

ПРАВИЛА
электронного документооборота в системе электронного документооборота
министерства финансов Кировской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Термины и определения

В целях настоящего документа используются следующие термины и определения:

Автоматизированное рабочее место (АРМ) – установленные у Организатора и Участника (далее – Стороны) программное обеспечение (далее – ПО) и технические средства, включая средства криптографической защиты информации (далее – СКЗИ), предназначенные для работы в системе электронного документооборота.

Программное обеспечение (ПО) – совокупность программ и программных средств, необходимых для их эксплуатации.

Система электронного документооборота (СЭД) – совокупность ПО и технического оборудования, обеспечивающая процесс обмена электронными документами между Сторонами.

Удостоверяющий центр (УЦ) – учреждение, осуществляющее выполнение функций удостоверяющего центра.

Уполномоченное лицо – лицо, имеющее право подписи электронного документа (ЭД).

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 подписи (Сертификат) – документ на бумажном носителе или электронный документ, заверенный ЭП УЦ, который включает в себя открытый ключ подписи владельца Сертификата. Сертификат выдается УЦ для подтверждения подлинности ЭП и идентификации владельца Сертификата.

Владелец сертификата ключа подписи – физическое лицо, на имя которого УЦ выдан Сертификат, и которое владеет соответствующим закрытым ключом подписи, позволяющим с помощью средств ЭП создавать свою ЭП в ЭД (подписывать ЭД).

Закрытый ключ аутентификации – уникальная последовательность символов, известная владельцу Сертификата открытого ключа аутентификации (Администратору АРМ Участника) и предназначенная для аутентификации Участника на стороне Организатора с последующим установлением защищенного (шифрованного) канала связи при информационном взаимодействии в СЭД между Сторонами с использованием СКЗИ (для защиты информации при ее передаче по открытым каналам связи).

Закрытый ключ подписи – уникальная последовательность символов, известная владельцу Сертификата и предназначенная для проверки в ЭД электронной подписи с использованием СКЗИ.

Заявка на получение сертификата ключа подписи – документ на бумажном носителе, содержащий распечатку значения открытого ключа подписи Пользователя в шестнадцатеричной системе исчисления, наименование Участника и иные идентифицирующие Пользователя реквизиты, подписанный собственноручными подписями Пользователя и руководителя Участника и заверенный оттиском печати Участника.

Компрометация закрытого ключа подписи – событие, определенное владельцем Сертификата, как ознакомление неуполномоченным лицом (лицами) с его закрытым ключом подписи, хищение, утеря носителя закрытого ключа подписи, несанкционированное копирование или другие причины появления у владельца Сертификата сомнений в сохранении тайны закрытого ключа подписи.

Корректная ЭП – ЭП лица, имеющего право подписи соответствующего документа, и для этой ЭП соблюдены следующие условия:

- ЭП оформлена на лицо, имеющее право первой или второй подписи платежных документов, включенное в карточку образцов подписей к лицевым счетам, открытым в министерстве финансов Кировской области;
- сертификат ключа подписи (далее – Сертификат), относящийся к этой ЭП, издан УЦ и не утратил силу (действует) на момент подписания и проверки ЭД;
- подтверждена подлинность этой ЭП в ЭД;
- ЭП используется в соответствии со сведениями, указанными в Сертификате.

Носитель ключевой информации – материальный носитель информации, содержащий закрытый ключ подписи или аутентификации.

Открытый ключ аутентификации – уникальная последовательность символов, соответствующая закрытому ключу аутентификации, доступная Сторонам и предназначенная для подтверждения подлинности Участника при его аутентификации на стороне Организатора с последующим установлением защищенного (шифрованного) канала связи при информационном взаимодействии в СЭД между Сторонами с использованием СКЗИ (для защиты информации при ее передаче по открытым каналам связи). Принадлежность открытого ключа аутентификации владельцу подтверждается Сертификатом открытого ключа аутентификации, изданным Администратором безопасности информации Организатора.

Открытый ключ подписи – уникальная последовательность символов, соответствующая закрытому ключу подписи, доступная Сторонам и предназначенная для подтверждения подлинности ЭП в ЭД. Принадлежность открытого ключа владельцу Сертификата в СЭД подтверждается Сертификатом, изданным УЦ.

Отправитель – юридическое лицо в СЭД, которое само непосредственно отправляет ЭД или от имени которого направляется ЭД.

Подтверждение подлинности ЭП в ЭД – положительный результат проверки принадлежности ЭП в ЭД владельцу Сертификата и отсутствия искажений в подписанном данной ЭП ЭД.

Получатель – юридическое лицо в СЭД, которому ЭД отправлен самим отправителем или от имени отправителя.

Пользователи – лица Сторон, осуществляющие формирование, подписание, отправку, получение, проверку, хранение и учет ЭД и обеспечивающие эксплуатацию ПО и технических средств АРМ.

Пользователь сертификата ключа подписи – физическое лицо, использующее полученные у Организатора сведения о Сертификате для проверки принадлежности ЭП владельцу Сертификата.

Сертификат открытого ключа аутентификации – электронный документ, который включает в себя открытый ключ аутентификации владельца. Сертификат открытого ключа аутентификации издается Администратором безопасности информации Организатора для обеспечения аутентификации Участника на стороне Организатора с последующим установлением защищенного (шифрованного) канала связи при информационном взаимодействии в СЭД между Сторонами с использованием СКЗИ (для защиты информации при ее передаче по открытым каналам связи).

Администратор АРМ Участника – сотрудник Участника, отвечающий за обеспечение бесперебойной эксплуатации ПО и технических средств АРМ Участника, контроль мероприятий по защите информации, хранение и учет ЭД, взаимодействие с Организатором по техническим вопросам и вопросам обеспечения безопасности информации. На администратора АРМ Участника могут возлагаться задачи по отправке/приему электронных документов и информации об их исполнении.

Администратор безопасности информации Организатора (далее – администратор безопасности информации) – лицо, организующее, обеспечивающее и контролирующее выполнение требований безопасности информации при осуществлении обмена ЭД с Участником.

1.2. Предмет регулирования настоящих Правил электронного документооборота в системе электронного документооборота министерства финансов Кировской области

1.2.1. Настоящие Правила электронного документооборота в системе электронного документооборота министерства финансов Кировской области (далее – Правила) устанавливают общие принципы осуществления электронного документооборота (далее – ЭДО) между Сторонами.

1.2.2. Настоящие Правила не регулируют вопросы обмена электронными сообщениями, не являющимися ЭД в соответствии с договором об обмене ЭД, заключаемыми между Сторонами (далее – Договор).

1.3. Документы, регулирующие ЭДО в СЭД

1.3.1. ЭДО в СЭД регулируется следующими документами:

- Договором;
- руководством пользователя на АРМ Участника;
- законодательными и другими нормативными правовыми актами Российской Федерации.

1.4. Порядок и условия допуска Участника к осуществлению документооборота в СЭД

1.4.1. Участник допускается к осуществлению документооборота в СЭД после выполнения им следующих мероприятий:

- заключения Договора с Организатором об обмене ЭД;
- приобретение и установка СКЗИ;
- регистрации Участника в системе ЭДО министерства финансов Кировской области;
- получение Участником ЭП в УЦ;
- предоставление в министерство финансов Кировской области открытого ключа ЭП.

1.4.2. Участник обеспечивает установку и эксплуатацию СКЗИ, защиту АРМ Участника от несанкционированного доступа в соответствии с требованиями нормативных документов и законодательства Российской Федерации.

1.5. Пользователи Участника

1.5.1. Пользователи Участника несут персональную ответственность за безопасность ключевой информации, в том числе закрытых ключей подписи и аутентификации, и обязаны обеспечивать ее сохранность, неразглашение и нераспространение.

1.5.2. Пользователи Участника должны быть ознакомлены под роспись с внутренними документами Участника, регулирующими использование ЭП в ЭД.

1.6. Порядок вступления в действие настоящих Правил, а также внесения в них изменений

1.6.1. Настоящие Правила вступают в силу в отношении Участника после заключения Договора между Сторонами.

1.6.2. Изменения и дополнения в настоящие Правила вносятся в порядке, установленном Договором.

1.7. Прекращение действия настоящих Правил

1.7.1. Обязательства Сторон по исполнению настоящих Правил прекращаются при расторжении Договора.

1.7.2. Прекращение действия настоящих Правил не влияет на юридическую силу и действительность ЭД, которыми Стороны обменивались до прекращения действия настоящих Правил.

2. ЭЛЕКТРОННЫЕ ДОКУМЕНТЫ

2.1 Требования, предъявляемые к ЭД

2.1.1. ЭД, сформированные в СЭД и подписанные ЭП, имеют юридическую силу наравне с бумажными документами, подписанными собственноручными подписями.

2.1.2. ЭД считаются надлежащим образом оформленными при условии их соответствия законодательству Российской Федерации, а также документам, регулирующим ЭДО в СЭД.

2.1.3. ЭД, не отвечающие требованиям, предъявляемым к ЭД настоящими Правилами,

рассматриваются Сторонами, как ЭД, не имеющие юридической силы.

2.2. Использование ЭП в ЭД

2.2.1. ЭД может быть подписан только ЭП уполномоченных лиц Сторон, для которых УЦ изданы действующие Сертификаты.

2.2.2. Прекращение действия Сертификатов уполномоченных лиц Сторон не влияет на юридическую силу и действительность ЭД, которыми Стороны обменивались до прекращения действия Сертификатов.

2.3. Использование ЭД

2.3.1. ЭД, подписанный надлежащими корректными ЭП уполномоченных лиц Сторон, имеет равную юридическую силу с документом, представленным на бумажном носителе, подписанном собственноручными подписями уполномоченных лиц Сторон, и не может быть оспорен только на том основании, что он выполнен в электронном виде.

2.3.2. ЭД может иметь неограниченное количество экземпляров, в том числе выполненных на машиночитаемых носителях различного типа.

2.4. Представление сведений, содержащихся в ЭД, на бумажном носителе

2.4.1. Сведения, содержащиеся в ЭД, могут быть представлены (распечатаны) на бумажном носителе. В этом случае их соответствие ЭД должно быть заверено Организатором или Участником в установленном порядке.

2.4.2. Программы, осуществляющие представление сведений, содержащихся в ЭД на бумажных носителях, являются составной частью ПО, используемого в СЭД.

3. ОРГАНИЗАЦИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

3.1. ЭДО

3.1.1. ЭДО включает:

- формирование ЭД и их ЭП с использованием закрытых ключей подписи соответствующих уполномоченных лиц Сторон;
- отправку и доставку ЭД;
- проверку подлинности ЭП в доставленном ЭД;
- проверка корректности заполнения ЭД;
- прием документов на исполнение ЭД;
- учет ЭД;
- хранение ЭД;
- создание дополнительных экземпляров ЭД;
- создание представлений (распечатывание) ЭД в бумажном виде.

3.2. Формирование ЭД и их ЭП

3.2.1. Формирование ЭД выполняется Участником ЭДО в строгом соответствии с документом-основанием на бумажном носителе, Участник несет полную ответственность за соответствие ЭД документу-основанию. ЭД заверяется ЭП уполномоченного лица.

3.3. Отправка и доставка ЭД

3.3.1. В отношениях между отправителем и получателем ЭД считается исходящим от отправителя, если ЭД создан и подписан ЭП лицом, уполномоченным действовать от имени отправителя в отношении данного ЭД.

3.3.2. ЭД не считается исходящим от отправителя, если получатель знал или должен был знать, в том числе в результате выполнения проверки, о том, что ЭД не исходит от отправителя, или получатель знал или должен был знать, в том числе в результате выполнения проверки, о том, что получен искаженный ЭД.

3.4. Проверка подлинности доставленного ЭД

3.4.1. Проверка подлинности ЭД включает:

- проверку ЭД на соответствие документам, регулирующим ЭДО в СЭД, определенным настоящими Правилами;
- проверку подлинности ЭП в ЭД;
- проверку статуса соответствующих Сертификатов на момент подписания или приема соответствующего ЭД.

3.4.2. В случае положительного результата проверки подлинности ЭД, данный ЭД принимается к исполнению. В противном случае данный ЭД к исполнению не принимается, о чем получатель уведомляет отправителя с указанием причины непринятия документа к исполнению.

3.5. Подтверждение получения ЭД

3.5.1. Подтверждение получения ЭД выполняется Участником путем получения информации о документе через АРМ Участника.

3.6. Отзыв ЭД

3.6.1. Участник вправе отозвать (удалить) созданный ЭД до начала его обработки (исполнения) получателем.

3.7. Хранение ЭД

3.7.1. ЭД должны храниться с сохранением всех реквизитов (полей), включая ЭП. Допускается хранение ЭД в виде последовательности всех полей ЭД (включая ЭП) в записи базы данных.

3.7.2. Срок хранения ЭД должен соответствовать сроку хранения соответствующих документов на бумажных носителях.

4. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Управление ключевой информацией

4.1.1. Управление ключевой информацией осуществляют администраторы безопасности информации, УЦ и администраторы АРМ Участника.

4.1.2. Ключевая информация содержит сведения конфиденциального характера, хранится Участниками на учтенных в установленном порядке носителях ключевой информации и не подлежит передаче третьим лицам.

4.1.3. Носители ключевой информации относятся к материальным носителям, содержащим информацию ограниченного распространения. При обращении с ними должны выполняться требования документов, регламентирующих порядок обращения с информацией ограниченного распространения в органах исполнительной власти, и настоящих Правил.

4.1.4. Учет носителей ключевой информации осуществляют администраторы безопасности информации и администраторы АРМ Участника по соответствующим учетным формам.

4.1.5. Требования по организации хранения и использования носителей ключевой информации.

4.1.5.1. Порядок хранения и использования носителей ключевой информации должен исключать возможность несанкционированного доступа к ним.

4.1.5.2. Во время работы с носителями ключевой информации доступ к ним посторонних лиц должен быть исключен.

4.1.5.3. Не разрешается:

- производить несанкционированное копирование носителей ключевой информации;
- знакомить или передавать носители ключевой информации лицам, к ним не допущенным;
- выводить закрытые ключи подписи на дисплей или принтер;
- вставлять носитель ключевой информации в считывающее устройство других компьютеров, кроме того, на котором установлен АРМ Участника;
- оставлять носитель ключевой информации без присмотра на рабочем месте;
- записывать на носитель ключевой информации посторонние файлы.

4.1.6. Порядок работы с ключами подписи.

4.1.6.1. Формирование открытого и закрытого ключей подписи по соответствующей заявке на получение Сертификата должен осуществлять УЦ.

4.1.6.2. Ответственность за соответствие сведений, указанных в Сертификате, сведениям, указанным в Заявке для регистрации уполномоченных лиц Участника, несет УЦ.

4.1.6.3. Пользователи Участника получают изданные УЦ Сертификаты ЭП в установленном порядке.

4.1.6.4. Владельцы Сертификатов несут персональную ответственность за безопасность (сохранение в тайне) своих закрытых ключей ЭП и обязаны обеспечивать их сохранность, неразглашение и нераспространение.

4.1.6.5. Срок действия Сертификата ЭП указывается в Сертификате. Владелец Сертификата получает право использования соответствующего закрытого ключа ЭП для подписания ЭД в течение срока действия Сертификата.

4.1.6.6. Срок действия открытого и закрытого ключей ЭП и соответствующих Сертификатов обычно составляет один год.

4.1.6.7. Не менее чем за 10 рабочих дней до окончания срока действия Сертификата его владелец обязан оформить заявку на получение нового Сертификата в УЦ.

4.1.6.8. После окончания срока действия Сертификата его владелец теряет право использования закрытого ключа ЭП, соответствующего отзываемому Сертификату.

4.1.6.9. УЦ обеспечивает хранение Сертификатов в течение срока хранения ЭД.

4.1.7. Все работы, связанные с управлением списком отозванных сертификатов и поддержанием его в актуальном состоянии обеспечиваются УЦ.

4.2. Порядок действий при компрометации закрытых ключей подписи или аутентификации

4.2.1. К событиям, связанным с компрометацией закрытых ключей подписи или аутентификации, относятся хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых закрытые ключи подписи или аутентификации могли стать доступными неуполномоченным лицам и (или) процессам.

4.2.2. При компрометации закрытого ключа ЭП владелец соответствующего ему Сертификата немедленно прекращает его использование и незамедлительно сообщает об этом в соответствующий УЦ. При компрометации закрытого ключа аутентификации уполномоченное лицо Участника немедленно прекращает его использование и незамедлительно сообщает об этом администратору АРМ Участника, а тот, в свою очередь, администратору безопасности.

4.2.3. После получения от владельца Сертификата Участника сообщения о компрометации закрытого ключа подписи или аутентификации уполномоченное лицо УЦ или администратор безопасности информации проверяет достоверность полученного сообщения. В случае подтверждения полученной информации, инициируется процедура отзыва или приостановления действия соответствующего Сертификата.

4.2.4. Дата и время, с которой Сертификат считается недействительным в СЭД, устанавливается равной дате и времени отзыва или приостановления действия Сертификата, указанного в списке отозванных сертификатов.

4.2.5. Уведомление о компрометации закрытых ключей подписи или аутентификации должно быть подтверждено официальным уведомлением Участника о компрометации в письменном виде. Уведомление должно содержать идентификационные параметры Сертификата. В случае непредставления уведомления, Администратор безопасности информации вправе отказать в выдаче нового Сертификата.

4.2.6. Использовать скомпрометированные закрытые ключи подписи для подписи ЭД и закрытые ключи аутентификации для организации защищенного канала связи запрещается. При получении ЭД, подписанного скомпрометированным закрытым ключом подписи, данный ЭД считается недействительным, о чем получатель обязан отправить уведомление отправителю с указанием причины отказа исполнения документа.

4.2.7. В случае компрометации закрытого ключа и отзыва соответствующего Сертификата с публикацией в списке отозванных сертификатов, Участник установленным порядком изготавливает новые открытый и закрытый ключи подписи (аутентификации).

4.2.8. Сертификат, соответствующий скомпрометированному закрытому ключу, хранится в установленном порядке в УЦ для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением ЭП.

4.3. Отзыв сертификата ключа подписи

4.3.1. УЦ отзыват Сертификат Участника в следующих случаях:

- в случае компрометации;
- в случае прекращения действия Договора в отношении данного Участника;

– по заявлению в письменном виде владельца Сертификата, заверенному Участником.

4.3.2. В случае отзыва или приостановления действия Сертификата пользователя Участника УЦ обеспечивает публикацию списка отозванных сертификатов с указанием серийного номера Сертификата, даты, времени и причины аннулирования. Дата и время, с которых Сертификат считается недействительным в СЭД, устанавливается равной дате и времени отзыва или приостановления действия Сертификата, указанных в списке отозванных сертификатов.

5. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ В СВЯЗИ С ОСУЩЕСТВЛЕНИЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

5.1. Возникновение конфликтных ситуаций в связи с осуществлением ЭДО в СЭД

5.1.1. В связи с осуществлением ЭДО 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:

- оспаривание факта отправления и/или получения ЭД;
- оспаривание времени отправления и/или получения ЭД;
- оспаривание содержания отправленного/полученного ЭД;
- оспаривание подлинности экземпляров ЭД;
- оспаривание целостности ЭД;
- оспаривание идентичности лица, заверившего ЭД ЭП;
- оспаривание полномочий лица, заверившего ЭД ЭП;

5.1.2. Конфликтные ситуации разрешаются (урегулируются) Сторонами в рабочем порядке и/или по итогам работы комиссии по разрешению конфликтной ситуации (далее – Комиссия).

5.1.3. В случае невозможности разрешения конфликтной ситуации в рабочем порядке и/или по итогам работы Комиссии, Стороны разрешают конфликтную ситуацию в претензионном порядке, либо направляют имеющиеся разногласия на рассмотрение вышестоящих органов, либо суда в порядке, установленном законодательством Российской Федерации.

5.2. Уведомление о конфликтной ситуации

5.2.1. В случае возникновения обстоятельств, свидетельствующих, по мнению одной из Сторон, о возникновении и/или наличии конфликтной ситуации, данная Сторона (далее – Сторона-инициатор) незамедлительно извещает другую заинтересованную Сторону о возможном возникновении и/или наличии конфликтной ситуации, обстоятельствах, свидетельствующих о ее возникновении или наличии, а также ее предполагаемых причинах.

5.2.2. Стороны, которым было направлено извещение о конфликтной ситуации и участвующие в ее разрешении (далее – Стороны-ответчики), обязаны не позднее чем в течение следующего рабочего дня проверить наличие указанных в извещении обстоятельств, и по необходимости принять меры по разрешению конфликтной ситуации со своей стороны.

5.2.3. В тот же срок Стороны-ответчики извещают доступными способами Сторону-инициатора о результатах проверки и, при необходимости, о мерах, принятых для разрешения конфликтной ситуации.

5.3. Разрешение конфликтной ситуации в рабочем порядке

5.3.1. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если Сторона-инициатор удовлетворена информацией, полученной в извещениях Сторон-ответчиков, и не имеет к ним претензий в связи с конфликтной ситуацией.

5.3.2. В случае если Сторона-инициатор не удовлетворена информацией, полученной от Сторон-ответчиков, для рассмотрения конфликтной ситуации формируется Комиссия.

5.4. Формирование Комиссии по разрешению конфликтной ситуации

5.4.1. В случае если конфликтная ситуация не была разрешена в рабочем порядке, Сторона-инициатор должна не позднее трех рабочих дней после возникновения конфликтной ситуации, направить уведомление о конфликтной ситуации (далее – Уведомление) и

предложение о создании комиссии по разрешению конфликтной ситуации (далее – Предложение) Стороне-ответчику.

5.4.2. Уведомление должно содержать информацию о предмете и существе конфликтной ситуации, обстоятельствах, по мнению Стороны-инициатора, свидетельствующих о наличии конфликтной ситуации, возможных причинах и последствиях ее возникновения.

5.4.3. Уведомление должно содержать информацию с указанием фамилий, имен, отчеств, должностей и контактной информации должностных лиц Стороны-инициатора, уполномоченных в разрешении конфликтной ситуации.

5.4.4. Предложение должно содержать информацию о предлагаемом месте, дате и времени сбора комиссии, но не позднее трех рабочих дней со дня отправления Предложения, список предлагаемых для участия в работе Комиссии представителей Стороны-инициатора с указанием фамилий, имен, отчеств, должностей, при необходимости исполняемых при обмене ЭД функциональных ролей (администратор, администратор безопасности и т.п.), их контактной информации (телефон, факс, электронная почта).

5.4.5. Уведомление и Предложение составляются на бумажном носителе, подписываются должностными лицами Стороны-инициатора, уполномоченными в разрешении конфликтной ситуации и передаются Стороне-ответчику в установленном порядке, обеспечивающим подтверждение вручения корреспонденции.

5.4.6. Уведомление и Предложение могут быть составлены и направлены в форме электронных документов. При этом факт их доставки должен быть подтвержден.

5.5. Формирование комиссии по разрешению конфликтной ситуации, ее состав

5.5.1. Не позднее, чем на третий рабочий день после получения Предложения Сторонами, участвующими в разрешении конфликтной ситуации, должна быть сформирована Комиссия.

5.5.2. Комиссия формируется на основании совместного приказа Сторон. Приказ устанавливает состав Комиссии, время и место ее работы.

5.5.3. Устанавливается тридцатидневный срок работы Комиссии. В исключительных случаях срок работы Комиссии по согласованию Сторон может быть дополнительно продлен не более, чем на тридцать дней.

5.5.4. Если Стороны не договорятся об ином, в состав Комиссии входит равное количество уполномоченных лиц каждой из Сторон, участвующих в разрешении конфликтной ситуации.

5.5.5. В состав Комиссии назначаются представители служб информационно-технического обеспечения и служб обеспечения информационной безопасности, а также представители подразделений-исполнителей ЭД.

5.5.6. В состав Комиссии могут быть включены представители юридических служб Сторон, представители органов, осуществляющих государственное регулирование и контроль соответствующих видов деятельности.

5.5.7. Независимо от соглашения Сторон в состав Комиссии должен входить хотя бы один уполномоченный представитель УЦ.

5.5.8. По инициативе любой из Сторон к работе Комиссии для проведения технической экспертизы могут привлекаться независимые эксперты, в том числе представители поставщиков средств защиты информации. При этом Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.

5.5.9. Лица, входящие в состав Комиссии должны обладать необходимыми знаниями и опытом работы в области подготовки и исполнения электронных документов, построения и функционирования СЭД, организации и обеспечения информационной безопасности при обмене ЭД, должны иметь соответствующий допуск к необходимым для проведения работы Комиссии документальным материалам и программно-техническим средствам.

5.5.10. При участии в Комиссии представителей сторонних органов и организаций их право представлять соответствующие органы и организации должно подтверждаться официальным документом (доверенностью, предписанием, копией приказа или распоряжения).

5.6. Задачи, права и полномочия комиссии по разрешению конфликтной ситуации

5.6.1. Задача Комиссии – установить на организационно-техническом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о наличии конфликтной ситуации, ее причинах и последствиях.

5.6.2. Комиссия имеет право получать доступ к необходимым для проведения ее работы документальным материалам Сторон, на бумажных и электронных носителях.

5.6.3. Комиссия имеет право ознакомления с условиями и порядком подготовки, формирования, обработки, доставки, исполнения, хранения и учета электронных документов.

5.6.4. Комиссия имеет право ознакомления с условиями и порядком эксплуатации Сторонами программно-технических средств обмена электронными документами.

5.6.5. Комиссия имеет право ознакомления с условиями и порядком изготовления, использования и хранения Сторонами ключевой информации, а также иной конфиденциальной информации и ее носителей, необходимых для работы средств обмена ЭД.

5.6.6. Комиссия имеет право получать объяснения от должностных лиц Сторон, обеспечивающих обмен ЭД.

5.6.7. Комиссия вправе получать от Сторон любую иную информацию, относящуюся, по ее мнению, к рассматриваемой конфликтной ситуации.

5.6.8. Для проведения необходимых проверок и документирования данных, Комиссией могут применяться специальные программно-технические средства.

5.6.9. Комиссия не вправе давать правовую или какую-либо иную оценку установленных ею фактов, кроме организационно-технической.

5.7. Протокол работы комиссии по разрешению конфликтной ситуации

5.7.1. Все действия, предпринимаемые Комиссией для выяснения фактических обстоятельств, а также выводы, сделанные комиссией, заносятся в Протокол работы Комиссии.

5.7.2. Протокол работы Комиссии должен содержать следующие данные:

- состав Комиссии с указанием сведений о фамилиях, именах, отчествах, местах работы, занимаемых должностях, допусках к необходимым работам, при необходимости исполняемых при обмене ЭД функциональных ролях, контактной информации и квалификации каждого из членов комиссии;

- краткое изложение обстоятельств, свидетельствующих, по мнению Стороны-инициатора, о возникновении и/или наличии конфликтной ситуации;

- установленные Комиссией фактические обстоятельства;

- мероприятия, проведенные Комиссией для установления наличия, причин возникновения и последствий возникшей конфликтной ситуации, с указанием даты времени и места их проведения;

- выводы, к которым пришла Комиссия в результате проведенных мероприятий;

- подписи всех членов комиссии.

5.7.3. В случае, если мнение члена или членов Комиссии относительно порядка, методики, целей проводимых мероприятий не совпадает с мнением большинства членов Комиссии, в Протокол заносится соответствующая запись, которая подписывается членом или членами Комиссии, чье особое мнение отражает соответствующая запись.

5.7.4. Протокол составляется в форме документа на бумажном носителе, по экземпляру каждой Стороне. По обращению любого из членов Комиссии Стороной, к которой было направлено обращение, ему должна быть выдана заверенная копия Протокола.

5.8. Акт по итогам работы комиссии по разрешению конфликтной ситуации

5.8.1. По итогам работы Комиссии составляется Акт, при этом Акт должен содержать следующую информацию:

- состав Комиссии;

- дату и место составления Акта;

- даты и время начала и окончания работы Комиссии;

- фактические обстоятельства, установленные Комиссией;

- краткий перечень мероприятий, проведенных Комиссией;

- выводы, к которым пришла Комиссия в результате проведенных мероприятий;

- подписи членов Комиссии;

- в случае наличия – особое мнение члена или членов Комиссии.

5.8.2. К Акту может прилагаться особое мнение члена или членов Комиссии, не согласных с выводами Комиссии, указанными в Акте. Особое мнение составляется в произвольной форме, подписывается членом или членами Комиссии, чье мнение оно отражает.

5.8.3. Акт составляется в форме документа на бумажном носителе, по одному экземпляру каждой Стороне. По обращению любого из членов Комиссии, Стороной, к которой было направлено обращение, ему должна быть выдана заверенная копия Акта.

5.9. Разрешение конфликтной ситуации по итогам работы комиссии

5.9.1. Акт Комиссии является основанием для принятия Сторонами решения по урегулированию конфликтной ситуации.

5.9.2. В срок не более трех рабочих дней со дня окончания работы Комиссии, Стороны на основании выводов Комиссии принимают меры по разрешению конфликтной ситуации и извещают другие Стороны о принятых мерах.

5.9.3. Конфликтная ситуация признается разрешенной по итогам работы Комиссии, если Стороны удовлетворены выводами, полученными Комиссией, мерами, принятыми другими участвующими в разрешении конфликтной ситуации Сторонами, и не имеют взаимных претензий.

5.9.4. В случае, если конфликтная ситуация признается Сторонами разрешенной, то в срок не позднее пяти рабочих дней со дня окончания работы Комиссии Стороны оформляют решение об урегулировании конфликтной ситуации (далее – Решение).

5.9.5. Решение составляется Сторонами в форме документа на бумажном носителе по одному экземпляру каждой Стороне. Решение подписывается уполномоченными в разрешении конфликтной ситуации лицами Сторон, и утверждается руководителями Сторон либо их заместителями.

5.10. Претензионный порядок разрешения конфликтной ситуации

5.10.1. В случае, если конфликтная ситуация не разрешена по итогам работы Комиссии, в случае прямого или косвенного отказа одной из Сторон от участия в работе, или если одной из Сторон создавались препятствия работе Комиссии, а также в иных случаях, если одна из Сторон считает, что ее права в связи с обменом ЭД были нарушены, она обязана направить Стороне, которая, по его мнению, нарушила ее права, Претензию.

5.10.2. Претензия должна содержать:

- изложение существа требований Стороны-инициатора;
- при возможности денежной оценки претензии – ее сумму и расчет;
- изложение фактических обстоятельств, на которых основываются требования Стороны-инициатора и доказательства, подтверждающие их, со ссылкой на соответствующие нормы законодательства и нормативных правовых актов;
- сведения о работе Комиссии и, в случае, если Комиссия работала в связи с рассматриваемой конфликтной ситуацией, копии материалов работы Комиссии, независимо от выводов Комиссии, согласия или несогласия с этими выводами Стороны-инициатора;
- иные документы, имеющие значение, по мнению Стороны-инициатора;
- перечень прилагаемых к Претензии документов и других доказательств, а также иные сведения, необходимые для урегулирования разногласий по Претензии.

5.10.3. Претензия составляется в форме документа на бумажном носителе, подписывается руководителем Стороны-инициатора либо его заместителем, заверяется печатью Стороны-инициатора. Претензия и прилагаемые к ней документы направляются в адрес Стороны-ответчика в установленном порядке, обеспечивающим подтверждение вручения корреспонденции.

5.10.4. Сторона, в адрес которой направлена Претензия, обязана в срок не позднее трех рабочих дней удовлетворить требования Претензии или представить мотивированный отказ в их удовлетворении. Непредставление ответа на Претензию в течение указанного срока является нарушением установленного настоящими Правилами претензионного порядка и может рассматриваться в качестве отказа в удовлетворении требований Претензии.

5.11. Разрешение конфликтной ситуации судами

В случае невозможности разрешения споров и разногласий по конфликтной ситуации в рабочем порядке, по итогам работы Комиссии или в претензионном порядке Стороны передают их на рассмотрение суда в порядке, установленном законодательством Российской Федерации.