Утвержден
распоряжением Правления ПФР

от__11.10.2007__

№ ___190р_____

РЕГЛАМЕНТ

обеспечения безопасности информации при защищенном обмене электронными документами в системе электронного документооборота Пенсионного фонда Российской Федерации по телекоммуникационным каналам связи

Согласовано:
Начальник Управления по защите информации

_____Е.В. Колесник

“_____”_____2007 г.

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Настоящий Регламент обеспечения безопасности информации при защищенном обмене электронными документами в системе электронного документооборота (СЭД) ПФР по телекоммуникационным каналам связи (далее – Регламент) устанавливает и определяет:

- порядок взаимодействия удостоверяющих центров, обслуживающих Абонентов и специалистов территориальных органов ПФР, в целях организации обмена юридически значимыми электронными документами;
- набор требований, условий и регламентных процедур сторон, участвующих в информационном обмене при издании сертификатов и управления ими в системе электронного документооборота ПФР;
- порядок организации защищенного электронного документооборота;
- порядок разбора конфликтных ситуаций, возникающих при осуществлении электронного документооборота.

Детализация конкретных действий участников Системы при использовании инфраструктуры открытых ключей определяется в Регламентах Удостоверяющих центров.

Отношения между участниками Системы в рамках настоящего Регламента регулируются: Гражданским кодексом Российской Федерации, Налоговым кодексом Российской Федерации, Федеральным законом от 10.01.2002 № 1-ФЗ “Об электронной цифровой подписи”, Федеральным законом от 27.07.2006 №152-ФЗ “О персональных данных”, Федеральным законом от 27.07.2006 № 149-ФЗ “Об информации, информационных технологиях и защите информации”, Федеральным законом от 01.04.1996 № 27-ФЗ “Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования” и другими федеральными законами, нормативными правовыми актами, постановлениями Правления ПФР.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Система электронного документооборота ПФР (СЭД ПФР) – совокупность программных и технических средств, а также организационных мер, обеспечивающих функционирование процесса документооборота между сторонними организациями и органами ПФР.

Абонент СЭД – юридическое (физическое) лицо - участник СЭД ПФР.

Удостоверяющий центр (далее - УЦ) — организационно-технический комплекс, осуществляющий выполнение целевых функций Удостоверяющего центра в соответствии с Федеральным законом от 10.01.2002 №1-ФЗ “Об электронной цифровой подписи”. Деятельность УЦ в системе электронного документооборота ПФР по телекоммуникационным каналам связи основывается на **установленных доверительных** отношениях между УЦ ПФР и УЦ Абонента СЭД согласно Регламенту работы УЦ ПФР.

Центр Регистрации (далее - ЦР) – элемент территориально-распределенной структуры сети УЦ. Выполняет функции регистрации пользователей, формирования различных запросов в УЦ, выдачи сертификатов открытых ключей ЭЦП для пользователей.

Средства криптографической защиты информации (СКЗИ) – программно-аппаратные средства, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности.

Средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание ЭЦП в электронном документе с использованием закрытого ключа ЭЦП, подтверждение с

использованием открытого ключа ЭЦП подлинности ЭЦП в электронном документе, создание закрытых и открытых ключей ЭЦП.

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

Закрытый ключ ЭЦП – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания электронной цифровой подписи в электронных документах с использованием средств электронной цифровой подписи.

Открытый ключ ЭЦП - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю системы электронного документооборота путем включения в сертификат ключа подписи и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Сертификат ключа подписи (далее - сертификат) — документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;

Владелец сертификата ключа подписи - физическое лицо, на имя которого УЦ выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Список отозванных сертификатов - электронный документ с электронной цифровой подписью уполномоченного лица УЦ формата X.509, включающий в себя список серийных номеров сертификатов открытых ключей подписи, которые на момент времени формирования списка отозванных сертификатов были отозваны или действие которых было приостановлено.

Корневой сертификат - сертификат, являющийся вышестоящим в иерархии сертификации. Корневой сертификат выдается УЦ и подписывается уполномоченным лицом УЦ.

Уполномоченное лицо УЦ - физическое лицо, являющееся сотрудником Удостоверяющего Центра и наделенное Удостоверяющим Центром полномочиями по заверению сертификатов ключей подписи и Списков отозванных сертификатов.

Уполномоченное лицо Абонента – должностное лицо страхователя, уполномоченное использовать средства электронной цифровой подписи и шифрования в рамках СЭД ПФР по каналам связи.

Уполномоченное лицо органа ПФР – должностное лицо органа ПФР, уполномоченное использовать средства электронной цифровой подписи и шифрования в рамках СЭД ПФР по каналам связи.

Администратор безопасности – уполномоченное должностное лицо, осуществляющее формирование ключевых дистрибутивов, их выдачу и проведение работ в области защиты информации.

Электронный документооборот (ЭДО) – последовательность обмена электронными документами по настоящему протоколу.

Этап документооборота – единичный шаг отправки пакета от отправителя к получателю в рамках процесса документооборота.

Электронный документ (далее – **Документ**) – документ, в котором информация представлена в электронно-цифровой форме.

Коммуникационная составляющая – транспортный модуль**,** обеспечивающий обмен электронными документами между органом ПФР и абонентами СЭД.

Транспортный сервер – комплекс технических и программных средств, обеспечивающих доставку электронного документа в СЭД ПФР.

Доверенный способ передачи информации - способ передачи информации на основе взаимной договоренности и обеспечивающий требуемую степень ее защищенности.

АРМ [Администратор] – автоматизированное рабочее место Администратора безопасности. Представляет собой компьютер с установленным программным обеспечением - Центр управления сетью (ЦУС) и Удостоверяющий ключевой центр (УКЦ).

Файлы экспорта - набор файлов, автоматически формируемых в АРМ [Администратор] для каждого другого АРМ [Администратор] при организации защищенного взаимодействия между узлами защищенных сетей и при изменениях, происходящих в процессе взаимодействия.

ПО ViPNet [Клиент] – ПО, которое обеспечивает защиту компьютера от сетевых атак и установление криптографически защищенных соединений (туннелей) при взаимодействии с другими узлами защищенной сети, а также возможность гарантированной доставки подписанных ЭЦП документов (файлов) по назначению с автоматическим подтверждением доставки и прочтения документов.

ПО ViPNet [КриптоСервис] - средство реализации функций ЭЦП.

ПО КриптоПРО CSP – средство реализации функций ЭЦП и шифрования.

ПО Верба OW версии 6.0 и выше – средство реализации функций ЭЦП и шифрования.

Узел защищенной сети - компьютер с ПО ViPNet [Клиент] или ПО ViPNet [КриптоСервис], участвующий в системе защищенного документооборота.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. В Системе используются, принимаются и признаются сертификаты ключей подписи, изданные УЦ ПФР, доверенными УЦ ПФР и другими УЦ, прошедшими процедуру кросс-сертификации с доверенными УЦ ПФР.

3.2. Сертификат ключа подписи признается изданным УЦ, если подтверждена подлинность электронной цифровой подписи издателя сертификата ключа подписи с использованием сертификата ключа подписи уполномоченного лица УЦ.

3.3. Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи владельца сертификата ключа подписи при одновременном соблюдении следующих условий:

- сертификат ключа подписи, соответствующий электронной цифровой подписи, издан Удостоверяющим Центром ПФР или доверенным УЦ;

- серийный номер сертификата ключа подписи, относящийся к этой электронной цифровой подписи, не содержится в актуальном списке отозванных сертификатов на момент подписания электронного документа;
- срок действия сертификата ключа подписи, относящегося к этой электронной цифровой подписи, наступил и не окончен на момент подписания электронного документа;
- положительный результат проверки с использованием средства электронной цифровой подписи на предмет отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

4. ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ СДАЧЕ ОТЧЕТНОСТИ СТРАХОВАТЕЛЯМИ В ОРГАНЫ ПФР С ИСПОЛЬЗОВАНИЕМ УСЛУГ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ И ОПЕРАТОРОВ СВЯЗИ

4.1. В целях обеспечения защиты персональных данных при сдаче отчетности страхователями в органы ПФР с использованием услуг удостоверяющих центров и операторов связи в соответствии с Федеральными законами от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», приказом ФАПСИ от 13.06.2001 № 152, приказом ФСБ России от 09.02.2005 № 66 и руководящими документами ПФР по защите информации устанавливаются следующие требования по информационной безопасности:

4.1.1. Услуги при сдаче отчетности страхователями в органы ПФР должны предоставляться операторами связи, являющимися юридическими лицами, имеющими необходимые лицензии и сертификаты на используемое программное обеспечение и технические средства.

4.1.2. Устанавливаемое на автоматизированные рабочие места (АРМ) сотрудников органов ПФР и страхователей прикладное программное обеспечение, реализующее технологию сдачи отчетности от страхователей в органы ПФР и имеющее в своем составе средства криптографической защиты информации (СКЗИ), должно иметь заключение ФСБ России о корректности встраивания СКЗИ.

4.1.3. Технологии сдачи отчетности от страхователей в органы ПФР должны предусматривать использование только сертифицированных СКЗИ, обеспечивающих технологическую совместимость с СКЗИ, принятыми в системе ПФР («Домен-К», «Верба-OW»), на уровне процедур шифрования и электронной цифровой подписи. Конкретные типы СКЗИ, предлагаемые операторами к использованию, должны согласовываться с Управлением по защите информации ПФР, выполняющим функции координирующего органа криптографической защиты с правами, предусмотренными п. 9 Приказа ФАПСИ от 23.06.2001 № 152.

4.1.4. Удостоверяющие центры (УЦ), оказывающие услуги страхователям или операторам связи по сдаче отчетности в органы ПФР, должны провести кросс-сертификацию с одним из доверенных удостоверяющих центров ПФР. Порядок проведения кросс-сертификации УЦ определяется технологическими документами УЦ ПФР.

4.1.5. Управление ключами шифрования, сертификатами ключей подписи (передача действующих сертификатов ключей подписи и списков отозванных

сертификатов между операторами и органами ПФР) должно осуществляться в соответствии с Регламентом работы УЦ ПФР.

4.1.6. Генерация (выработка) ключей шифрования и ЭЦП должна производиться страхователями самостоятельно на своих рабочих местах с последующей передачей в УЦ открытого ключа.

Изготовление закрытых ключей ЭЦП и шифрования удостоверяющим центром допускается только при включении этой услуги в договор со страхователем. При этом, существенным условием оказания услуги является обязанность обеспечения УЦ конфиденциальности представляемых ключей и обеспечение безусловного их уничтожения в аппаратно-программных средствах УЦ после переноса на передаваемый страхователю ключевой носитель.

4.1.7. Все передаваемые сведения в открытом виде могут быть представлены только на рабочих местах страхователей и сотрудников органов ПФР. Сведения страхователей должны быть защищены и недоступны для третьих лиц, включая операторов, оказывающих услуги при сдаче отчетности. Программно-аппаратные средства операторов, используемые при информационном обмене между страхователем и органом ПФР, не должны осуществлять следующие действия: расшифровывать – зашифровывать (перешифровывать), снимать ЭЦП и переподписывать другой ЭЦП

4.1.8. Технологическая проверка полноты и достоверности подготовленных сведений осуществляется встроенными средствами контроля непосредственно на рабочих местах страхователей или сотрудников органов ПФР без привлечения услуг операторов.

АРМы страхователей и работников ПФР должны иметь возможность автономный работы, для формирования (приема) отчета, его подписи, шифрования (расшифрования) с последующим сохранением на внешние машинные носители информации (режим off-line).

4.1.9. Взаимодействие программно-аппаратных средств операторов с КСПД ПФР должно осуществляться только через сертифицированные средства межсетевой защиты.

4.1.10. Для обеспечения гарантированной доставки данных между транспортным сервером оператора и сотрудниками органов ПФР рекомендуется использовать транспортный уровень MFTP технологии ViPNet.

В случае использования сетевых протоколов SMTP/POP3 или HTTP обмен должен осуществляться через транспортные серверы операторов связи или органов ПФР.

Должны быть приняты меры гарантирующие доставку данных в обе стороны, исключающие рассылку СПАМа на рабочие места участников обмена информацией и обеспечена антивирусная защита трафика обмена, как на стороне оператора, так и на стороне органа ПФР.

4.1.11. Операторы обязаны исключить хранение и архивирование на своих программно-аппаратных средствах зашифрованных посылок содержащих персональные данные свыше времени, необходимого для их гарантированной доставки (гарантия доставки – получение соответствующей квитанции).

4.1.12. Технологии по бесконтактной сдаче отчетности страхователями в органы ПФР с использованием услуг операторов, до их внедрения (приема в опытную и промышленную эксплуатацию) должны быть представлены в Департамент организации персонифицированного учета, взаимодействия со страхователями и взыскания недоимки и в Управление по защите информации ПФР для проведения стендовых испытаний, оценки организационной и технологической документации на соответствие требованиям ПФР и получения заключения о возможности использования в системе ПФР.

4.1.13. При изменениях программного обеспечения или технологии, затрагивающих вопросы защиты информации, оператор обязан письменно известить о

произведенных изменениях Управление по защите информации ПФР до начала использования измененного программного обеспечения или технологии в системе сдачи отчетности в органы ПФР.

По решению Управления по защите информации могут быть проведены дополнительные стендовые испытания с выдачей заключения (предписания) на внесение изменений в представленное программное обеспечение или технологию. Оператор, предложивший изменения обязан провести доработки в соответствии с рекомендациями заключения (предписания).

4.1.14. Координирующий орган криптографической защиты – Управление по защите информации ПФР имеет право проверки выполнения операторами настоящих Требований и в случае их нарушения, приостановки использования технологии сдачи отчетности до устранения выявленных несоответствий.

4.2. При организации приема отчетности от страхователей с использованием услуг операторов между органом ПФР и оператором заключается Соглашение с приложением к нему технологии подготовки, пересылки и обработки информационных посылок и регламента обеспечения защиты информации, в которых должны быть учтены требования, изложенные в данном Регламенте.

4.3. Участники электронного документооборота с ПФР, сдающие отчетность без использования услуг операторов связи, руководствуются ранее изданными нормативными документами ПФР, а также указаниями Управления по защите информации - координирующего органа криптографической защиты ПФР.

5. ПОРЯДОК ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

5.1. Межсетевое взаимодействие

Для передачи данных страхователей через транспортный сервер удостоверяющего центра или оператора связи (далее – Операторы связи, если это не оговорено особо) в территориальный орган ПФР используется технология VipNet, компонент VipNet[Клиент] “Деловая почта” или другие программы, разрешенные к использованию в ПФР. “Деловая почта” и другие программы, разрешенные к использованию в ПФР, обеспечивают передачу файлов между транспортным сервером Оператора связи и территориальным органом ПФР.

Типовая схема бесконтактного приема органами ПФР от страхователей сведений о застрахованных лицах с применением услуг удостоверяющих центров и операторов связи приведена в приложении 1.

Организация взаимодействия производится путем обмена доверенным способом файлами экспорта и межсетевым ключом связи в соответствии с документацией на АРМ [Администратор].

После обмена файлами экспорта в АРМ [Администратор] задаются необходимые связи между узлами защищенной сети ПФ и импортированными узлами другой сети.

В каждой из сетей формируется необходимая ключевая и справочная информация и рассылается для узлов своей сети. После рассылки этой информации возможен обмен данными между транспортным сервером Абонента и органа ПФР.

5.2. Средства криптографической защиты информации

Для организации юридически значимого документооборота используются СКЗИ:

- В органах ПФР – «Домен-К», версии не ниже v. 2.0 или «Верба- OW», версии не ниже v. 6.1;
- Абонент Системы может использовать СКЗИ КриптоПРО не ниже v.2.0, «Домен-К» версии не ниже v.2.0 или «Верба OW» версии не ниже 6.1. СКЗИ используются для формирования и проверки подлинности ЭЦП, и шифрования/расшифрования данных.

5.3. Установление доверительных отношений между Удостоверяющими центрами

Установление доверительных отношений между удостоверяющим центром Абонента и органа ПФР производится в соответствии с Регламентом работы УЦ ПФР.

5.4. Регистрация участников электронного документооборота

Для уполномоченных лиц органов ПФР:

- регистрация уполномоченных, изготовление для них ключей подписи и сертификатов ключей ЭЦП осуществляется в соответствии с Регламентом работы УЦ ПФР.

Для уполномоченных лиц Абонентов:

- регистрация, изготовление ключей подписи и сертификатов ключей подписи Абонента устанавливается Регламентом УЦ, обслуживающим Абонента СЭД.

Порядок смены ключей подписи и шифрования регламентируются документами доверенных УЦ.

6. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ, ВОЗНИКАЮЩИХ ПРИ ИСПОЛЬЗОВАНИИ ЭЦП В ПРОЦЕССЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА МЕЖДУ АБОНЕНТАМИ СИСТЕМЫ И ТЕРРИТОРИАЛЬНЫМИ ОРГАНАМИ ПФР.

Данный раздел устанавливает порядок организации разбора конфликтных ситуаций и споров, связанных с практикой применения ЭЦП. Проведение технической экспертизы определяется Регламентом работы УЦ ПФР.

6.1. Возникновение конфликтных ситуаций в процессе электронного документооборота ПФР

6.1.1. Возникновение конфликтных ситуаций может быть связано с формированием, доставкой, получением, подтверждением получения ЭД, а также использованием в данных документах ЭЦП. Конфликтные ситуации могут возникать в следующих случаях:

не подтверждение подлинности защищенных электронных документов средствами проверки ЭЦП получателя;

оспаривание факта идентификации владельца ЭЦП, 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.

6.1.2 Конфликтные ситуации разрешаются (урегулируются) Сторонами в рабочем порядке и/или по итогам работы Экспертной комиссии.

6.1.3. В случае невозможности разрешения конфликтной ситуации в рабочем порядке и по итогам работы Экспертной комиссии, стороны разрешают конфликтную ситуацию в судебном порядке, в соответствии с законодательством Российской Федерации.

6.2. Уведомление о конфликтной ситуации

6.2.1. 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.

6.2.2. Сторона, которой было направлено извещение о конфликтной ситуации и участвующие в ее разрешении (далее - Сторона-ответчик), обязана 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.

6.2.3. В тот же срок Сторона-ответчик извещает доступными способами сторону-инициатора о результатах проверки и, при необходимости, о мерах, принятых для разрешения конфликтной ситуации.

6.3. Разрешение конфликтной ситуации в рабочем порядке

6.3.1. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если Сторона-инициатор удовлетворена информацией, полученной в извещениях Стороны – ответчика, и не имеет к ней претензий в связи с конфликтной ситуацией.

6.3.2. В случае если Сторона-инициатор не удовлетворена информацией, полученной от Стороны-ответчика, для рассмотрения конфликтной ситуации формируется Экспертная комиссия.

6.4. Предложение по формированию экспертной комиссии по разрешению конфликтной ситуации

6.4.1. В случае, если конфликтная ситуация не была разрешена в рабочем порядке, Сторона-инициатор, должна не позднее чем в течение трех рабочих дней после возникновения конфликтной ситуации, направить уведомление о конфликтной ситуации (далее - Уведомление) и предложение о создании Экспертной комиссии по разрешению конфликтной ситуации (далее - Предложение) Стороне-ответчику.

6.4.2. 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.

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

6.4.4. Предложение должно содержать информацию о предлагаемом месте, дате и времени сбора Экспертной комиссии, список предлагаемых для участия в работе Экспертной комиссии представителей Стороны-инициатора с указанием фамилий, имен, отчеств, должностей, при необходимости исполняемых при обмене электронными документами функциональных ролей (администратор, администратор безопасности и т.п.), их контактной информации (телефон, факс, электронная почта).

6.4.5. 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.

6.4.6. Уведомление и Предложение могут быть составлены и направлены в форме электронного документа. При этом факт их доставки должен быть подтвержден.

6.5. Формирование экспертной комиссии по разрешению конфликтной ситуации, ее состав

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

6.5.2. Экспертная комиссия формируется на основании писем Сторон и оформляется приказом. В приказе определяется состав Экспертной комиссии, время и место ее работы.

6.5.3. Устанавливается тридцатидневный срок работы Экспертной комиссии. В исключительных случаях срок работы Экспертной комиссии по согласованию Сторон может быть дополнительно продлен не более чем на тридцать дней.

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

6.5.5. В состав Экспертной комиссии назначаются представители служб информационно-технического обеспечения и служб обеспечения информационной безопасности, а также представители подразделений – исполнителей электронного документа.

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

6.5.7. В состав Экспертной комиссии должен входить уполномоченный представитель УЦ ПФР.

6.5.8. По инициативе любой из сторон к работе Экспертной 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.

6.5.9. Лица, входящие в состав Экспертной комиссии должны обладать необходимыми знаниями и опытом работы в области подготовки и исполнения электронных документов, построения и функционирования Системы, организации и обеспечения информационной безопасности при обмене электронными документами, должны иметь соответствующий допуск к необходимым для проведения работы Экспертной комиссии документальным материалам и программно-техническим средствам.

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

6.6. Права и полномочия экспертной комиссии по разрешению конфликтной ситуации

6.6.1. Экспертная комиссия имеет право:

- получать доступ к необходимым для проведения ее работы документальным материалам Сторон, на бумажных и электронных носителях;
- проводить ознакомление с условиями и порядком подготовки, формирования, обработки, доставки, исполнения, хранения и учета электронных документов;

- проводить ознакомление с условиями и порядком эксплуатации Сторонами программно-технических средств обмена электронными документами;
- проводить ознакомление с условиями и порядком изготовления, использования и хранения Сторонами ключевой информации, а также иной конфиденциальной информации и ее носителей, необходимых для работы Экспертной комиссии;
- получать объяснения от должностных лиц Сторон, обеспечивающих обмен электронными документами;
- получать от Сторон любую иную информацию, относящуюся, по ее мнению, к рассматриваемой конфликтной ситуации.

6.6.2. Для проведения необходимых проверок и документирования данных, Экспертной комиссией могут применяться специальные программно-технические средства.

6.7. Оформление результатов работы экспертной комиссии по разрешению конфликтной ситуации

6.7.1. Все мероприятия Экспертной комиссии по проверке с применением аппаратно-программных средств должны протоколироваться. Протоколы прилагаются к акту работы комиссии.

6.7.2. . По итогам работы Экспертной комиссии составляется акт, при этом акт должен содержать следующую информацию:

- состав Экспертной комиссии;
- дату и место составления акта;
- даты и время начала и окончания работы Комиссией;
- фактические обстоятельства, установленные Комиссией;
- краткий перечень мероприятий, проведенных Комиссией;
- выводы, к которым пришла Экспертная комиссия в результате проведенных мероприятий;
- подписи членов Экспертной комиссии;

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

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

6.7.5. Акт Экспертной комиссии является основанием для принятия Сторонами решения по урегулированию конфликтной ситуации.

Приложение
к Регламенту обеспечения
безопасности информации

Типовая схема бесконтактного приема от страхователей органами ПФР сведений
о застрахованных лицах с использованием услуг операторов связи и удостоверяющих центров