**Процедуры электронного документооборота**

**1. Термины и определения**

1.1. В настоящих Процедурах применяются следующие термины:

## **Авторство документа** - принадлежность документа одной из Сторон по настоящему Соглашению.

## **Аутентификация информации** - установление подлинности информации исключительно на основе внутренней структуры самой информации, установление того факта, что полученная законным получателем информация была передана подписавшим ее законным отправителем (источником) и при этом не была искажена.

## **Документ в бумажной форме (документированная информация)** - зафиксированная в бумажной форме информация с реквизитами, позволяющими ее идентифицировать.

**Документ в электронной форме (электронный документ)** - информация, представленная в электронной форме в виде файла или записи базы данных, подписанная электронной цифровой подписью и хранящаяся на магнитном носителе

## **Доступность информации** - свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

## **Зашифрование данных** - процесс преобразования открытых данных в зашифрованные при помощи шифра. Для зашифрования данных используется сертифицированные ФСБ программное средство криптографической защиты информации «КриптоПро CSP» и ПО «КриптоАРМ».

## **Защита информации** – комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.

## **Компрометация ключа** - утрата доверия к тому, что используемые ключи обеспечивают подлинность, защищенность и безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

1. утрата ключевого носителя;
2. утрата ключевого носителя с последующим обнаружением;
3. увольнение сотрудников, имевших доступ к ключевой информации;
4. возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
5. нерасшифровывание входящих или исходящих сообщений у абонентов;

## **Конфиденциальная информация -** документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и соглашением сторон.

## **Конфиденциальность информации** - субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

## **Контроль доступа** - процесс ограничения доступа к ресурсам системы предотвращающих их несанкционированное использование.

## **Криптографическая защита** - защита данных при помощи криптографического преобразования данных.

## **Криптографический ключ** - конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

## **Криптографическое преобразование** - преобразование данных при помощи шифрования и (или) выработки имитовставки.

## **Некорректный электронный документ** - электронный документ, не прошедший процедуры расшифрования данных, проверки электронной цифровой подписи, контроля формата документов, а также документ, имеющий искажения в тексте сообщения (наличие символов, букв или цифр в расшифрованном (открытом) тексте документа, не позволяющих понять его смысл).

## **Несанкционированный доступ к информации** - доступ к информации, нарушающий установленные правила разграничения доступа в результате случайных или преднамеренных действий пользователей или других субъектов, с использованием штатных средств, предоставляемых автоматизированной системой. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения автоматизированной системы.

## **Обработка информации** - передача, прием, хранение, преобразование и отображение информации.

## **Пароль** - секретная информация аутентификации, обычно представляющая собой строку знаков, которой должен обладать пользователь для доступа к защищенным данным.

## **Плановая смена ключей** - смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

## **Полномочный представитель** - представитель из числа первых должностных лиц в соответствии с уставным документом или, имеющий соответствующую доверенность.

## **Проверка электронной подписи документа** - проверка соотношения подписи под этим документом и открытого ключа подписавшего абонента. Если рассматриваемое соотношение оказывается выполненным, то подпись признается правильной, а сам документ - подлинным, в противном случае документ считается измененным, а подпись под ним - недействительной.

## **Открытый ключ** - криптографический ключ, который связан с секретным с помощью особого математического соотношения. Открытый ключ известен всем другим пользователям системы и предназначен для проверки электронной цифровой подписи и расшифрования, позволяет определить автора подписи и достоверность электронного документа, но не позволяет вычислить секретный ключ.

## **Расшифрование данных** - процесс преобразования зашифрованных данных в открытые при помощи шифра.

## **Секретный ключ** - криптографический ключ, который хранится пользователем системы в тайне. Он используется для формирования электронной цифровой подписи и шифрования.

## **Управление ключами** - создание (генерация) ключей, их хранение, распространение, удаление (уничтожение), учет и применение в соответствии с политикой безопасности.

## **Целостность информации** - свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

## **Электронная цифровая подпись (ЭЦП)** - данные, добавляемые к блоку данных или полученные в результате его криптографического преобразования, которые позволяют приемнику данных удостовериться в целостности блока данных и подлинности источника данных, а так же обеспечить защиту от подлога со стороны приемника данных. Для выработки и проверки электронной цифровой подписи используется сертифицированные ФСБ программное средство криптографической защиты информации «КриптоПро CSP» и ПО «КриптоАРМ».

## **Шифрование** - процесс зашифрования или расшифрования.

## **Шифрование документов (текстов)** - преобразование формы исходных (открытых) текстов сообщений таким образом, что их смысл становится непонятным для любого лица, не владеющего секретом обратного преобразования.

1.2. Остальные термины и определения, используемые в настоящих Процедурах ЭДО, должны пониматься в соответствии с действующим законодательством Российской Федерации.

**2. Общие положения**

2.1. Настоящие Процедуры ЭДО устанавливают условия перехода Сторон к ЭДО, порядок формирования, передачи, приема и обработки электронных документов.

2.2. Для начала работы Стороны:

2.2.1. подписывают Соглашение об электронном документообороте;

2.2.2. подписывают Договор на предоставление и техническое сопровождение программных продуктов;

2.2.3. устанавливают СКЗИ и обмениваются открытыми криптографическими ключами для проверки ЭЦП и открытыми криптографическими ключами шифрования;

2.2.4. подписывают Акт о начале электронного документооборота.

2.3. Обмен электронными документами между Сторонами в соответствии с настоящими Процедурами осуществляется следующими средствами:

* электронной почтой по протоколу SMTP;
* средствами передачи файлов по протоколу FTP.

2.4. Стороны обязуются использовать для реализации шифрования и ЭЦП программный продукт «КриптоПро CSP». Использование иных программных продуктов должно оговариваться в отдельном соглашении Сторон.

2.5. Стороны осуществляют проверку аутентичности электронных документов:

- с использованием средства криптографической защиты информации «КриптоПро CSP» (далее – СКЗИ) и ПО «КриптоАРМ», сертифицированных ФСБ;

- с использованием легальных электронных ключей, выданных лицензированной ФСБ организацией.

2.6. Используемые при информационном взаимодействии Сторон электронные документы, подготовленные с использованием СКЗИ, имеют равную юридическую силу с документами на бумажном носителе, подписанными уполномоченными представителями и скрепленными печатями Сторон (независимо от того существуют такие документы на бумажных носителях или нет).

2.7. Стороны признают, что использование ими СКЗИ, обеспечивающего шифрование и ЭЦП, достаточно для защиты информации от несанкционированного доступа, а также подтверждения подлинности и авторства электронных документов, а также разбора конфликтных ситуаций по ним.

**3. Формирование электронных документов**

3.1. Для формирования электронных документов Стороны вправе использовать собственное программное обеспечение или стандартное программное обеспечение.

3.2. Все формы документов, передаваемые в соответствии с настоящими Процедурами ЭДО, должны соответствовать формам документов, представленным в \_\_\_\_\_\_\_\_\_\_\_, а также иным требованиям, устанавливаемым \_\_\_\_\_\_\_\_\_\_\_\_.

3.2. К файлам с электронными документами предъявляются следующие требования:

* имя файла могут составлять только буквы латинского алфавита (независимо от регистра) и цифры;
* документы могут передаваться в текстовом или графическом форматах, а также формате XML (extended markup language) на основе спецификации \_\_\_\_\_\_\_\_\_\_\_\_\_\_ и переносимом формате документов PDF;
* файл с документом в текстовом формате должен иметь одно из следующих расширений RTF, DOC, TXT, XLS;
* файл с документом в графическом формате должен иметь расширение TIFF (тип формата – сжатый TIFF) или JPEG;
* файл с документом в формате XML должен иметь такое же расширение (XML).

Допускается передача электронных документов, соответствующих указанным выше требованиям, в заархивированном виде (файлы с расширением ZIP, RAR).

**4. Прием-передача и обработка электронных документов**

4.1. Прием-передача и обработка электронных документов Сторонами осуществляется в сроки не позднее времени, определенного соответствующими договорами и соглашениями Сторон об оказании услуг.

4.2. Прием электронных документов \_\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ производится путем расшифрования и сверки ЭЦП на полученных документах. По результатам приема электронных документов \_\_\_\_\_\_\_\_\_ направляет \_\_\_\_\_\_\_\_\_\_ электронное письмо, подтверждающее получение письма с электронными документами.

4.3. Прием электронных документов \_\_\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_ производится аналогично порядку, описанному в п. 4.2

4.4. Если Сторона-отправитель электронного документа не получила в течение дня, следующего за датой отправки соответствующего Отчета, то Сторона-отправитель по телефону информирует об этом Сторону-получателя. Последняя обязана незамедлительно отправить соответствующий Отчет.

4.5. Сторона-отправитель, допустившая некорректность при формировании электронного документа, после получения уведомления об этом от стороны-получателя, обязана незамедлительно направить другой Стороне исправленный электронный документ.

**5. Порядок разрешения конфликтных ситуаций и споров, возникших в связи с осуществлением электронного документооборота.**

5.1. При возникновении конфликтных ситуаций, споров между Сторонами, связанных с установлением авторства и целостности электронного документа, подготовленного и переданного по электронной почте в соответствии с Соглашением об электронном документообороте, Сторона-инициатор в срок три рабочих дня с момента, когда ей стало известно о нарушении ее права, обязана направить другой Стороне уведомление о конфликтной ситуации, с подробным изложением обстоятельств происшедшего.

5.2. Сторона, которой направлено уведомление, обязана незамедлительно, но не позднее, чем в течение следующего рабочего дня, проверить наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и направить уведомителю информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации.

5.3. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от Стороны, которой направлялось уведомление.

5.4. В случае, если уведомитель не удовлетворен информацией, полученной от другой Стороны, для рассмотрения конфликтной ситуации формируется Согласительная комиссия.

5.5. Не позднее чем на следующий рабочий день после того, как принято решение о необходимости сформировать Согласительную комиссию, или не позднее, чем на шестой рабочий день после получения уведомления о конфликтной ситуации, в случае, если конфликтная ситуация не была урегулирована в рабочем порядке, Согласительная комиссия должна быть сформирована.

5.6. В состав Согласительной комиссии входит равное количество, но не менее чем по одному уполномоченному представителю каждой из конфликтующих сторон. В состав Согласительной комиссии, как правило, назначаются специалисты из числа сотрудников технических служб, служб информационной безопасности сторон. Лица, входящие в состав Согласительной комиссии, должны обладать необходимыми знаниями в области построения системы криптозащиты, работы компьютерных информационных систем.

5.7. Сформированная Согласительная комиссия при рассмотрении конфликтной ситуации устанавливает на технологическом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о факте и времени составления и/или отправки электронного документа, его подлинности, а также о подписании электронного документа конкретной электронной подписью, аутентичности отправленного документа полученному.

5.8. По результатам работы Согласительной комиссией принимается решение простым большинством голосов членов комиссии. Решение комиссии фиксируется в Акте, который составляется и подписывается всеми членами Согласительной комиссии.

5.9.  В Акте в обязательном порядке отражаются:

* установленные обстоятельства;
* действия членов Комиссии;
* выводы, влияющие на возможность установления подлинности оспариваемых документов.

5.10. Акт, составленный Согласительной комиссией, является доказательством при дальнейшем разбирательстве спора в суде.

5.11. В случае, если конфликтная ситуация полностью или частично не урегулирована в результате работы Согласительной комиссии, то такие споры и/или разногласия разрешаются в порядке, установленном действующим законодательством Российской Федерации.

**6. Разрешение споров**

* 1. В случае возникновения споров о наличии ЭЦП на электронном документе бремя доказывания лежит на Стороне, не соглашающейся с наличием ЭЦП.
  2. В случае возникновении споров о факте внесения изменений в электронный документ после его подписания ЭЦП бремя доказывания лежит на Стороне, утверждающей, что в данный документ были внесены изменения после подписания данного документа сотрудником этой Стороны.
  3. В случае возникновения споров о факте получения одной из Сторон какого-либо документа, подписанного ЭЦП, от другой Стороны бремя доказывания лежит на Стороне, не соглашающейся с фактом получения кем-либо электронного документа, подписанного ЭЦП.