СОГЛАСОВАН

Директор
ООО по защите информации
«Секрет-Сервис»

_____ Б.Б. Измайлов
(подпись)
«26» декабря 2023г.

УТВЕРЖДЕН

Директор ТФОМС
Иркутской области

_____ Е.В. Градобоев
(подпись)
«28» декабря 2023г.

Регламент
Центра администрирования сети VipNet №559
Территориального фонда обязательного медицинского страхования
Иркутской области

Иркутск 2023

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Перечень сокращений

ЦАС	Центр администрирования сети
РФ	Российская Федерация
ЭП	Электронная подпись
ЭД	Электронный документ
СКЗИ	Средство криптографической защиты информации
ЦУС	Центр управления сетью
СУ	Сетевой узел
ПСЭ	Персональный сетевой экран
ViPNet	Торговая марка программного обеспечения компании ОАО «Инфотекс» г.Москва
Фонд	Территориальный фонд обязательного медицинского страхования Иркутской области
СЗОЭД	Система защищенного обмена электронными документами в системе
ОМС	обязательного медицинского страхования
ПКИ	Парольно-ключевая информация

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

АРМ [Администратора] - автоматизированное рабочее место Администратора сети ViPNet, реализующее, в том числе, все необходимые по управлению сетью ViPNet, связанные с изданием, отзывом, хранением ключей , а также иные функции в соответствии с законодательством РФ регламентирующее безопасность информации.

Администратор сети ViPNet - лицо, назначенное руководителем организации, эксплуатирующей АРМ [Администратора], и предоставляющей услуги администрирования сети ViPNet Фонда. Администратор обеспечивает эксплуатацию АРМ [Администратора] и является уполномоченным лицом.

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

Ключ (криптографический ключ) - это уникальный набор символов (байт), сформированный средством электронной подписи.

Ключевой носитель - носитель, содержащий один или несколько ключей.

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

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.

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

Пользователь защищенной сети ViPNet (Пользователь) – физическое лицо (уполномоченный представитель Стороны, присоединившейся к Регламенту), зарегистрированное в Удостоверяющем центре

Сторона пользователя - юридическое лицо, представителем которого является пользователь.

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.

Уполномоченное лицо ЦАС ViPNet (Уполномоченное лицо) – физическое лицо, являющееся сотрудником организации – лицензиата ФСБ России и ФСТЭК России в качестве участника ЦАС ViPNet и наделенное полномочиями по изготовлению ключей, распространению ключей, эксплуатации СКЗИ.

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

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

Электронная подпись (ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. ОБЗОРНАЯ ИНФОРМАЦИЯ

Регламент Центр администрирования сети ViPNet Территориального фонда обязательного медицинского страхования Иркутской области, именуемый в дальнейшем «Регламент», разработан в соответствии с законодательством РФ.

Центр администрирования сети ViPNet Территориального фонда обязательного медицинского страхования Иркутской области развернут на базе ТФОМС Иркутской области.

Целью настоящего Регламента является создание условий для организации защищенного обмена электронными документами и правовых условий использования СКЗИ согласно статьи 19 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 06.02.2023) «О персональных данных» и Приказа ФСБ России от 10 июля 2014 г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Настоящий Регламент устанавливает общий порядок и условия предоставления услуг Центра администрирования сети ViPNet Территориального фонда обязательного медицинского страхования Иркутской области (далее по тексту – ЦАС ViPNet) Пользователю Системы защищенного обмена электронными документами, присоединившемуся к Регламенту в порядке, предусмотренном положениями статьи 428 Гражданского Кодекса РФ, услуг по изготовлению и ключей шифрования и дополнительных услуг, связанных с управлением ключами шифрования, администрирования защищенной сети в части использования СКЗИ ViPNet.

Присоединение к Регламенту производится путем заключения Стороной Системы защищенного обмена электронными документами **Соглашения о присоединении к Регламенту Центра администрирования сети ViPNet 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 ЦАС ViPNet ТФОМС Иркутской области за один месяц до дня расторжения. Уведомление о расторжении Соглашения, полученное ЦАС ViPNet ТФОМС Иркутской области от Пользователя, является основанием для обязательного аннулирования ключей шифрования Пользователей, уполномоченных данным Пользователем. Датой аннулирования указанных ключей шифрования Пользователей 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 Центра администрирования сети VipNet Территориального фонда обязательного медицинского страхования Иркутской области». Регламент регулирует нормы связанные с процессом защищенного обмена электронными документами и взаимодействия информационных систем с использованием средств криптографической защиты.

1.3. ПУБЛИКАЦИЯ РЕГЛАМЕНТА

Настоящий Регламент распространяется:

В электронной форме

- на сайте www.irkoms.ru Фонда в разделе «О Фонде», «Центр администрирования сети VipNet ТФОМС Иркутской области».
- 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 ЦАС ViPNet ТФОМС Иркутской области, предоставляются по телефону (3952) 203-949.

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 ЦАС ViPNet ТФОМС Иркутской области.

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 Фонд официально не уведомит пользователей о прекращении действия Регламента, Регламент автоматически пролонгируется на следующие 5 лет.

Официальное уведомление о прекращении действия Регламента публикуется Фондом на сайте www.irkoms.ru Фонда в разделе «О Фонде», «Центр администрирования сети VipNet ТФОМС Иркутской области».

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», «Центр администрирования сети VipNet ТФОМС Иркутской области».

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. ЦАС ViPNet ТФОМС Иркутской области

2.1. СВЕДЕНИЯ ОБ ЦАС ViPNet

Физическое размещение:
Адрес: 664022, г. Иркутск, ул. 3 Июля, 20
Адрес электронной почты: irotfoms@irkoms.ru
Контактный телефон ЦАС ViPNet: 8 (3952) 203-949
Факс: 8 (3952) 34-16-58

Для

Юридическое лицо, выполняющее функции Администратора ЦАС ViPNet и предоставляющая услуги по изготовлению и выдаче криптографических ключей должно иметь действующие лицензии ФСБ России на осуществление следующих видов услуг:

- 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.

2.2. РЕЕСТР ЦАС ViPNet

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

- реестр заявлений на регистрацию пользователя;
- реестр зарегистрированных пользователей сети ViPNet;
- реестр заявлений на аннулирование регистрации пользователя сети ViPNet;
- реестр заявлений на приостановление/возобновление регистрации пользователя;
- служебные документы ЦАС ViPNet.

2.3. НАЗНАЧЕНИЕ ЦАС ViPNet

ЦАС ViPNet предназначен для обеспечения участников корпоративной защищенной информационной сети средствами и спецификациями для обеспечения:

- аутентификации участников информационных систем в процессе взаимодействия;
- 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 ЦАС ViPNet

В процессе своей деятельности ЦАС ViPNet предоставляет следующие виды услуг:

- внесение в реестр зарегистрированных Пользователей регистрационной информации о пользователях ЦАС ViPNet;
- формирование и обновление справочно-ключевой информации для организации защищенного обмена информации в рамках сети ViPNet;
- формирование ключей пользователя по обращениям пользователей ЦАС ViPNet, с записью их на ключевой носитель;
- ведение реестра пользователей ЦАС ViPNet;
- приостановление работы пользователя;
- возобновление работы пользователя;
- удаление пользователя;
- установление связи с узлами сети ViPNet;
- установление связи с пользователями сети ViPNet;
- распространение средств шифрования по обращениям пользователей ЦАС ViPNet.
- Администрирование узлов сети ViPNet (смена ключевой информации, смена парольной информации, смена сетевых адресов).

2.5. СТРУКТУРА ЦАС ViPNet

Директор Фонда подписывает договор в котором:

- Возлагается исполнение обязанностей администрирования сети ViPNet №559 на организацию имеющую Лицензию ФСБ России 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.)
- Возлагаются функции обеспечения информационной безопасности и технической эксплуатации ЦАС ViPNet на Уполномоченное лицо.

На организацию администрирующую ЦАС ViPNet возлагаются функции для решения задач ЦАС ViPNet по:

- управлению деятельностью ЦАС ViPNet;
- взаимодействию с пользователями ЦАС ViPNet в части разрешения вопросов, связанных с применением ключей и сертификатов открытых ключей, изготовляемых и/или распространяемых ЦАС ViPNet;
- взаимодействию с пользователями ЦАС ViPNet в части разрешения вопросов, связанных с подтверждением электронной подписи уполномоченного лица ЦАС ViPNet в сертификатах открытых ключей, изготовленных ЦАС ViPNet в электронной форме.
- регистрации пользователей ЦАС ViPNet;
- ведению реестра зарегистрированных пользователей ЦАС ViPNet;
- распространению СКЗИ;
- организации и выполнению мероприятий по защите ресурсов ЦАС ViPNet;
- формированию и обновлению справочно-ключевой информации для организации защищенного обмена информации в рамках сети ViPNet №559;
- обеспечению взаимодействия с другими сетями ViPNet;
- изготовлению и предоставлению ключей по обращению пользователей ЦАС ViPNet;

2.6. ПРЕКРАЩЕНИЕ ДЕЯТЕЛЬНОСТИ

Деятельность ЦАС ViPNet может быть прекращена в порядке, установленном законодательством РФ.

2.7. ПОЛЬЗОВАТЕЛИ УСЛУГ ЦАС ViPNet ТФОМС Иркутской области

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

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

Физическое лицо представляет юридическое лицо на основании внесения его в реестр Пользователей ЦАС ViPNet после подачи заявления на регистрацию Пользователя сети ViPNet №559 ТФОМС Иркутской области, предоставляющей право данному физическому лицу пользоваться услугами ЦАС ViPNet.

3. ПРАВА И ОБЯЗАННОСТИ, ОТВЕТСТВЕННОСТЬ

3.1. ПРАВА И ОБЯЗАННОСТИ ЦАС ViPNet

ЦАС ViPNet имеет право:

- Отказать в предоставлении услуг по регистрации пользователей ЦАС ViPNet, сторонним организациям, подавшим заявление на регистрацию, без предоставления информации о причинах отказа;
- Отказать в изготовлении ключей шифрования лицам, подавшим заявление на изготовление ключей шифрования, но не прошедшим регистрацию в ЦАС ViPNet , без предоставления информации о причинах отказа;
- Аннулировать (отозвать) ключи пользователя ЦАС ViPNet в случае установленного факта компрометации соответствующего закрытого ключа, с уведомлением владельца аннулированного (отозванного) ключа и указанием обоснованных причин;
- В одностороннем порядке приостановить действие ключей пользователя ЦАС ViPNet, с обязательным уведомлением владельца приостановленного сертификата открытого ключа и указанием обоснованных причин.

ЦАС ViPNet обязан:

- Организовывать проверку на предмет актуализации угроз безопасности информации по итогу которой выполняются:
- обновления системного программного обеспечения (нейтрализация известных уязвимостей операционной системы и прикладного обеспечения, при невозможности устранения уязвимостей функционалом и возможностями ЦАС ViPNet в рамках Регламента, Уполномоченное лицо направляет письмо в Фонд с указанием уязвимых мест в системе и предложениями дальнейших действий по их устранению);
- Обновление организационно-распорядительной документации;
- Использовать для изготовления ключей шифрования уполномоченного лица ЦАС ViPNet только СКЗИ сертифицированные по классу КС2 в соответствии с действующим законодательством РФ.
- Использовать ключи шифрования уполномоченного лица ЦАС ViPNet только в технологических процессах ЦАС ViPNet.

- Принять меры по защите ключей шифрования уполномоченного лица ЦАС ViPNet в соответствии с положениями настоящего Регламента.

- Синхронизировать по времени все программные и технические средства обеспечения деятельности ЦАС ViPNet. ЦАС ViPNet организует работу своих Служб по серверу синхронизации времени Фонда.

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

- Обеспечить уникальность регистрационной информации пользователей ЦАС ViPNet , заносимой в реестр ЦАС ViPNet и используемой для идентификации владельцев.

- Не разглашать (публиковать) регистрационную информацию пользователей ЦАС ViPNet , за исключением информации используемой для идентификации пользователей.

- Изготовить закрытый и открытый ключи зарегистрированному пользователю с использованием средств электронной подписи.

- Обеспечить сохранение в тайне изготовленных ключей пользователей.

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

- Обеспечить уникальность регистрационных (серийных) номеров изготавливаемых ключей шифрования.

- 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 ключей шифрования по заявлению его владельца.

- 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.

- Уведомить о факте аннулирования (отзыва), приостановлении и возобновлении действия сертификата ключа подписи лиц, зарегистрированных в ЦАС ViPNet. Срок уведомления – не позднее одного рабочего дня с момента занесения сведений об

аннулированном (отозванном), приостановленном, возобновленном сертификате в список отозванных сертификатов.

- 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

Реестр сертификатов открытых ключей ведется в электронном виде. Сертификаты открытых ключей представлены в реестре в форме электронных копий изготовленных сертификатов.

3.2. ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ЦАС ViPNet

Пользователи ЦАС ViPNet имеют права:

- обратиться в ЦАС ViPNet для изготовления ключей шифрования;
- получить и ввести в действие на своем рабочем месте изготовленные ключи шифрования;
- обратиться в ЦАС ViPNet для внесения в реестр ЦАС ViPNet регистрационной информации о пользователе;
- 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 ЦАС ViPNet, для проверки статуса сертификатов открытых ключей подписи;
- обратиться в ЦАС ViPNet для предоставления им закрытых и открытых ключей с записью их на ключевой носитель;
- обратиться в ЦАС ViPNet на предмет получения средства электронной подписи;
- обратиться в ЦАС ViPNet для аннулирования (отзыва) сертификата открытого ключа в течение срока действия соответствующего закрытого ключа;
- обратиться в ЦАС ViPNet для приостановления действия сертификата открытого ключей пользователя в течение срока действия соответствующего закрытого ключа;
- обратиться в ЦАС ViPNet для возобновления действия сертификата открытого ключа в течение срока действия соответствующего закрытого ключа.

Обязанности пользователей ЦАС ViPNet:

- лица, проходящие процедуру регистрации в реестре ЦАС ViPNet, обязаны представить регистрационную и идентифицирующую информацию в объеме, определенном положениями настоящего Регламента;
- хранить в тайне ключ, выданный ЦАС ViPNet , принимать все возможные меры для предотвращения его потери, раскрытия, модифицирования или несанкционированного использования;

- использовать ключ только для целей, разрешенных соответствующими областями использования (связь узлов, сервис быстрых сообщений, деловая почта ViPNet);

- немедленно обратиться в ЦАС ViPNet с заявлением на приостановление действия ключей шифрования в случае потери, раскрытия, искажения личного последнего, а также в случае если пользователю ЦАС ViPNet стало известно, что этот ключ используется или использовался ранее другими лицами;

- не использовать ключи шифрования, заявление на аннулирование (отзыв) которых подано в ЦАС ViPNet , в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) ключей шифрования ЦАС ViPNet по момент времени официального уведомления об аннулировании (отзыве) ключей шифрования, либо об отказе в аннулировании (отзыве);

- не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на приостановление действия, которого подано в ЦАС ViPNet, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в ЦАС ViPNet 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 ЦАС ViPNet, пользователь сертификата должен удостовериться, что назначение сертификата, определенное соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту, соответствует предполагаемому использованию.

3.3. ОТВЕТСТВЕННОСТЬ

- ЦАС ViPNet не несет ответственности в случае нарушения Пользователем положений настоящего Регламента.

- Претензии к ЦАС ViPNet ограничиваются указанием на несоответствие его действий настоящему Регламенту.

4. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

Ключи шифрования пользователей ЦАС ViPNet являются конфиденциальной информацией. ЦАС ViPNet не депонирует и не архивирует ключи шифрования пользователей.

Информация, хранящаяся в журналах аудита ЦАС ViPNet, считается конфиденциальной и не подлежит разглашению.

Отчетные материалы по выполненным проверкам деятельности ЦАС ViPNet являются конфиденциальными, за исключением заключения по результатам проверок.

Информация, не являющаяся конфиденциальной, может публиковаться по решению ЦАС ViPNet.

Место, способ и время публикации также определяется решением ЦАС ViPNet.

Также не считается конфиденциальной информация о настоящем Регламенте.

ЦАС ViPNet 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 ЦАС ViPNet применяется в отношении физических лиц, представляющих юридическое лицо, присоединившееся к Регламенту, обращающихся к услугам ЦАС ViPNet.

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

Регистрация пользователей ЦАС ViPNet , являющихся сотрудниками Фонда и участвующих в защищенном обмене электронными документами, осуществляется на основании утвержденного перечня пользователей ЦАС ViPNet руководителями структурных подразделений или на основании подписанной ЭП заявки уполномоченным сотрудником Фонда и направленной по защищенной (в зашифрованном виде) почте ViPNet на сетевой узел «Администратор» (сети ViPNet №559). Заявка должна содержать ФИО регистрируемого пользователя и подразделение (филиал) его работы.

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

Пользователь ЦАС ViPNet 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 Заявку 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) - 2 экз.;
- Внешняя организация (после подписания Соглашения о присоединении к Регламенту) направляет в Фонд:
- Заявление на регистрацию Пользователя ЦАС ViPNet (Приложение №4);

– Подписанное руководителями Фонда, внешней организацией, Соглашение о присоединении к Регламенту вместе с Заявлением на регистрацию Пользователя ЦАС ViPNet передается Администратору сети ViPNet;

– Администратор сети ViPNet на основании подписанного Соглашения о присоединении к Регламенту, Заявления на регистрацию Пользователя ЦАС ViPNet регистрирует абонентские пункты и пользователей внешней организации в АРМ [Администратора]. Задает необходимые связи с абонентскими пунктами, с которыми требуется установить взаимодействие, формирует ключевую информацию;

– После выполнения всех процедур, Администратор сети ViPNet передает Пользователю внешней организации или представителю Пользователя внешней организации парольно-ключевую информацию для установки ПО ViPNet [Клиент] на отчуждаемом машинном носителе.

При этом обязательно должно быть выполнено следующее:

– пользователь внешней организации или его представитель получает лично парольно-ключевую информацию, аутентификация проводиться по паспорту;

– Представитель внешней организации должен иметь доверенность на право получения за Пользователя организации сформированного ключевого носителя (Приложение №5).

После получения всех необходимых ключевых носителей Пользователь:

– Выполняет установку ПО ViPNet Клиент;

– Вводит первичную ПКИ на рабочем месте;

– 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 ЦАС ViPNet осуществляется по идентификатору зарегистрированного пользователя, занесенному в реестр ЦАС ViPNet.

Аутентификация зарегистрированного пользователя ЦАС ViPNet выполняется средствами СКЗИ ViPNet или по сертификату открытого ключа или по парольно-ключевой информации пользователя.

5.4. ИЗГОТОВЛЕНИЕ КЛЮЧЕЙ

Первичное изготовление ключей выполняется Администратором сети ViPNet 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, определяемый Администратором сети ViPNet;
- быть проинициализированным (отформатированным);
- не содержать никакой информации.

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 поэкземплярного учета ключевых документов под подпись владельца или его представителя (Приложение №6).

5.5. ИЗГОТОВЛЕНИЕ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА И ПРЕДОСТАВЛЕНИЕ ЕГО ВЛАДЕЛЬЦУ

Изготовление сертификата открытого ключа в процессе работы осуществляется ЦАС ViPNet на основании заявления на регистрацию пользователя ЦАС ViPNet.

После изготовления сертификата открытого ключа его владельцу направляется уведомление.

Изготовленный сертификат открытого ключа в электронной форме, предоставляется его владельцу :

- при личном обращении к Администратору ЦАС ViPNet;
- по доверенному каналу с использованием СКЗИ ViPNet с использованием сервиса - «Деловая почта» ViPNet или встроенного механизма рассылки ключевой информации ViPNet.

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 [Администратора], 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 [Администратора], обслуживающих соответствующие сети.

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 в АРМ [Администратора] 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.

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]», проводится 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 взаимодействии, между данными узлами сетей Фондов и организаций можно производить защищенный электронный документооборот.

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

Порядок модификации 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 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]» выполняется 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 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 взаимодействии.

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 проводится в соответствии с «Руководством администратора. ViPNet [Удостоверяющий и ключевой центр]».

- Процедура создания экспорта и приема импорта.

После смены межсетевого мастер-ключа проводится 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]».

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.

6.ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

6.1. ИДЕНТИФИЦИРУЮЩИЕ ДАННЫЕ УПОЛНОМОЧЕННОГО ЛИЦА ЦАС ViPNet

Уполномоченное лицо ЦАС ViPNet, идентифицируется по следующим данным:
Фамилия, имя, отчество:
Наименование организации:
Адрес электронной почты Уполномоченного лица ЦАС ViPNet
Субъект Федерации:

6.2. СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ УПОЛНОМОЧЕННОГО ЛИЦА ЦАС ViPNet

Срок действия закрытого ключа и открытого ключа, соответствующего закрытому ключу, уполномоченного лица ЦАС ViPNet составляет не более 1 года.

Начало периода действия закрытого ключа уполномоченного лица 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, составляет 1 год.

6.3. СРОКИ ДЕЙСТВИЯ ЗАКРЫТЫХ КЛЮЧЕЙ И СЕРТИФИКАТОВ ОТКРЫТЫХ КЛЮЧЕЙ ПОЛЬЗОВАТЕЛЕЙ СЕРТИФИКАТОВ ОТКРЫТЫХ КЛЮЧЕЙ

Срок действия закрытого ключа пользователя ЦАС ViPNet, соответствующего сертификату открытого ключа, владельцем которого он является, составляет не более 12 месяцев.

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

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

Срок действия сертификата открытого ключа устанавливается ЦАС ViPNet в момент его изготовления.

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

Ключи и сертификат открытого ключа предназначены для:

- обеспечения аутентификации зарегистрированного пользователя ЦАС ViPNet при использовании программного обеспечения зарегистрированного пользователя;
- обеспечения шифрования в сервисе «Деловая почта»;
- формирования электронной подписи в заявлении на сертификат открытого ключа в электронном виде;
- использования в соответствии со сведениями, указанными в сертификате в областях использования.

6.5. АРХИВНОЕ ХРАНЕНИЕ ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИИ

Архивированию подлежит следующая документированная информация:

- Заявления на изготовление ключей пользователей ЦАС ViPNet;
- Заявления на аннулирование (отзыв) ключей шифрования;
- Служебные документы ЦАС ViPNet.

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

Срок хранения архивных документов устанавливается 5 лет.

Выделение архивных документов к уничтожению и уничтожение осуществляется Уполномоченным лицом ЦАС ViPNet.

6.6. УПРАВЛЕНИЕ КЛЮЧАМИ

Плановая смена ключей уполномоченного лица Удостоверяющего Центра

Плановая смена ключей уполномоченного лица ЦАС ViPNet выполняется в соответствии со сроком действия закрытого ключа уполномоченного лица ЦАС ViPNet.

Процедура плановой смены ключей уполномоченного лица ЦАС ViPNet осуществляется в следующем порядке:

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

Внеплановая смена ключей уполномоченного лица ЦАС ViPNet

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации закрытого ключа уполномоченного лица ЦАС ViPNet.

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

Процедура внеплановой смены ключей уполномоченного лица ЦАС ViPNet выполняется после получения уведомления о компрометации закрытого ключа 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 ЦАС ViPNet, сертификат скомпрометированного открытого ключа уполномоченного лица Удостоверяющего Центра аннулируется (отзывается) путем занесения в список отозванных сертификатов.

Плановая смена ключей Пользователя Удостоверяющего Центра

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

Процедура плановой смены ключей Пользователя осуществляется в следующем порядке:

- Уполномоченное лицо формирует новый закрытый и соответствующий ему открытый ключ;

- Уполномоченное лицо изготавливает сертификат нового открытого ключа и подписывает его электронной подписью с использованием нового закрытого ключа.

Внеплановая смена ключей Пользователя

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

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

Ключи пользователя могут считаться скомпрометированными в следующих случаях:

- посторонним лицам мог быть доступным файл ключевого дистрибутива;

- посторонним лицам мог быть доступным съемный носитель с ключевой информацией;

- посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на компьютере;

- уволился пользователь, имевший доступ к паролям и ключам.

Процедура внеплановой смены ключей Пользователя выполняется Администратором сети ViPNet. Администратор сети ViPNet после получения уведомления о компрометации ключей Пользователя в течение рабочей смены:

- аннулирует сертификат ключа подписи;

- объявляет ключи данного пользователя скомпрометированными;

- выполняет 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, сертификат скомпрометированного открытого ключа Пользователя аннулируется (отзывается) путем занесения в список отозванных сертификатов.

7. ПРОГРАММНЫЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ЦАС ViPNet

7.1. ОСНОВНЫЕ СРЕДСТВА ЦАС ViPNet

Для реализации своих услуг и обеспечения жизнедеятельности ЦАС ViPNet использует следующие программные и технические средства:

- Программный комплекс обеспечения реализации целевых функций ЦАС ViPNet (далее по тексту – ПК УЦКУ);

- Технические средства обеспечения работы ЦАС ViPNet (далее по тексту – ТС ЦАС ViPNet);

- Программные и программно-аппаратные средства защиты информации (далее по тексту – СЗИ ЦАС ViPNet).

7.2. ПРОГРАММНЫЙ КОМПЛЕКС ОБЕСПЕЧЕНИЯ РЕАЛИЗАЦИИ ЦЕЛЕВЫХ ФУНКЦИЙ ЦАС ViPNet

Программный комплекс обеспечения реализации целевых функций ЦАС ViPNet включает в себя следующие программные компоненты:

– Администратор

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

ViPNet [Администратора] является базовым компонентом ЦАС ViPNet, включает в себя программы ViPNet [Администратора] [Центр управления сетью] и ViPNet [Удостоверяющий и Ключевой Центр].

Программа ViPNet [Администратора] [Центр управления сетью], далее ЦУС, предназначена для формирования и изменения структуры корпоративной сети. Обеспечивает реализацию следующих целевых функций ЦАС ViPNet:

- 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 ЦАС ViPNet:

- 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 ЦАС ViPNet:

- Создание ключей подписи и издание сертификатов уполномоченных лиц УЦ;
- Регистрация данных внешнего пользователя.
- Ведения Реестра зарегистрированных внешних пользователей ЦАС ViPNet.
- Генерация закрытого ключа подписи и сохранение его на персональном ключевом носителе внешнего пользователя.
- Ведение Реестра запросов изданных сертификатов.
- Формирование запросов на отзыв, приостановление или возобновление сертификатов.
- 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;
- Хранение информации о запросах и ведение эталонной копии Реестра 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.

Ответственность за эксплуатацию ViPNet [Администратора] возлагается на Уполномоченное лицо ЦАС ViPNet.

7.3. ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ РАБОТЫ ПК ЦАС ViPNet

Технические средства обеспечения работы ПК ЦАС ViPNet включают в себя:

- Выделенный АРМ Администратора с ПО ViPNet [Администратора] [УКЦ и ЦУС];
- Программный или программно-аппаратный комплекс защиты от несанкционированного доступа;
- Система обнаружения вторжений (СОВ);
- Антивирусное программное обеспечение;
- Устройство печати на бумажных носителях (принтеры).

7.4. ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

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

- ViPNet [Координатор], предназначенный для обеспечения защищенного служебного информационного обмена между компонентами ЦАС ViPNet 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 ЦАС ViPNet;
- Устройства обеспечения противопожарной безопасности помещений ЦАС ViPNet.

7.5. ПЕРЕЧЕНЬ СОБЫТИЙ, РЕГИСТРИРУЕМЫХ ПРОГРАММНЫМ КОМПЛЕКСОМ ОБЕСПЕЧЕНИЯ РЕАЛИЗАЦИИ ЦЕЛЕВЫХ ФУНКЦИЙ ЦАС ViPNet

- 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.

7.6. ПЕРЕЧЕНЬ ДАННЫХ ПРОГРАММНОГО КОМПЛЕКСА ОБЕСПЕЧЕНИЯ РЕАЛИЗАЦИИ ЦЕЛЕВЫХ ФУНКЦИЙ ЦАС ViPNet, ПОДЛЕЖАЩИХ РЕЗЕРВНОМУ КОПИРОВАНИЮ

При эксплуатации программного комплекса обеспечения реализации целевых функций ЦАС ViPNet выполняется резервное копирование данных компонент ПК ЦАС ViPNet. Периодичность создания резервных копий определяется настройками программы ЦАС ViPNet и может варьироваться в зависимости от числа выполненных операций, но не реже одного раза в месяц.

Перечень данных ПК ЦАС ViPNet, 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 аудита программных компонентов ViPNet.

8. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

8.1. ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Размещение технических средств ЦАС ViPNet

АРМ Администратора ЦАС ViPNet установлен на оборудовании ЦАС ViPNet и размещен в защищенном помещении.

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

Физический доступ в помещения

Для защищенного помещения ЦАС ViPNet 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 ЦАС ViPNet и Серверная оборудованы системой контроля доступа, охранной сигнализацией и механическими замками.

Электроснабжение и кондиционирование воздуха

Технические средства ЦАС ViPNet подключены к общегородской сети электроснабжения.

Электрические сети и электрооборудование, используемые в ЦАС ViPNet, 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 ЦАС ViPNet, 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 ЦАС ViPNet оборудованы средствами вентиляции и кондиционирования воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством РФ.

Подверженность воздействию влаги

Защита «АРМ Администратор» и телекоммуникационного оборудования от воздействия влаги обеспечивается поддержанием нормального режима влажности, также размещением «АРМ Администратор» и телекоммуникационного оборудования на расстоянии не менее 0.8 м от уровня пола.

Предупреждение и защита от возгорания

Помещение ЦАС ViPNet оборудовано системой пожарной сигнализации.

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

Хранение документированной информации

Хранение документированной информации ЦАС ViPNet проводиться в соответствии с утвержденной инструкцией о делопроизводстве ЦАС ViPNet, на основе действующего законодательства РФ по делопроизводству.

Уничтожение документированной информации

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

8.2. ПРОГРАММНО-АППАРАТНЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Организация доступа к техническим средствам ЦАС ViPNet

Доступ к техническим средствам ЦАС ViPNet 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 ЦАС ViPNet, размещенных на рабочих местах сотрудников ЦАС ViPNet, возлагается на сотрудников, ответственных за эксплуатацию данных технических средств.

Организация доступа к программным средствам ЦАС ViPNet

Рабочее место ЦАС ViPNet, на котором эксплуатируется программные приложения ViPNet [Администратора] [ЦУС] и ViPNet [Администратора] [УКЦ] также оснащено сертифицированным средством защиты от НСД.

Доступ системных администраторов общесистемного программного обеспечения для выполнения регламентных работ с оборудованием осуществляется в присутствии сотрудников Отдела системного администрирования и защиты информации, отвечающих за эксплуатацию соответствующего прикладного программного обеспечения.

Контроль целостности программного обеспечения

Контролю целостности подлежат следующие программные компоненты из состава программного обеспечения, эксплуатируемого ЦАС ViPNet:

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

Состав программных модулей, подлежащих контролю целостности, определяется внутренним документом ЦАС ViPNet.

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 – при загрузке операционной системы «АРМ Администратор».

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 ЦАС ViPNet 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 (программными) средствами обеспечения деятельности ЦАС ViPNet и программными средствами, предоставляемыми ЦАС ViPNet пользователям, в процессе обмена документами в электронной форме, осуществляется путем шифрования информации с использованием шифровальных (криптографических) средств, сертифицированных по классу в соответствии с действующим законодательством РФ.

В качестве шифровальных (криптографических) средств пользователей ЦАС ViPNet, используемых для защиты конфиденциальной информации, используется только сертифицированные ФСБ России средства.

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 ЦАС ViPNe

- программные модули ЦУС и УКЦ;
- парольно-ключевая информация ЦАС ViPNet;
- журналы ЦАС ViPNet;
- организационно-распорядительная документация ЦАС ViPNet;
- ресурсы АРМ Администратора (процессорное время)
- список аннулированных и действующих сертификатов ЦАС ViPNet;
- служебная переписка в сервисе «Деловая почта» ViPNet.

8.3. ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Предъявляемые требования к персоналу ЦАС ViPNet

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

Профессиональная переподготовка и повышение квалификации персонала

Сотрудники ЦАС ViPNet ТФОМС Иркутской области осуществляют повышение квалификации в областях знаний согласно занимаемым должностям.

Организация сменной работы

Деятельность ЦАС ViPNet ТФОМС Иркутской области по работе с пользователями в части приема заявлений в бумажной форме и изготовления парольно-ключевой информации 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 ЦАС ViPNet ТФОМС Иркутской области 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) ЦАС ViPNet ТФОМС Иркутской области;
- Сохранность материальных ценностей и документов;
- Предупреждение происшествий и ликвидацию их последствий.