Приложение 5

к приказу ОПФР по Ивановской области

от 29.12.2017 № 173

Регламент взаимодействия

 удостоверяющего центра Отделения Пенсионного фонда Российской Федерации (государственное учреждение) по Ивановской области с удостоверяющими центрами внешних организаций

## ****Общие положения****

* 1. Регламент взаимодействия удостоверяющего центра ОПФР (УЦ ОПФР) с удостоверяющими центрами (УЦ) внешних организаций (далее – Регламент) предназначен для организации защищенного обмена информацией и установления отношений доверия между УЦ ОПФР и УЦ внешних организаций, оказывающими услуги по организации защищенного от несанкционированного доступа электронного документооборота (ЭДО) органов ПФР с внешними организациями и выдаче сертификатов ключей проверки электронной подписи пользователям внешних организаций.
	2. Целью настоящего Регламента является создание условий для организации защищенного от несанкционированного доступа ЭДО органов ПФР с внешними организациями через открытые каналы связи и правовых условий использования электронной подписи (ЭП) в электронных документах (ЭД), при соблюдении которых ЭП в ЭД признается равнозначной собственноручной подписи в документе на бумажном носителе в соответствии с Федеральным законом от 06 апреля 2011 г. 63-ФЗ «Об электронной подписи».
	3. Регламент разработан с учетом требований законодательства Российской Федерации, нормативных документов Федеральной службы безопасности Российской Федерации, других федеральных органов исполнительной власти Российской федерации и Пенсионного фонда Российской Федерации (ПФР).
	4. Настоящий регламент является неотъемлемой частью Соглашения между ОПФР и Удостоверяющим центром внешней организации о взаимном признании сертификатов ключей проверки электронной подписи уполномоченных лиц удостоверяющих центров и организации взаимодействия.
	5. Подписание Соглашения означает, что Стороны:

признают сертификаты ключей проверки электронной подписи уполномоченных лиц УЦ каждой из Сторон;

проводят все необходимые процедуры, предусмотренные Регламентом и обеспечивающие подтверждение подлинности ЭП в ЭД, если сертификат ключа проверки электронной подписи подписавшего ЭД заверен ЭП уполномоченного лица УЦ любой из Сторон;

проводят все необходимые процедуры, предусмотренные Регламентом и обеспечивающие подтверждение подлинности ЭП в ЭД, если сертификат ключа проверки электронной подписи подписавшего ЭД заверен ЭП уполномоченного лица УЦ другой Стороны или ЭП уполномоченного лица иного УЦ при наличии кросс-сертификата этого УЦ, выпущенного противоположной Стороной.

## ****Термины и определения****

* 1. **АРМ [Администратор]** – автоматизированное рабочее место, представляющее собой один или два компьютера с установленным программным обеспечением (ПО) ViPNet обеспечивающим:

**ЦУС** – создание инфраструктуры виртуальной защищенной сети на базе распределенной системы персональных и межсетевых экранов технологии ViPNet, обеспечивающей защиту функционирования компьютеров и передаваемой информации в распределенной сети.

**УКЦ -** выполнение всех необходимых функций **УЦ**, связанных с изданием, отзывом, хранением сертификатов ключей проверки электронной подписи, а также других функций, предусмотренных Федеральным законом от 06 апреля 2011 г. 63-ФЗ «Об электронной подписи».

* 1. **Внешняя организация** – юридическое лицо, не входящее в структуру органов ПФР, но осуществляющее с ними информационное взаимодействие.
	2. **Доверенный способ** **передачи информации** – способ передачи информации, определенный и используемый двумя или несколькими юридическими или физическими лицами на основе взаимной договоренности, и обеспечивающий требуемую степень ее защищенности.
	3. **Доверенный УЦ** – УЦ, с которым УЦ ОПФР или УЦ внешней организации установил доверенные отношения.
	4. **Ключ электронной подписи -** уникальная последовательность символов, предназначенная для создания электронной подписи.
	5. **Ключевой дистрибутив -** зашифрованный на парольном ключе файл, формируемый УЦ для зарегистрированных пользователей УЦ. Включает в себя необходимую первичную ключевую информацию для обеспечения защищенного взаимодействия с УЦ, первичный закрытый ключ и сертификат ключа проверки электронной подписи пользователя, сертификат уполномоченного лица УЦ, другие файлы, необходимые для реализации функций ЭП.
	6. **Кросс-сертификат ключа электронной подписи** – сертификат ключа проверки электронной подписи уполномоченного лица УЦ внешней организации, передаваемый в УЦ ОПФР, с ключом проверки электронной подписи уполномоченного лица этого УЦ и ЭП уполномоченного лица, доверенного УЦ. Обеспечивает признание ЭП, сертификат ключа проверки которой выдан в УЦ внешней организации.
	7. **Ключ проверки электронной подписи -** уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.
	8. **Плановая смена ключей –** смена ключей, не вызванная компрометацией ключей, в соответствии с документацией на СКЗИ.
	9. **Пользователь УЦ –** физическое лицо, зарегистрированное в УЦ.
	10. **Подтверждение подлинности ЭП в ЭД** – положительный результат проверки соответствующим сертифицированным средством ЭП с использованием сертификата ключа проверки электронной подписи принадлежности ЭП в ЭД владельцу сертификата ключа проверки электронной подписи и отсутствия искажений в подписанном данной ЭП ЭД.
	11. **Распределенная система сетевой защиты (технология ViPNet) –** технология, основанная на использовании системы персональных и межсетевых экранов, объединяющая взаимодействующие компьютеры (рабочие станции и серверы) в распределенной информационной сети через безопасные криптографически защищенные виртуальные соединения (туннели), обеспечивающая защиту трафика любых приложений, функционирующих на этих компьютерах, инфраструктуры электронной подписи, самих технических средств от несанкционированного доступа через каналы связи.
	12. **Средство криптографической защиты информации** **(СКЗИ)** – программное или аппаратное средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее шифрования и (или) электронной подписи.
	13. **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.
	14. **Сертификат ключа проверки электронной подписи –** 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.
	15. **Список аннулированных сертификатов (САС)** - ЭД с ЭП уполномоченного лица УЦ, включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, которые на определенный момент времени были аннулированы или действие которых было приостановлено.
	16. **Уполномоченное лицо УЦ** – физическое лицо, являющееся сотрудником УЦ и наделенное УЦ полномочиями по заверению сертификатов ключей проверки электронной подписи и САС.
	17. **Участник ЭДО** – пользователь, наделенный правом использования ЭП с соответствующими правами для участия в ЭДО.
	18. **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.
	19. **Электронный документ (ЭД)** – документ, в котором информация представлена в электронной форме.
	20. **Электронный документооборот (ЭДО)** – обмен и работа с электронными документами.
	21. **Электронная подпись –** 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.

## ****Организация защищенного взаимодействия между УЦ ОПФР и УЦ внешней организации на основе технологии ViPNet****

* 1. Защищенное взаимодействие между УЦ ОПФР и УЦ внешней организации осуществляется путем установления взаимодействия между АРМами [Администратор] Сторон с целью автоматизации процесса организации защищенного ЭДО юридически значимыми документами между участниками ЭДО разных ViPNet сетей.
	2. Первоначальная процедура организации защищенного взаимодействия между АРМами [Администратор] Сторон выполняется путем обмена доверенным способом файлами экспорта и межсетевым ключом связи в соответствии с документацией на АРМ [Администратор]. С этой целью:
		1. В АРМ [Администратор] одной из Сторон формируются межсетевой ключ, а также файлы экспорта для АРМ [Администратор] другой Стороны со списком узлов, которым требуется взаимодействие с другой сетью.
		2. Файлы экспорта вместе с паролями доступа к межсетевому ключу связи передаются в УЦ другой Стороны, который производит ввод (импорт) данных из полученных файлов экспорта в свой АРМ [Администратор] и задание необходимых связей своих узлов с импортированными узлами другой сети. Формируются ответные файлы экспорта.
		3. Ответные файлы экспорта передаются в УЦ другой Стороны, где они вводятся в АРМ [Администратор].
	3. В дальнейшем при модификации структуры сетей, регистрации (удалении) абонентских пунктов и пользователей, изменении связей, выпуске новых сертификатов ключей проверки электронной подписи уполномоченных лиц УЦ, САС производится автоматическое формирование файлов экспорта с соответствующей информацией и их отправка на АРМ [Администратор] другой Стороны через установленное межсетевое защищенное соединение.
	4. На основании полученной информации в АРМ [Администратор] каждой из Сторон формируется необходимая ключевая и справочная информация для узлов своей сети, после рассылки которой между соответствующими узлами двух сетей появляется возможность защищенного ЭДО юридически значимыми документами.

## ****Порядок взаимодействия УЦ Сторон при формировании новых списков отозванных сертификатов, при смене ключей электронной подписи уполномоченных лиц УЦ****

* 1. При изменении САС в случае отзыва или приостановки действия сертификатов ключей проверки электронной подписи пользователей УЦ новый САС высылается в УЦ каждой из Сторон. Полученные САС подписываются уполномоченным лицом УЦ и размещаются в точках публикации УЦ.
	2. Уполномоченные лица УЦ каждой из Сторон обязаны производить периодическую (плановую) замену своих ключей проверки электронной подписи не реже заданного срока действия ключа подписи. В целях обеспечения действительности сертификатов ключей проверки электронной подписи пользователей УЦ, заверенных подписью уполномоченного лица, соответствующего УЦ, замена ключей проверки электронной подписи уполномоченного лица УЦ должна быть произведена до окончания его срока действия не менее чем за срок действия сертификатов пользователей УЦ.
	3. В случае компрометации ключей проверки электронной подписи уполномоченное лицо УЦ обязано:

немедленно сообщить об этом ответственным лицам УЦ другой Стороны;

аннулировать сертификат ключа проверки электронной подписи и отправить новые САС в УЦ другой Стороны;

сформировать новые ключи проверки электронной подписи и сертификат ключа проверки электронной подписи.

Начальник Отдела

по защите информации Д. С. Полянин