на протокол входного контроля, отправленный Ведомством Абоненту. Формируется Абонентом при получении Протокола входного контроля;

СКЗИ – средство криптографической защиты информации.

Средства связи – технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки электронных документов, сообщений, а также иные технические и программные средства, используемые при оказании услуги связи или обеспечения функционирования Системы.

Также в настоящем Регламенте используются термины определенные в федеральных законах

- «О связи»;
- «Об электронной цифровой подписи»;
- «Об информации, информационных технологиях и защите информации»;
- «О персональных данных»

### **3. ПОРЯДОК ПОДКЛЮЧЕНИЯ НОВОГО АБОНЕНТА К СИСТЕМЕ «ОТЧЕТНОСТЬ».**

- 3.1. Для начала работы в системе Абонент направляет в Ведомство письмо установленного образца (см. Приложение № \_\_\_\_).
- 3.2. Должностное лицо Абонента обращается к Оператору со следующим пакетом документов:
  - Оформленный типовой договор (Приложение № \_\_\_\_\_) на подключение к системе «Отчетность», включающий приложения:
    - Заявка на регистрацию в Системе;
    - Регистрационная информация Абонента.
  - Документ, удостоверяющий личность лица, ответственного за предоставление информации в Системе.
- 3.3. Абонент подписывает оформленный договор «на подключение и работу в системе обмена юридически значимыми документами «ОТЧЕТНОСТЬ»» и оплачивает предоставляемые услуги.
- 3.4. Оператор, регистрирует АБОНЕНТА в Системе; предоставляет ему комплект установки Системы и временный сертификат ЭЦП Абонента. Также передается комплект документации к СКЗИ «Крипто-Про CSP», и инструкция по защите информации при работе в Системе.
- 3.5. Должностное лицо АБОНЕНТА, руководствуясь Инструкцией Пользователя Удостоверяющего центра (Приложение \_\_\_\_), настраивает рабочее место; генерирует личный закрытый и открытый ключ ЭЦП и ключ шифрования и формирует запрос на сертификат ЭЦП Абонента для передачи информации в СИСТЕМЕ.
- 3.6. При надлежащем оформлении договорных отношений и оплаты услуг со стороны Абонента, Оператор подтверждает запрос и публикует открытый сертификат ЭЦП Абонента и сертификат открытого ключа шифрования.
- 3.7. После выпуска сертификата должностное лицо Абонента устанавливает сертификат ЭЦП на своем рабочем месте и предоставляет два экземпляра подписанного со своей стороны бланка сертификата Оператору на утверждение.
- 3.8. Оператор утверждает оформленный Абонентом бланк, публикует его на удостоверяющем центре, передает утвержденный бланк сертификата Абоненту.

### **4. ПРАВИЛА ИСПОЛЬЗОВАНИЯ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ**

- 4.1. Электронные документы представляются по каналам связи с использованием средств криптографической защиты информации (СКЗИ).
- 4.2. Распространение и учет СКЗИ организуется оператором связи или его партнерами (агентами) в соответствии с нормативными документами, а также требованиями технической документации организаций - разработчиков СКЗИ.
- 4.3. Правила использования СКЗИ в Системе устанавливаются специализированным оператором связи.
- 4.4. Применение Абонентами СКЗИ в Системе не требует получения специальной лицензии.
- 4.5. Риск неправомерного подписания электронного документа ЭЦП несет Абонент, на уполномоченное лицо которого зарегистрирован сертификат соответствующего открытого ключа ЭЦП.
- 4.6. Сертификат ЭЦП считается действующим, если до момента получения адресатом подписанного ЭЦП электронного документа, не было заявлено о недействительности этого сертификата ЭЦП.
- 4.7. Абоненты (Участники информационного обмена) должны обеспечить сохранность открытых ключей ЭЦП и их сертификатов в течение всего периода хранения электронных документов в хранилище.

## 5. ПОРЯДОК ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ ПО КАНАЛАМ СВЯЗИ В СИСТЕМЕ ПРИ ПРЕДОСТАВЛЕНИИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В СЭОД ВЕДОМСТВ

- 5.1. При доставке электронных документов по каналам связи Абонент осуществляет обмен электронными документами с Ведомством и Оператором (СОС), с которым у него заключен договор о предоставлении услуг.
- 5.2. Оператор обеспечивает Абонентам возможность обмена электронными документами со всеми подразделениями Ведомства, взаимодействующими с ним при представлении электронных документов по каналам связи при условии соблюдения Абонентом технических условий, опубликованных на веб-сайте Оператора [www.serverc.ru](http://www.serverc.ru).
- 5.3. Электронный документ считается исходящим от Абонента, если он подписан ЭЦП Абонента.
- 5.4. При представлении Абонентом электронных документов по каналам связи соблюдается следующий порядок обмена электронными документами:
  - 5.4.1. После подготовки электронного документа в соответствии с утвержденным Ведомством форматом уполномоченное лицо Абонента подписывает этот документ своей ЭЦП, шифрует и отправляет его в адрес Ведомства через Систему.
  - 5.4.2. При отсылке документа, Абонент сохраняет его в хранилище отправленных документов.
  - 5.4.3. В течение суток (без учета выходных и праздничных дней) с момента отправки документа Абонент получает следующие документы:
    - подтверждение Оператора о получении документа;
    - квитанцию о получении Ведомством электронного документа;
    - протокол входного контроля из Ведомства.
  - 5.4.4. Абонент проверяет подлинность ЭЦП Оператора на Подтверждении Оператора и сохраняет подтверждение в своем хранилище.
  - 5.4.5. Абонент проверяет подлинность ЭЦП Ведомства на квитанции о получении декларации в электронном виде и соответствие ее отправленной декларации, а затем сохраняет квитанцию в своем хранилище.
  - 5.4.6. Протокол входного контроля электронного документа после дешифрования и подтверждения подлинности ЭЦП Ведомства заверяется ЭЦП Абонента и в течение суток с момента получения протокола (без учета выходных и праздничных дней) квитанция на протокол высылается в адрес Ведомства. Второй экземпляр протокола входного контроля электронного документа, подписанный ЭЦП Ведомства и заверенный ЭЦП Абонента, сохраняется в хранилище Абонента.
  - 5.4.7. Абонент обязан ознакомиться с протоколом входного контроля. Если в протоколе содержится информация о том, что электронный документ не прошёл входной контроль, то Абонент в течение суток (без учета выходных и праздничных дней) устраняет указанные в протоколе ошибки и повторяет всю процедуру подачи электронного документа, по которому зафиксированы ошибки.  
Исправленный таким образом электронный документ считается представленным в срок.
  - 5.4.8. Если Абонент не получил от Ведомства в установленное время протокол входного контроля и (или) квитанцию о получении электронного документа, он уведомляет Оператора и Ведомство о данном факте и, при необходимости, повторяет процедуру подачи электронного документа.
  - 5.4.9. Если Абонент не получил в установленное время от Оператора связи подтверждение Оператора связи и (или) от Ведомства квитанцию о получении электронного документа, он уведомляет Оператора о данном факте и, при необходимости, повторяет процедуру сдачи декларации.
- 5.5. При получении электронного документа по каналам связи Ведомство соблюдает следующий порядок электронного обмена документами:
  - 5.5.1. В течение суток (без учета выходных и праздничных дней) с момента получения электронного документа Ведомство выполняет следующие действия:
    - расшифровывает электронный документ, полученный от Абонента;
    - проверяет подлинность ЭЦП Абонента;
    - формирует квитанцию о получении электронного документа (т.е. заверяет полученный электронный документ ЭЦП Ведомства) и направляет ее Абоненту. Второй экземпляр квитанции сохраняется в хранилище Ведомства;
    - проверяет подлинность ЭЦП Оператора на подтверждении оператора и сохраняет подтверждение в своем хранилище;

- проверяет полученный электронный документ на соответствие утвержденному формату и формирует протокол входного контроля;
  - направляет Абоненту протокол входного контроля, в зашифрованном виде.
- 5.5.2. Квитанция на протокол входного контроля, полученная от Абонента, после подтверждения подлинности ЭЦП Абонента сохраняется в хранилище Ведомства.
  - 5.5.3. Электронный документ, подписанный ЭЦП Абонента, подлинность которой подтверждена, и прошедшая входной контроль на соответствие утвержденному формату, регистрируется в установленном порядке и вводится в базу данных СЭОД Ведомства.
  - 5.5.4. При необходимости обращения к электронному документу по распоряжению руководителя Ведомства может быть сделана копия электронного документа на бумажном носителе, на которой следует указать реквизиты документа-оригинала, а также дату и время изготовления копии. Бумажные копии электронных документов заверяются уполномоченным должностным лицом Ведомства.
  - 5.5.5. При передаче дела Абонента в другое подразделение Ведомства, имеющее техническую возможность приема электронных документов по каналам связи, передаются оригинальные файлы электронных документов и файлы подтверждений Оператора из хранилища электронных документов. При необходимости могут быть изготовлены бумажные копии, заверяемые уполномоченным должностным лицом Ведомства.
- 5.6. При отправке Абонентом электронного документа в СЭОД Ведомства, Оператор связи совершает следующие действия:
    - 5.6.1. Оператор фиксирует дату попадания электронного документа, отправленного Абонентом, на свои интерфейсы в качестве даты его представления и формирует подтверждение оператора с указанием даты и времени представления электронного документа. Формирование, обмен и хранение подтверждений осуществляются в течение суток (без учета выходных и праздничных дней) после получения электронного документа.
    - 5.6.2. Подтверждение подписывается ЭЦП оператора и высылается одновременно в адрес Ведомства и Абонента.
    - 5.6.3. Оператор хранит в своем хранилище все подтверждения, отправленные в адрес Абонентов системы (Участников информационного обмена).
    - 5.6.4. В течение суток (без учета выходных и праздничных дней) после получения электронного документа Оператор связи отправляет его в адрес Ведомства.
  - 5.7. Электронный документ считается представленным в Ведомство, если Абонент получил квитанцию о получении электронного документа, подписанную ЭЦП Ведомства. Дата и время предоставления электронного документа зафиксированы в подтверждении, подписанном ЭЦП Оператора.
  - 5.8. Электронный документ считается принятыми в случае, если Абонент получил протокол входного контроля, подтверждающий, что документ не содержит ошибок и прошёл входной контроль в СЭОД Ведомства.
  - 5.9. Электронный документ не считается принятыми, в случае если Абонент не получил протокол входного контроля или получил протокол входного контроля, в котором содержится информация о том, что данный документ содержит ошибки и не прошёл входной контроль.
  - 5.10. Все документы сохраняются в хранилищах участников информационного обмена подписанными ЭЦП уполномоченных лиц в течении срока установленным законодательством Российской Федерации для хранения документов.
  - 5.11. Электронные документы, являются оригиналами, имеют юридическую силу, подлежат хранению в хранилище юридически значимых документов и могут использоваться в качестве доказательств в суде, а также при рассмотрении споров в досудебном порядке.
  - 5.12. Если Абонент с целью контроля самостоятельно или по согласованию с Ведомством копирует электронные документы на бумажный носитель, то на первом листе бумажной копии электронного документа следует отметить, что оригинал был отправлен в электронном виде, и указать реквизиты электронного документа-оригинала, заверив подписью уполномоченного лица Абонента и печатью. При необходимости, принятый документ может быть заверен подписью уполномоченного лица и печатью Ведомства.
  - 5.13. Каталоги жестких дисков и разделы баз данных, содержащие хранилище юридически значимых электронных документов, формируемые программным обеспечением поддержки электронного обмена документами, подлежат регулярному резервному копированию на оборудовании всех участников электронного обмена документами. Ответственность за сохранность своих хранилищ несут сами участники электронного обмена документами.

## **6. ПОРЯДОК ЗАМЕНЫ ПАРОЛЬНО-КЛЮЧЕВОЙ ИНФОРМАЦИИ**

- 6.1. Сертификат ключа ЭЦП и шифрования Абонента системы, равно как и парольная информация, могут быть изменены как по заявке Абонента системы, так и по инициативе Оператора.
- 6.2. Штатная замена сертификата ключа ЭЦП и шифрования производится не реже одного раза в год.
- 6.3. Абонент системы продляет действующий или заключает новый договор о предоставлении услуг по работе в Системе.
- 6.4. Абонент системы получает от Оператора предупреждение о скором прекращении действия сертификата (за месяц до окончания срока действия).
- 6.5. Штатная замена сертификата ключа ЭЦП и шифрования должна быть выполнена не менее, чем за семь рабочих дней до истечения срока действия старого сертификата.
- 6.6. Штатная замена сертификата ключа ЭЦП и шифрования Абонентом системы выполняется по следующей процедуре:
  - Абонент системы средствами АРМ ЗАРЕГИСТРИРОВАННОГО ПОЛЬЗОВАТЕЛЯ на своем рабочем месте генерирует новый личный закрытый и открытый ключ ЭЦП/шифрования и формирует запрос на сертификат. Запрос подписывается ЭЦП Абонента системы.
  - СПЕЦИАЛИЗИРОВАННЫЙ ОПЕРАТОР СВЯЗИ выпускает сертификат
  - Абонент системы устанавливает сертификат и передает СПЕЦИАЛИЗИРОВАННОМУ ОПЕРАТОРУ СВЯЗИ два экземпляра бланка сертификата.
  - Новый сертификат используется для формирования ЭЦП и шифрования данных при работе в Системе. Старый сертификат при этом отзывается Абонентом системы самостоятельно, что отражается в списке отозванных сертификатов;
  - работа Абонента в Системе при штатной замене сертификата не приостанавливается.
- 6.7. Штатная замена пароля производится письмом в адрес СПЕЦИАЛИЗИРОВАННОГО ОПЕРАТОРА СВЯЗИ.
- 6.8. При наличии данных, позволяющих предположить, что сертификат ключа ЭЦП и шифрования или пароль Абонента системы стал известен третьим лицам, Абонент системы немедленно информирует об этом СПЕЦИАЛИЗИРОВАННОГО ОПЕРАТОРА СВЯЗИ. В этом случае работа в Системе с применением старого сертификата или пароля приостанавливается с момента поступления сообщения о компрометации ключа ЭЦП и шифрования.
- 6.9. Для внештатной замены сертификата, вызванной причинами, указанными в предыдущем пункте, уполномоченный представитель Абонента системы лично получает новый сертификат у СПЕЦИАЛИЗИРОВАННОГО ОПЕРАТОРА СВЯЗИ.

## **7. ПРОЧЕЕ**

- 7.1. Парольная информация и сертификат ключа ЭЦП и шифрования Абонента системы не может быть передан третьим лицам.