СОГЛАСОВАНО

Директор ТФОМС
Иркутской области

_____ Е.В. Градобоев
(подпись)
«05» апреля 2019г.

УТВЕРЖДЕН

Директор
ООО по защите информации
«Секрет-Сервис»

_____ Б.Б. Измайлов
(подпись)
«05» апреля 2019 г.

Регламент
Удостоверяющего Центра корпоративного уровня развернутого в интересах Территориального фонда обязательного медицинского страхования Иркутской области

Иркутск 2019

СОДЕРЖАНИЕ

Перечень сокращений, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 5
1. Общие положения 8
1.2. Идентификация Регламента 9
1.3. Публикация Регламента 9
1.4. Область применения Регламента 9
1.5. Срок действия Регламента 9
1.6. Порядок утверждения и внесения изменений в Регламент 10
2. Удостоверяющий центр корпоративного уровня, пользователи услуг УЦКУ 10
2.1. Сведения об Удостоверяющем Центре 10
2.2. Реестр Удостоверяющего центра корпоративного уровня 12
2.3. Назначение Удостоверяющего Центра корпоративного уровня 12
2.4. Услуги, предоставляемые Удостоверяющим Центром корпоративного уровня 12
2.5. Структура Удостоверяющего Центра 13
2.6. Прекращение деятельности 15
2.7. Пользователи услуг Удостоверяющего Центра 15
3. Права и обязанности, ответственность 15
3.1. Права и обязанности Удостоверяющего Центра корпоративного уровня 15
3.2. Права и обязанности пользователей УЦКУ 18
3.3. Ответственность 20
4. Политика конфиденциальности 20
5. Порядок регистрации пользователей, изготовления и управления сертификатами ключей подписей 20
5.1. Регистрация пользователей УЦКУ, являющихся сотрудниками территориального фонда ОМС Иркутской области и участвующих в защищенном обмене электронными документами 21
5.2. Регистрация и подключение внешних организаций к системе защищенного обмена электронными документами и взаимодействия информационных систем 21
5.3. Идентификация, Аутентификация зарегистрированного пользователя 22
5.4. Изготовление ключей 22
5.5. Изготовление сертификата открытого ключа и предоставление его владельцу 23
5.5.1. Изготовление сертификата открытого ключа в процессе работы 23
5.5.2. Аннулирование (отзыв) сертификата открытого ключа 23
5.5.3. Приостановление действия сертификата открытого ключа 24
5.5.4. Возобновление действия сертификата открытого ключа 24
5.5.5. Хранение сертификата открытого ключа пользователей 25
5.6. Организация защищенного информационного взаимодействия между сторонами с использованием процедур межсетевого обмена сетей ViPNet 25
5.6.1. Порядок организации защищенного межсетевого информационного взаимодействия между сторонами 25
5.6.2. Порядок организации межведомственного защищенного 26

информационного взаимодействия между ViPNet - сетями организаций
5.6.3. Порядок модификации защищенного информационного взаимодействия между ViPNet - сетями организаций при изменении состава узлов 26
5.6.4. Журнал изменений межведомственного защищенного информационного взаимодействия. 27
5.6.5. Порядок организации защищенного информационного взаимодействия между ViPNet-сетями организаций в случае плановой смены межсетевого мастер-ключа 27
6. Процедура Разбора конфликтных ситуаций и споров в связи с осуществлением ЭДО 28
6.1. Порядок проведения технической экспертизы 29
6.2. Оформление результатов технической экспертизы 31
7. Дополнительные положения 31
7.1. Идентифицирующие данные уполномоченного лица Удостоверяющего Центра корпоративного уровня 31
7.2. Сроки действия ключей уполномоченного лица Удостоверяющего Центра 31
7.3. Требования к средствам электронной подписи пользователей УЦКУ 32
7.4. Сроки действия закрытых ключей и сертификатов открытых ключей владельцев сертификатов открытых ключей 32
7.5. Назначение ключей и Сертификата открытого ключа, Меры защиты закрытых ключей 32
7.6. Архивное хранение документированной информации 33
7.7. Управление ключами 34
7.7.1. Плановая смена ключей уполномоченного лица Удостоверяющего Центра 34
7.7.2. Внеплановая смена ключей уполномоченного лица Удостоверяющего Центра 34
7.7.3. Плановая смена ключей Пользователя Удостоверяющего Центра 35
7.7.4. Внеплановая смена ключей Пользователя Удостоверяющего Центра 35
8. Структуры сертификатов и списков отозванных сертификатов 36
8.1. Структура сертификата открытого ключа, изготавливаемого Удостоверяющим Центром в электронной форме 36
8.1.1. Базовые поля сертификата открытого ключа 36
8.1.2. Дополнения сертификата 36
8.1.3. Поддерживаемые объектные идентификаторы алгоритмов 37
8.1.4. Формы имени 37
8.1.5. Ограничения на имена 37
8.2. Структура списка отозванных сертификатов, изготавливаемого Удостоверяющим Центром в электронной форме Дополнения СОС 38
9. Программные и технические средства обеспечения деятельности Удостоверяющего Центра 38
9.1. Программный комплекс обеспечения реализации целевых функций Удостоверяющего Центра корпоративного уровня 39
9.2. Технические средства обеспечения работы ПК УЦКУ 40
9.3. Программные и программно-аппаратные средства защиты информации 41
9.4. Перечень событий, регистрируемых программным комплексом 41

обеспечения реализации целевых функций Удостоверяющего Центра
9.5. *Перечень данных программного комплекса обеспечения реализации целевых функций Удостоверяющего Центра, подлежащих резервному копированию* 41
10. Обеспечение безопасности 42
10.1. *Инженерно-технические меры защиты информации* 42
Размещение технических средств Удостоверяющего Центра 42
Физический доступ в помещения 42
Электроснабжение и кондиционирование воздуха 42
Подверженность воздействию влаги 43
Предупреждение и защита от возгорания 43
Хранение документированной информации 43
Уничтожение документированной информации 43
10.2. *Программно-аппаратные меры защиты информации* 43
Организация доступа к техническим средствам Удостоверяющего Центра 43
Организация доступа к программным средствам Удостоверяющего Центра 43
Контроль целостности программного обеспечения 44
Контроль целостности технических средств 44
Защита внешних сетевых соединений 44
Перечень информации, подлежащей защите 45
10.3. *Организационные меры защиты информации* 45
Предъявляемые требования к персоналу Удостоверяющего Центра 45
Профессиональная переподготовка и повышение квалификации персонала 45
Организация сменной работы 45
Организация доступа персонала к документам и документации 45
Охрана здания и помещений 45
10.4. *Юридические меры защиты информации* 45
Приложение №1. Письмо на подключение к системе обмена электронными документами в защищенной сети ОМС Иркутской области 47
Приложение №2. Заявка на подключение к системе 48
Приложение №3. Соглашение о присоединении к Регламенту Удостоверяющего Центра корпоративного уровня, развернутого в интересах Территориального фонда обязательного медицинского страхования Иркутской области 49
Приложение №4. Заявка на изготовление сертификатов ключей подписей сотрудников 55
Приложение №5. Заявка на отзыв сертификатов ключей подписей сотрудников 56
Приложение №6. Заявка на приостановление действия сертификатов ключей подписей сотрудников 57
Приложение №7. Заявка на возобновление действия сертификатов ключей подписей сотрудников 58
Приложение №8. Заявка на получение информации о статусе сертификата ключа подписи сотрудников, изданного 59

Удостоверяющим центром
Приложение №9. Заявление на регистрацию Пользователя Удостоверяющего центра 60
Приложение №10. Доверенность Пользователя Удостоверяющего центра 61
Приложение №11. Доверенность Пользователя на предоставление заявительных документов и получения ключей подписей и сертификата 62
Приложение №12. Заявление на изготовление сертификата ключа подписи Пользователя Удостоверяющего центра 64
Приложение №13. Заявление на аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра 65
Приложение №14. Заявление на приостановление действия сертификата ключа подписи Пользователя Удостоверяющего центра 66
Приложение №15. Заявление на возобновление действия сертификата ключа подписи Пользователя Удостоверяющего центра 67
Приложение №16. Заявление на получение информации о статусе сертификата ключа подписи, изданного Удостоверяющим центром 68
Приложение №17. Сертификат ключа подписи 69
Приложение №18. Журнал учета изготовления и выдачи ключей под роспись 70
Приложение №19. Протокол установления межсетевого взаимодействия 71
Приложение №20. Журнал изменений 72

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Перечень сокращений

УЦ	Удостоверяющий центр
ЭП	Электронная подпись
РФ	Российская Федерация
СОС	Список отозванных сертификатов
ЭД	Электронный документ
УЦКУ	Удостоверяющий центр корпоративного уровня
УКЦ	Удостоверяющий и Ключевой центр
СКЗИ	Средство криптографической защиты информации
ЦУС	Центр управления сетью
СУ	Сетевой узел
СУЦ	Система удостоверяющих центров
ПСЭ	Персональный сетевой экран
ViPNet	Торговая марка программного обеспечения компании ОАО «Инфотекс» г.Москва
ДК	Домен–К
Фонд	Территориальный фонд обязательного медицинского страхования Иркутской области
СЗОЭД ОМС	Система защищенного обмена электронными документами в системе обязательного медицинского страхования

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

АРМ [Администратор] - автоматизированное рабочее место Администратора сети ViPNet, реализующее, в том числе, все необходимые функции корпоративного удостоверяющего центра (УЦКУ), связанные с изданием, отзывом, хранением сертификатов ключей подписи, а также иные функции в соответствии с Законом об электронной подписи.

Администратор сети ViPNet - лицо, назначенное руководителем организации, эксплуатирующей АРМ [Администратор], и предоставляющей услуги корпоративного удостоверяющего центра. Администратор безопасности обеспечивает эксплуатацию АРМ [Администратор] и является уполномоченным лицом, подписывающим своей электронной подписью сертификаты ключей подписей пользователей, зарегистрированных на данном АРМ [Администратор].

Владелец сертификата ключа подписи – физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом ЭП, позволяющим с помощью средств ЭП создавать свою ЭП в электронных документах (подписывать электронные документы).

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

Запрос на сертификат - сообщение, содержащее необходимую информацию для получения сертификата.

Запрос на отзыв сертификата - сообщение, содержащее необходимую информацию для отзыва сертификата.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Ключ (криптографический ключ) - конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Ключевая пара - открытый и закрытый ключи.

Ключевой носитель - носитель, содержащий один или несколько ключей.

Компрометация ключа - утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

Копия сертификата ключа подписи – документ на бумажном носителе, содержащий информацию из сертификата ключа подписи и заверенный собственноручной подписью уполномоченного лица Удостоверяющего центра и печатью Удостоверяющего центра.

Ключевой Центр (КЦ) - компонент удостоверяющего центра. Входит в программу ViPNet [Удостоверяющий и Ключевой Центр]. Предназначен для формирования пользовательской ключевой информации. Эта программа формирует ключевую информацию на основе информации, поступающей из ЦУС. Созданные программой КЦ ключи передаются пользователям, после чего при наличии соответствующего ПО ViPNet пользователи сети смогут безопасно обмениваться конфиденциальной информацией.

Открытый ключ электронной подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной подписи подлинности электронной подписи в электронном документе.

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

Пользователь Удостоверяющего центра (Пользователь УЦКУ) – физическое лицо (уполномоченный представитель Стороны, присоединившейся к Регламенту), зарегистрированное в Удостоверяющем центре

Сторона пользователя - юридическое лицо, представителем которого является пользователь.

Сертификат ключа подписи - документ на бумажном носителе или электронный документ с электронной подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной подписи и которые выдаются удостоверяющим центром пользователю информационной системы для подтверждения подлинности электронной подписи и идентификации владельца сертификата ключа подписи.

Список отозванных сертификатов (СОС) - документ на бумажном носителе или электронный документ с электронной подписью уполномоченного лица удостоверяющего центра, содержащий список сертификатов, действие которых прекращено или приостановлено до истечения их срока действия.

Средство электронной подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций -

создание электронной подписи в электронном документе с использованием закрытого ключа электронной подписи, подтверждение с использованием открытого ключа электронной подписи подлинности электронной подписи в электронном документе, создание закрытых и открытых ключей электронных подписей.

Удостоверяющий центр (УЦ) - компонент удостоверяющего центра. Входит в программу ViPNet [Удостоверяющий и Ключевой Центр]. Предназначен для обслуживания следующих запросов: на издание сертификатов ЭП, на отзыв, приостановление и возобновления приостановленного действия сертификатов пользователей УЦКУ, сформированных на сетевых узлах сети ViPNet (пользователями корпоративной сети) или в Центрах регистрации для внешних пользователей.

Уполномоченное лицо Удостоверяющего центра – физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов ключей подписей и списков отозванных сертификатов

Центр регистрации - компонент удостоверяющего центра. Входит в программу ViPNet [Пункт Регистрации]. Предназначен для регистрации внешних пользователей, создания ключей подписи и формирования запросов на издание, приостановление, отзыв и возобновление сертификата ключа подписи.

Центр сертификации - компонент удостоверяющего центра. Выполняет функции службы сертификации: выпуск сертификатов, отзыв сертификатов, а также генерацию списков отзыва.

Центр управления сетью (ЦУС) - компонент удостоверяющего центра. Предназначен для формирования и изменения структуры корпоративной сети.

Электронный документ (ЭД) - документ, в котором информация представлена в электронно- форме, и который может быть представлен в виде файла, хранящегося на носителе.

Электронная подпись (электронная подпись, ЭП) - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1.ОБЗОРНАЯ ИНФОРМАЦИЯ

Регламент Удостоверяющего Центра корпоративного уровня развернутого в интересах Территориального фонда обязательного медицинского страхования Иркутской области, именуемый в дальнейшем «Регламент», разработан в соответствии с законодательством РФ, регулирующим деятельность удостоверяющих центров.

Удостоверяющий центр развернут на базе ООО по защите информации «Секрет-Сервис»

Целью настоящего Регламента является создание условий для организации защищенного обмена электронными документами и правовых условий использования электронной подписи в электронных документах, при соблюдении которых электронная подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе в соответствии с Федеральным законом РФ от 06.04.2011 г. N 63-ФЗ «Об электронной подписи».

Настоящий Регламент устанавливает общий порядок и условия предоставления Удостоверяющим Центром корпоративного уровня (далее по тексту – УЦКУ) Пользователю Системы защищенного обмена электронными документами, присоединившемуся к Регламенту в порядке, предусмотренном положениями статьи 428 Гражданского Кодекса РФ, услуг по изготовлению и выдаче сертификатов ключей электронной подписи и дополнительных услуг, связанных с управлением сертификатами ключей подписи и шифрования, включая обязанности пользователей, и членов группы администрирования УЦ, режимы работы, принятые форматы данных и мероприятия, необходимые для безопасной работы удостоверяющего центра.

Присоединение к Регламенту производится путем заключения Стороной Системы защищенного обмена электронными документами **Соглашения о присоединении к Регламенту Удостоверяющего Центра корпоративного уровня развернутого в интересах Территориального фонда обязательного медицинского страхования Иркутской области для организации защищенного обмена электронными документами и взаимодействия информационных систем** (далее по тексту – Соглашение о присоединении к Регламенту), указанного в Приложении № 3 к Регламенту.

После присоединения в установленном порядке Пользователя к Регламенту, Стороны вступают в соответствующие договорные отношения на неопределённый срок.

Пользователь имеет право в одностороннем порядке без обращения в суд расторгнуть Соглашение о присоединении к Регламенту, письменно уведомив об этом УЦКУ за один месяц до дня расторжения. Уведомление о расторжении Соглашения, полученное УЦКУ от Пользователя, является основанием для обязательного аннулирования сертификатов ключей подписей Пользователей УЦ, уполномоченных данным Пользователем. Датой аннулирования указанных сертификатов ключей Пользователей УЦ будет дата расторжения Соглашения о присоединении к Регламенту. При этом Стороны до дня прекращения действия Соглашения о присоединении к Регламенту обязаны разрешить между собой все вопросы, связанные с Соглашением о присоединении к Регламенту.

Расторжение Соглашения о присоединении к Регламенту не освобождает Стороны от исполнения обязательств, возникших до указанного прекращения, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

1.2.ИДЕНТИФИКАЦИЯ РЕГЛАМЕНТА

Наименование документа: «Регламент Удостоверяющего Центра корпоративного уровня развернутого в интересах Территориального фонда обязательного медицинского страхования Иркутской области».

Идентификация удостоверяющего центра корпоративного уровня развернутого в интересах Территориального фонда обязательного медицинского страхования Иркутской области для организации юридической значимости:

- защищенного обмена электронными документами и взаимодействия информационных систем путем формирования объектных идентификаторов, сертификатов открытых ключей;
- утверждения перечня объектных идентификаторов областей применения сертификатов открытых ключей;
- включения перечня объектных идентификаторов в форму соглашения с пользователями удостоверяющего центра.

1.3.ПУБЛИКАЦИЯ РЕГЛАМЕНТА

Настоящий Регламент распространяется:

В электронной форме

- на сайте www.irkoms.ru Фонда в разделе «О Фонде», «Удостоверяющий центр», «Регламент удостоверяющего центра сети ViPNet»;
- на машинном носителе, передаваемом Пользователю при его подключении к Системе защищенного электронного обмена документами.

Регламент, предназначенный для распространения в электронной форме, распространяется в виде файла формата PDF.

Любое заинтересованное лицо может ознакомиться с Регламентом на сайте www.irkoms.ru.

Любые справки по вопросам, связанным с оказанием услуг Удостоверяющего Центра корпоративного уровня, предоставляются по телефону (3952) 708782.

1.4.ОБЛАСТЬ ПРИМЕНЕНИЯ РЕГЛАМЕНТА

Настоящий Регламент предназначен служить соглашением, налагающим обязательства на все вовлеченные Стороны, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦКУ.

Регламент применим при организации защищенного обмена электронными документами и взаимодействия информационных систем в системе обязательного медицинского страхования, организованным Фондом, в том числе и в интересах других юридических лиц.

1.5.СРОК ДЕЙСТВИЯ РЕГЛАМЕНТА

Настоящий Регламент вступает в силу со дня его утверждения.

Срок действия Регламента - 5 лет.

Если Удостоверяющий Центр официально не уведомит пользователей УЦКУ о прекращении действия Регламента, Регламент автоматически пролонгируется на следующие 5 лет.

Официальное уведомление о прекращении действия Регламента публикуется на сайте www.irkoms.ru Фонда в разделе «О Фонде», «Удостоверяющий центр», «Регламент удостоверяющего центра сети ViPNet» и направляется Сторонам по защищенной сети ViPNet.

1.6.ПОРЯДОК УТВЕРЖДЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ

Настоящий Регламент согласовывается директором Фонда, заверяется его подписью и печатью Фонда.

Все изменения и дополнения к настоящему Регламенту составляются в письменной форме и являются его составной и неотъемлемой частью.

Публикация изменений и дополнений осуществляется в порядке, соответствующему порядку утверждения и публикации Регламента.

Все изменения и дополнения, вносимые в Регламент и не связанные с изменением законодательства РФ, вступают в силу и становятся обязательными для Сторон по истечении 10 (Десяти) календарных дней с даты размещения указанных изменений и дополнений в Регламенте на сайте www.irkoms.ru Фонда в разделе «О Фонде», «Удостоверяющий центр», «Регламент удостоверяющего центра сети ViPNet».

Все изменения и дополнения, вносимые в Регламент в связи с изменением законодательной и нормативной базы, вступают в силу одновременно с вступлением в силу изменений и дополнений в указанных актах.

2. УДОСТОВЕРЯЮЩИЙ ЦЕНТР КОРПОРАТИВНОГО УРОВНЯ, ПОЛЬЗОВАТЕЛИ УСЛУГ УЦКУ

2.1.СВЕДЕНИЯ ОБ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ

Полное наименование юридического лица УЦКУ: Удостоверяющий Центр корпоративного уровня ООО по защите информации «Секрет-Сервис».

Почтовый адрес: 6640075, г. Иркутск, ул. Байкальская 234-в/2, офис 1.
Адрес электронной почты: info@irksecret.ru
Контактный телефон УЦКУ: (395-2) 79-87-82
Факс: (395-2) 59-15-25, 79-87-82

Удостоверяющий Центр корпоративного уровня развернутого в интересах Фонда:

- (фирменное наименование: Удостоверяющий Центр корпоративного уровня ООО по защите информации «Секрет-Сервис»,
- сокращенное наименование: Удостоверяющий Центр Секрет-Сервис.

Удостоверяющий Центр корпоративного уровня ООО по защите информации «Секрет-Сервис» зарегистрирован на территории РФ в городе Иркутске.

Свидетельство о постановке на учет юридического лица в налоговом органе по месту нахождения на территории РФ: серия 38 №002613246, ИНН 3812066441, КПП 381201001.

Свидетельство о внесении в Единый государственный реестр юридических лиц о юридическом лице, зарегистрированном до 1 июля 2002 года: серия 38 №001585475, ОГРН 1023801759860.

Удостоверяющий Центр корпоративного уровня в качестве участника предоставления услуг по изготовлению и выдаче сертификатов ключей подписи осуществляет свою деятельность на территории Иркутской области на основании:

Лицензии ФСБ России № 1948 от 27 сентября 2016 г. (бессрочная) на осуществление:

разработки, производства, распространения шифровальных, (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя.

- работы предусмотренные пунктами 12,13,14,15,20,21,22,23,24,25,26,27,28 перечня выполняемых работ и оказываемых услуг, являющегося приложением к Положению утвержденному постановлением Правительства РФ от 16 апреля 2012 г. №313

- Использования сертифицированного программного обеспечения для создания защищенной телекоммуникационной сети ViPNet №559 на платформе ПО «ViPNet 4», разработанный и производимый ОАО «ИнфоТеКС» в соответствии с техническими условиями ФРКЕ.00131-01 30 01, функционирующий на аппаратных платформах в среде операционных систем, указанных в формуляре ФРКЕ.00131-01 30 01, является программным средством защиты от несанкционированного доступа к информации в сетях с IP-протоколом.

- Сертификат соответствия ФСТЭК России № 3727 от 29.08.2018 на программный комплекс защиты информации «ViPNet 4» подтверждает соответствие требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа В четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК России, 2016) и заданию по безопасности ФРКЕ.00131-01 98 01 при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00131-01 30 01;

- Сертификат соответствия ФСБ России № СФ/124-3657 от 20.03.2019 удостоверяет, что изделие «Программный комплекс ViPNet Administrator 4» соответствует Требованиям ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, Требованиям к средствам криптографической защиты информации, не содержащей сведений, составляющих государственную тайну, классов КС1, КС2, КС3, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для классов КС1, КС2, КС3 и может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.

Реквизиты Удостоверяющего центра корпоративного уровня
Юридический адрес: 6640074, Иркутск, ул. 4-я Железнодорожная, д. 100, к.61.
Для почты: 6640075, г. Иркутск, ул. Байкальская 234-в/2, офис 1.
Банковские реквизиты:
ИНН: 3812066441
КПП 381201001
р/с40702810703780000031, БИК042520702.
Руководитель: директор Измайлов Борис Борисович

2.2.РЕЕСТР УДОСТОВЕРЯЮЩЕГО ЦЕНТРА КОРПОРАТИВНОГО УРОВНЯ

Реестр Удостоверяющего Центра - набор документов Удостоверяющего Центра в электронной и/или бумажной форме, включающий следующую информацию:

- реестр заявлений на регистрацию пользователя в Удостоверяющем Центре;
- реестр зарегистрированных пользователей Удостоверяющего Центра;
- реестр заявлений на сертификат ключа подписи;
- реестр заявлений на аннулирование (отзыв) сертификата ключа подписи;
- реестр заявлений на приостановление/возобновление действия сертификата ключа подписи;
- реестр сертификатов ключей подписи;
- реестр изготовленных списков отозванных сертификатов ключей подписи;
- служебные документы Удостоверяющего Центра.

2.3.НАЗНАЧЕНИЕ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА КОРПОРАТИВНОГО УРОВНЯ

Удостоверяющий Центр корпоративного уровня предназначен для обеспечения участников корпоративной защищенной информационной сети средствами и спецификациями для использования сертификатов ключей в целях обеспечения:

- аутентификации участников информационных систем в процессе взаимодействия;
- применения электронной подписи;
- контроля целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем;
- конфиденциальности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем.

2.4.УСЛУГИ, ПРЕДОСТАВЛЯЕМЫЕ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ КОРПОРАТИВНОГО УРОВНЯ

В процессе своей деятельности Удостоверяющий Центр предоставляет пользователям УЦКУ следующие виды услуг:

- внесение в реестр Удостоверяющего Центра регистрационной информации о пользователях УЦКУ;
- формирование и обновление справочно-ключевой информации для организации защищенного обмена информации в рамках корпоративной сети;

- изготовление сертификатов открытых ключей пользователей УЦКУ в электронной форме;

- изготовление копии сертификатов открытых ключей пользователей УЦКУ на бумажном носителе;

- формирование закрытых и открытых ключей по обращениям пользователей УЦКУ, с записью их на ключевой носитель;

- ведение реестра изготовленных сертификатов открытых ключей пользователей УЦКУ;

- предоставление копий сертификатов открытых ключей в электронной форме, находящихся в реестре изготовленных сертификатов, по запросам пользователей УЦКУ;

- аннулирование (отзыв) сертификатов открытых ключей по обращениям владельцев сертификатов открытых ключей;

- приостановление и возобновление действия сертификатов открытых ключей по обращениям владельцев сертификатов открытых ключей;

- предоставление пользователям УЦКУ сведений об аннулированных и приостановленных сертификатах открытых ключей;

- подтверждение подлинности электронных подписей в документах, представленных в электронной форме, по обращениям пользователей УЦКУ;

- подтверждение подлинности электронных подписей уполномоченного лица Удостоверяющего Центра в изготовленных им сертификатах открытых ключей по обращениям пользователей УЦКУ;

- распространение средств электронной подписи и шифрования по обращения пользователей УЦКУ.

Услуги Удостоверяющего Центра корпоративного уровня предоставляются на возмездной основе.

2.5.СТРУКТУРА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Директор Фонда подписывает договор в котором:

- Возлагается исполнение обязанностей Администратора сети ViPNet №559 (Уполномоченное лицо удостоверяющего центра) имеющее:

- Лицензию ФСБ России № 1948 от 27 сентября 2016 г. (бессрочная) на осуществление: разработки, производства, распространения шифровальных, (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя;

- Наделяется Уполномоченное лицо УКЦУ правом подписывать своей электронной подписью сертификаты ключей подписей пользователей УКЦУ,

зарегистрированных на АРМ [Администратор] и заверять собственноручной подписью копии сертификатов ключей на бумажном носителе;

– Возлагаются функции обеспечения информационной безопасности и технической эксплуатации УЦКУ.

На ООО по защите информации «Секрет-Сервис» возлагаются функции для решения задач УЦКУ по:

- управлению деятельностью УЦКУ;

- взаимодействию с пользователями УЦКУ в части разрешения вопросов, связанных с применением средств ЭП, ключей и сертификатов открытых ключей, изготовляемых и/или распространяемых УЦКУ;

- взаимодействию с пользователями УЦКУ в части разрешения вопросов, связанных с подтверждением электронной подписи уполномоченного лица УЦКУ в сертификатах открытых ключей, изготовленных Удостоверяющим Центром в электронной форме, или подтверждения собственноручной подписи уполномоченного лица Удостоверяющего Центра в копиях сертификатов открытых ключей, изготовленных Удостоверяющим Центром на бумажном носителе.

- регистрации пользователей УЦКУ;

- ведению реестра зарегистрированных пользователей УЦКУ;

- предоставлению ключей и сертификатов открытых ключей по обращению пользователей УЦКУ;

- распространению средств электронной подписи и шифрования;

- организации и выполнению мероприятий по защите ресурсов УЦКУ;

- формированию и обновлению справочно-ключевой информации для организации защищенного обмена информации в рамках корпоративной сети;

- обеспечению взаимодействия с другими УЦКУ, участниками СУЦ, на основе кросс-сертификации;

- изготовлению и предоставлению ключей по обращению пользователей УЦКУ;

- изготовлению и предоставлению изготовленных сертификатов открытых ключей в электронной форме по обращению пользователей УЦКУ (корпоративных и внешних);

- изготовлению и предоставлению копий сертификатов открытых ключей на бумажном носителе по обращению их владельцев;

- аннулированию (отзыву) сертификатов открытых ключей по обращениям владельцев сертификатов открытых ключей;

- приостановлению и возобновлению действия сертификатов открытых ключей по обращению владельцев сертификатов открытых ключей;

- предоставлению пользователям УЦКУ сведений об аннулированных и приостановленных сертификатах открытых ключей;

- предоставлению копий сертификатов открытых ключей, находящихся в реестре изготовленных сертификатов, по запросам пользователей УЦКУ;

- техническому обеспечению процедуры подтверждения электронной подписи в документах, представленных в электронной форме, по обращениям пользователей УЦКУ;

- техническому обеспечению процедуры подтверждения подлинности электронных подписей уполномоченного лица УЦКУ в изготовленных сертификатах открытых ключей, по обращениям пользователей УЦКУ.

2.6.ПРЕКРАЩЕНИЕ ДЕЯТЕЛЬНОСТИ

Деятельность Удостоверяющего Центра может быть прекращена в порядке, установленном законодательством РФ.

2.7.ПОЛЬЗОВАТЕЛИ УСЛУГ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Пользователями услуг Удостоверяющего Центра называются лица, зарегистрированные в УЦКУ и осуществляющие обмен электронными документами и взаимодействие информационных систем в рамках заключенного соглашения о присоединении к Регламенту.

Проходить процедуру регистрации в Удостоверяющем Центре, либо быть зарегистрированным пользователем, может только физическое лицо, представляющее юридическое лицо.

Физическое лицо представляет юридическое лицо на основании доверенности, предоставляющей право данному физическому лицу пользоваться услугами Удостоверяющего Центра. Представитель юридического лица должен иметь доверенность (Приложение №10) и наделяется правом расписываться в соответствующих документах Удостоверяющего центра для исполнения поручений, определенных настоящей Доверенностью.

Все пользователи в данном Регламенте разделяются на 2 категории:
- владельцы сертификатов ключей ЭП;
- пользователи сертификатов открытых ключей ЭП.

3.ПРАВА И ОБЯЗАННОСТИ, ОТВЕТСТВЕННОСТЬ

3.1.ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА КОРПОРАТИВНОГО УРОВНЯ

УЦКУ имеет право:

- Предоставлять копии сертификатов открытых ключей в электронной форме, находящихся в реестре Удостоверяющего Центра, всем Пользователям УКЦУ, обратившимся за копиями в Удостоверяющий Центр;

- Отказать в предоставлении услуг по регистрации пользователей УЦКУ, сторонним организациям, подавшим заявление на регистрацию, без предоставления информации о причинах отказа;

- Отказать в изготовлении ключей лицам, подавшим заявление на изготовление ключей, но не прошедшим регистрацию в УЦКУ, без предоставления информации о причинах отказа;

- Отказать в изготовлении сертификата открытого ключа зарегистрированным пользователям УЦКУ, подавшим заявление на изготовление сертификата открытого ключа, с указанием причин отказа;

- Аннулировать (отозвать) сертификат открытого ключа пользователя УЦКУ в случае установленного факта компрометации соответствующего закрытого ключа, с уведомлением владельца аннулированного (отозванного) сертификата открытого ключа и указанием обоснованных причин;

- В одностороннем порядке приостановить действие сертификата открытого ключа пользователя УЦКУ, с обязательным уведомлением владельца приостановленного сертификата открытого ключа и указанием обоснованных причин.

УЦКУ обязан:

- Организовывать проверку на предмет соответствия деятельности Удостоверяющего Центра требованиям настоящего Регламента и предоставлять необходимые материалы для проверки. Проверка Удостоверяющего Центра должна проводиться не реже одного раза в год. Для проведения проверок создается комиссия из сотрудников Фонда, имеющих необходимые навыки и умения в количестве трех человек и назначается председатель комиссии. Заключение, подписанное председателем комиссии, осуществлявшим проверку, и Уполномоченным лицом УЦКУ предоставляется директору Фонда.

- Использовать для изготовления закрытого ключа уполномоченного лица Удостоверяющего Центра и формирования электронной подписи только средства электронной подписи, сертифицированные по классу КС2 в соответствии с действующим законодательством РФ.

- Использовать закрытый ключ уполномоченного лица Удостоверяющего Центра только для подписи издаваемых им сертификатов открытых ключей и списков отозванных сертификатов.

- Принять меры по защите закрытого ключа уполномоченного лица Удостоверяющего Центра в соответствии с положениями настоящего Регламента.

- Синхронизировать по времени все программные и технические средства обеспечения деятельности по предназначению. Удостоверяющий Центр организует работу своих Служб по серверу синхронизации времени Фонда.

- Обеспечить регистрацию пользователей УЦКУ по заявлениям на регистрацию в соответствии с порядком регистрации, изложенным в настоящем Регламенте.

- Обеспечить уникальность регистрационной информации пользователей УЦКУ, заносимой в реестр Удостоверяющего Центра и используемой для идентификации владельцев сертификатов открытых ключей.

- Не разглашать (публиковать) регистрационную информацию пользователей УЦКУ, за исключением информации используемой для идентификации владельцев сертификатов открытых ключей и заносимой в изготавливаемые сертификаты.

- Публикация информации, используемой для идентификации владельцев сертификатов открытых ключей, осуществляется путем включения ее в изготавливаемые сертификаты.

- Изготовить закрытый и открытый ключ зарегистрированному пользователю по заявлению с использованием средств электронной подписи, сертифицированных в соответствии с действующим законодательством РФ.

- Обеспечить сохранение в тайне изготовленного закрытого ключа.

- Записать ключ на отчуждаемый машинный носитель, в соответствии с требованиями по эксплуатации программного и/или аппаратного средства, выполняющего процедуру генерации ключей.

- Выполнять процедуру генерации ключей и запись ключей на отчуждаемый магнитный носитель только с использованием программного и/или аппаратного средства, сертифицированного в соответствии с законодательством РФ.

- Обеспечить защиту ключевого носителя от копирования.

- Обеспечить изготовление сертификата открытого ключа зарегистрированному пользователю по заявлению, в соответствии с форматом и порядком идентификации владельца сертификата открытого ключа, определенным в настоящем Регламенте.

- Обеспечить уникальность регистрационных (серийных) номеров изготавливаемых сертификатов открытых ключей пользователей УЦКУ.

- Обеспечить уникальность значений открытых ключей в изготовленных сертификатах открытых ключей пользователей УЦКУ.

УЦКУ обеспечивает изготовление двух копий сертификата ключа подписи на бумажном носителе по форме, определенной Приложением №16 настоящего Регламента. Все копии сертификата ключа подписи на бумажном носителе заверяются собственноручной подписью лица, проходящего процедуру регистрации, или собственноручной подписью его доверенного представителя, а также собственноручной подписью Уполномоченного лица УЦКУ.

- Аннулировать (отозвать) сертификат открытого ключа по заявлению его владельца.

- В течение одного рабочего дня занести сведения об аннулированном (отозванном) сертификате в список отозванных сертификатов с указанием даты и времени занесения.

- Приостановить действие сертификата открытого ключа по заявлению его владельца.

- В течение одного рабочего дня занести сведения о приостановленном сертификате в список отозванных сертификатов с указанием даты и времени занесения и признака приостановления.

- Возобновить действие сертификата открытого ключа по заявлению его владельца (если было приостановлено действие сертификата).

- В течение одного рабочего дня исключить сведения о приостановленном сертификате из списка отозванных сертификатов.

- Уведомить о факте изготовления сертификата открытого ключа его владельца. Срок уведомления – не позднее двух рабочих дней с момента изготовления сертификата открытого ключа.

- Официально уведомить о факте аннулирования (отзыва), приостановлении и возобновлении действия сертификата ключа подписи лиц, зарегистрированных в УЦКУ. Срок уведомления – не позднее одного рабочего дня с момента занесения сведений об аннулированном (отозванном), приостановленном, возобновленном сертификате в список отозванных сертификатов. Официальным уведомлением является рассылка всем пользователям списка отозванных сертификатов и опубликование на сайте удостоверяющего центра.

- Временем аннулирования (отзыва), приостановления, возобновления сертификата ключа признается время занесения сведений в список отозванных сертификатов и включенное в его структуру.

- Обязан вести реестр всех изготовленных сертификатов открытых ключей пользователей

УЦКУ в течение установленного срока хранения. Реестр сертификатов открытых ключей ведется в электронном виде. Сертификаты открытых ключей представлены в реестре в форме электронных копий изготовленных сертификатов. Выписка из реестра Удостоверяющего Центра предоставляется в виде списка отозванных сертификатов в электронной форме и формате, определенном настоящим Регламентом.

- Осуществлять выдачу копий сертификатов открытых ключей в электронной форме по обращениям пользователей УЦКУ.

- Уведомлять владельца сертификата открытого ключа о фактах, которые стали известны Удостоверяющему Центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата открытого ключа.

3.2.ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ УЦКУ

Пользователи УЦКУ имеют права:

- обратиться в Удостоверяющий Центр для изготовления сертификата ЭП;
- получить и ввести в действие на своем рабочем месте изготовленный сертификат ЭП в электронной форме;
- обратиться в Удостоверяющий Центр для внесения в реестр Удостоверяющего Центра регистрационной информации о пользователе УЦ, с целью в дальнейшем стать владельцем сертификата открытого ключа;
- получить список аннулированных (отозванных) и приостановленных сертификатов открытых ключей, изготовленный Удостоверяющим Центром;
- получить сертификат открытого ключа уполномоченного лица Удостоверяющего Центра;
- получить копию сертификата открытого ключа в электронной форме, находящегося в Реестре сертификатов открытых ключей Удостоверяющего Центра;
- применять сертификат открытого ключа уполномоченного лица Удостоверяющего Центра для проверки электронной подписи уполномоченного лица Удостоверяющего Центра в сертификатах открытого ключа, изготовленных Удостоверяющим Центром.
- применять копии сертификатов открытого ключа в электронной форме для проверки электронной подписи электронного документа в соответствии со сведениями, указанными в сертификате открытого ключа подписи;
- применять список аннулированных (отозванных) и приостановленных сертификатов открытых ключей, изготовленный Удостоверяющим Центром, для проверки статуса сертификатов открытых ключей подписи;
- обратиться в Удостоверяющий Центр для предоставления им закрытых и открытых ключей с записью их на ключевой носитель;
- обратиться в Удостоверяющий Центр за подтверждением подлинности электронных подписей уполномоченного лица Удостоверяющего центра в изготовленных им сертификатах открытых ключей;
- обратиться в Удостоверяющий Центр на предмет получения средства электронной подписи;

- обратиться в Удостоверяющий Центр для аннулирования (отзыва) сертификата открытого ключа в течение срока действия соответствующего закрытого ключа;

- обратиться в Удостоверяющий Центр для приостановления действия сертификата открытого ключа в течение срока действия соответствующего закрытого ключа;

- обратиться в Удостоверяющий Центр для возобновления действия сертификата открытого ключа в течение срока действия соответствующего закрытого ключа.

Обязанности пользователей УЦКУ:

- лица, проходящие процедуру регистрации в реестре Удостоверяющего Центра, обязаны представить регистрационную и идентифицирующую информацию в объеме, определенном положениями настоящего Регламента;

- хранить в тайне закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, модифицирования или несанкционированного использования;

- не использовать для электронной подписи закрытые ключи электронной подписи, если ему известно, что эти ключи используются или использовались ранее другими лицами;

- использовать закрытый ключ только для целей, разрешенных соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту;

- немедленно обратиться в Удостоверяющий центр с заявлением на приостановление действия сертификата ключа подписи в случае потери, раскрытия, искажения личного закрытого ключа, а также в случае если пользователю Удостоверяющего центра стало известно, что этот ключ используется или использовался ранее другими лицами;

- не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на аннулирование (отзыв) которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) сертификата в Удостоверяющий центр по момент времени официального уведомления об аннулировании (отзыве) сертификата, либо об отказе в аннулировании (отзыве);

- не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия;

- не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, который аннулирован (отозван) или действие его приостановлено;

- перед тем как использовать сертификат открытого ключа, изготовленный Удостоверяющим Центром, пользователь сертификата должен удостовериться, что назначение сертификата, определенное соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту, соответствует предполагаемому использованию.

3.3. ОТВЕТСТВЕННОСТЬ

- Удостоверяющий Центр корпоративного уровня не несет ответственности в случае нарушения Пользователем положений настоящего Регламента.
- Претензии к Удостоверяющему Центру ограничиваются указанием на несоответствие его действий настоящему Регламенту.

4. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

Закрытый ключ владельца сертификата открытого ключа является конфиденциальной информацией данного пользователя УЦКУ. Удостоверяющий Центр не депонирует и не архивирует закрытые ключи.

Персональная и корпоративная информация пользователей УЦКУ, содержащаяся в Удостоверяющем Центре, не подлежащая непосредственной рассылке в качестве части сертификата открытого ключа, списка отозванных сертификатов, считается конфиденциальной и не публикуется.

Информация, хранящаяся в журналах аудита Удостоверяющего Центра, считается конфиденциальной и не подлежит разглашению.

Отчетные материалы по выполненным проверкам деятельности Удостоверяющего Центра являются конфиденциальными, за исключением заключения по результатам проверок.

Информация, не являющаяся конфиденциальной, может публиковаться по решению Удостоверяющего Центра.

Место, способ и время публикации также определяется решением Удостоверяющего Центра.

Информация, включаемая в сертификаты открытых ключей пользователей УЦКУ и списки отозванных сертификатов, издаваемые Удостоверяющим Центром, не считаются конфиденциальными.

Также не считается конфиденциальной информация о настоящем Регламенте.

Удостоверяющий Центр не должен раскрывать конфиденциальную информацию каким бы то ни было третьим лицам за исключением случаев:

- определенных в настоящем Регламенте;
- требующих раскрытия в соответствии с действующим законодательством РФ или при наличии судебного постановления.

5. ПОРЯДОК РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ, ИЗГОТОВЛЕНИЯ И УПРАВЛЕНИЯ СЕРТИФИКАТАМИ КЛЮЧЕЙ ПОДПИСЕЙ

Процедура регистрации пользователей УЦКУ применяется в отношении физических лиц, представляющих юридическое лицо, присоединившееся к Регламенту, обращающихся к услугам Удостоверяющего Центра в части изготовления сертификатов открытых ключей пользователей УЦКУ и/или формирования закрытых и открытых ключей пользователей УЦКУ с записью их на ключевой носитель.

5.1. РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ УЦКУ, ЯВЛЯЮЩИХСЯ СОТРУДНИКАМИ ФОНДА И УЧАСТВУЮЩИХ В ЗАЩИЩЕННОМ ОБМЕНЕ ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

Регистрация пользователей УЦКУ, являющихся сотрудниками Фонда и участвующих в защищенном обмене электронными документами, осуществляется на основании утвержденного перечня должностей по заявкам руководителей подразделений.

5.2. РЕГИСТРАЦИЯ И ПОДКЛЮЧЕНИЕ ВНЕШНИХ ОРГАНИЗАЦИЙ К СИСТЕМЕ ЗАЩИЩЕННОГО ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ И ВЗАИМОДЕЙСТВИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Пользователь УЦКУ допускается к осуществлению защищенного обмена электронными документами и взаимодействия информационных систем после выполнения им совокупности следующих действий:

– Руководитель внешней организации направляет на имя директора Фонда письмо на подключение организации к системе защищенного обмена электронными документами и взаимодействия информационных систем (Приложение №1) с указанием необходимого количества рабочих мест и Заявки на подключение к системе (Приложение №2);

– На основании письма с положительной резолюцией директора Фонда и заявки, Фонд подготавливает и передает во внешнюю организацию Соглашение о присоединении к Регламенту (Приложение №3) - 3 экз.;

– Внешняя организация (после подписания Соглашения о присоединении к Регламенту) направляет в Фонд:

- Заявление на регистрацию Пользователя Удостоверяющего центра (Приложение №9);

- Заявление на изготовление сертификата ключа подписи Пользователя Удостоверяющего центра (Приложение №12);

– Подписанное руководителями Фонда, внешней организацией, ООО по защите информации «Секрет-Сервис» Соглашение о присоединении к Регламенту вместе с Заявлением на регистрацию Пользователя Удостоверяющего центра и Заявлением на изготовление сертификата ключа подписи передается Администратору сети ViPNet;

– Администратор сети ViPNet на основании подписанного Соглашения о присоединении к Регламенту, Заявления на регистрацию Пользователя Удостоверяющего центра и Заявления на изготовление сертификата ключа подписи, регистрирует абонентские пункты и пользователей внешней организации в АРМ [Администратор]. Задает необходимые связи с абонентскими пунктами, с которыми требуется установить взаимодействие, формирует ключевую информацию и генерирует ЭП для пользователей УЦКУ;

– После выполнения всех процедур, Администратор сети ViPNet передает Пользователю внешней организации или представителю Пользователя внешней организации:

- копии Сертификата открытой части ключа ЭП - 2 экз.;

- ключевую информацию (Ключ шифрования и открытую часть ключа ЭП) для установки ПО ViPNet[Клиент] на отчуждаемом машинном носителе;

При этом обязательно должно быть выполнено следующее:

– Две копии Сертификата открытой части ключа ЭП на бумажном носителе заверяются собственноручной подписью Уполномоченного лица УЦКУ и печатью ООО по защите информации «Секрет-Сервис», а также собственноручной подписью пользователя или его представителя.

– Пользователь внешней организации должен иметь Доверенность Пользователя Удостоверяющего центра (Приложение №10);

– Представитель внешней организации должен иметь доверенность:

- на право получения за Пользователя организации,

- на право подписи копии Сертификата открытой части ключа ЭП

- получения сформированного ключевого носителя (Приложение №11).

– Один экземпляр оформленных документов хранится во внешней организации, второй экземпляр хранится у Администратора сети ViPNet.

После получения всех необходимых ключевых носителей и сертификата Пользователь:

– Производит установка ПО ViPNet Клиент;

– Вводит полученный электронный сертификат на своем рабочем месте в действие;

– Приступает к выполнению задачи по защищенному обмену электронными документами и взаимодействию информационных систем с разрешенными абонентскими пунктами.

5.3.ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ ЗАРЕГИСТРИРОВАННОГО ПОЛЬЗОВАТЕЛЯ

Идентификация зарегистрированного пользователя УЦКУ осуществляется по идентификатору зарегистрированного пользователя, занесенному в реестр Удостоверяющего Центра.

Очная аутентификация зарегистрированного пользователя УЦКУ выполняется по паспорту или другому документу удостоверяющего личность, предъявляемого лично.

Аутентификация зарегистрированного пользователя УЦКУ по сертификату открытого ключа выполняется путем выполнения процедуры подтверждения электронной подписи с использованием сертификата открытого ключа.

5.4. ИЗГОТОВЛЕНИЕ КЛЮЧЕЙ

Изготовление ключей подписи осуществляется Удостоверяющим Центром по обращению уполномоченных представителей юридических лиц, оформляется в форме Заявления на изготовление ключей.

Заявление на изготовление ключей оформляется заявителем по образцу (Приложение №12).

Изготовление ключей выполняется Администратором сети ViPNet УЦКУ на специализированном рабочем месте, на основании принятого заявления.

Изготовленные ключи записываются на отчуждаемый машинный носитель, предоставляемый заявителем.

Предоставляемый заявителем ключевой носитель должен удовлетворять следующим требованиям:

– иметь тип устройства, входящий в перечень, определяемый Администратором сети ViPNet;

- быть проинициализированным (отформатированным);
- не содержать никакой информации, за исключением данных инициализации.

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

Ключевой носитель, содержащий изготовленные ключи, передается владельцу (заявителю). Факт выдачи ключей заносится в Журнал учета изготовления и выдачи ключей под роспись владельца (Приложение №18).

5.5.ИЗГОТОВЛЕНИЕ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА И ПРЕДОСТАВЛЕНИЕ ЕГО ВЛАДЕЛЬЦУ

5.5.1. Изготовление сертификата открытого ключа в процессе работы

Изготовление сертификата открытого ключа в процессе работы осуществляется Удостоверяющим Центром на основании заявления на изготовление сертификата открытого ключа зарегистрированного пользователя УЦКУ.

Заявление на изготовление сертификата открытого ключа в бумажной форме подается зарегистрированным пользователем УЦКУ Администратору сети ViPNet. Срок рассмотрения заявления на изготовление сертификата открытого ключа составляет 2-х рабочих дней, с момента его поступления Администратору сети ViPNet.

После изготовления сертификата открытого ключа его владельцу направляется официальное уведомление.

Изготовленный сертификат открытого ключа в электронной форме, заверенный электронной подписью уполномоченного лица Удостоверяющего Центра, предоставляется его владельцу при личном обращении к Администратору сети ViPNet. Также предоставляется копия сертификата открытого ключа на бумажном носителе

Заявление на изготовление сертификата открытого ключа в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя

Заявление включает в себя следующие обязательные реквизиты:

- Фамилию, имя, отчество заявителя;
- Дата и подпись заявителя;
- Текст запроса на сертификат.

Владелец сертификата открытого ключа идентифицируется по значениям атрибутов поля Subject сертификата открытого ключа (см. раздел [8.1.1.] настоящего Регламента).

5.5.2.Аннулирование (отзыв) сертификата открытого ключа

Аннулирование (отзыв) сертификата открытого ключа изготовленного Удостоверяющим Центром, осуществляется Удостоверяющим Центром по заявлению на отзыв сертификата открытого ключа его владельца (Приложение №13).

Заявление на отзыв сертификата открытого ключа в бумажной форме подается заявителем в УЦКУ лично.

Срок рассмотрения заявления на отзыв сертификата открытого ключа составляет один рабочий день с момента его поступления в УЦКУ.

После аннулирования (отзыва) сертификата открытого ключа его владельцу направляется официальное уведомление.

Заявление на отзыв сертификата открытого ключа в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление включает в себя следующие обязательные реквизиты:

- Идентификационные данные заявителя;
- Серийный номер отзываемого сертификата;
- Причину отзыва сертификата;
- Дата и подпись заявителя.

5.5.3.Приостановление действия сертификата открытого ключа

Приостановление действия сертификата открытого ключа изготовленного Удостоверяющим Центром, осуществляется Удостоверяющим Центром по заявлению на приостановление действия сертификата открытого ключа его владельца (Приложение №14).

Заявление на приостановление действия сертификата открытого ключа в бумажной форме подается заявителем в УЦКУ лично.

Срок рассмотрения заявления на приостановление действия сертификата открытого ключа составляет один рабочий день с момента его поступления в УЦКУ.

Официальным уведомлением о приостановлении действия сертификата ключа подписи является опубликование списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено.

После приостановления действия сертификата открытого ключа его владельцу направляется официальное уведомление.

Заявление на приостановление действия сертификата открытого ключа в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление включает в себя следующие обязательные реквизиты:

- Идентификационные данные заявителя;
- Серийный номер сертификата, действие которого приостанавливается;
- Срок, на который приостанавливается действие сертификата;
- Причина приостановки действия сертификата;
- Дата и подпись заявителя.

5.5.4.Возобновление действия сертификата открытого ключа.

Возобновление действия сертификата открытого ключа изготовленного Удостоверяющим Центром, осуществляется Удостоверяющим Центром по заявлению на возобновление действия сертификата открытого ключа его владельца (Приложение №15).

Заявление на возобновление действия сертификата открытого ключа в бумажной форме подается заявителем в УЦКУ лично.

Срок рассмотрения заявления на возобновление действия сертификата открытого ключа составляет 2 рабочих дня с момента его поступления в УЦКУ.

После возобновления действия сертификата открытого ключа его владельцу направляется официальное уведомление.

Заявление на возобновление действия сертификата открытого ключа в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление включает в себя следующие обязательные реквизиты:

- Идентификационные данные заявителя;
- Серийный номер сертификата, действие которого возобновляется;
- Причина возобновления действия сертификата;
- Дата и подпись заявителя.

5.5.5.Хранение сертификата открытого ключа пользователей

Хранение сертификата открытого ключа пользователей УЦКУ в Реестре сертификатов открытых ключей Удостоверяющим Центром, осуществляется в течение установленного срока действия сертификата открытого ключа.

Срок архивного хранения сертификата открытого ключа устанавливается в соответствии со сроком, определенным разделом [7.6] настоящего Регламента.

5.6. ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ МЕЖДУ СТОРОНАМИ С ИСПОЛЬЗОВАНИЕМ ПРОЦЕДУР МЕЖСЕТЕВОГО ОБМЕНА СЕТЕЙ VIPNET

Регистрация пользователей внешней организации в данном случае производится на АРМ [Администратор] Системы, который обслуживает внешнюю организацию, в соответствии с Регламентом этой организацией.

Между Фондом и внешней организацией заключается Соглашение о присоединении к Регламенту. Копия Соглашения о присоединении передается Администраторам сети ViPNet АРМов [Администратор], обслуживающих соответствующие сети. При необходимости, стороны обмениваются также соответствующими доверенностями пользователям на право подписания электронных документов от имени своей организации.

5.6.1. Порядок организации защищенного межсетевого информационного взаимодействия между сторонами

Защищенное информационное взаимодействие в рамках защищенного сегмента единого информационного пространства системы обязательного медицинского страхования организуется на базе технологии межсетевого взаимодействия ViPNet-сетей.

Защищенное информационное взаимодействие организуется с помощью Индивидуального Симметричного Межсетевого Мастер-ключа (ИСММК).

ИСММК формирует Администратор безопасности в АРМ [Администратор] для каждой из сетей, с которой должно осуществляться взаимодействие.

Администраторы сетей ViPNet Организаций выделяют сетевые узлы своих сетей, которые будут участвовать в межведомственном взаимодействии. Выделенные узлы сетей будут связаны в ЦУСах взаимодействующих сетей, а также будут иметь ключи для шифрования и подтверждения достоверности и подлинности передаваемых данных.

Администраторы безопасности выбирают Координаторы, которые будут выполнять функции серверов-шлюзов при межведомственном взаимодействии сетей.

5.6.2. Порядок организации межведомственного защищенного информационного взаимодействия между ViPNet - сетями организаций.

Порядок организации защищенного информационного взаимодействия между ViPNet-сетями Организаций предполагает выполнение следующих технологических и организационных мероприятий:

- В Центре управления сетью (ЦУС) и Удостоверяющем Ключевом центре (УКЦ), в соответствии с «Руководством администратора. ViPNet [Центр управления сетью]» и «Руководством администратора. ViPNet [Удостоверяющий и ключевой центр]», производится формирование необходимой адресной и ключевой информации – формирование начального экспорта (индивидуальные симметричные межсетевые мастер-ключи связи и шифрования, справочная информация), включая свои корневые сертификаты для каждой из сетей, с которой должно осуществляться взаимодействие.

- Указанные данные (начальный экспорт) доверенным способом передаются в соответствующие ЦУСы сторонних организаций, с которыми должно осуществляться защищенное взаимодействие.

- В ЦУСе и УКЦ других организаций в соответствии с «Руководством администратора. ViPNet [Центр управления сетью]» и «Руководством администратора. ViPNet [Удостоверяющий и ключевой центр]» производится ввод и обработка (импорт) полученных из других ЦУСов данных (начального экспорта), установление связей своих узлов с узлами ЦУСов, предоставившими информацию. Далее в ЦУСах и УКЦ создается ответная информация (ответный экспорт) для ЦУСов, приславших первичную информацию, включая свои корневые сертификаты.

- Ответная информация (ответный экспорт) доверенным способом передается в ЦУС Фонда, где она обрабатывается и вводится в действие. На этом этапе завершается процесс создания межведомственного защищенного взаимодействия между ЦУСами, и дальнейший обмен данными между ними производится в автоматическом режиме.

- После рассылки каждым ЦУСом сформированных обновлений ключевой и справочной информации на свои узлы, участвующие в межведомственном взаимодействии, между данными узлами сетей Фондов и организаций можно производить защищенный электронный документооборот.

- После завершения процедуры организации защищенного информационного взаимодействия между ViPNet-сетью Фонда и сетями организаций подписывается Протокол установления межсетевого взаимодействия (Приложение №19).

5.6.3.Порядок модификации защищенного информационного взаимодействия между ViPNet - сетями организаций при изменении состава узлов

Порядок модификации межведомственного защищенного информационного взаимодействия между ViPNet - сетями Организаций предполагает выполнение следующих технологических и организационных мероприятий:

- В процессе функционирования защищенного информационного взаимодействия между сетями ViPNet Организаций в одной или нескольких сетях может потребоваться модификация межведомственного защищенного информационного взаимодействия, т.е. изменение состава узлов, участвующих в

межведомственном защищенном взаимодействии, - добавление или удаление сетевого узла.

- При модификации защищенного информационного взаимодействия в какой-либо сети, администратор данной сети в своем ЦУСе производит соответствующие изменения в структуре связей своей сети, формирует экспортные данные и передает их в соответствующие ЦУСы в автоматическом режиме в соответствии с «Руководством администратора. ViPNet [Центр управления сетью]».

- В ЦУСах сетей, которых касается данная модификация, в соответствии с «Руководством администратора. ViPNet [Центр управления сетью]» производится обработка (импорт) полученных данных. Далее в ЦУСах создается ответная информация (ответный экспорт) для ЦУСов, приславших первичную информацию ЦУСов.

- Ответная информация передается в ЦУСы сетей, от которых поступила первичная информация, в автоматическом режиме по защищенному каналу связи, где она обрабатывается и вводится в действие. На этом завершается процесс модификации межведомственного защищенного взаимодействия между ЦУСами Организаций.

- После рассылки каждым ЦУСом сформированных обновлений ключевой и справочной информации на свои узлы, которых касается модификация, данные узлы продолжают или прекращают производить защищенный электронный документооборот при межведомственном взаимодействии.

5.6.4.Журнал изменений межведомственного защищенного информационного взаимодействия.

При каждой модификации межведомственного защищенного информационного взаимодействия Администраторы безопасности заносят соответствующие записи в Журнал изменений (Приложение №20).

5.6.5.Порядок организации защищенного информационного взаимодействия между ViPNet-сетями организаций в случае плановой смены межсетевого мастер-ключа

Порядок модификации межведомственного защищенного информационного взаимодействия между ViPNet - сетями Организаций в случае плановой смены межсетевого мастер-ключа предполагает выполнение следующих технологических и организационных мероприятий:

- Предварительные организационные мероприятия.

Перед тем, как осуществлять плановую смену межсетевого мастер-ключа, Администраторы ViPNet-сетей Организаций, для связи которых будет использоваться новый межсетевой мастер-ключ, должны договориться по следующим вопросам:

- Выбрать тип межсетевого мастер – ключа, который будет использоваться для связи между сетями.
- Если предполагается использовать симметричный мастер-ключ, то выбрать Администратора, который будет создавать новый межсетевой мастер – ключ.
- Выбрать время проведения смены межсетевого мастер-ключа и последующего обновления ключей шифрования для узлов своих сетей.

- Формирование нового межсетевого мастер-ключа

Формирование нового межсетевого мастер-ключа производится в соответствии с «Руководством администратора. ViPNet [Удостоверяющий и ключевой центр]».

- Процедура создания экспорта и приема импорта.

После смены межсетевого мастер-ключа производится процедура создания экспортных данных и приема импортных данных в соответствии с «Руководством администратора. ViPNet [Центр управления сетью]» и «Руководством администратора. ViPNet [Удостоверяющий и ключевой центр]».

- Межведомственное Взаимодействие после Смены Межсетевого Мастер-Ключа.

После смены межсетевого мастер-ключа связь между сетевыми узлами взаимодействующих сетей Организаций возможна только после прохождения обновлений ключевой информации на всех соответствующих сетевых узлах данных сетей.

Записи в журнале изменений межведомственного защищенного информационного взаимодействия:

После смены межсетевого мастер-ключа Администраторы сетей ViPNet и сторонних организаций заносят соответствующие записи в Журнал изменений (Приложение №20).

6. ПРОЦЕДУРА РАЗБОРА КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ В СВЯЗИ С ОСУЩЕСТВЛЕНИЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Возникновение конфликтных ситуаций может быть связано 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.

В случае возникновения конфликтной ситуации пользователь, предполагающий возникновение конфликтной ситуации, должен направить Администратору безопасности УЦКУ (непосредственно или через Доверенное лицо), выдавшему ему сертификат ключа подписи:

- Уведомление о конфликтной ситуации с изложением обстоятельств ее возникновения.
- ЭД, подлинность которого оспаривается. ЭД вместе с ЭП и сертификатом ключей подписи экспортируется из приложения, в котором он был получен или создан, в соответствии с Руководством пользователя данного приложения.
- Если в качестве приложения используется ПО ViPNet Клиент [Деловая почта], то ЭП и сертификат ключей подписи содержится в составе экспортируемого файла вместе с ЭД.

- Если используется приложение, файл с экспортированным ЭД которого не содержит в своем составе ЭП или сертификат ключей подписи, то данные элементы экспортируются и направляются Администратору безопасности в виде отдельных файлов.

Администратор сети ViPNet обязан незамедлительно 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.

Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от Администратора сети ViPNet.

В случае если уведомитель не удовлетворен полученной информацией, для разрешения конфликтной ситуации проводится техническая экспертиза.

В случае невозможности разрешения конфликтной ситуации в рабочем порядке и по итогам работы Экспертной комиссии, конфликтная ситуация рассматривается в судебном порядке, согласно действующему законодательству.

6.1.Порядок проведения технической экспертизы

Экспертная комиссия созывается УЦКУ на основании письменного заявления (претензии) Стороны пользователя, оспаривающего ЭД. В указанном заявлении, помимо реквизитов оспариваемого документа, должно быть указано лицо (лица), уполномоченные представлять интересы Стороны в составе экспертной комиссии. Количество указанных лиц не может превышать 3 человек.
Не позднее 10 рабочих дней с момента получения претензии назначается дата место и время начала работы комиссии, о чем письменно уведомляются обе Стороны.

Состав экспертной комиссии формируется в равных пропорциях из представителей Сторон. В состав комиссии, также включается эксперт – Администратор сети ViPNet.

Экспертиза оспариваемого электронного документа осуществляется на предоставленном Администратором сети ViPNet персональном компьютере с установленным ПО ViPNet Клиент (абонентском пункте), обеспечивающим проверку подписи электронного документа.

В случае если представители одной из Сторон по оспариваемому электронному документу не явились для участия в экспертной комиссии, экспертиза проводится без их участия, а об отсутствии представителей по оспариваемому электронному документу составляется акт, подписываемый всеми присутствующими участниками экспертной комиссии.

Экспертиза осуществляется в три этапа:

- Проверка оборудования и программного обеспечения и тестирование их работоспособности;

- Контроль целостности оспариваемого электронного документа путем проверки ЭП при помощи сертификата открытого ключа ЭП, представленного Стороной;

- Проверка принадлежности, актуальности и целостности сертификата, использованного комиссией для проверки ЭП.

Проверка работоспособности оборудования и программного обеспечения проводится путем проведения тестов пробной подписи и проверки подписи в присутствии членов экспертной комиссии.

Контроль целостности оспариваемого документа производится посредством стандартной процедуры импорта файлов ЭД с ЭП и сертификатом в ПО ViPNet Клиент и затем, проверки ЭП импортированного документа, в соответствие с руководством пользователя.

Проверка принадлежности, актуальности и целостности сертификата ключей подписи производится путем вызова в программе диалога просмотра сертификата, представленного вместе с ЭД. Просматриваемый сертификат распечатывается на бумажном носителе, и передается членам экспертной комиссии.

В случае если сертификат, используемый при проверке подписи, издавался на основании письменного запроса пользователя, то для доказательства принадлежности актуальности и целостности сертификата, использованного для проверки ЭП, Администратором сети ViPNet и соответствующей Стороной комиссии предъявляется сертификаты на бумажном носителе, оформленные при получении сертификата. Члены комиссии производят визуальную сверку данных сертификатов с распечатанным сертификатом, использованным при подписи оспариваемого документа.

В случае, если сертификат был издан на основании электронного запроса, подписанного ЭП с использованием ранее изданного официально оформленного сертификата, комиссии предъявляется логически связанная цепочка запросов на сертификаты и сертификаты, распечатанные на бумажных носителях, которые в совокупности подтверждают принадлежность сертификата лицу, сформировавшему ЭП. Распечатка этих запросов и сертификатов на бумажные носители производится Администратором безопасности в АРМ [Администратора]. Цепочка запросов признается действительной, а сертификат принадлежащим указанному владельцу, если выполнены следующие условия:

- Цепочка логически связана, т.е. каждый следующий запрос подписан с использованием сертификата, изданного на основании предыдущего запроса.

- Подпись под каждым запросом в цепочке действительна на момент издания сертификата по данному запросу.

- Сертификат, которым подписан каждый запрос, действителен на момент подписания запроса.

- Последним элементом в цепи является электронный сертификат (распечатывается), соответствующий (при визуальном сравнении) сертификату, используемому комиссией для проверки ЭП по оспариваемому электронному документу;

- Сертификат, которым заверен первый запрос в цепочке (распечатывается), и проверяется на соответствие (при визуальном сравнении) официально оформленному сертификату, предъявленному комиссии.

Подтверждением подлинности оспариваемого электронного документа, является единовременное выполнение следующих условий:

- Проверка ЭП оспариваемого электронного документа с сертификатом ключей подписи, предъявленного Стороной, дала положительный результат.

– Подтверждена принадлежность, актуальность и целостность сертификата ключей подписи пользователя Стороны, с помощью которого проводится проверка ЭП оспариваемого электронного документа.

– Если у заявителя отсутствуют сомнения в принадлежности сертификата, то проверка принадлежности, актуальности и целостности сертификата ключей подписи может не производиться.

При необходимости подтверждения факта доставки и сроков доставки ЭД производится экспертиза извещения о доставке, представленного отправителем ЭД, и подписанного ЭП получателя ЭД. Извещение содержит контрольные суммы принятого ЭД из состава ЭП этого ЭД, однозначно идентифицирующие ЭД, на который оно сформировано. Проверка подлинности извещения производится аналогично процедурам проверки ЭД, приведенным выше.

6.2.Оформление результатов технической экспертизы

Результаты экспертизы оформляются в виде письменного заключения – Акта экспертной комиссии, подписываемого всеми членами комиссии. Акт составляется немедленно после завершения экспертизы. В Акте фиксируются результаты всех этапов, проведенной экспертизы, а также все существенные реквизиты оспариваемого электронного документа. Акт составляется в трех экземплярах - по одному для каждой из Сторон и УЦКУ. Акт комиссии является окончательным и пересмотру не подлежит.

К акту прилагаются распечатки материалов, предоставленных на экспертизу (сертификаты, запросы на сертификат, извещения о доставке) и результаты проверки подписи представленных ЭД

7.ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1.ИДЕНТИФИЦИРУЮЩИЕ ДАННЫЕ УПОЛНОМОЧЕННОГО ЛИЦА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА КОРПОРАТИВНОГО УРОВНЯ

Уполномоченное лицо Удостоверяющего Центра корпоративного уровня, утвержденное директором Фонда, идентифицируется по следующим данным:
Фамилия, имя, отчество:
Организация:
Адрес электронной почты:
Субъект Федерации: Сибирский Федеральный округ
Сертификат ключа подписи Уполномоченного лица УЦКУ ТФОМС Иркутской области.

7.2.СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ УПОЛНОМОЧЕННОГО ЛИЦА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Срок действия закрытого ключа и открытого ключа, соответствующего закрытому ключу, уполномоченного лица Удостоверяющего Центра составляет 2 года.

Начало периода действия закрытого ключа уполномоченного лица Удостоверяющего Центра исчисляется с даты и времени начала действия соответствующего сертификата открытого ключа.

Максимальный срок, который может быть установлен в качестве срока действия сертификатов открытых ключей уполномоченного лица УЦКУ, составляет 5 лет.

7.3.ТРЕБОВАНИЯ К СРЕДСТВАМ ЭЛЕКТРОННОЙ ПОДПИСИ ПОЛЬЗОВАТЕЛЕЙ УЦКУ

Средство электронной подписи должно обеспечивать выполнение следующих процедур:

- Генерацию закрытых и открытых ключей;
- Формирование электронной подписи;
- Проверку электронной подписи.

Средство электронной подписи должно обеспечивать выполнение мер защиты закрытых ключей.

В качестве средства электронной подписи пользователи должны использовать сертифицированные в соответствии с правилами сертификации средства криптографической защиты информации по уровню защиты не ниже «КС2».

Идентификаторы алгоритмов представлены в настоящем Регламенте в разделе [8.1.3.].

7.4.СРОКИ ДЕЙСТВИЯ ЗАКРЫТЫХ КЛЮЧЕЙ И СЕРТИФИКАТОВ ОТКРЫТЫХ КЛЮЧЕЙ ВЛАДЕЛЬЦЕВ СЕРТИФИКАТОВ ОТКРЫТЫХ КЛЮЧЕЙ

Срок действия закрытого ключа пользователя УЦКУ, соответствующего сертификату открытого ключа, владельцем которого он является, составляет 12 месяцев.

Начало периода действия закрытого ключа пользователя УЦКУ исчисляется с даты и времени начала действия соответствующего сертификата открытого ключа пользователя УЦКУ.

Срок действия открытого ключа устанавливается равным сроку действия сертификата открытого ключа.

Максимальный срок, который может быть установлен в качестве срока действия сертификатов открытых ключей пользователей УЦКУ, составляет 1 год.

Срок действия сертификата открытого ключа устанавливается

Удостоверяющим Центром в момент его изготовления.

7.5.НАЗНАЧЕНИЕ КЛЮЧЕЙ И СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА, МЕРЫ ЗАЩИТЫ ЗАКРЫТЫХ КЛЮЧЕЙ

Ключи и сертификат открытого ключа предназначены для:

- обеспечения аутентификации и авторизации зарегистрированного пользователя УЦКУ при использовании программного обеспечения зарегистрированного пользователя УЦКУ;
- формирования электронной подписи в заявлении на рабочий сертификат открытого ключа в электронном виде;
- использования в соответствии со сведениями, указанными в сертификате в областях использования.

Закрытые ключи пользователей УЦКУ должны записываться при их генерации на отчуждаемые (относительно рабочего места) внешние носители ключевой информации.

Закрытые ключи на внешние носителе защищаются паролем (ПИН-кодом). Пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, учитывая следующие требования:

- Длин пароля (ПИН-кода) не должна быть меньше 8 символов;
- Пароль (ПИН-код) должен содержать символы цифр и букв латинского алфавита.

Если процедуру генерации ключей пользователя УЦКУ выполняет сотрудник Удостоверяющего Центра, то он должен сообщить сформированный пароль (ПИН-код) владельцу закрытых ключей.

Ответственность за сохранение пароля (ПИН-кода) в тайне возлагается на владельца закрытых ключей.

Не допускается использовать одно и тоже значение пароля (ПИН-кода) для защиты нескольких закрытых ключей.

Сотрудники Удостоверяющего Центра, являющиеся владельцами закрытых ключей, также выполняют указанные в разделе меры защиты закрытых ключей.

Копия сертификата открытого ключа пользователя УЦКУ в электронной форме представляет собой электронный документ, имеющий структуру, соответствующую стандарту Международного союза телекоммуникаций ITU-T X.509 версии 3 и рекомендаций IETF (Internet Engineering Task Force) RFC 2459 и представленный в кодировке Der или Base64.

Копия сертификата открытого ключа пользователя УЦКУ на бумажном носителе, представляет собой документ, содержащий следующие обязательные реквизиты:

- Серийный номер сертификата открытого ключа;
- Идентификационные данные владельца сертификата;
- Идентификационные данные издателя сертификата (идентификационные данные из сертификата открытого ключа уполномоченного лица Удостоверяющего Центра);
- Сведения о средстве ЭП уполномоченного лица Удостоверяющего Центра;
- Сведения об открытом ключе владельца сертификата и алгоритме его формирования;
- Сведения об областях использования закрытого ключа и сертификата;
- Собственноручную подпись уполномоченного лица Удостоверяющего Центра;
- Печать УЦКУ.

Копия сертификата открытого ключа печатается на листах белой бумаги формата А4, не содержащих средств защиты от копирования и подделки.

7.6. АРХИВНОЕ ХРАНЕНИЕ ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИИ

Архивированию подлежит следующая документированная информация:

- Реестр сертификатов открытых ключей пользователей УЦКУ;
- Сертификаты открытых ключей уполномоченного лица Удостоверяющего Центра;
- Журналы аудита программно-аппаратных средств обеспечения деятельности Удостоверяющего Центра;
- Реестр зарегистрированных пользователей Удостоверяющего Центра;

- Заявления на изготовление ключей пользователей УЦКУ;
- Заявления на изготовление сертификатов открытых ключей пользователей УЦКУ;
- Заявления на аннулирование (отзыв) сертификатов открытых ключей;
- Заявления на приостановление действия сертификатов открытых ключей;
- Заявления на возобновление действия сертификатов открытых ключей:
- Служебные документы Удостоверяющего Центра.

Источником комплектования архивного фонда Удостоверяющего Центра являются подразделения Удостоверяющего Центра, обеспечивающие документирование.

Архивные документы хранятся в специально оборудованном помещении - архивохранилище, обеспечивающим режим хранения архивных документов, устанавливаемый законодательством РФ.

Срок хранения архивных документов устанавливается 10 лет.

Выделение архивных документов к уничтожению и уничтожение осуществляется постоянно действующей комиссией, формируемой из числа сотрудников отдела системного администрирования и защиты информации и назначаемой приказом руководителя Удостоверяющего Центра.

7.7. УПРАВЛЕНИЕ КЛЮЧАМИ

7.7.1.Плановая смена ключей уполномоченного лица Удостоверяющего Центра

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) уполномоченного лица Удостоверяющего Центра выполняется в соответствии со сроком действия сертификата уполномоченного лица Удостоверяющего Центра.

Процедура плановой смены ключей уполномоченного лица Удостоверяющего Центра осуществляется в следующем порядке:

- Уполномоченное лицо Удостоверяющего Центра формирует новый закрытый и соответствующий ему открытый ключ;
- Уполномоченное лицо Удостоверяющего Центра изготавливает сертификат нового открытого ключа и подписывает его электронной подписью с использованием нового закрытого ключа.

7.7.2.Внеплановая смена ключей уполномоченного лица Удостоверяющего Центра

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации закрытого ключа уполномоченного лица Удостоверяющего Центра.

При компрометации ключей шифрования уполномоченного лица прекращается работа по их использованию.

Процедура внеплановой смены ключей уполномоченного лица Удостоверяющего Центра выполняется после получения уведомления о компрометации закрытого ключа ЭП в течение одного рабочего дня:

- аннулируется сертификат уполномоченного лица ключа подписи;
- объявляются ключи уполномоченного лица скомпрометированными;
- производится рассылка сформированных обновлений ключей на узлы своей сети.

После выполнения процедуры внеплановой смены ключей уполномоченного лица Удостоверяющего Центра, сертификат скомпрометированного открытого

ключа уполномоченного лица Удостоверяющего Центра аннулируется (отзывается) путем занесения в список отозванных сертификатов.

7.7.3.Плановая смена ключей Пользователя Удостоверяющего Центра

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) Пользователя Удостоверяющего Центра выполняется в соответствии со сроком действия сертификата Пользователя Удостоверяющего Центра.

Процедура плановой смены ключей Пользователя Удостоверяющего Центра осуществляется в следующем порядке:

- Уполномоченное лицо Удостоверяющего Центра формирует новый закрытый и соответствующий ему открытый ключ;
- Уполномоченное лицо Удостоверяющего Центра изготавливает сертификат нового открытого ключа и подписывает его электронной подписью с использованием нового закрытого ключа.

7.7.4.Внеплановая смена ключей Пользователя Удостоверяющего Центра

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации закрытого ключа Пользователя Удостоверяющего Центра.

В случае компрометации только ключей подписи пользователь обязан немедленно сообщить об этом Администратору сети ViPNet и не использовать эти ключи для подписи документов. При компрометации ключей шифрования пользователь обязан прекратить работу на своем абонентском пункте.

Ключи пользователя могут считаться скомпрометированными в следующих случаях:

- посторонним лицам мог стать доступным файл ключевого дистрибутива;
- посторонним лицам мог стать доступным съемный носитель с ключевой информацией;
- посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на компьютере;
- в локальной сети считается возможным присутствие посторонних лиц или на границе локальной сети отсутствует (отключен) сертифицированный межсетевой экран;
- уволился пользователь, имевший доступ к паролям и ключам.

Процедура внеплановой смены ключей Пользователя Удостоверяющего Центра выполняется Администратором сети ViPNet. Администратор сети ViPNet после получения уведомления о компрометации закрытого ключа ЭП в течение одного рабочего дня:

- аннулирует сертификат ключа подписи;
- объявляет ключи данного пользователя скомпрометированными;
- производит рассылку сформированных обновлений ключей на узлы своей сети, в том числе и пользователю при наличии у него запасных ключей, выданных ему при получении ключевого дистрибутива.

После выполнения процедуры внеплановой смены ключей Пользователя Удостоверяющего Центра, сертификат скомпрометированного открытого ключа Пользователя Удостоверяющего Центра аннулируется (отзывается) путем занесения в список отозванных сертификатов.

8. СТРУКТУРЫ СЕРТИФИКАТОВ И СПИСКОВ ОТОЗВАННЫХ СЕРТИФИКАТОВ

8.1. СТРУКТУРА СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА, ИЗГОТАВЛИВАЕМОГО УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ В ЭЛЕКТРОННОЙ ФОРМЕ

Удостоверяющий Центр издает сертификаты открытых ключей пользователей УЦКУ и уполномоченного лица Удостоверяющего Центра в электронной форме (далее по тексту раздела - сертификаты открытых ключей) формата X.509 версии 3.

8.1.1.Базовые поля сертификата открытого ключа

Сертификаты открытых ключей содержат следующие базовые поля X.509: Signature:	Электронная цифровая подпись уполномоченного лица Удостоверяющего Центра
Issuer:	Идентифицирующие данные уполномоченного лица Удостоверяющего Центра
Validity:	Даты начала и окончания срока действия сертификата
Subject:	Идентифицирующие данные владельца сертификата открытого ключа
SubjectPublicKeyInformation:	Идентификатор алгоритма средства электронной подписи, с которыми используется данный открытый ключ, значение открытого ключа
Version:	Версия сертификата формата X.509 - версия 3
SerialNumber:	Уникальный серийный (регистрационный) номер сертификата в Реестре сертификатов открытых ключей Удостоверяющего Центра

8.1.2.Дополнения сертификата

Сертификаты открытых ключей содержат следующие дополнения: authorityKeyIdentifier	Идентификатор ключа уполномоченного лица Удостоверяющего Центра
subjectKeyIdentifier	Идентификатор ключа владельца сертификата
ExtendedKeyUsage	Область (области) использования ключа, при которых электронный документ с электронной подписью будет иметь юридическое значение
cRLDistributionPoint	Точка распространения списка аннулированных (отозванных) сертификатов открытых ключей, изданных Удостоверяющим Центром (может включаться или нет в соответствии с настройками УЦКУ)

KeyUsage	Назначение ключа
FreshestCRL	Точка распространения обновлений к регулярному списку аннулированных (отозванных) сертификатов открытых ключей, изданных УЦ (в соответствии с RFC 5280 используется для прикладных систем, в которых оперативная реакция на изменения статуса сертификата является ключевым требованием)
Basic Constraints	Определяет принадлежность сертификата Удостоверяющему Центру и ограничение длины цепочки сертификатов для подчиненного УЦ.

8.1.3.Поддерживаемые объектные идентификаторы алгоритмов

Удостоверяющий Центр использует следующие объектные идентификаторы алгоритмов средства электронной подписи: ГОСТ Р 34.10-2012	1.2.643.2.2.20	Алгоритм открытых ключей
ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	1.2.643.2.2.19	Алгоритм открытых ключей
ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	1.2.643.2.2.4	Алгоритм подписи
ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	1.2.643.2.2.3	Алгоритм подписи
Диффи-Хеллмана	1.2.643.2.2.99	Алгоритм на базе экспоненциальной функции
Диффи-Хеллмана	1.2.643.2.2.98	Алгоритм на базе эллиптической кривой
ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012	1.2.643.2.2.9	Алгоритм хеширования
ГОСТ 28147-89	1.2.643.2.2.21	Алгоритм шифрования

8.1.4.Формы имени

В сертификате открытого ключа поля идентификационных данных уполномоченного лица Удостоверяющего Центра и владельца сертификата содержат атрибуты имени формата X.509.

8.1.5.Ограничения на имена

Обязательными атрибутами поля идентификационных данных уполномоченного лица	Фамилия, имя, отчество

Удостоверяющего Центра являются: Common Name	
Organization	Наименование организации, являющейся владельцем Удостоверяющего Центра
Organization Unit	Наименование подразделения, сотрудником которого является уполномоченное лицо Удостоверяющего Центра
Email	Адрес электронной почты
Country	RU
State	Субъект Федерации, где зарегистрирована организация, являющейся владельцем Удостоверяющего Центра
Email	Адрес электронной почты
Country	RU
State	Субъект Федерации, где зарегистрирована организация, которую представляет владелец сертификата

8.2.СТРУКТУРА СПИСКА ОТОЗВАННЫХ СЕРТИФИКАТОВ, ИЗГОТАВЛИВАЕМОГО УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ В ЭЛЕКТРОННОЙ ФОРМЕ

Удостоверяющий Центр издает списки отозванных сертификатов открытых ключей пользователей УЦКУ и уполномоченного лица Удостоверяющего Центра в электронной форме (далее по тексту раздела – СОС) формата X.509 версии 3.

Дополнения СОС

Удостоверяющий Центр использует следующие дополнения: Authority Key Identifier	идентификатор ключа уполномоченного лица Удостоверяющего Центра
Reason Code	Код причины отзыва сертификата открытого ключа

9. ПРОГРАММНЫЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Для реализации своих услуг и обеспечения жизнедеятельности Удостоверяющий Центр использует следующие программные и технические средства:

- Программный комплекс обеспечения реализации целевых функций Удостоверяющего Центра (далее по тексту – ПК УЦКУ);
- Технические средства обеспечения работы ПК УЦКУ (далее по тексту – ТС УЦКУ);
- Программные и программно-аппаратные средства защиты информации (далее по тексту – СЗИ УЦКУ).

9.1. ПРОГРАММНЫЙ КОМПЛЕКС ОБЕСПЕЧЕНИЯ РЕАЛИЗАЦИИ ЦЕЛЕВЫХ ФУНКЦИЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА КОРПОРАТИВНОГО УРОВНЯ

Программный комплекс обеспечения реализации целевых функций Удостоверяющего Центра корпоративного уровня включает в себя следующие программные компоненты:

- Администратор
- ViPNet [Администратор] [Центр управления сетью].
- ViPNet [Администратор] [Удостоверяющий и ключевой центр].
- ViPNet [Клиент] [Монитор]
- ViPNet [Клиент] [Деловая почта]

ViPNet [Администратор] является базовым компонентом ПК УЦКУ, включает в себя программы ViPNet [Администратор] [Центр управления сетью] и ViPNet [Удостоверяющий и Ключевой Центр].

Программа ViPNet [Администратор] [Центр управления сетью], далее ЦУС, предназначена для формирования и изменения структуры корпоративной сети. Обеспечивает реализацию следующих целевых функций Удостоверяющего Центра корпоративного уровня:

- регистрация сетевых узлов (СУ);
- распределение задач для СУ (Координатор, Клиент, Пункт регистрации);
- регистрация клиентов (абонентов) в сети на СУ;
- задание и изменение разрешенных связей для СУ;
- формирование и рассылка адресных справочников для СУ;
- формирование справочников для Удостоверяющего и ключевого центра (УКЦ);
- рассылка для СУ обновлений справочно-ключевой информации, формируемой УКЦ;
- рассылка для СУ списков отозванных сертификатов и списков сертификатов уполномоченных лиц удостоверяющих центров своей и смежных сетей;
- прием и передача в УКЦ запросов на сертификаты ключей подписи и обновление сертификатов от пользователей корпоративной сети и Центров регистрации, рассылка изданных сертификатов на СУ.

Программу ViPNet [Удостоверяющий и Ключевой Центр], далее УКЦ, по функциям можно условно разделить на две программы: Ключевой Центр и Удостоверяющий Центр.

Программа Ключевой Центр (КЦ) предназначена для формирования пользовательской ключевой информации. Эта программа формирует ключевую информацию на основе информации, поступающей из ЦУС. Созданные программой КЦ ключи передаются пользователям, после чего при наличии соответствующего ПО ViPNet пользователи сети смогут безопасно обмениваться конфиденциальной информацией.

КЦ обеспечивает реализацию следующих целевых функций Удостоверяющего Центра корпоративного уровня:

- формирование ключевых носителей для пользователей сети ViPNet;
- формирование ключевых наборов для сетевых узлов;
- формирование паролей;
- обновление ключевых носителей и ключевых наборов.

Программа Удостоверяющий центр (УЦ) предназначена для обслуживания следующих запросов: на издание сертификатов ЭП, на отзыв, приостановление и возобновления приостановленного действия сертификатов пользователей УЦКУ, сформированных на сетевых узлах сети ViPNet (пользователями корпоративной сети).

УЦ обеспечивает реализацию следующих целевых функций Удостоверяющего Центра корпоративного уровня:

- Создание ключей подписи и издание сертификатов уполномоченных лиц УЦ;
- Регистрация персональных данных внешнего пользователя.
- Ведения Реестра зарегистрированных внешних пользователей УЦКУ.
- Генерация секретного ключа подписи и сохранение его на персональном ключевом носителе внешнего пользователя.
- Отправка запроса в Центр сертификации (в УЦ через ЦУС), прием и ввод в действие изданных сертификатов.
- Ведение Реестра справочников запросов и изданных сертификатов.
- Формирование запросов на отзыв, приостановление или возобновление сертификатов.
- Формирование запросов к ГУЦ на издание сертификата уполномоченного лица УЦ;
- Импорт сертификатов уполномоченных лиц УЦ смежных сетей и ГУЦ;
- Ведение эталонной копии Реестра справочников сертификатов уполномоченных лиц УЦ, формирование и отправка в ЦУС обновлений справочников;
- Создание ключей подписи пользователей и издание сертификатов корпоративной сети по запросам ЦУС;
- Рассмотрение запросов на издание сертификатов ключей подписи от пользователей корпоративной сети;
- Рассмотрение запросов от Центров регистрации на издание сертификатов ключей подписи внешних пользователей;
- Хранение информации о запросах и ведение эталонной копии Реестра справочников изданных сертификатов;
- Рассмотрение запросов на отзыв, приостановление и возобновление сертификатов;
- Отправка в ЦУС для обновления списков отозванных сертификатов;
- Ведения эталонной копии списка аннулированных (отозванных) и приостановленных сертификатов открытых ключей пользователей УЦКУ.

УЦ обеспечивает возможность формирования и сертификации ключей подписи для алгоритмов ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012.

Ответственность за эксплуатацию VipNet [Администратор] возлагается на Уполномоченное лицо Удостоверяющего Центра.

9.2. ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ РАБОТЫ ПК УЦКУ

Технические средства обеспечения работы ПК УЦКУ включают в себя:

- Выделенный сервер с ПО ViPNet [Администратор] [УКЦ];
- Выделенный сервер с ПО ViPNet [Координатор];

- Программно-аппаратные комплексы защиты от несанкционированного доступа типа «электронный замок»;
- Телекоммуникационное оборудование;
- Компьютеры рабочих мест сотрудников УЦКУ;
- Устройства печати на бумажных носителях (принтеры).

9.3.ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Программные и программно-аппаратные средства защиты информации включают в себя:

- Средства криптографической защиты информации (СКЗИ "Домен-К");
- ViPNet [Координатор], предназначенный для обеспечения защищенного служебного информационного обмена между компонентами УЦКУ через открытые сети, реализующий все серверные функции в рамках сети ViPNet: сервер IP-адресов, межсетевой экран, сервер маршрутизатор и др.
- ViPNet [Клиент], обеспечивающий надежную защиту компьютеров от несанкционированного доступа к различным информационным и аппаратным ресурсам на нем при работе компьютера в локальных или глобальных сетях.
- Устройства обеспечения бесперебойного питания серверов ViPNet [Координатор];
- Устройства обеспечения температурно-влажностного режима и кондиционирования служебных и рабочих помещений Удостоверяющего Центра корпоративного уровня;
- Устройства обеспечения противопожарной безопасности помещений Удостоверяющего Центра корпоративного уровня.

9.4.ПЕРЕЧЕНЬ СОБЫТИЙ, РЕГИСТРИРУЕМЫХ ПРОГРАММНЫМ КОМПЛЕКСОМ ОБЕСПЕЧЕНИЯ РЕАЛИЗАЦИИ ЦЕЛЕВЫХ ФУНКЦИЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Вход администратора в программу УКЦ.
Регистрация администратора УКЦ.
Издание сертификата администратора УКЦ.
Издание СОС.
Принят запрос на сертификат открытого ключа.
Отклонен запрос на издание открытого ключа.
Издание сертификата открытого ключа.
Принят запрос на отзыв сертификата.
Удовлетворен запрос на отзыв сертификата.
Отклонен запрос на отзыв сертификата.
Невыполнение внутренней операции программной компоненты.
Системные события общесистемного программного обеспечения.

9.5.ПЕРЕЧЕНЬ ДАННЫХ ПРОГРАММНОГО КОМПЛЕКСА ОБЕСПЕЧЕНИЯ РЕАЛИЗАЦИИ ЦЕЛЕВЫХ ФУНКЦИЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА, ПОДЛЕЖАЩИХ РЕЗЕРВНОМУ КОПИРОВАНИЮ

При эксплуатации программного комплекса обеспечения реализации целевых функций Удостоверяющего Центра выполняется резервное копирование данных компонент ПК УЦКУ. Периодичность создания резервных копий определяется настройками программы УКЦ и может варьироваться в зависимости от числа выполненных операций.

Перечень данных ПК УЦКУ, подлежащих резервному копированию, включает в себя:

- Списки сертификатов открытых ключей уполномоченных лиц Удостоверяющего Ключевого Центра, и Удостоверяющих центров смежных сетей в электронном виде;
- Базу данных пользователей корпоративной сети (ЦУС);
- Базу данных изданных сертификатов, включая очередь входящих запросов и историю запросов на сертификаты;
- Журналы УКЦ.

10.ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

10.1.ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Размещение технических средств Удостоверяющего Центра

АРМ Администратора УЦ установлен на оборудовании УЦКУ и размещен в защищенном помещении Удостоверяющего Центра.

Сервер, сетевое и телекоммуникационное оборудование, принадлежащие Фонду, размещены в выделенном защищенном помещении (далее по тексту – Серверная).

Физический доступ в помещения

Для защищенного помещения УЦ и Серверной устанавливается статус помещения ограниченного доступа с ограничением физического доступа посетителей.

Санкционированный доступ в Серверную происходит в соответствии со Списком доступа в помещения ограниченного доступа. Порядок доступа в серверное помещение и Список доступа утверждается директором Фонда.

Защищенное помещение Удостоверяющего Центра и Серверная оборудованы системой контроля доступа, охранной сигнализацией и механическими замками.

Помещения ограниченного доступа оборудованы исполнительными устройствами системы контроля доступа механического типа и находится в опечатанном состоянии в нерабочее время.

Электроснабжение и кондиционирование воздуха

Технические средства Удостоверяющего Центра корпоративного уровня подключены к общегородской сети электроснабжения.

Электрические сети и электрооборудование, используемые в Удостоверяющем Центре, отвечают требованиям действующих «Правил устройства электроустановок», «Правил технической эксплуатации электроустановок потребителей», «Правил техники безопасности при эксплуатации электроустановок потребителей».

Сервер, сетевое и телекоммуникационное оборудование подключены к источникам бесперебойного питания, обеспечивающие их работу при кратковременном отключении электропитания в течение 15 минут и корректное завершение работы всех систем при более длительном отключении основного электроснабжения.

Серверное помещение оборудовано средствами вентиляции и кондиционирования воздуха, обеспечивающих соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

Служебные помещения Удостоверяющего Центра, используемые для архивного хранения документов на бумажных, магнитных и оптических носителях оборудованы средствами вентиляции и кондиционирования воздуха, обеспечивающих соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

Рабочие и прочие служебные помещения Удостоверяющего Центра оборудованы средствами вентиляции и кондиционирования воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством РФ.

Подверженность воздействию влаги

Защита серверов и телекоммуникационного оборудования от воздействия влаги обеспечивается их размещением в шкафу-стойке.

Предупреждение и защита от возгорания

Помещение Удостоверяющего Центра корпоративного уровня оборудовано системой пожарной сигнализации.

Пожарная безопасность помещений Удостоверяющего Центра обеспечивается в соответствии с нормами и требованиями СНиП, устанавливаемыми законодательством РФ.

Хранение документированной информации

Хранение документированной информации УКЦУ производится в соответствии с утвержденной инструкцией о делопроизводстве УЦКУ, на основе действующего законодательства РФ по делопроизводству и архивному делу.

Уничтожение документированной информации

Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется сотрудниками УЦКУ, обеспечивающих документирование.

10.2.ПРОГРАММНО-АППАРАТНЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Организация доступа к техническим средствам Удостоверяющего Центра

Доступ к техническим средствам Удостоверяющего Центра разрешен только лицам из Списка доступа с использованием контроля доступа.

Ключи для доступа в помещение сотрудникам выдает лицо ответственное за снятие и установку режима охраны.

Организация доступа к техническим средствам Удостоверяющего Центра, размещенных на рабочих местах сотрудников Удостоверяющего Центра, возлагается на сотрудников Удостоверяющего Центра, ответственных за эксплуатацию данных технических средств.

Организация доступа к программным средствам Удостоверяющего Центра

Рабочее место Удостоверяющего Центра, на котором эксплуатируется программные приложения ViPNet [Администратор] [ЦУС] и ViPNet [Администратор] [УКЦ] также оснащено программно-аппаратными комплексами защиты от НСД.

Доступ системных администраторов общесистемного программного обеспечения для выполнения регламентных работ с оборудованием осуществляется

в присутствии сотрудников Отдела защиты информации, отвечающих за эксплуатацию соответствующего прикладного программного обеспечения.

Контроль целостности программного обеспечения

Контролю целостности подлежат следующие программные компоненты из состава программного обеспечения, эксплуатируемого Удостоверяющим Центром:

- Программные модули средств электронной подписи и криптографической защиты информации;
- Программные модули Администратора;

Состав программных модулей, подлежащих контролю целостности, определяется внутренним документом Удостоверяющего Центра, утверждаемый руководителем Удостоверяющего Центра.

Система контроля целостности программных модулей, подлежащих контролю целостности, основывается на аппаратном контроле целостности и общесистемного программного обеспечения до загрузки операционной системы.

Контроль целостности программных модулей средств электронной подписи и криптографической защиты информации осуществляется средствами средств электронной подписи и криптографической защиты информации.

Периодичность выполнения мероприятий по контролю целостности – ежесуточно.

Ответственность за выполнение мероприятий по контролю целостности программных средств возложена на Отдел системного администрирования и защиты информации.

Контроль целостности технических средств

Контроль целостности технических средств Удостоверяющего Центра обеспечивается опечатыванием корпусов устройств, препятствующих их неконтролируемому вскрытию.

Опечатывание устройств выполняется перед вводом технических средств в эксплуатацию, и после выполнения регламентных работ.

Контроль целостности печатей осуществляется в начале каждой рабочей смены.

Ответственность за выполнение мероприятий по контролю целостности технических средств возложена на Отдел системного администрирования и защиты информации.

Защита внешних сетевых соединений

Защита конфиденциальной информации, передаваемой между программно-техническими средствами обеспечения деятельности Удостоверяющего Центра и программными средствами, предоставляемыми Удостоверяющим Центром пользователям УЦКУ, в процессе обмена документами в электронной форме, осуществляется путем шифрования информации с использованием шифровальных (криптографических) средств, сертифицированных в соответствии с действующим законодательством РФ.

В качестве шифровальных (криптографических) средств пользователей УЦКУ, используемых для защиты конфиденциальной информации, используется средство электронной подписи пользователя УЦКУ.

Требуемый уровень безопасности (класс КС2) обеспечивается использованием программного обеспечения технологии ViPNet, сертифицированного по указанному классу, а также по другим требованиям ФСТЭК России.

Перечень информации, подлежащей защите

Передаваемая из Удостоверяющего Центра информация:

- Бланк копии сертификата открытого ключа для вывода на бумажный носитель;
- Список сертификатов открытого ключа пользователя УЦКУ и их статус;
- Список запросов на сертификаты открытых ключей пользователя УЦКУ и их статус;
- Список запросов на аннулирование (отзыв), приостановление и возобновление действия сертификатов открытых ключей пользователя УЦКУ и их статус.

10.3.ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Предъявляемые требования к персоналу Удостоверяющего Центра

Уполномоченное лицо Удостоверяющего Центра имеет высшее профессиональное образование и (или) профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области не менее 5 лет.

Инженерно-технические работники УЦКУ имеют высшее профессиональное образование или прошедшие курсы повышение квалификации в области информационной безопасности с получением специализации, необходимой для работы с шифровальными (криптографическими) средствами.

Профессиональная переподготовка и повышение квалификации персонала

Профессиональная переподготовка персонала Удостоверяющего Центра не осуществляется.

Сотрудники Удостоверяющего Центра осуществляют повышение квалификации в областях знаний согласно занимаемым должностям.

Организация сменной работы

Деятельность Удостоверяющего Центра по работе с пользователями УЦКУ в части приема заявлений в бумажной форме и изготовления сертификатов открытых ключей организована в одну рабочую смену с 10.00 до 17.00 в будние дни.

Выходными днями являются: суббота, воскресение, а также дни общенациональных праздников.

Организация доступа персонала к документам и документации

Доступ сотрудников Удостоверяющего Центра к документам и документации, составляющей документальный фонд организации, организован в соответствии с должностными инструкциями и функциональными обязанностями.

Охрана здания и помещений

Охрану здания и помещений выполняют штатные сторожа-вахтеры, обеспечивающие:

- Обнаружение и задержание нарушителей, пытающихся проникнуть в здание (помещения) Удостоверяющего Центра;
- Сохранность материальных ценностей и документов;
- Предупреждение происшествий и ликвидацию их последствий.

10.4. ЮРИДИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Удостоверяющий Центр имеет разрешение (лицензии) по всем видам деятельности, связанных с предоставлением услуг (см.[2.1.] настоящего Регламента).

Системы безопасности Удостоверяющего Центра и защиты информации созданы и функционируют в рамках режима обеспечения информационной безопасности Территориального фонда обязательного медицинского страхования Иркутской области.

Все меры по защите информации в Удостоверяющем Центре введены в действие приказами директора Фонда.

Для обеспечения деятельности Удостоверяющий Центр использует средства электронной подписи и криптографической защиты информации, сертифицированные в соответствии с действующим законодательством РФ.

Исключительным имущественным обладателем информационных ресурсов Удостоверяющего Центра является Территориальный фонд обязательного медицинского страхования Иркутской области.

Пользователям УЦКУ предоставляются неисключительные имущественные права на копии сертификатов и списков отозванных сертификатов, изготавливаемые Удостоверяющим Центром в объеме прав согласно разделу [3.2] настоящего Регламента.

ПРИЛОЖЕНИЕ №1

ПИСЬМО НА ПОДКЛЮЧЕНИЕ К СИСТЕМЕ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ В ЗАЩИЩЕННОЙ СЕТИ ОМС ИРКУТСКОЙ ОБЛАСТИ

Образец письма

Директору
ТФОМС Иркутской области
_____
_____

О подключении организации к системе защищенного обмена электронными документами и взаимодействия информационных систем в защищенной сети ОМС Иркутской области

Прошу подключить (наименование организации) к системе защищенного обмена электронными документами и взаимодействия информационных систем в защищенной сети ОМС Иркутской области.

Необходимое число рабочих мест - ___ (указывается требуемое количество рабочих мест).

Руководитель организации Подпись
(ФИО)

ПРИЛОЖЕНИЕ №2
ЗАЯВКА НА ПОДКЛЮЧЕНИЕ К СИСТЕМЕ

Заявка на подключение к системе защищенного обмена электронными документами и взаимодействия информационных систем сети ViPNet №559 по телекоммуникационным каналам связи

Директору ТФОМС Иркутской области

_____

от -

_____

1. Полное наименование организации без сокращений (на основании учредительных документов)_____

_____

2. Код МО(СМО) в системе ОМС _____

3. Сокращенное наименование организации _____

4. Юридический адрес организации с индексом _____

5. Фактический (почтовый) адрес организации с индексом _____

6. ИНН _____

7. КПП организации/обособленного подразделения _____

8. Расчетный счет _____

9. БИК _____

10. Банк _____

11. ФИО руководителя _____

12. Должность руководителя _____

13. Действует на основании (указать документ: устав, положение, доверенность или другое) _____

14. Контактные телефоны _____

15. Контактный E-mail _____

Дата Подпись руководителя М.П.

ПРИЛОЖЕНИЕ №3.
СОГЛАШЕНИЕ О ПРИСОЕДИНЕНИИ К РЕГЛАМЕНТУ

Соглашение
о присоединении к Регламенту Удостоверяющего Центра корпоративного уровня развернутого в интересах Территориального фонда обязательного медицинского страхования Иркутской области для организации защищенного обмена электронными документами и взаимодействия информационных систем

г. Иркутск « »_____201__ г.

Территориальный фонд обязательного медицинского страхования Иркутской области, именуемое в дальнейшем «Фонд», в лице директора _____, действующего на основании Положения, с одной стороны, и _____, именуемый в дальнейшем «Пользователь», в лице _____, действующего на основании _____, вместе именуемые «Сторонами» на основании Федерального Закона «Об электронной подписи» от 06.04.2011 №63-ФЗ и положениями статьи 428 Гражданского кодекса РФ в целях организации использования средств защиты информации при осуществлении защищенного обмена электронными документами между Сторонами, заключили настоящее соглашение (далее - Соглашение) о нижеследующем,

1. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. В силу настоящего Соглашения Пользователь присоединяется к Регламенту Удостоверяющего центра корпоративного уровня развернутого в интересах Территориального фонда обязательного медицинского страхования Иркутской области (далее по тексту Регламент).

1.2. Стороны, присоединившиеся к Регламенту, осуществляют обмен документами в электронном виде и взаимодействие информационных систем с использованием сетевых продуктов, объединенных под торговой маркой ViPNet, обеспечивающих создание защищенной виртуальной сети с возможностью использования электронной подписи (далее ЭП) ViPNet CSP.

1.3. Соглашение регулирует отношения между Сторонами при организации защищенного обмена электронными документами и взаимодействия информационных систем в соответствии с Регламентом и использованием программного обеспечения «ViPNet».

1.4. Соглашение определяет права и обязанности Сторон, возникающие при осуществлении в системе защищенного обмена электронными документами (далее - ЗОЭД) с учетом обеспечения информационной безопасности.

1.5. Соглашение определяет условия и порядок обмена электронными документами (далее - ЭД) с использованием средств электронной подписи при осуществлении ЗОЭД между Сторонами.

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1. Фонд осуществляет все права, вытекающие из Регламента, включая следующие:

- в одностороннем порядке вносить изменения, дополнения в Регламент, а также прекращать их действие;

- производить обновление программных средств СЗОЭД. При этом, если обновление приводит к необходимости реконфигурации технических средств или общесистемного ПО для АРМ Стороны, Фонд обязан сообщить об этом другой Стороне не менее чем за 20 рабочих дней до даты начала работы в новых условиях;
- при возникновении в Системе защищенного обмена электронными документами ситуаций, признаваемых чрезвычайными в соответствии с Регламентом, принимать меры, направленные на преодоление чрезвычайных ситуаций, а также требовать от Пользователя Системы защищенного обмена электронными документами совершения действий или воздержания от совершения действий в связи с осуществлением мер, предпринимаемых в соответствии с Регламентом для преодоления чрезвычайных ситуаций.
- в одностороннем порядке расторгать Соглашение в случае неисполнения или ненадлежащего исполнения Пользователем Системы защищенного обмена электронными документами обязанностей, предусмотренных настоящим Соглашением и Регламентом, включая нарушение Пользователем установленного Регламентом порядка разрешения конфликтных ситуаций и споров;
- выборочно производить аудит аттестованных автоматизированных рабочих мест на предмет выполнения требований по защите персональных данных.
- осуществлять иные права, возникающие в соответствии с Регламентом.
2.2. Фонд обязуется исполнять Регламент, в том числе своевременно и в полном объеме выполнять следующие обязанности:
- своевременно извещать Пользователя об изменениях и дополнениях, вносимых в Регламент или прекращении их действия;
- организовывать работу с криптографическими ключами Пользователя в объеме и в соответствии с порядком, определяемым Регламентом и Приложениями к нему.
- соблюдать режим конфиденциальности информации (паролей, идентификаторов, криптографических ключей), которая становится доступной Удостоверяющему центру в связи с выполнением им своих функций в соответствии с Регламентом;
- выполнять иные обязанности перед Пользователем, возникающие в соответствии с Регламентом.
2.3. Стороны признают, что:
2.3.1. Применяемые в СЗОЭД сертифицированные средства криптографической защиты информации (далее СКЗИ) обеспечивают аутентификацию, конфиденциальность, целостность и подлинность ЭД и достаточны для осуществления Сторонами обмена ЭД с использованием общедоступных каналов связи при условии использования не скомпрометированных закрытых ключей.
2.3.2. ЭП ЭД, при выполнении условий Соглашения, признается равнозначной собственноручной подписи представителей Сторон, наделенных правом подписи.
2.3.3. Удостоверенные корректными ЭП ЭД, подтверждают Сторонам при ЗОЭД:
- аутентификацию участников информационных систем в процессе взаимодействия;
- контроль целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем;
- конфиденциальность информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем.
2.4. Стороны обязуются:
2.4.1. Принимать на себя в полном объеме все обязательства, связанные с ЭД, удостоверенные корректной ЭП.

2.4.2. При проведении обмена ЭД с использованием СЗОЭД руководствоваться законодательством Российской Федерации, Регламентом, настоящим Соглашением и документацией на программные средства СЗОЭД, включая средства криптографической защиты информации.
2.4.3. При компрометации закрытых ключей участников СЗОЭД руководствоваться разделом [7.7.] Регламента.
2.4.4. Обеспечивать целостность прикладного и системного программного обеспечения на автоматизированном рабочем месте Стороны и отсутствие в программной среде злонамеренного программного кода.
2.4.5. Оперативно обрабатывать оформленные должным образом ЭД участника системы ЗОЭД в соответствии с настоящим Соглашением.
2.4.6. Осуществить подключение АРМ Стороны к СЗОЭД при выполнении Стороной необходимых условий, изложенных в разделе [5.2.] Регламента, а также корректировать настройки в случае изменения параметров подключения в соответствии с настоящим Соглашением.
2.4.7. Использовать АРМ Стороны исключительно в целях, предусмотренных настоящим Соглашением.
2.4.8. Не вносить исправления, изменения или дополнения, а также не передавать третьим лицам средства ЭП, ПО и соответствующую техническую документацию.
2.4.9. Содержать в исправном состоянии компьютеры, участвующие в электронном взаимодействии, принимать организационные и технические меры для предотвращения несанкционированного доступа к данным компьютерам, установленному на них программному обеспечению и средствам защиты информации, а также в помещения, в которых они установлены, не допускать появления на взаимодействующих компьютерах вредоносного программного обеспечения. Выполнять требования по защите информации от несанкционированного доступа в соответствии с законодательством Российской Федерации, нормативными документам ФСБ России, ФСТЭК России, учитывая категорию информации (информация для служебного пользования, персональные данные)
2.4.10. Сторона, для которой создалась невозможность исполнения обязательств по настоящему Соглашению, должна о наступлении и прекращении обстоятельств, препятствующих исполнению обязательств, немедленно извещать другую сторону. Обмен электронными документами, передаваемыми по каналам связи, использующие программное обеспечение «ViPNet», на время действия этих обстоятельств приостанавливается.
2.5. Сторона имеет право:
2.5.1. Отказывать другой Стороне в приеме/передачи ЭД с указанием мотивированной причины отказа.
2.5.2. Приостанавливать обмен ЭД при:
- несоблюдении Стороной требований к приему/передаче ЭД и обеспечению информационной безопасности, предусмотренных законодательством Российской Федерации и условиями настоящего Соглашения;
- разрешении спорных ситуаций, а также для выполнения неотложных, аварийных и ремонтно-восстановительных работ на АРМ Стороны, с уведомлением другой Стороны о сроках проведения этих работ.

При возникновении споров, связанных с принятием или непринятием и (или) с исполнением или неисполнением электронного документа, стороны обязаны соблюдать порядок согласования разногласий, предусмотренный Регламентом.
2.5.3. Требовать от другой стороны приостановления обработки всех ЭД в случаях компрометации закрытых ключей ЭП.
2.5.4. В случае невозможности обмена ЭД в СЗОЭД Сторона принимает/передает документы на бумажных носителях или в виде файлов на машинном носителе по согласованию с другой Стороной.

3. ТЕХНИЧЕСКИЕ УСЛОВИЯ

3.1. Стороны за свой счет приобретают, устанавливают и обеспечивают работоспособность средств защиты информации, необходимых для электронного взаимодействия на основе программного обеспечения «VipNet».
3.2. Каждая из Сторон самостоятельно оплачивают средства связи и каналы связи, необходимые для работы в системе электронного документооборота.

4. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

4.1. Защищенный обмен электронными документами Сторон осуществляется по открытым каналам связи с использованием средств криптографической защиты информации и ЭП, в соответствии с Регламентом.

В исключительных случаях, при отсутствии каналов связи или их отказах, обмен не конфиденциальной информацией по настоящему Соглашению осуществляется на машинных носителях (далее «электронных носителях») в заархивированном виде с контрольной суммой CRC. К электронному носителю с информацией прилагается Акт приема-передачи информации и сопроводительное письмо, в котором указываются все прилагаемые документы. Обмен конфиденциальной информацией (персональными данными) осуществляется на предназначенных для этого учтенных машинных носителях информации, защищенных согласно требованиям законодательства Российской Федерации.
4.2. Обмен информацией в электронном виде между Сторонами осуществляется в соответствии с составом и форматами файлов обмена данными, заранее согласованными Сторонами.
4.3. Обмен электронными документами, их подпись и подтверждение целостности и подлинности документа осуществляется в соответствии с руководствами пользователей на технические средства и средства защиты, обеспечивающие такой обмен.
4.4. Отправленные и полученные электронные документы сохраняются и могут быть перенесены на машинные носители.
4.5 Стороны должны обеспечить защиту от несанкционированного доступа и непреднамеренного уничтожения и/или искажения учетных данных, содержащихся в электронных журналах регистрации электронных документов.
4.6. Осуществлять хранение подписанных электронных документов. Все электронные документы в подписанном виде должны храниться в течение сроков, предусмотренных законодательством Российской Федерации, нормативными документами сторон, а в случае возникновения споров - до их разрешения.
4.7. Обязанности по организации сохранности архивов электронных документов возлагаются на каждую из Сторон, в части их касающейся.
4.8. Электронные архивы подлежат защите от несанкционированного доступа и непреднамеренного уничтожения и/или искажения.

4.9. ЭД, подписанные некорректными ЭП, в обработку не принимаются.

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Соглашению Стороны несут ответственность в соответствии с законодательством Российской Федерации.

5.2. Каждая из Сторон несет ответственность за содержание всех ЭД принятых/переданных в СЗОЭД, подписанных владельцем Сертификата ключа подписи Стороны.

5.3. Стороны не несут ответственность за возможные временные задержки исполнения и/или искажения ЭД, возникающие по вине третьих лиц, предоставляющих услуги связи для использования в СЗОЭД.

5.4. Сторона не несет ответственность за убытки другой Стороны, возникшие вследствие несвоевременного другой Стороной сообщения о компрометации закрытых ключей ЭП ее представителей.

5.5. Сторона не несет ответственность за убытки, возникшие вследствие несвоевременного контроля другой Стороной электронных сообщений, подтверждающих получение и обработку ЭД, неисполнения другой Стороной ЭД, а также за несоблюдение мер обеспечения защиты от несанкционированного доступа к АРМ другой Стороны.

5.6. Сторона не несет ответственности за ущерб, возникший вследствие разглашения пользователем другой Стороной собственного конфиденциального ключа ЭП, его утраты или его передачи, вне зависимости от причин, неуполномоченным лицам.

5.7. Сторона не несет ответственности за последствия изменения электронного документа, защищенного корректной ЭП другой Стороны, в т.ч. в случае использования ключей ЭП и программно-аппаратных средств клиентской части другой Стороны неуполномоченным лицом.

5.8. Сторона не несет ответственности за неработоспособность оборудования и программных средств другой Стороны, повлекшую за собой невозможность доступа к защищенной сети «VipNet» и возникшие в результате задержки в осуществлении передачи информации, а также за возможное уничтожение (в полном или частичном объеме) информации, содержащейся на вычислительных средствах другой Стороны, подключенных к сети Интернет.

5.9. Сторона полностью несет всю ответственность за риски, связанные с подключением его вычислительных средств к сети Интернет. Сторона самостоятельно обеспечивает защиту собственных вычислительных средств и криптографических ключей от несанкционированного доступа и вирусных атак из сети Интернет.

6. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

6.1. При возникновении конфликтных ситуаций, возникающих в ходе обмена ЭД между Сторонами, Стороны должны стремиться разрешить их путем переговоров.

6.2. В случае, если конфликтная ситуация не урегулирована в результате переговоров Сторон, создается экспертная комиссия из представителей Сторон в соответствии с положениями изложенными в разделе [6.1.] Регламента.

6.3. Споры и разногласия, по которым Стороны не могут достигнуть соглашения, подлежат разрешению в Арбитражном суде в соответствии с законодательством Российской Федерации.

7. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

7.1. По взаимному согласию Сторон в текст Соглашения могут вноситься изменения и дополнения.
7.2. Все изменения и дополнения к настоящему Соглашению имеют юридическую силу и являются действительными, если они составлены в письменном виде и подписаны Сторонами.
7.3. Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

8. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ

8.1. Настоящее Соглашение заключено на неопределенный срок.
8.2. Настоящее Соглашение вступает в силу и становится обязательным для Сторон с момента его заключения.
8.3. Изменения и дополнения к настоящему Соглашению оформляются в письменной форме и действительны с момента подписания Сторонами.
8.4. Настоящее Соглашение может быть расторгнуто по инициативе любой из Сторон, о чем необходимо письменно уведомить другую Сторону не позднее, чем за один месяц до дня его расторжения.
8.5. Настоящее Соглашение составлено в двух экземплярах, имеющих равную юридическую силу:
первый - для Фонда;
второй - для _____.

9. РЕКВИЗИТЫ СТОРОН

Фонд	**Организация**
Территориальный фонд обязательного медицинского страхования Иркутской области	
Юридический адрес: 664022, г.Иркутск, ул. 3 Июля, 20	Юридический адрес:
Почтовый адрес: 664022, г.Иркутск, а/я 47	Почтовый адрес:
тел.: 34-19-20, 24-05-31	тел.:
факс: 34-16-58	факс:
e-mail: irotfoms@irkoms.ru	e-mail:
Банковские реквизиты:	Банковские реквизиты:
УФК по Иркутской области (ТФОМС Иркутской области, л/с 03345026280)	Расчетный счет
БИК 042520001	
ОТДЕЛЕНИЕ ИРКУТСК	БИК _____ КПП _____
Р/счет 40404810925200000001	ИНН _____
ИНН 3811028531	ОГРН
КПП 381102001	

10. ПОДПИСИ СТОРОН

Директор Фонда	Руководитель организации
_____	_____
МП	МП

ПРИЛОЖЕНИЕ №4.
ЗАЯВКА НА ИЗГОТОВЛЕНИЕ СЕРТИФИКАТОВ КЛЮЧЕЙ ПОДПИСЕЙ СОТРУДНИКОВ ФОНДА

ЗАЯВКА
на изготовление сертификатов ключей подписей сотрудников

_____
(Наименование подразделения)

Прошу сформировать ключи и изготовить сертификаты ключей подписей следующих сотрудников:

№ п/п	Фамилия Имя Отчество	Должность	Дополнительная идентификационная информация, заносимая в сертификат	Подпись сотрудника
1	2	3	4	5
1.				
2.				
3.				

Руководитель подразделения /_____/
(Фамилия И.О.)

ПРИЛОЖЕНИЕ №5
ЗАЯВКА НА ОТЗЫВ СЕРТИФИКАТОВ КЛЮЧЕЙ ПОДПИСЕЙ СОТРУДНИКОВ ФОНДА

ЗАЯВКА
на отзыв сертификатов ключей подписей сотрудников

_____
(Наименование подразделения)

Прошу отозвать следующие сертификаты ключей подписей сотрудников:

№ п/п	Серийный номер сертификата	Фамилия Имя Отчество	Должность	Причина отзыва сертификата	Подпись владельца сертификата
1	**2**	**3**	**4**	**5**	**6**
1.					
2.					
3.					

Руководитель подразделения /_____/
(Фамилия И.О.)

ПРИЛОЖЕНИЕ №6
ЗАЯВКА НА ПРИОСТАНОВЛЕНИЕ ДЕЙСТВИЯ СЕРТИФИКАТОВ КЛЮЧЕЙ ПОДПИСЕЙ СОТРУДНИКОВ ФОНДА

ЗАЯВКА
на приостановление действия сертификатов ключей подписей сотрудников

_____
(Наименование подразделения)

Прошу приостановить действие следующих сертификатов ключей подписей сотрудников:

№ п/п	Серийный номер сертификата	Фамилия Имя Отчество	Должность	Причина отзыва сертификата	Подпись владельца сертификата
1	2	3	4	5	6
1.					
2.					
3.					

Руководитель подразделения /_____/
(Фамилия И.О.)

ПРИЛОЖЕНИЕ №7
ЗАЯВКА НА ВОЗОБНОВЛЕНИЕ ДЕЙСТВИЯ СЕРТИФИКАТОВ КЛЮЧЕЙ ПОДПИСЕЙ СОТРУДНИКОВ ФОНДА

ЗАЯВКА
на возобновление действия сертификатов ключей подписей сотрудников

_____
(Наименование подразделения)

Прошу возобновить действие следующих сертификатов ключей подписей сотрудников:

№ п/п	Серийный номер сертификата	Фамилия Имя Отчество	Должность	Причина отзыва сертификата	Подпись владельца сертификата
1	2	3	4	5	6
1.					
2.					
3.					

Руководитель подразделения /_____/
(Фамилия И.О.)

ПРИЛОЖЕНИЕ №8
ЗАЯВКА НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ О СТАТУСЕ СЕРТИФИКАТА КЛЮЧА ПОДПИСИ СОТРУДНИКОВ, ИЗДАННОГО УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

ЗАЯВКА
на получение информации о статусе сертификата ключа подписи сотрудников, изданного Удостоверяющим центром

Прошу предоставить информацию о статусе следующего сертификата ключа подписи:

Serial Number (SN)	Серийный номер сертификата
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
Title (T)	Должность
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
OrganizationUnit (OU)	Наименование подразделения
Locality (L)	Город
Contry (C)	Страна

Время[1] (период времени) на момент наступления которого требуется установить статус сертификата: с «_____» по «_____».

Пользователь Удостоверяющего центра
/_____/
(Фамилия И.О.)

Руководитель подразделения /_____/
(Фамилия И.О.)

[1] Время и дата должны быть указаны по московскому времени. Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Оператором Удостоверяющего центра

ПРИЛОЖЕНИЕ №9
ЗАЯВЛЕНИЕ НА РЕГИСТРАЦИЮ ПОЛЬЗОВАТЕЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Заявление
на регистрацию Пользователя Удостоверяющего центра

_____
(Наименование Организации)

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)
действующего на основании _____
Просит зарегистрировать уполномоченного представителя

_____
(фамилия, имя, отчество)
в Реестре Удостоверяющего центра и наделить полномочиями Пользователя Удостоверяющего центра, установленными Соглашением от «___» _____ 20__ г. № _____ «О присоединении к Регламенту Удостоверяющего Центра корпоративного уровня развернутого в интересах Территориального фонда обязательного медицинского страхования Иркутской области».
Настоящим _____
(фамилия, имя, отчество)
соглашается с обработкой своих персональных данных Удостоверяющим центром и признает, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Пользователь Удостоверяющего центра _____
/_____/

«____» _____ 20____ г.

Должность и Ф.И.О. руководителя Организации
Подпись руководителя Организации, дата подписания заявления
МП

ПРИЛОЖЕНИЕ №10
ДОВЕРЕННОСТЬ ПОЛЬЗОВАТЕЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Доверенность
Пользователя Удостоверяющего центра

г. _____ «_____» _____20___ г.

_____
(Наименование Организации)
в лице _____,
(должность руководителя)
_____,
(фамилия, имя, отчество руководителя)
действующего на основании _____
уполномочивает _____
(фамилия, имя, отчество)
_____
(серия и номер паспорта, кем и когда выдан)

выступать в роли Пользователя Удостоверяющего центра и осуществлять действия в рамках Соглашения от «___» _____ 20__ г. № _____ «О присоединении к Регламенту Удостоверяющего Центра корпоративного уровня развернутого в интересах Территориального фонда обязательного медицинского страхования Иркутской области».

Представитель наделяется правом расписываться в соответствующих документах Удостоверяющего центра для исполнения поручений, определенных настоящей Доверенностью.

Настоящая доверенность действительна по «____» _____ 20____ г.

Подпись уполномоченного представителя _____ _____
(Фамилия И.О.) (Подпись)
подтверждаю.

Должность и Ф.И.О. руководителя Организации
Подпись руководителя Организации, дата подписания заявления
МП

ПРИЛОЖЕНИЕ №11
ДОВЕРЕННОСТЬ ПОЛЬЗОВАТЕЛЯ НА ПРЕДОСТАВЛЕНИЕ ЗАЯВИТЕЛЬНЫХ ДОКУМЕНТОВ И ПОЛУЧЕНИЯ КЛЮЧЕЙ ПОДПИСЕЙ И СЕРТИФИКАТА

Доверенность
на предоставление заявительных
документов и получения ключей подписей и сертификата
Пользователя Удостоверяющего центра

г. _____ «___» _____20___ г.

_____
(Наименование организации)
в лице _____,
(должность руководителя)
_____,
(фамилия, имя, отчество руководителя)
действующего на основании _____
уполномочивает _____
(фамилия, имя, отчество)
_____
(серия и номер паспорта, кем и когда выдан)

1. Предоставить в Удостоверяющий центр необходимые документы, определенные Соглашением от «___» _____ 20__ г. № _____ «О присоединении к Регламенту Удостоверяющего Центра корпоративного уровня развернутого в интересах Территориального фонда обязательного медицинского страхования Иркутской области» для регистрации, генерации ключей и изготовления сертификата ключа подписи своего полномочного представителя - Пользователя Удостоверяющего центра _____
(Ф.И.О. Пользователя Удостоверяющего центра)

2. Получить сертификат ключа подписи Уполномоченного лица Удостоверяющего центра и иные документы, определенные Соглашением от «___» _____ 20__ г. № _____ «О присоединении к Регламенту Удостоверяющего Центра корпоративного уровня Территориального фонда обязательного медицинского страхования Иркутской области».

3. Получить сформированный ключевой носитель, содержащий закрытый ключ подписи и сертификат Пользователя Удостоверяющего центра _____.
(Ф.И.О. Пользователя Удостоверяющего центра)

Представитель наделяется правом расписываться в копии сертификата ключа подписи на бумажном носителе и в соответствующих документах

Удостоверяющего центра для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по «____» _____ 20____ г.

Подпись _____ подтверждаю.
(Фамилия И.О. уполномоченного лица)

Пользователь Удостоверяющего центра _____ /_____/
«____» _____ 20____ г.

Должность и Ф.И.О. руководителя Организации
Подпись руководителя Организации, дата подписания заявления
МП

ПРИЛОЖЕНИЕ №12
ЗАЯВЛЕНИЕ НА ИЗГОТОВЛЕНИЕ СЕРТИФИКАТА КЛЮЧА ПОДПИСИ ПОЛЬЗОВАТЕЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Заявление
на изготовление сертификата ключа подписи
Пользователя Удостоверяющего центра
при генерации ключей подписей в Удостоверяющем центре

_____
(Наименование организации)
в лице
_____,
(должность руководителя)
_____,
(фамилия, имя, отчество руководителя)
действующего на основании _____

Просит сформировать ключи подписи, записать сформированный закрытый ключ подписи на предоставленный ключевой носитель и изготовить сертификат ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра

_____
(фамилия, имя, отчество)
в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

CommonName (CN)	Фамилия, Имя, Отчество или псевдоним
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
Organization Unit (OU)	Наименование подразделения
Locality (L)	Город
State (S)	Субъект Федерации
Contry (C)	RU
Extended Key Usage	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)

Пользователь Удостоверяющего центра _____ /_____/
«____» _____ 20____ г.

Должность и Ф.И.О. руководителя Организации
Подпись руководителя Организации, дата подписания заявления
МП

ПРИЛОЖЕНИЕ №13
ЗАЯВЛЕНИЕ НА АННУЛИРОВАНИЕ (ОТЗЫВ) СЕРТИФИКАТА КЛЮЧА ПОДПИСИ ПОЛЬЗОВАТЕЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Заявление
на аннулирование (отзыв) сертификата ключа подписи
Пользователя Удостоверяющего центра

_____
(Наименование организации)
в лице
_____,
(должность руководителя)
_____,
(фамилия, имя, отчество руководителя)
действующего на основании _____

Просит аннулировать (отозвать) сертификат ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра:

_____
(фамилия, имя, отчество)
содержащий следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
CommonName (CN)	Фамилия, Имя, Отчество или псевдоним
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
Organization Unit (OU)	Наименование подразделения
Locality (L)	Город
State (S)	Область
Contry (C)	Страна

Пользователь Удостоверяющего центра _____ /_____/
«____» _____ 20____ г.

Должность и Ф.И.О. руководителя Организации
Подпись руководителя Организации, дата подписания заявления
МП

ПРИЛОЖЕНИЕ №14
ЗАЯВЛЕНИЕ НА ПРИОСТАНОВЛЕНИЕ ДЕЙСТВИЯ СЕРТИФИКАТА КЛЮЧА ПОДПИСИ ПОЛЬЗОВАТЕЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Заявление
на приостановление действия сертификата ключа подписи
Пользователя Удостоверяющего центра

_____
(Наименование Организации)
в лице
_____,
(должность руководителя)
_____,
(фамилия, имя, отчество руководителя)
действующего на основании _____

Просит приостановить действие сертификата ключа подписи своего полномочного представителя - Пользователя Удостоверяющего центра:
_____,
(фамилия, имя, отчество)
содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
CommonName (CN)	Фамилия, Имя, Отчество или псевдоним
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
Organization Unit (OU)	Наименование подразделения
Locality (L)	Город
State (S)	Область
Contry (C)	Страна

Срок приостановления действия сертификата _____ дней.
(количество дней прописью)

Пользователь Удостоверяющего центра _____ /_____/
«____» _____ 20____ г.

Должность и Ф.И.О. руководителя Организации
Подпись руководителя Организации, дата подписания заявления
МП

ПРИЛОЖЕНИЕ №15
ЗАЯВЛЕНИЕ НА ВОЗОБНОВЛЕНИЕ ДЕЙСТВИЯ СЕРТИФИКАТА КЛЮЧА ПОДПИСИ ПОЛЬЗОВАТЕЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Заявление
на возобновление действия сертификата ключа подписи
Пользователя Удостоверяющего центра

_____
(Наименование Организации)
в лице
_____,
(должность руководителя)
_____,
(фамилия, имя, отчество руководителя)
действующего на основании _____

Просит возобновить действие сертификата ключа подписи своего полномочного представителя – Пользователя Удостоверяющего центра:

_____
(фамилия, имя, отчество)
содержащий следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
CommonName (CN)	Фамилия, Имя, Отчество или псевдоним
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
Organization Unit (OU)	Наименование подразделения
Locality (L)	Город
State (S)	Область
Contry (C)	Страна

Пользователь Удостоверяющего центра _____ /_____/
«____» _____ 20____ г.

Должность и Ф.И.О. руководителя Организации
Подпись руководителя Организации, дата подписания заявления
МП

ПРИЛОЖЕНИЕ №16
ЗАЯВЛЕНИЕ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ О СТАТУСЕ СЕРТИФИКАТА КЛЮЧА ПОДПИСИ, ИЗДАННОГО УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

Заявление
на получение информации о статусе сертификата ключа подписи,
изданного Удостоверяющим центром

Пользователь Удостоверяющего центра

_____

(Наименование Организации)

Просит предоставить информацию о статусе следующего сертификата ключа подписи:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
CommonName (CN)	Фамилия, Имя, Отчество или псевдоним
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
OrganizationUnit (OU)	Наименование подразделения
Title (T)	Должность
Locality (L)	Город
State (S)	Область
Contry (C)	Страна

Время[2] (период времени) на момент наступления которого требуется установить статус сертификата: «_____» по «_____».

Пользователь Удостоверяющего центра _____ /_____/
«____» _____ 20____ г.

Должность и Ф.И.О. руководителя Организации
Подпись руководителя Организации, дата подписания заявления
МП

[2] Время и дата должны быть указаны с учетом местного времени. Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром.

ПРИЛОЖЕНИЕ №17 СЕРТИФИКАТ КЛЮЧА ПОДПИСИ

ViPNet
Virtual Private Network

Удостоверяющий центр

Сертификат ключа подписи

Кому выдан: Администратор
Кем выдан: Администратор
Действителен с 6 апреля 2010 г. по 6 апреля 2015 г.

Версия:	V3
Серийный номер:	01 CA D5 2B 1C FF B2 F0 00 00 00 1D 02 2F 00 1E
Алгоритм подписи:	ГОСТ Р 34.10/34.11-2001
Издатель:	Имя: Администратор Должность: Администратор Подразделение: Удостоверяющий и Ключевой центр Организация: Секрет - Сервис Электронная почта: secret-servis@rambler.ru Область: Иркутская Город: Иркутск Страна: RU
Действителен с:	6 апреля 2010 г. 9:47:30 (GMT+08:00)
Действителен по:	6 апреля 2015 г. 9:47:30 (GMT+08:00)
Владелец:	Имя: Администратор Организация: Секрет Сервис
Открытый ключ:	ГОСТ Р 34.10-2001 (512 бит) 0440 D496 222E 2CAA 9FCD C741 717D CD14 E343 782B 4231 79C2 8D13 F1F1 4C55 159C 8746 E43A 9DE4 D844 A4AB D24A BA08 981E 7B1C 795C E297 3D18 46DB 85BE 02F6 63F0 0DE1

Расширения сертификата X.509

Использование ключа:	Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (F8)
Расширенное использование ключа:	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2), Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
Идентификатор ключа субъекта:	45 21 1C FC 84 7F 3D 1B 8D B8 B8 60 B0 4F 63 B9 FE 98 37 6D
Срок действия секретного ключа:	С 6 апреля 2010 г. 9:47:30 (GMT+08:00) по 6 апреля 2011 г. 9:47:30 (GMT+08:00)
Идентификатор ключа центра сертификатов:	Идентификатор ключа=40 91 34 1A 17 4B FE 20 14 E1 C8 EA B9 A5 54 AE 63 60 C5 AB
Основные ограничения:	Тип субъекта=Пользователь

Результат проверки сертификата: Сертификат действителен. Проверен 9 октября 2012 г. 15:52:01 (GMT+08:00).

Допускается использование в приложениях, оснащенных
СКЗИ "Домен-К", ОАО "Инфотекс", г. Москва

Владелец ***Подпись*** ***«____» _____ 200__ г.***	***Уполномоченное лицо Удостоверяющего центра*** ***Подпись*** **МП.** ***«____» _____ 200__ г.***

ПРИЛОЖЕНИЕ №18

ЖУРНАЛ УЧЕТА ИЗГОТОВЛЕНИЯ И ВЫДАЧИ КЛЮЧЕЙ ПОД РОСИПСЬ

1	2	3	4	5	6	7	8	9	10	11
п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационой и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении	Отметка о рассылке (передаче)	Отметка о возврате	Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ,ключевых документов	Примечание

12	13	14	15	16	17	18	19	20
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	дата и номер сопроводительного письма	дата и номер подтверждения	Дата уничтожения	Номер акта или расписка об уничтожении

ПРИЛОЖЕНИЕ №19
ПРОТОКОЛ УСТАНОВЛЕНИЯ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

ПРОТОКОЛ
установления межсетевого взаимодействия

«__» _____ 20___г. г. _____

1. Межсетевое взаимодействие устанавливается между сетями:

Номер сети	Наименование организации
№ ____	_____
№ ____	_____

2. Целью установления межсетевого взаимодействия является межведомственное защищенное информационное взаимодействие ViPNet-сетей _____ и _____.
3. Процедуру установления межсетевого взаимодействия осуществляли:

Номер сети	Должность	ФИО
№ ___	_____	_____
№ ___	_____	_____

4. Передача начального и ответного экспорта между сетями № ___ и № ___ осуществлялась через специалиста _____.
5. Для установления межсетевого взаимодействия использовался индивидуальный симметричный межсетевой мастер-ключ, созданный в сети №___.
6. Для установления межсетевого взаимодействия были назначены серверы-маршрутизаторы для организации шлюза:
в сети № ___– «_____»,
в сети № ____ – «_____».
7. При установлении межсетевого взаимодействия в части электронной подписи, были произведены импорты справочников ЭЦП главных абонентов сети № ____ и сети № ___.
8. Смена межсетевых ключей, изменение состава АП, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствами взаимного экспорта/импорта, о чем администраторы защищенных сетей уведомляют друг друга с помощью ПО ViPNet [Клиент] [Деловая почта] с указанием производимых изменений.
9. Стороны обязуются без предварительного согласования не производить изменений в настройках и структуре защищенных сетей, которые могут привести к нарушению межсетевого взаимодействия.

Руководитель (должность)
ФИО _____

Специалист (должность)
ФИО _____
«____»_____20___ г.

Руководитель (должность)
ФИО _____

Специалист (должность)
ФИО _____
«____»_____20___ г.

ПРИЛОЖЕНИЕ №20
ЖУРНАЛ ИЗМЕНЕНИЙ

Журнал изменений
ТФОМС Иркутской области (либо название сторонней организации)
по организации защищенного информационного взаимодействия
с _название сторонней организации_ (либо ТФОМС)

№ п/п	Наименование произведенного изменения в межсетевом взаимодействии с ФОМС (ТФОМС) (либо _название сторонней организации_)	Дата изменения	Подпись специалиста, проводившего изменения
1			
2			
3			

Пояснение по ведению журнала изменений:
1. В журнал заносятся все события, которые относятся к организации защищенного информационного взаимодействия с название сторонней организации (либо ТФОМС)
- установление межсетевого взаимодействия,
- выбор Координатора, выполняющего функции сервера-шлюза,
- формирование межсетевого мастер-ключа,
- плановая смена межсетевого мастер-ключа,
- смена ключей при компрометации,
- модификация межсетевого взаимодействии (добавление или удаление сетевого узла и т.д.

2. Каждая запись журнала должна заверяться специалистом, производившим изменение.

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум.	№ Документа	Входящий № сопроводительного документа и дата	Подп.	Дата
Изм.	измененных	Замененных	новых	Аннулированных					