УТВЕРЖДАЮ
Директор
ООО «Стандарт безопасности»

_____ Рачков М.С.
« 14 » апреля 2011 г.

РЕГЛАМЕНТ
деятельности Удостоверяющего центра ООО «Стандарт безопасности» и абонентов системы защищенного обмена персонифицированной информацией ООО «Стандарт безопасности» ViPNet

2012

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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.

Сертификат ключа проверки электронной подписи (СКП ЭП) - 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 - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо Министерство связи и массовых коммуникаций Российской Федерации (www.minsvyaz.ru).

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи.

Ключ электронной подписи - 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 (далее - проверка электронной подписи).

Удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом.

Уполномоченное лицо удостоверяющего центра – физическое лицо, владелец СКП ЭП удостоверяющего центра.

Средства криптографической защиты информации (СКЗИ). К СКЗИ относятся:

1) средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;
2) средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;
3) 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;

4) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;
5) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);
6) ключевые документы (независимо от вида носителя ключевой информации).

Компрометация ключа электронной подписи – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых ключи ЭП могут стать доступными несанкционированным лицам и (или) процессам. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

1) потеря ключевых носителей;
2) потеря ключевых носителей с их последующим обнаружением;
3) увольнение сотрудников, имевших доступ к ключевой информации;
4) нарушение правил хранения и уничтожения (после окончания срока действия) ключа ЭП;
5) возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
6) нарушение печати на сейфе с ключевыми носителями;
7) случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

Кроссертификация – установление доверительных отношений между удостоверяющими центрами, при котором владельцы сертификатов, выданных одним удостоверяющим центром, доверяют сертификатам, выданных другим удостоверяющим центром.

Список отозванных сертификатов (СОС) – электронный документ с ЭП уполномоченного лица удостоверяющего центра, включающий в себя список серийных номеров СКП ЭП, которые на определенный момент времени были отозваны или действие которых было приостановлено. УЦ изготавливает СОС в электронной форме – формат X.509 версии 2.

Подтверждение подлинности ЭП в электронном документе – положительный результат проверки соответствующим сертифицированным средством ЭП с использованием СКП ЭП принадлежности ЭП в электронном документе владельцу СКП ЭП и отсутствия искажений в подписанном данной ЭП электронном документе.

Пользователь СКП ЭП – физическое лицо, использующее полученные в удостоверяющем центре сведения о СКП ЭП для проверки принадлежности ЭП владельцу СКП ЭП.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Регистрация – внесение регистрационной информации о пользователях УЦ в реестр УЦ.

Реестр – набор документов УЦ в электронной и/или бумажной форме, включающий следующую информацию:

1) реестр регистрационных карт пользователей;
2) реестр договоров;
3) реестр зарегистрированных пользователей;
4) реестр приказов о назначении ответственных лиц за работу с СКЗИ;
5) реестр актов о готовности эксплуатации СКЗИ;
6) реестр заявлений на изготовление сертификата ключа ЭП;

7) реестр заявлений на аннулирование (отзыв) сертификата ключа ЭП;
8) реестр заявлений на приостановление/возобновление действия сертификата ключа ЭП;
9) реестр СКП ЭП;
10) реестр изготовленных СОС;
11) служебные документы УЦ.

2. ВВЕДЕНИЕ

2.1. Обзорная информация

Данный Регламент Удостоверяющего центра ООО «Стандарт безопасности» системы защищенного обмена персонифицированной информацией ViPNet (далее СЗОПИ ViPNet) определяет механизмы предоставления и использования услуг УЦ, включая обязанности пользователей СЗОПИ ViPNet и членов группы администраторов УЦ, процедуры взаимодействия, форматы документов и данных, а также основные организационно-технические меры по обеспечению безопасной работы УЦ.

Целью настоящего Регламента является создание условий для организации взаимодействия информационных систем и правовых условий использования электронной подписи (ЭП), при соблюдении которых ЭП в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

Присоединение к Регламенту производится путем заключения договора между УЦ и клиентом, или любое использование сертификатов ключей подписей, выданных УЦ.

2.2. Идентификация Регламента

Наименование документа: «Регламент Удостоверяющего Центра ООО «Стандарт безопасности».
Версия 1.0
Дата: 17.07.2012

2.3. Публикация Регламента

Настоящий Регламент распространяется электронном виде на сайте www.yarsec.ru.

2.4. Область применения Регламента

Настоящий Регламент предназначен служить соглашением, налагающим обязательства на все вовлеченные Стороны, а так же средством уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ. Регламент применим при организации защищенного обмена электронными документами и взаимодействия информационных систем.

2.5. Контактная информация

Удостоверяющий центр:
ООО «Стандарт безопасности»
Юридический адрес: 150047, г. Ярославль, ул. Угличская 39В, офис 211
Почтовый адрес: 150047, г. Ярославль, ул. Угличская 39В, офис 211
Телефон: 587-300
Факс 587-302
E-mail: nalog@secst.ru
Web: www.yarsec.ru

2.6. Порядок утверждения и внесения изменений в Регламент

Оригинал Регламента составляется в бумажной форме и заверяется собственноручной подписью директора и печатью ООО «Стандарт безопасности».

Ошибки или предложения по уточнению положений настоящего Регламента должны направляться в УЦ согласно контактной информации представленной в разделе 2.5. настоящего Регламента.

Изменения в разделы настоящего Регламента, которые по оценкам УЦ не оказывают, либо оказывают незначительное влияние на работу Клиентов сети УЦ, вносятся без изменения номера версии данного документа и оповещения Клиентов.

Изменения в разделы настоящего Регламента, которые по оценкам УЦ могут иметь значительное влияние на работу Клиентов сети УЦ, вносятся с увеличением номера версии данного документа при условии оповещения этих Клиентов.

2.7. Срок действия регламента

- Настоящий Регламент вступает в силу со дня его публикации;
- Срок действия Регламента составляет 7 лет;
- Если УЦ официально не уведомит пользователей УЦ о прекращении действия Регламента, Регламент автоматически пролонгируется на следующие 7 лет;
- Официальное уведомление о прекращении действия Регламента осуществляется способами, определенными в разделе «Публикация Регламента».

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Услуги предоставляемые УЦ

В процессе своей деятельности УЦ предоставляет следующие виды услуг:

- внесение в реестр УЦ регистрационной информации о пользователях УЦ;
- изготовление СКП ЭП пользователей УЦ в электронной форме;
- изготовление для владельцев СКП ЭП копии СКП ЭП на бумажном носителе;

формирование ключей ЭП и ключей проверки ЭП по обращениям пользователей УЦ с записью их на ключевой носитель;

- ведение реестра изготовленных СКП ЭП пользователей УЦ;

предоставление копий СКП ЭП в электронной форме, находящихся в реестре изготовленных сертификатов, по запросам пользователей УЦ;

- аннулирование (отзыв) СКП ЭП по обращениям владельцев СКП ЭП;
- приостановление и возобновление действия СКП ЭП по обращениям владельцев СКП ЭП;
- предоставление пользователям УЦ сведений об аннулированных и приостановленных СКП ЭП;
- подтверждение подлинности ЭП уполномоченного лица УЦ в изготовленных им СКП ЭП по обращениям пользователей УЦ;
- предоставление средств СКЗИ и средств ЭП по обращениям пользователей УЦ;
- Сопровождение системы защищенного обмена “VipNet Client”;
- другие виды услуг.

3.2. Оплата услуг УЦ

Стоимость услуг предоставляемых УЦ определяется согласно договору между УЦ и пользователем.

3.3. Структура сети УЦ

Сеть УЦ состоит из следующих основных компонент:

- УЦ в составе:
  - Центр Управления Сетью (ЦУС);
  - Удостоверяющий Ключевой Центр (УКЦ);
  - Группа Администраторов УЦ;
- Пользователи, подразделяющиеся на группы.

3.3.1. Центр Управления Сетью

ЦУС выполняет следующие функции:

- регистрация СУ;
- распределение задач для СУ;
- регистрация пользователей (абонентов) в сети на СУ;
- задание и изменение разрешенных связей для СУ;
- формирование и рассылка адресных справочников для СУ;
- формирование справочников связей СУ для УКЦ (необходимы для формирования ключевой информации для связываемых СУ);
- рассылка для СУ обновлений справочно-ключевой информации, формируемой УКЦ;
- рассылка для СУ списков отозванных сертификатов и списков сертификатов уполномоченных лиц УЦ своей и смежных сетей;
- прием и передача в УКЦ запросов на сертификаты и обновление сертификатов от абонентов сети, рассылка изданных сертификатов на СУ.

3.3.2. Удостоверяющий Ключевой Центр

УКЦ выполняет следующие функции:

- формирование ключевых дискет для СУ сети услуг УЦ;
- формирование паролей для СУ;
- обновление ключевых дискет;
- создание ключей подписи и издание сертификатов Администраторов (Уполномоченных лиц) УЦ;
- ведение справочников сертификатов Администраторов УЦ, формирование и отправка в ЦУС обновлений справочников;
- создание ключей подписи абонентов и издание сертификатов по запросам ЦУС;
- рассмотрение запросов на издание сертификатов от абонентов сети;
- хранение информации о запросах и ведение справочников изданных сертификатов;
- рассмотрение запросов на отзыв, приостановление и возобновление сертификатов;
- ведение и отправка в ЦУС для обновления списков отозванных сертификатов.

3.3.3. Группа Администраторов УЦ

Группа администраторов УЦ выполняет следующие функции:

- реализует функции ЦУС и УКЦ сети УЦ;
- организует и выполняет мероприятия по техническому сопровождению распространяемых СКЗИ и ЭП;
- распространяет СКЗИ и ЭП;
- выполняет учет СКЗИ эксплуатационной и технической документацией к этим средствам;
- участвует в мероприятиях по защите информации;

- участвует в мероприятиях по расследованию инцидентов в области информационной безопасности.

3.3.4. Пользователи УЦ

Пользователями (потребителями) услуг УЦ могут быть как физические, так и юридические лица, подписавшие договор о предоставлении услуг ООО «Стандарт безопасности» и зарегистрированные в УЦ.

3.3.4.1. Владельцы сертификатов

Владельцем сертификата может быть только физическое лицо. В случае, когда в качестве пользователя выступает юридическое лицо, его интересы представляет физическое лицо, действующее на основании учредительных документов, либо доверенности.

3.3.4.2. Пользователи СКП ЭП

Пользователями сертификатов (Доверенными участниками) могут быть любые лица, которым владельцы сертификатов доверяют использовать их сертификаты.

3.3.4.3. Группы пользователей

Группа пользователей - подмножество узлов сети, объединенные в одну группу, имеющие возможность обмениваться персонифицированной информацией.

4. ПРАВА УЧАСТНИКОВ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ

4.1. Права УЦ

УЦ имеет право:

- создавать сертификаты ключей проверки электронных подписей и выдавать такие сертификаты лицам, обратившимся за их получением (заявителям);
- устанавливать сроки действия сертификатов ключей проверки электронных подписей;
- Хранить информацию, внесенную в реестр сертификатов, в течение всего срока деятельности, если более короткий срок не установлен нормативными правовыми актами;

предоставлять копии СКП ЭП в электронной форме, находящиеся в реестре УЦ, всем лицам, обратившимся за копиями в УЦ;

аннулировать (отозвать) СКП ЭП пользователя УЦ в случае установленного факта компрометации соответствующего ключа ЭП с уведомлением владельца аннулированного (отозванного) СКП ЭП и указанием обоснованных причин;

отказать в аннулировании (отзыве) СКП ЭП владельцу сертификата, подавшем заявление на аннулирование (отзыв) сертификата в случае, если истек установленный срок действия СКП ЭП;

отказать в приостановлении или возобновлении действия СКП ЭП владельцу сертификата, подавшему заявление на приостановлении или возобновлении действия сертификата, в случае если истек установленный срок действия СКП ЭП;

приостановить действие СКП ЭП пользователя УЦ с уведомлением владельца приостановленного СКП ЭП и указанием обоснованных причин.

4.2. Права участников электронного взаимодействия

- получить и применять список аннулированных (отозванных) и приостановленных СКП ЭП, изготовленный УЦ, для проверки статуса СКП ЭП;
- получить СКП ЭП уполномоченного лица УЦ;

- получить копию СКП ЭП в электронной форме, находящегося в реестре изготовленных СКП ЭП УЦ;
- получить копию сертификата ключа проверки электронной подписи в форме документа на бумажном носителе, заверенную удостоверяющим центром.
- применять СКП ЭП уполномоченного лица УЦ для проверки ЭП уполномоченного лица УЦ в СКП ЭП, изготовленных УЦ;
- применять копии СКП ЭП в электронной форме для проверки ЭП электронного документа в соответствии со сведениями, указанными в СКП ЭП;
- обращаться в УЦ с требованием проверки электронных подписей.
- обратиться в УЦ за подтверждением подлинности ЭП в документах, представленных в электронной форме;
- обратиться в УЦ для внесения в реестр УЦ регистрационной информации о пользователе с целью в дальнейшем стать владельцем СКП ЭП;
- обратиться в УЦ на предмет получения (приобретения) средств ЭП;
- сформировать ключ проверки ЭП и ключ ЭП на своем рабочем месте с использованием средств ЭП;
- обратиться в УЦ с заявлением в бумажной форме на изготовление СКП ЭП;

  получить и установить на свое рабочее место изготовленный СКП ЭП в электронной форме.

4.3. Права пользователей УЦ

Зарегистрированные в УЦ лица имеют права участников электронного взаимодействия, а также дополнительно к ним следующие права:

- право применять ключи ЭП и СКП ЭП, владельцами которых они являются, для формирования ЭП в электронных документах в соответствии со сведениями указными в СКП ЭП.
- обратиться в УЦ для аннулирования (отзыва) СКП ЭП в течение срока его действия;
- обратиться в УЦ для приостановления действия СКП ЭП в течение срока его действия;
- обратиться в УЦ для возобновления действия СКП ЭП в течение срока его действия.

5. ОБЯЗАННОСТИ УЧАСТНИКОВ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ

5.1. Обязанности УЦ

УЦ обязан:

- предоставить пользователю УЦ Сертификат Уполномоченного лица УЦ в электронной форме;
- Использовать для изготовления ключа электронной подписи Уполномоченного лица УЦ, только сертифицированные СКЗИ;
- принимать меры по защите ключа электронной подписи Уполномоченного лица УЦ от несанкционированного доступа;
- информировать Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей и о мерах, необходимых для обеспечения;
- обеспечить работоспособность аппаратных и программных средств УЦ;

- организовать работу своих служб по GMT (Greenwich Mean Time) с учетом часового пояса (г. Москва) и синхронизировать по времени все программные и технические средства обеспечения деятельности по предназначению;

обеспечить регистрацию пользователей УЦ по заявкам на подключение к СЗОПИ ViPNet с порядком регистрации, изложенным в настоящем Регламенте;

- не разглашать (публиковать) регистрационную информацию пользователей УЦ, за исключением информации, заносимой в изготавливаемые сертификаты;
- предоставлять безвозмездно лицам по их обращениям в соответствии с установленным порядком доступа к реестру сертификатов информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи;
- обеспечивать актуальность информации, содержащейся в реестре сертификатов и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- обеспечить уникальность серийных номеров в изготовленных сертификатах пользователей УЦ.
- приостановить действие Сертификата ключа подписи пользователя УЦ по заявлению на приостановление действия сертификата, в соответствии с порядком определенным в п. 9.7 настоящего Регламента.
- возобновить действие Сертификата пользователя УЦ по заявлению на возобновление действия сертификата (исключительно в случае поступления заявления в период срока, на который действие Сертификата было приостановлено), в соответствии с порядком, в п.9.8 настоящего Регламента.
- обеспечивать актуальность списка отозванных сертификатов (обновление СОС проводится УЦ по факту аннулирования (отзыва) или приостановления действия любого сертификата);
- публиковать Регламент и другие документы, необходимые для работы УЦ и пользователей УЦ;

организовать проверку готовности пользователей УЦ к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ (с указанием типа и номеров используемых СКЗИ, номеров аппаратных, программных и аппаратно-программных средств, где установлены или к которым подключены СКЗИ, с указанием также номеров печатей (пломбиров), которыми опечатаны (опломбированы) технические средства, включая СКЗИ, и результатов проверки функционирования СКЗИ);

разрабатывать мероприятия по обеспечению функционирования и безопасности применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам;

организовать обучение лиц, использующих СКЗИ, правилам работы с ними;

вести поэкземплярный учет, используемых СКЗИ, эксплуатационной и технической документации к ним;

- вести учет обслуживаемых пользователей УЦ, а также физических лиц, непосредственно допущенных к работе с СКЗИ;

осуществлять контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом на СКЗИ и настоящим Регламентом;

- организовать расследование с составлением заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты конфиденциальной информации, вести разработку и принимать меры по предотвращению возможных опасных последствий подобных нарушений;

5.2. Обязанности пользователей УЦ

5.2.1. Обязанности лиц, проходящих процедуру регистрации

- Лица, проходящие процедуру регистрации в сети услуг УЦ, обязаны представить регистрационную и идентифицирующую информацию в объеме, определенном положениями настоящего Регламента.
- Лица, проходящие процедуру регистрации в УЦ, несут ответственность за достоверность предоставленной регистрационной информации.
- Клиент обязан хранить в тайне предоставляемую ему ключевую и парольную информацию, однозначно идентифицирующую его в сети УЦ

5.2.2. Обязанности владельца сертификата ключей подписи

Владелец сертификата обязан:

- обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;
- уведомлять УЦ о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
- уничтожить ключи ЭП, срок действия которых закончен, которые были сгенерированны ошибочно и не подлежат использованию либо были скомпрометированы и их копии;
- вести поэкземплярный учет, используемых СКЗИ, эксплуатационной и технической документации к ним;
- организовать обучение лиц, использующих СКЗИ, правилам работы с ними;
- не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о ключах ЭП;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключи ЭП при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.

5.2.3. Обязанности Доверенных участников

Доверенный участник (пользователь, не являющийся владельцем сертификата) принимает на себя обязанности владельца сертификата.

Перед тем как использовать сертификат, Доверенный Участник должен удостовериться, что назначение сертификата соответствует предполагаемому использованию.

6. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

- Ключ электронной подписи пользователя УЦ является конфиденциальной информацией данного пользователя УЦ. Удостоверяющий центр не осуществляет хранение ключей электронной подписи пользователей УЦ;
- Персональная и корпоративная информация пользователей УЦ, содержащаяся в УЦ, не подлежащая непосредственной в качестве части СКП ЭП, списка отозванных сертификатов, считается конфиденциальной и не публикуется;
- Информация, не являющаяся конфиденциальной, публикуется по решению УЦ. Место, способ и время публикации определяется УЦ.

- Информация, включаемая в СКП ЭП пользователей УЦ и списки отозванных сертификатов, издаваемые УЦ, не считается конфиденциальной;
- Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной;
- Удостоверяющий центр не должен раскрывать информацию, относящуюся к типу конфиденциальной и информации, каким бы то ни было третьим лицам за исключением случаев требующих раскрытия в соответствии с действующим законодательством РФ или при наличии судебного постановления.

6.1. Обработка персональных данных

Подав заявление на подключение к системе СЗОПИ ViPNet и на изготовление сертификата ЭП, лицо, запросившее сертификат, дает согласие на обработку его персональных данных (а именно: фамилия, имя, отчество, серия и номер паспорта, кем и когда выдан, место работы, должность, телефон, факс, адрес электронной почты), для выпуска СКП ЭП на его имя. УЦ не имеет права передачи этих сведений третьим лицам (за исключением случаев, установленных законодательством РФ) и обязуется сохранить конфиденциальность этих данных**.**

6.2. Защита конфиденциальной информации

УЦ «Стандарт безопасности» обеспечивает сохранность и контроль доступа к конфиденциальной информации в соответствии с ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ «О персональных данных», «Специальными требованиями и рекомендациями по защите конфиденциальной информации от ее утечки по техническим каналам (СТР-К)», настоящим Регламентом, и другими нормативными документами в области обеспечения безопасности информации.

7. КРОССЕРТИФИКАЦИЯ

Процедуры и механизмы кроссертификации регламентируются отдельным соглашением между участниками кроссертификации. При проведении кроссертификации с другим удостоверяющим центром УЦ обращает внимание на следующие моменты: содержание Регламента и Политики применения сертификатов удостоверяющего центра, на его учредительные документы, общую информацию удостоверяющего центра, необходимую для установления доверительных отношений.

8. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ УЦ

- УЦ имеет разрешительную правовую базу для предоставления услуг удостоверяющего центра. Свою деятельность УЦ ведет в соответствие с Федеральными Законами РФ, полученными лицензиями, требованиями ФСБ РФ, руководящими документами Гостехкомиссии и ФСТЭК РФ, другими нормативно-правовыми документами в области защиты информации.
- Персонал УЦ имеет соответствующую подготовку для работы с СКЗИ;
- Помещения УЦ, где установлены СКЗИ, хранятся ключевые документы к ним, ведутся работы с использованием СКЗИ, обеспечивают сохранение конфиденциальности информации;
- Помещения УЦ имеют прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время, обеспечиваются меры по обеспечению контроля их вскрытия;

- Двери помещений постоянно закрыты на замок и открываются только для санкционированного прохода сотрудников и посетителей;
- Помещения УЦ оборудованы пожарно-охранной сигнализацией;
- Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей, документов, содержащих конфиденциальную информацию, помещения УЦ оборудованы необходимым числом металлических хранилищ, оборудованных внутренними замками с приспособлениями для опечатывания.
- Размещение, специальное оборудование, охрана и организация режима в помещениях ООО «Стандарт безопасности» исключают возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ;
- Установлен режим охраны помещений ООО Стандарт безопасности, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время. Установленный режим охраны предусматривает периодический контроль состояния технических средств охраны;
- Правом входа в помещения УЦ и правом их вскрытия обладают только лица, непосредственно допущенные к проведению регламентных работ в них.
- Правом входа в помещения УЦ и правом их вскрытия обладают только лица, непосредственно допущенные к проведению регламентных работ в них;
- Для обеспечения бесперебойной и отказоустойчивой работы программного комплекса производится периодическое резервное копирование электронной информации. Резервному копированию подлежат представленные в электронной форме: реестр УЦ, журналы аудита происходящих в УЦ событий, другие документы, определяемые УЦ. Доступ к резервным копиям устанавливается такой же, как и для действующих экземпляров;
- Проводится периодический контроль состояния защищенности информации, анализируется необходимость, и достаточность принятых мер по сохранению конфиденциальности информации;
- Для реализации предоставления услуг УЦ используются сертифицированные СКЗИ.

9. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ

9.1. Условия взаимоотношений

Взаимодействие Клиентов на предмет подключения и дальнейшего обслуживания в рамках сети УЦ производится УЦ.

Получение УЦ любых запросов на действия с сертификатами, не имеющих документального подтверждения необходимости этих действий непосредственно от Клиента, не обязывает УЦ производить эти действия.

9.2. Порядок подключения к услугам УЦ

9.2.1. Первичная регистрация

Для подключения к услугам УЦ пользователь заключает с УЦ Договор на предоставление услуг УЦ.

После заключения договора, пользователь оформляет и передает в УЦ следующие заверенные документы:

- копию Свидетельства о государственной регистрации и о постановке организации на налоговый учет

- Заявку пользователя на подключение к системе защищенного обмена персонифицированной информацией ООО «Стандарт Безопасности» ViPNet (Приложение №1);
- копию приказа о назначение ответственных лиц по работе с СКЗИ (Приложение №2).

После проверки полученных документов от пользователя УЦ регистрационная информация о пользователе УЦ вносится в реестр УЦ.

9.2.2. Перерегистрация

Перерегистрация производится в случае изменения данных (информации) пользователя УЦ, полученных УЦ в процессе первичной регистрации (перерегистрации).

В случае изменения данных пользователя УЦ, пользователь УЦ передает в УЦ документы, поданные при первичной регистрации, подтверждающие изменения данных (информации) пользователя УЦ.

Если при перерегистрации изменились данные, указанные в действующем сертификате пользователя УЦ, то происходит внеплановая замена ключей.

9.2.3. Удаление регистрационной информации

Удаление регистрационной информации пользователя УЦ из реестра УЦ производится в случае прекращения договорных отношений между пользователем УЦ и УЦ. Информация, документы пользователя УЦ передаются на хранение.

9.2.4. Ключевые носители

Для хранения и использования ключей электронной подписи, ключей проверки электронной подписи и Сертификатов пользователь УЦ должен иметь личный ключевой носитель. Ключевой носитель предоставляется пользователем УЦ, или по его заявлению и за отдельную плату предоставляется УЦ. Ключевой носитель, предоставляемый пользователем УЦ, должен удовлетворять следующим требованиям:

- входить в перечень ключевых носителей, определяемый УЦ;
- быть проинициализированным (отформатированным);
- не содержать ни какой информации, за исключением данных инициализации.

Ключевые носители, не удовлетворяющие указанным требованиям, для записи ключевой информации не принимаются.

При несанкционированном использовании ключевых носителей неуполномоченными лицами, и вследствие этого, возникновении ущерба для пользователя УЦ, всю полноту ответственности за последствия несет пользователь УЦ.

При использовании сертифицированных ключевых носителей к носителю прилагается сертификат соответствия, который подтверждает, что носитель прошел дополнительную проверку сертификационными центрами на предмет безопасности при соблюдении условий их использования и хранения в соответствии с требованиями эксплуатационной документации производителя.

9.2.5. Передача СКЗИ

Ключевой дистрибутив вместе с паролем доступа к нему, и эксплуатационно-технической документацией ПО ViPNet [Клиент] передается лично абоненту или его доверенному лицу по доверенности (по форме приложения 5) под роспись в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (форма 1)(Приложение №4) или в актах приема передачи СКЗИ (Приложение № 6). Журнал ведётся Уполномоченным лицом УЦ.

Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи ключей, то его каждый раз следует регистрировать отдельно.

Пользователи УЦ ведут у себя «Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (форма 2)» (Приложение №3).

9.3. Издание и получение СКП ЭП и ключей

9.3.1. Централизованная схема выпуска сертификатов

Процедура издания и получения сертификата заключается в следующем:

- Клиент заполняет «Заявку на изготовление сертификата ключа подписи для системы защищенного обмена ViPNet» (по форме приложения Приложение 1) и оформляет ее на бумажном носителе в двух экземплярах, заверив их своей рукописной подписью и печатью организации, и передает один экземпляр в УЦ;
- Клиент согласовывает с УЦ время прибытия в офис УЦ;
- Владелец сертификата (либо его полномочный представитель при наличии доверенности по форме Приложения 5) прибывает в УЦ, получает вырабатываемые администратором УЦ на «Заявки на изготовление сертификата ключа проверки электронной подписи для системы защищенного обмена ViPNet» ключи ЭП на ключевом носителе;
- Администратор УЦ оформляет СКП ЭП на бумажном носителе в двух экземплярах, заверяет их собственноручной подписью и печатью УЦ;
- Владелец (либо его полномочный представитель при наличии доверенности), заверяет собственноручной подписью два экземпляра сертификата, оформленных на бланках УЦ, с содержащимися на них печатью УЦ и подписью администратора УЦ. Один возвращает администратору УЦ, а второй оставляет себе;
- Клиент, на своем рабочем месте, либо представитель УЦ, в случае заказа услуги по установке ЭП клиентом, с помощью СКЗИ и согласно Руководству пользователя на СКЗИ вводит изданный сертификат в действие а так же проверяет статус всех сертификатов согласно их пути сертификации на предмет их действительности.

9.3.2. Удаленная схема выпуска сертификатов

Формирование ключей ЭП и ключей проверки ЭП и электронного запроса в УЦ на издание соответствующего сертификата производится Клиентом (владельцем сертификата) на рабочем месте абонента сети УЦ с помощью СКЗИ и в соответствии с руководством пользователя на СКЗИ. Электронный запрос в УЦ на сертификат по умолчанию шифруется и подписывается с помощью установленного СКЗИ и текущих ключей данного СУ.

Процедура издания и получения сертификата по удаленной схеме заключается в следующем:

- Клиент заполняет «Заявку пользователя на изготовление сертификата ключа подписи» (по форме приложения Приложение 1) и оформляет ее на бумажном носителе в двух экземплярах, заверив их своей рукописной подписью и печатью организации, и передает один экземпляр в УЦ;
- УЦ после получения Заявки, издает и автоматизировано по каналам сети УЦ высылает на рабочее место клиента изданный сертификат;
- для получения сертификата на бумажном носителе владелец сертификата (либо его полномочный представитель при наличии доверенности по форме Приложения 5) должен лично прибыть в УЦ, заверить собственноручной подписью два экземпляра сертификата оформленных на бланках УЦ с содержащейся на них печатью и подписью уполномоченного лица УЦ, и получить один экземпляр на руки.

9.3.3. Начало работы с сертификатом

Перед использованием сертификата Клиент обязан с помощью СКЗИ и согласно Руководству пользователя на СКЗИ ввести изданный УЦ сертификат в действие, а также проверить статус всех сертификатов согласно их пути сертификации на предмет их действительности.

Вводить сертификат в действие разрешается только после получения сертификата на бумажном носителе.

9.3.4. Хранение ключевых носителей

Личные ключевые носители рекомендуется хранить в сейфе. Пользователь УЦ несет персональную ответственность за хранение личных ключевых носителей.

9.3.5. Уничтожение ключей на ключевых носителях

Ключи на ключевых носителях, срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации.

Факт уничтожения оформляется актом (Приложение 7). Один экземпляр акта передается в УЦ.

Об уничтожении ключей делается соответствующая запись в журнале поэкземплярного учета СКЗИ.

9.3.6. Срок действия ключей подписи пользователя

Сроки действия ключей подписи и соответствующего сертификата пользователя составляют 1 (один) год.

9.4. Плановая смена ключей подписи

9.4.1. Плановая смена ключей пользователя УЦ

Плановая смена ключей пользователя УЦ происходит через год после начала действия сертификата СКП ЭП пользователя УЦ согласно разделу 5.5.1 либо 5.5.2 в зависимости от используемой клиентом схемы выпуска сертификатов.

9.4.2. Плановая смена ключей уполномоченного лица УЦ

Срок действия ключа ЭП Уполномоченного лица УЦ составляет 1 (один) год. Начало действия ключа ЭП Уполномоченного лица УЦ исчисляется с даты, времени начала действия соответствующего СКП ЭП.

Плановая смена ключей подписи Уполномоченного лица УЦ выполняется в соответствии со сроком действия и не позднее окончания срока действия текущего ключа ЭП Уполномоченного лица УЦ.

Процедура плановой смены ключей подписи Уполномоченного лица УЦ выполняется в порядке, определенном эксплуатационной документацией на программно-аппаратный комплекс УЦ.

9.5. Внеплановая смена ключей подписи

9.5.1. Внеплановая смена ключей подписи пользователя УЦ

Внеплановая смена ключей пользователя УЦ производится по инициативе пользователя в случае компрометации (угрозы компрометации) ключа ЭП пользователя УЦ, изменения данных, указанных в СКП ЭП пользователя УЦ, или в случае каких-либо объективных причин невозможности использования ключа ЭП. Пользователь УЦ подает в УЦ документы, подтверждающие причины внеплановой и переходит к процедуре замены согласно разделу 5.9.1 настоящего Регламента.

9.5.2. Внеплановая смена ключей подписи Уполномоченного лица УЦ

Внеплановая замена ключей уполномоченного лица УЦ происходит в случае компрометации (угрозы компрометации) ключа ЭП уполномоченного лица УЦ, изменения данных, указанных в СКП ЭП уполномоченного лица УЦ, или в случае каких-либо объективных причин невозможности использования ключа ЭП.

Процедура по внеплановой смене ключей подписи Уполномоченного лица УЦ выполняется в порядке, определенном эксплуатационно-технической документацией на СКЗИ.

9.6. Аннулирование (отзыв) СКП ЭП

Аннулирование (отзыв) СКП ЭП, изготовленного УЦ, осуществляется УЦ на основании письменного заявления от пользователя (Приложение 8).

При выполнении УЦ процедуры аннулирования (отзыва) СКП ему присваивается статус «отозван», серийный номер этого СКП вносится в СОС.

Срок обработки заявления на аннулирование СКП составляет 1 (один) рабочий день с момента поступления заявления в УЦ.

УЦ может по собственной инициативе отозвать СКП пользователя в случае установленного факта компрометации ключа подписи с уведомлением владельца отозванного сертификата с указанием обоснованных причин отзыва.

9.7. Приостановление действия сертификата

Приостановление действия СКП ЭП пользователя УЦ осуществляется УЦ на основании письменного заявления, поступающего в УЦ (Приложение №8).

При приостановлении действия СКП ЭП серийный номер этого СКП ЭП вносится в СОС.

Срок обработки заявления на приостановление действия СКП ЭП составляет 1 (один) рабочий день с момента поступления заявления в УЦ.

В случае если в течение срока приостановления действия СКП ЭП пользователя УЦ в УЦ не поступает заявление от пользователя УЦ о возобновлении действия СКП ЭП, СКП ЭП аннулируется (отзывается) УЦ.

УЦ может по собственной инициативе приостановить действие СКП пользователя, с уведомлением владельца приостановленного сертификата с указанием причин приостановления действия.

9.8. Возобновление действия сертификата ключа подписи

Возобновление действия СКП ЭП пользователя УЦ осуществляется УЦ на основании письменного заявления, поступающего в УЦ (Приложение №9).

При возобновлении действия СКП ЭП серийный номер этого СКП ЭП удаляется из СОС.

Срок обработки заявления на возобновление СКП ЭП пользователя составляет 1 (один) рабочий день с момента поступления заявления в УЦ.

10. ДЕЙСТВИЯ ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕЙ

Пользователь УЦ самостоятельно должен определить факт компрометации закрытого ключа и оценить значение этого события для пользователя УЦ.

Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует и осуществляет сам пользователь УЦ.

При компрометации ключа пользователя УЦ, он должен немедленно прекратить связь по сети с другими пользователями и немедленно подать заявление на аннулирование СКП ЭП (Приложение 6) в УЦ и выполнить процедуры, описанные в разделе 5.8 «Внеплановая смена ключа подписи».

При компрометации ключа уполномоченного лица УЦ, выполняются процедуры, описанные в разделе «Внеплановая смена ключа уполномоченного лица УЦ ».

11. ОБУЧЕНИЕ

УЦ осуществляет проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ и составление заключений (Приложение №10) о возможности эксплуатации СКЗИ (с указанием типа и номеров используемых СКЗИ, номеров аппаратных, программных и аппаратно-программных средств, где установлены или к которым подключены СКЗИ, с указанием также номеров печатей (пломбиров), которыми опечатаны (опломбированы) технические средства, включая СКЗИ, и результатов проверки функционирования СКЗИ).

Непосредственно к самостоятельной работе с СКЗИ допускаются лица, прошедшие специальную подготовку (обучение) правилам работы с СКЗИ.

Документом, подтверждающим должную специальную подготовку лица и возможность его допуска к самостоятельной работе с СКЗИ, является заключение (Приложение №11), составленное комиссией сотрудников УЦ.

12. ХРАНЕНИЕ СКП ЭП В УЦ

Срок хранения СКП ЭП в УЦ осуществляется в течение всего периода его действия и 5 (пять) лет после его аннулирования (отзыва). По истечении указанного срока хранения СКП ЭП переводятся в режим архивного хранения.

13. АРХИВНОЕ ХРАНЕНИЕ

13.1. Документы, подлежащие архивному хранению

Следующие документы подлежат архивному хранению в УЦ:

- аннулированные СКП ЭП уполномоченного лица УЦ;
- копия приказа о назначении лица, ответственного за работу с СКЗИ с правом оформления документов от имени организации пользователя УЦ;
- акт о готовности эксплуатации СКЗИ;
- заключение о допуске ответственного лица к самостоятельной работе с СКЗИ;
- аннулированные СКП ЭП пользователей УЦ;
- акт уничтожения криптографических ключей;
- заявка на изготовление СКП ЭП;
- заявления на аннулирование (отзыв) СКП ЭП;
- заявления на приостановление действия СКП ЭП;
- заявления на возобновление действия СКП ЭП;
- служебные документы УЦ.

13.2. Срок архивного хранения

Документы, подлежащие архивному хранению, являются документами временного хранения. Срок хранения архивных документов – 5 (пять) лет.

13.3. Уничтожение архивных документов.

Выделение архивных документов к уничтожению и уничтожение осуществляется комиссией, формируемой и сотрудников УЦ.

14. ПОРЯДОК РАЗБОРА КОНФЛИКТНЫХ СИТУАЦИЙ

14.1. Между участниками сети УЦ возможно возникновение конфликтных ситуаций, связанных с формированием, доставкой, получением, подтверждением получения ЭД, а также использованием в данных документах ЭП. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

- не подтверждение подлинности защищенных электронных документов средствами проверки ЭП получателя;
- оспаривание факта идентификации владельца ЭП, подписавшего ЭД;
- заявление отправителя или получателя ЭД об его искажении;
- оспаривание факта отправления и/или получения защищенного ЭД;
- оспаривания времени отправления и/или получения защищенного ЭД;
- иные случаи возникновения конфликтных ситуаций.

При возникновении споров стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть, путем переговоров. В случае невозможности разрешения споров путем переговоров они будут разрешаться в Арбитражном суде Ярославской области в порядке, предусмотренным законодательством РФ.

14.2. Разбор конфликтных ситуаций осуществляется в два этапа. Сначала, путем взаимодействия пользователя УЦ, у которого возникли претензии, с Уполномоченным лицом УЦ. В случае если абонент не удовлетворен полученной информацией, для разрешения конфликтной ситуации проводится техническая экспертиза в соответствии с Порядком разрешения конфликтных ситуаций (Приложение №12 к настоящему Регламенту)

15. ФОРС-МАЖЕР

15.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по настоящему Регламенту, если оно явилось следствием непреодолимой силы. Под обстоятельствами непреодолимой силы понимаются возникшие после присоединения к настоящему Регламенту непредвиденные, неотвратимые и непреодолимые для Сторон События чрезвычайного характера (пожар, наводнение и другие стихийные бедствия), а, также, события, имеющие обязательную силу хотя бы для одной из Сторон, постановления и распоряжения Правительства РФ, делающие Регламент невыполнимым и невыгодным.

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

15.3. Сторона, для которой создалась невозможность исполнения своих обязательств по настоящему Регламенту, должна немедленно известить в письменной форме другую сторону о наступлении, но в любом случае не позднее 5 (пяти) календарных дней после начала их действия, предполагаемом сроке действия и прекращении форс-мажорных обстоятельств, а также представить документальные доказательства существования названных обстоятельств и их влиянии на исполнение Регламента и других соглашений.
15.4. Не извещение или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства.
15.5. В случае, если невозможность полного или частичного исполнения сторонами какого-либо обязательства по Регламенту или другим соглашениям обусловлена действием форс-мажорных обстоятельств и существует свыше 1 (одного) месяца, то каждая из сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства (либо внесения в соглашения соответствующих изменений и дополнений) путем направления одной из сторон другой стороне письменного уведомления (но не позднее, чем за 10 (десять) календарных дней до отказа от исполнения обязательства) и в этом случае ни одна из сторон не обязана возмещать реальный ущерб, а финансовые расчеты производятся за фактически оказанные по настоящему Регламенту или другим соглашениям услуги.

16. ПРИЛОЖЕНИЯ

Приложение №1
к Регламенту

Заявка на изготовление сертификата ключа проверки электронной подписи для системы защищенного обмена персонифицированной информацией ViPNet

Директору
ООО "Стандарт безопасности"
Рачкову М.С.

от _____

(должность, фамилия, имя, отчество руководителя)

ИНН | | | | | | | | | | | |
КПП | | | | | | | | | |
ОГРН | | | | | | | | | | | | | |

Полное наименование организации

Юридический адрес организации

Фактический адрес организации (адрес установки)

Прошу сформировать ключевую информацию для сотрудника нашей организации:

Личная подпись _____

Фамилия
Имя
Отчество
Должность
СНИЛС

Паспортные данные: **серия** | | | | **номер** | | | | | | **когда выдан** | | . | | | . | | |

кем выдан

Записать ключ на etoken ☐
(если отмечено стоимость etoken будет включена в счет)

Контактное лицо

Направление обмена
(с кем необходимо обмениваться)
-Электоронный документооборот с
-Электоронный документооборот с
-Электоронный документооборот с

телефон **факс**
e-mail организации
выставление счетов: ☐ **по факсу** ☐ **по email** ☐ **оригинал**

М.П. "___"_____201_ г. **Руководитель** _____/_____/

Согласие на обработку персональных данных

Я, нижеподписавшийся(аясь), даю согласие оператору персональных данных - ООО "Стандарт безопасности", находящемуся по адресу: г. Ярославль, ул. Угличская, д.39В, офис 211 на обработку моих персональных данных.
Мои персональные данные, в отношении которых дается согласие включают в себя:
фамилию, имя, отчество, паспортные данные, сведения о месте работы и занимаемой должности, служебный телефон, факс, адрес электронной почты.
Согласие на обработку вышеобозначенных персональных данных дается оператору в целях формирования (генерации) и обслуживания ключевого материала, необходимого для установления и поддержания защищенного соединения между участниками защищенного информационного обмена, а так же разбора конфликтных ситуаций.
Действия с вышеобозначенными персональными данными включают в себя: сбор, систематизацию, накопление, хранение, уточнение, использование, уничтожение персональных данных.
Обработка обозначенных выше персональных данных осуществляется строго для достижения вышеизложенных целей.
Характер обработки обозначенных выше персональных данных: частично автоматизированная обработка персональных данных с использованием средств вычислительной техники.
Данное согласие действует в течение всего срока действия соглашения о защищенном информационном взаимодействии.
Данное согласие может быть отозвано в порядке, установленном Законодательством РФ.

"____"_____201_ _____ _____
дата подпись расшифровка подписи

Заявка заполняется на компьютере или вручную печатными буквами и передается вместе с реквизитами в ООО "Стандарт безопасности" по адресу: 150047, г. Ярославль, ул. Угличская 39В, офис 207. Тел. 8-(4852)-587-300 Факс 8-(4852)-587-302
Наш адрес в сети Интернет http://www.secst.ru , email:nalog@secst.ru

Приложение №2
к Регламенту
Форма приказа о назначении ответственных лиц по работе с СКЗИ

_____
(наименование организации)

ПРИКАЗ

«____» _____20___г. № _____

_____
(город)

О назначении ответственных лиц по работе с СКЗИ

Во исполнение «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13.06.2001г. №152

ПРИКАЗЫВАЮ:

Назначить _____
(ФИО и должность)

_____
(ФИО и должность)

Ответственным (и) за работу со средствами криптографической защиты информации (СКЗИ) (ПК) ViPNet Клиент, конфиденциальными сведениями, ключевыми дискетами и ключевой документацией и представлять интересы

_____
(название организации)

с правом подписывать с применением электронной цифровой подписи документы в соответствии со следующими областями применения:

- Электронный документооборот с _____
- Электронный документооборот с _____

* - выбрать области, в которых ЭЦП будет иметь юридическую значимость.

Руководитель организации: _____ /_____/
(подпись) *(инициалы и фамилия)*

М.П.

С приказом ознакомлен (ы):

_____ /_____/ «___» _____ 20___ г.
(подпись ответственного лица) *(инициалы и фамилия)*

_____ /_____/ «___» _____ 20___ г.
(подпись ответственного лица) *(инициалы и фамилия)*

Приложение №3
к Регламенту

Форма журнала
поэкземплярного учета СКЗИ

Журнал
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (форма 2)

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографи-ческие номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводи-тельного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение №4
к Регламенту
Форма журнала
поэкземплярного учета СКЗИ

Журнал
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (форма 1)

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о рассылке (передаче)		
				От кого получены или Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводительного письма	Дата и номер подтверждения или расписка в получении
1	2	3	4	5	6	7	8	9

Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
Дата и номер сопроводительного письма	Дата и номер сопроводительного письма			Дата уничтожения	Номер акта или расписка об уничтожении	
10	11	12	13	14	15	16

Приложение №5
к Регламенту
Форма доверенности

Д О В Е Р Е Н Н О С Т Ь № _____

Дата выдачи «____» _____ 20__ г. Действительна по «____» _____ 20__ г.

Я, _____ ,
(фамилия, имя, отчество)

_____
(должность, название организации)

ДОВЕРЯЮ _____
(фамилия, имя, отчество)

_____
(должность, название организации)

Паспорт _____ _____
(серия) (номер)

Выдан _____ _____
(кем выдан) (дата выдачи)

ВЫПОЛНИТЬ СЛЕДУЮЩЕЕ:

- Получить Договора с ООО «Стандарт безопасности»;
- Вместо меня присутствовать при изготовлении моих криптографических ключей (ЭП, шифрования) и сертификатов;
- Получить СКЗИ;
- Получить ключевые носители;
- Получить и подписать сертификат ключа проверки электронной подписи и акты выполненных работ;
- Расписаться за меня в соответствующих документах для исполнения поручений.

Подпись лица, получившего доверенность _____ _____
(подпись) (фамилия, имя, отчество)

Подпись лица, выдавшего доверенность _____ _____
(подпись) (фамилия, имя, отчество)

УДОСТОВЕРЯЮ _____ _____ _____
(руководитель организации) (подпись) (фамилия, имя, отчество)

М. П.

Приложение №6
к Регламенту
Форма акта приема-передачи СКЗИ

АКТ№
Приема-передачи средств криптографической защиты информации(СКЗИ), эксплуатационной документации к ним и электронной цифровой подписи.

Настоящий Акт составлен в том, что представитель органа криптографической защиты компании ООО «Стандарт безопасности» передал ,а
Пользователь СКЗИ: _____
(фамилия, имя, отчество, должность)

Получил(а):

- СКЗИ ПК ViPNet Клиент КС2 № _____
  ЭЦП регистрационный номер:_____
  (действительна с: _____ по _____)
- USB-ключ eToken PRO (Java) № _____

для осуществления информационного обмена в электронном виде по телекоммуникационным каналам связи.

От центра криптографической защиты
ООО «Стандарт безопасности»

_____ _____
(подпись) (расшифровка)

Специалист отдела электронного документооборота

М.П.

_____/_____

« » _____ 2011 г.

М. П.

Приложение №7
к Регламенту
Форма акта уничтожения ключей

Акт №____

Уничтожения криптографических ключей

Настоящий акт составлен в том, что уничтожены следующие криптографические ключи (путем форматирования или физического разрушения ключевого носителя):

_____
(наименование организации)

№	ID ключа	Владелец ключа
1.		
2.		
3.		

Всего уничтожено _____(_____) криптографических ключей

От центра криптографической защиты
ООО «Стандарт безопасности»

Специалист электронного документооборота
_____/Платонов В.С./

_____ _____
(подпись) (фамилия, имя, отчество пользователя)

М.П.

М.П.

« » _____ 201__ г.

Приложение №8
к Регламенту
Форма заявления на аннулирование (отзыв) сертификата ключа проверки ЭП

Директору ООО «Стандарт безопасности»
Рачкову М.С.

От: _____
(Ф.И.О. ответственного лица)
_____

ЗАЯВЛЕНИЕ
на аннулирование (отзыв) сертификата ключа проверки ЭП

Прошу Вас аннулировать (отозвать) сертификат ключа проверки ЭП, серийный номер сертификата: _____, владельцем которого я являюсь, в связи с _____.
(указать причину отзыва)

Владелец сертификата ключа проверки ЭП: _____ /_____/
(подпись) *(расшифровка подписи)*

«___» _____ 20___ г.

Приложение №9
к Регламенту
Форма заявления на приостановление действия сертификата ключа проверки ЭП

Директору ООО «Стандарт безопасности»
Рачкову М.С.

От: _____
(Ф.И.О. ответственного лица)
_____

ЗАЯВЛЕНИЕ
на приостановление действия сертификата ключа проверки ЭП

Прошу Вас приостановить действие сертификата ключа проверки ЭП, серийный номер сертификата: _____, владельцем которого я являюсь, сроком на _____ в связи с_____
_____.
(указать причину приостановления)

Владелец сертификата ключа проверки ЭП: _____ /_____/
(подпись) *(расшифровка подписи)*

«___» _____ 20___ г.

Приложение №10
к Регламенту
Форма акта о готовности эксплуатации СКЗИ

АКТ
о готовности эксплуатации СКЗИ

Настоящий Акт составлен в том, что представитель органа криптографической защиты в лице __(должность, ФИО)__, являющийся представителем ООО «Стандарт безопасности» выполнил настройку и запуск СКЗИ (ПК) ViPNet Клиент КС2, версии 3.х
№ _____.
И в соответствии с «Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации (СКЗИ) с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной Приказом ФАПСИ №152 от 13.06.2001г., эксплуатационно-технической документацией и следующими данными о

_____
(название организации)

1. Расположение тех. средств с СКЗИ (насел. пункт, ул., дом, каб.)_____
_____.
2. Инвентарный или заводской № ПЭВМ (где используется СКЗИ) _____
_____.
3. Печать (которой опечатана ПЭВМ):_____ .
4. Используемое программное обеспечение (версия и код операционной системы, ПО):_____
_____.

проведенными работами по проверке функционирования СКЗИ, а также на основании соответствующей подготовки лиц, использующих СКЗИ, делает вывод о
_____ вышеуказанной организации требованиям
(соответсвует\не соответствует)

«Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной Приказом ФАПСИ №152 от 13.06.2001г. и она _____к самостоятельному использованию СКЗИ.
(Готова\не готова)

Представитель Заказчика, в лице

_____
(ФИО и должность ответственного лица)
принял в эксплуатацию систему с установленным СКЗИ. Замечаний по настройке и вводу в эксплуатацию нет.

Специалист отдела электронного
Документооборота

_____ _____ _____/_____
(подпись) (расшифровка)

М.П. М.П.

« » _____ 201_ г.

Приложение №11
к Регламенту
Форма заключения о допуске ответственного лица к самостоятельной работе с СКЗИ

ЗАКЛЮЧЕНИЕ
о допуске ответственного лица к самостоятельной работе с СКЗИ

Комиссия сотрудников ООО «Стандарт безопасности» в составе:

_____
_____
_____
в соответствии с «Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной Приказом ФАПСИ №152 от 13.06.2001г. установила, что лицо, ответственное за использование СКЗИ обучено правилам работы с ними.

ФИО, должность лица, ответственного за работу с СКЗИ: _____
Организация:_____

Прошел(а) обучение по использованию СКЗИ (ПК) ViPNet Клиент КС2. С правилами работы в соответствии с нормативными документами формуляра на СКЗИ ознакомлен(а)**,** их содержание понял(а)**,** полностью с ними согласен(а) и при работе с криптографическими ключами и СКЗИ обязуется:

- не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе сведения о криптоключах;
- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
- сообщать в орган криптографической защиты о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с установленным порядком при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ (сейфов), личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений;
- устанавливать и использовать на ПЭВМ на котором установлено СКЗИ только лицензионное программное обеспечение;
- зарегистрировать СКЗИ согласно Приказу ФАПСИ от 13 июня 2001 г. N 152

Ответственное за работу с СКЗИ лицо: _____/_____
подпись *расшифровка*

Комиссия делает вывод, что ответственное лицо вышеуказанной организации _____ к самостоятельной работе с СКЗИ.

	Члены комиссии:
	_____/_____ _____/_____ _____/_____