Приложение
УТВЕРЖДЕНО
приказом ТФОМС
Саратовской области
от 20.08.2024 № 220

РЕГЛАМЕНТ

Удостоверяющего Центра корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области

Термины и определения

ViPNet - линейка продуктов компании «ИнфоТеКС», включающая программные и программно-аппаратные комплексы (средства защиты информации ограниченного доступа, в том числе персональных данных), предназначенных для:

- создания защищенной, доверенной среды передачи информации ограниченного доступа с использованием публичных и выделенных каналов связи (Интернет, телефонные и беспроводные линии связи) путем организации виртуальной частной сети (VPN) с одним или несколькими центрами управления;
- развертывания инфраструктуры открытых ключей (PKI) с организацией Удостоверяющего Центра с целью использования механизмов электронной подписи.

ViPNet Administrator (Администратор) - набор программного обеспечения для администрирования сети ViPNet, включающий в себя серверное и клиентское приложения ViPNet Центр управления сетью, а также программу ViPNet Удостоверяющий и ключевой центр.

ViPNet Удостоверяющий и ключевой центр (УКЦ) - программа, входящая в состав программного обеспечения ViPNet Administrator. Администратор УКЦ формирует и обновляет ключи для сетевых узлов ViPNet, а также управляет сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС) - это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

Координатор (ViPNet-координатор) - сетевой узел, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или специальный программно-аппаратный комплекс. В рамках сети ViPNet координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Клиент (ViPNet-клиент) - сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Транспортный модуль (MFTP) - компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

ViPNet Деловая почта –компонент программного обеспечения ViPNet, предназначена для обмена электронной почтой между пользователями сети ViPNet. С помощью программы «Деловая почта» можно отправлять и получать сообщения и вложения, подписывать сообщения и вложения электронной подписью. В программе предусмотрена система автоматической обработки входящих сообщений и файлов в соответствии с заданными правилами (автопроцессинг).

Администратор сети ViPNet - лицо, назначенное руководителем организации, отвечающее за управление сетью ViPNet, создание и обновление справочников и ключей для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями и обладающее правом доступа к программе ViPNet Центр управления сетью и (или) ViPNet Удостоверяющий и ключевой центр.

Аутентификация - процесс идентификации пользователя, как правило, на основании его учетной записи. Аутентификация служит для подтверждения того, что входящий в систему пользователь является тем, за кого себя выдает, но процесс аутентификации не затрагивает права доступа пользователя (в отличие от авторизации).

Владелец сертификата ключа проверки электронной подписи (владелец сертификата) - лицо, которому в установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Доступ к информации - возможность получения информации и ее использования.

Дистрибутив ключей - файл с расширением .dst, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Информация - сведения (сообщения, данные) независимо от формы их представления.

Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Ключ электронной подписи (далее - ключ ЭП) - в соответствии с федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» ключом электронной подписи называется закрытый ключ, который является секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Ключ проверки электронной подписи (далее - ключ проверки ЭП) - В соответствии с федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» ключом проверки электронной подписи называется открытый ключ, который является не секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, однозначно связанную с закрытым ключом и предназначенную для проверки подлинности электронной подписи.

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (ключи электронной подписи).

Ключи пользователя ViPNet – совокупность ключей, которые необходимы пользователю для аутентификации в сети ViPNet и шифрования других ключей, и к которым имеет доступ только данный пользователь. Ключи пользователя могут содержать:

- действующий персональный ключ пользователя;
- ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной
- подписи;
- хэш пароля пользователя.

Содержимое ключей пользователя формируется в зависимости от типа аутентификации пользователя.

Компрометация ключей - утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства). Ключи администратора программы ViPNet Удостоверяющий и ключевой центр считаются скомпрометированными в следующих случаях:

- при утрате пароля или ключей администратора;
- при увольнении администратора;
- если посторонние лица получили доступ к компьютеру с УКЦ.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Межсетевая информация - информация о доверенной сети или своей сети, предназначенная для организации или изменения межсетевого взаимодействия. В состав межсетевой информации входят связи между сетевыми объектами, параметры сетевых узлов ViPNet и служебная информация (сертификаты издателей, списки аннулированных сертификатов).

Межсетевое взаимодействие - информационное взаимодействие, организованное между сетями ViPNet. Позволяет узлам различных сетей ViPNet обмениваться информацией по защищенным каналам. Для организации взаимодействия между узлами различных сетей ViPNet администраторы этих сетей обмениваются межсетевой информацией.

Несанкционированный доступ к информации - доступ к информации в нарушение должностных полномочий сотрудника или доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Область применения сертификатов - перечень объектных идентификаторов (OID), определяющих области применения сертификатов ключей проверки электронной подписи, создаваемых Удостоверяющим Центром.

Обновление справочников и ключей - файлы, формируемые администратором сети ViPNet в управляющем приложении (ViPNet Центр управления сетью, ViPNet Удостоверяющий и ключевой центр, ViPNet Network Manager) при изменении справочников и ключей для сетевых узлов ViPNet, то есть, в случае добавления, удаления сетевого узла ViPNet, добавления пользователя, издания нового сертификата и так далее. Администратор сети ViPNet централизованно высылает на сетевой узел сформированные новые ключи и справочники из ЦУСа или ViPNet Network Manager.

Обязательное медицинское страхование (ОМС) - вид обязательного социального страхования, представляющий собой систему создаваемых государством правовых, экономических и организационных мер, направленных на обеспечение при наступлении страхового случая гарантий бесплатного оказания застрахованному лицу медицинской помощи за счет средств обязательного медицинского страхования в пределах территориальной программы обязательного медицинского страхования и в установленных настоящим Федеральным законом случаях в пределах базовой программы обязательного медицинского страхования.

ПАК - программно-аппаратный комплекс.

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Плановая смена ключей электронной подписи - смена ключей электронной подписи, производимая в период действия ключей электронной подписи в соответствии с установленной в Удостоверяющем центре периодичностью, не вызванная компрометацией ключей электронной подписи.

Пользователь Удостоверяющего центра (пользователь) - лица, зарегистрированные в Удостоверяющем Центре и признающие настоящий Регламент.

Рабочий день Удостоверяющего Центра (далее - рабочий день) - промежуток времени с 9 часов до 18 часов каждого дня недели за исключением субботы, воскресенья и праздничных нерабочих дней.

Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации

неопределенному кругу лиц.

Регистрационная информация пользователя - информация, предоставляемая пользователем в целях создания сертификата ключа проверки электронной подписи.

Сертификат ключа проверки электронной подписи (сертификат) - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Список аннулированных (отозванных) сертификатов (CRL) - список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором Удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Справочники сетевого узла - набор файлов, содержащих информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях. Эти файлы формируются в программе ViPNet Центр управления сетью, предназначенной для создания структуры и конфигурирования сети ViPNet.

Средства электронной подписи (далее - средства ЭП) - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Средства Удостоверяющего центра (далее - средства УЦ) - программные и (или) аппаратные средства, используемые для реализации функций Удостоверяющего центра.

Сетевой узел ViPNet (Клиент, Сетевой узел) - узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью.

Сеть ViPNet - логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов ViPNet. Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Уполномоченное лицо Удостоверяющего центра (УЛ УЦ) - физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов ключей подписей и списков отозванных сертификатов.

Уполномоченный представитель юридического лица - физическое лицо, которое действует от имени заявителя – юридического лица на основании учредительных документов, приказа о представителе юридического лица или доверенности и которое указывается в сертификате ключа проверки электронной подписи юридического лица в качестве владельца наряду с

наименованием юридического лица.

Удостоверяющий центр корпоративного уровня ТФОМС Саратовской области (далее - УЦ) – Удостоверяющий Центр корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Усиленная неквалифицированная электронная подпись (неквалифицированная электронная подпись) - электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

Электронный документ (далее - ЭД) - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Электронная подпись (далее - 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.

Электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

1. Общие положения

Территориальный фонд обязательного медицинского страхования Саратовской области (далее - Фонд) является организатором и администратором защищенной сети ViPNet №602 (далее – Защищенная сеть) и выполняет функции Удостоверяющего центра корпоративного уровня.

Регламент Удостоверяющего Центра корпоративного уровня Фонда (далее – Регламент), разработан в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской федерации»;
- Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Гражданским кодексом Российской Федерации;
- Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Общими принципами построения и функционирования информационных систем и порядок информационного взаимодействия в сфере обязательного медицинского страхования, утв. приказом Федерального фонда обязательного медицинского страхования от 07.04.2011 № 79;
- Постановлением Правительства Российской Федерации от 05.11.2022 № 1998 «Об утверждении Правил ведения персонифицированного учета в сфере обязательного медицинского страхования»
- Приказом Министерства здравоохранения Российской Федерации от 28.02.2019 № 108н «Об утверждении Правил обязательного медицинского страхования»;
- Приказом ФСБ Российской Федерации от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам Удостоверяющего центра»;
- Приказом ФСБ Российской Федерации от 10.07.2014 № 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»;
- Приказом ФСБ Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказом ФАПСИ от 13.06.2001 №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи

по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Целью настоящего Регламента является создание условий для организации защищенного обмена электронными документами и взаимодействия информационных систем, 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 Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Настоящий Регламент устанавливает общий порядок и условия предоставления УЦ участникам Защищённой сети возможности участвовать в обмене юридически значимыми электронными документами с применением электронной подписи.

Регламент предназначен для определения сертификационной политики при организации защищенного обмена электронными документами и взаимодействия информационных систем всеми Участниками Защищенной сети.

Сертификационная политика УЦ определяет создание, управление и использование ***усиленных неквалифицированных*** сертификатов формата X.509 для обеспечения идентификации владельца сертификата и целостности электронной информации.

Организация защищенного обмена электронными документами и взаимодействия информационных систем, признание юридической значимости электронных документов в рамках Защищённой сети между Фондом и юридическим лицом производится путем заключения Соглашения о присоединении к Регламенту (далее - Соглашение) (Приложение №3 к Регламенту) в порядке, предусмотренном положениями статьи 428 Гражданского Кодекса Российской Федерации.

С момента заключения Соглашения о присоединении к Регламенту, юридическое лицо, считается присоединившемся к Регламенту и является Стороной Регламента (далее – Сторона).

Факт присоединения Стороны к Регламенту подтверждается полным принятием ею условий настоящего Регламента и всех его приложений в редакции, действующей на момент присоединения, и Сторона принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

Сторона имеет право в одностороннем порядке расторгнуть Соглашение, письменно уведомив об этом УЦ за один месяц до дня расторжения. Уведомление о расторжении Соглашения, полученное УЦ от Стороны, является основанием для обязательного аннулирования сертификатов ключей проверки электронных подписей Пользователей УЦ, уполномоченных данной Стороной. Датой аннулирования указанных сертификатов ключей подписей Пользователей УЦ будет дата расторжения Соглашения.

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

1.1 Порядок утверждения и внесения изменений в Регламент

Настоящий Регламент утверждается приказом директора 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, утвержденным Регламентом.

Все изменения и дополнения, вносимые в Регламент и не связанные с изменением законодательства Российской Федерации, вступают в силу и становятся обязательными для Сторон по истечении 10 (Десять) календарных дней с даты размещения указанных изменений и дополнений в Регламенте на сайте www.sartfoms.ru ТФОМС Саратовской области в разделе «Удостоверяющий Центр корпоративного уровня».

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.

1.2 Идентификация Регламента

Наименование документа: «Регламент Удостоверяющего Центра корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области».

Версия: 3.0.

Дата: 01.06.2024

Объектный идентификатор УЦ: **1.2.643.3.164**

1.3 Публикация Регламента

Настоящий Регламент публикуется в электронном виде на корпоративном сайте http://www.sartfoms.ru ТФОМС Саратовской области в разделе «Удостоверяющий Центр корпоративного уровня».

Регламент публикуется в виде файла формата PDF.

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

2. Удостоверяющий центр, Пользователи Удостоверяющего центра

2.1 Сведения об Удостоверяющем центре

Полное наименование юридического лица УЦ: Территориальный фонд обязательного медицинского страхования Саратовской области (ТФОМС Саратовской области)
Юридический адрес: 410012, Саратов, проспект им. Петра Столыпина, 10, 12
Фактический адрес: 410012, Саратов, проспект им. Петра Столыпина, 10, 12
Для почты: 410000, Саратов, Главпочтамт, а/я 1534
Адрес электронной почты: ucku@sartfoms.ru
Контактный телефон УЦ: (8452) 65-30-50 (165)
Факс: (8452) 65-30-50 (125)
Банковские реквизиты: УФК по Саратовской области (Территориальный фонд обязательного медицинского страхования Саратовской области, л/с 03605914990)
ИНН: 6455005067
КПП: 645501001
Единый казначейский счет: 40102810845370000052 в ОТДЕЛЕНИИ САРАТОВ БАНКА РОССИИ
Казначейский счет: 03271643630000096000
БИК: 016311121
ОКТМО: 63701000
Руководитель: директор – Заречнев Сергей Михайлович.

УЦ имеет разрешение (лицензии) по всем видам деятельности, связанным с осуществлением функций УЦ:

- Лицензия ФСБ Российской Федерации от 14.06.2022 № Л051-00105-64/00417167 на осуществление разработки, 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).

Система безопасности и защиты информации УЦ создана и поддерживается на договорной основе с юридическими лицами, осуществляющими свою деятельность на основании лицензий, полученных в

соответствии с действующим законодательством Российской Федерации.

Документы, регламентирующие обеспечение мер по защите информации УЦ, введены в действие соответствующими приказами.

Для обеспечения деятельности УЦ используют средства УЦ, включая средства электронной подписи, сертифицированные в соответствии с действующим законодательством Российской Федерации (разработчик АО «Инфотекс» г. Москва, https://infotecs.ru).

Директор Фонда своим приказом:

- возлагает исполнение обязанностей Уполномоченного лица УЦ на сотрудника управления информационных технологий;
- наделяет Уполномоченное лицо УЦ правом подписывать своей электронной подписью сертификаты ключей подписей пользователей УЦ и заверять собственноручной подписью копии сертификатов ключей проверки электронной подписи на бумажном носителе;
- возлагает функции обеспечения информационной безопасности и технической эксплуатации УЦ на ***отдел системного администрирования и защиты информации управления информационных технологий.***

2.2 Назначение УЦ

УЦ предназначен для обеспечения участников Защищенной сети средствами и спецификациями для использования сертификатов ключей проверки электронной подписи 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.

В процессе своей деятельности УЦ:

- создает сертификаты ключей проверки электронных подписей;
- устанавливает сроки действия сертификатов ключей проверки электронных подписей;
- аннулирует выданные УЦ сертификаты ключей проверки электронных подписей;
- создает ключи электронных подписей и ключи проверки электронных подписей;
- ведет реестр выданных и аннулированных этим Удостоверяющим центром сертификатов ключей проверки электронных подписей;
- проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

- осуществляет проверку электронных подписей по обращениям участников электронного взаимодействия;
- осуществляет иную связанную с использованием электронной подписи деятельность.
- Выполнение своих функций УЦ осуществляет на безвозмездной основе.

2.3 Функции, выполняемые Удостоверяющим центром

2.3.1 Административные функции:

- управление деятельностью УЦ;
- взаимодействие с пользователями в части разрешения вопросов, связанных с применением средств электронной подписи, ключей электронной подписи и сертификатов;
- взаимодействие с пользователями в части разрешения вопросов подтверждения подлинности электронной подписи в электронном документе в отношении созданных УЦ сертификатов;
- взаимодействие с пользователями в части разрешения вопросов, связанных с подтверждением электронной подписи УЦ в сертификатах, созданных УЦ в электронной форме.

2.3.2 Функции регистрации:

- заключение Соглашения о присоединении к Регламенту УЦ;
- ведение реестра пользователей;
- создание сертификатов ключей проверки электронных подписей и выдачи таких сертификатов лицам, обратившимся за их получением (Заявителям);
- установление сроков действия сертификатов ключей проверки электронных подписей;
- выдача по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи;
- ведение реестра выданных и аннулированных сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;
- создание по обращениям заявителей ключей электронных подписей и ключей проверки электронных подписей;
- проверка на уникальность ключей проверки электронных подписей в реестре сертификатов;
- осуществление по обращениям участников электронного взаимодействия проверки электронных подписей;
- предоставление копий сертификатов в электронной форме, находящихся в реестре сертификатов, по запросам пользователей;

- осуществляет иную связанную с использованием электронной подписи деятельность.

2.3.3 Функции безопасности:

- организация и выполнение мероприятий по защите информационных ресурсов УЦ от несанкционированного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- обеспечение выполнения процедур создания, использования, хранения и уничтожения ключевой информации в соответствии с требованиями эксплуатационной документации на средства УЦ;
- недопущение копирования ключевой информации (криптографических ключей, в том числе ключей электронной подписи) на носители, не являющиеся ключевыми носителями;
- обеспечение взаимодействия с внешними УЦ, участниками различных корпоративных информационных систем на основе установления доверительных отношений между УЦ путем организации межсетевого взаимодействия;
- аннулирование (отзыв) сертификатов ключей проверки электронных подписей;
- приостановление и возобновление действия сертификатов;
- предоставление в любое время любому лицу доступа к актуальному списку аннулированных (отозванных) сертификатов;
- техническое обеспечение процедуры подтверждения подлинности электронной подписи в электронном документе в отношении созданных УЦ сертификатах, по обращениям пользователей;
- техническое обеспечение процедуры подтверждения подлинности электронной подписи УЦ в созданных УЦ сертификатах, по обращениям пользователей;
- техническое обслуживание средств электронной подписи.

2.4 Пользователи Удостоверяющего центра

Пользователями УЦ называются ***юридические лица***, зарегистрированные в УЦ.

Интересы юридического лица может представлять физическое лицо, действующее на основании учредительных документов, либо приказа о наделении соответствующими полномочиями, либо доверенности.

ТФОМС Саратовской области является зарегистрированным пользователем УЦ.

3. Права, обязанности, ответственность

3.1 Права Удостоверяющего центра

Удостоверяющий центр имеет право:

- отказать в регистрации лицам, подавшим заявку на подключение, с указанием причин отказа.

- отказать в создании сертификата зарегистрированным пользователям, подавшим заявление на его создание, с указанием причин отказа.
- отказать в аннулировании (отзыве) сертификата в случае, если истек установленный срок действия ключа электронной подписи, соответствующего ключу проверки электронной подписи в сертификате.
- отказать в приостановлении или возобновлении действия сертификата в случае, если истек установленный срок действия ключа электронной подписи, соответствующего ключу проверки электронной подписи в сертификате.
- аннулировать (отозвать) сертификат в случае установленного факта компрометации соответствующего ключа электронной подписи, с уведомлением владельца аннулированного (отозванного) сертификата и указанием обоснованных причин.
- приостановить действие сертификата с обязательным уведомлением владельца сертификата, действие которого приостановлено, и указанием обоснованных причин.

3.2 Обязанности Удостоверяющего центра

Удостоверяющий центр обязан:

- обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.
- обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей.

3.3 Права Пользователей

Пользователи имеют право:

- Обращаться в Удостоверяющий центр для регистрации в качестве пользователя.
- Обращаться в Удостоверяющий центр с целью получения средств электронной подписи.
- Получить доступ к актуальному списку аннулированных (отозванных) сертификатов.
- Получить копии сертификатов, находящихся в реестре УЦ, как в форме электронных документов, так и в форме документов на бумажном носителе.
- Обращаться в Удостоверяющий центр за подтверждением подлинности электронной подписи пользователя в электронном документе в соответствии с порядком, определенным настоящим Регламентом.
- Обращаться в Удостоверяющий центр за подтверждением подлинности электронной подписи в созданных УЦ сертификатах в соответствии с порядком, определенным настоящим Регламентом.
- Обращаться в Удостоверяющий центр с заявлениями на:
  - создание сертификата;
  - аннулирование (отзыв) сертификата (в течение срока действия

соответствующего ключа электронной подписи);

- приостановление действия сертификата (в течение срока действия соответствующего ключа электронной подписи);
- возобновление действия сертификата (в течение срока действия соответствующего ключа электронной подписи).

3.4 Обязанности Пользователей

3.4.1 Обязанности лиц, проходящих процедуру регистрации

- Лица, проходящие процедуру регистрации в УЦ, обязаны представить регистрационную информацию в требуемом для создания сертификата объеме.
- Лица, проходящие процедуру регистрации в УЦ, несут ответственность за достоверность предоставленной регистрационной информации.

3.4.2 Обязанности владельца сертификата

- Использовать для создания и проверки усиленных неквалифицированных электронных подписей, создания ключей усиленных неквалифицированных электронных подписей и ключей их проверки, средства электронной подписи, получившие подтверждение соответствия требованиям установленным в соответствии с Федеральными законами, совместимых со средствами УЦ.
- Обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей.
- Применять ключ электронной подписи только в соответствии с областями применения, определенными в полях сертификата: KeyUsage, ExtendedKeyUsage и CertificatePolicies.
- Уведомлять УЦ, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении.
- Не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.
- Не использовать ключ электронной подписи и связанный с ним сертификат, заявление на аннулирование (отзыв) которого подано в УЦ.

3.5 Ответственность

- Ответственность Сторон регулируется законодательством Российской Федерации.
- УЦ не несет ответственности в случае нарушения Пользователем положений настоящего Регламента.
- Пользователь несет ответственность за достаточность применяемых им мер по обеспечению безопасности использования электронной подписи и средств электронной подписи, включая защиту ключа электронной подписи от компрометации, потери, уничтожения, изменения или иного

неавторизованного использования.

- Пользователь ***обязан*** известить УЦ обо всех изменениях своей регистрационной информации в течение 3-х рабочих дней с момента регистрации изменений. УЦ вправе затребовать у пользователя необходимые документы, подтверждающие изменения регистрационной информации.

4. Порядок регистрации пользователей Удостоверяющего центра и изготовления сертификатов ключей проверки электронной подписи

4.1 Регистрация Пользователей Удостоверяющего центра

Руководитель организации направляет на имя директора Фонда письмо на подключение к системе защищенного обмена электронными документами и взаимодействия информационных систем (Приложение № 1) с указанием необходимого числа сетевых узлов и Заявки на подключение к системе (Приложение № 2).

На основании письма с положительной резолюцией директора Фонда и заявки, Фонд подготавливает и передает в обратившуюся организацию Соглашение о присоединении к Регламенту (Приложение № 3) системы защищенного обмена электронными документами и взаимодействия информационных систем в двух экземплярах.

С момента заключения Соглашения о присоединении к Регламенту, юридическое лицо, считается присоединившимся к Регламенту и является Стороной Регламента –зарегистрированным Пользователем Удостоверяющего центра.

4.1.1 Регистрация сетевого узла и Пользователей сетевого Узла

Заявитель направляет Заявление на регистрацию Пользователя на сетевом узле VipNet (Приложение № 5).

4.1.2 Справочники сетевого узла

Заявитель направляет Заявление на формирование Справочника сетевого узла (Приложение № 6), содержащего информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях.

Администратор сети ViPNet регистрирует сетевые узлы и Пользователей сетевых узлов, задает необходимые связи с сетевыми узлами, с которыми требуется установить взаимодействие.

4.2 Изготовление сертификата ключа проверки электронной подписи

Изготовление сертификата ключа проверки электронной подписи Пользователя сетевого узла для участия в обмене юридически значимыми электронными документами с применением электронной подписи, осуществляется на основании Заявления (Приложение № 8) и заверенной копии приказа (форма приказа - Приложение № 7) о полномочиях Пользователя сетевого узла – уполномоченного представителя юридического лица,

определяющих области применения сертификатов ключей проверки электронной подписи (перечень объектных идентификаторов (OID) – Приложение № 14).

После предоставления заявки на изготовление сертификата ключа проверки электронной подписи Уполномоченное лицо в течение 3 (трех) рабочих дней осуществляет её рассмотрение и обработку.

В случае отказа в регистрации и изготовлении сертификата ключа проверки электронной подписи Уполномоченное лицо уведомляет Заявителя, с указанием причины отказа.

В случае принятия положительного решения Уполномоченное лицо в течение 3 (три) рабочих дней осуществляет регистрацию, генерацию ключевой информации, изготовление сертификата ключа проверки электронной подписи. После изготовления сертификата ключа проверки электронной подписи Уполномоченное лицо уведомляет об этом Заявителя, после чего Пользователь сетевого узла должен лично или через доверенное лицо получить сформированные ключевые документы у Уполномоченного лица УЦ.

Три экземпляра сертификата ключа проверки электронной подписи Пользователя УЦ на бумажном носителе визируются Уполномоченным лицом и заверяются печатью, а также собственноручной подписью пользователя или его доверенного лица.

Доверенное лицо Пользователя сетевого узла должно иметь доверенность на право подписи и получения сертификата ключа проверки электронной подписи за Пользователя сетевого узла и получения сформированной ключевой информации - Дистрибутива ключей (Приложение № 4).

Изготовленный Дистрибутив ключей записывается на отчуждаемый машинный носитель (ключевой носитель), предоставляемый Заявителем.

Ключевой носитель должен удовлетворять следующим требованиям:

- быть отформатированным;
- не содержать никакой информации.

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

Запись о факте выдачи ключей заносится в ***Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации ключевых документов*** и подтверждается подписью владельца или Доверенного лица (Приложение № 15).

4.3 Подключение к системе защищенного обмена электронными документами и взаимодействия информационных систем

После получения всех необходимых ключевых носителей и сертификата Пользователя сетевого узла:

- выполняется установка и настройка ПО ViPNet Client в соответствии с требованиями к конфигурации ПО ViPNet Client в пункте № 8. Регламента;
- выполняется установка полученного Дистрибутива ключей (первичная

инициализация) на сетевом узле ;
- выполняется тестовый обмен защищенными сообщениями и зашифрованными, подписанными электронной подписью файлами, с Администратором сети ViPNet.

После успешного тестового обмена зашифрованной информацией и проверки электронной подписи Пользователь сетевого узла становится Участником Защищенной сети и может выполненять защищенный обмен электронными документами и взаимодействовать с разрешенными абонентскими пунктами.

4.4 Смена ключей электронной подписи Пользователя

4.4.1 Сроки действия ключей электронной подписи Пользователя

Срок действия ключа электронной подписи, ключа проверки электронной подписи и соответствующего сертификата пользователя составляет 12 месяцев.

4.4.2 Плановая смена ключей электронной подписи (продление)

Плановая смена ключей электронной подписи производится не ранее, чем за 20 (двадцать) и не позднее, чем за 5 (пять) рабочих дней до окончания срока действия текущего сертификата (ключей электронной подписи и ключей проверки электронной подписи) пользователя.

При плановой смене ключей электронной подписи (продлении) выполняются действия в соответствии с п. 4.2. настоящего регламента.

4.4.3 Внеплановая смена ключей электронной подписи

Внеплановая смена ключей электронной подписи производится по инициативе пользователя в период срока действия ключей электронной подписи и сертификата пользователя, в следующих случаях:
- при изменении регистрационной информации пользователя;
- при компрометации ключа электронной подписи пользователя;
- при компрометации ключа электронной подписи Уполномоченного лица УЦ.

4.4.4 Аннулирование (отзыв) сертификата

Аннулирование (отзыв) сертификатов осуществляется УЦ в следующих случаях:
- по заявлению Пользователя сетевого узла на аннулирование (отзыв) сертификата;
- по инициативе УЦ в случаях невыполнения пользователем обязательств, предусмотренных Регламентом или установления факта компрометации ключа электронной подписи пользователя.
- Заявление на аннулирование (отзыв) сертификата представляет собой документ на бумажном носителе, заверенный собственноручной подписью Пользователя сетевого узла (Приложение № 9).

При выполнении УЦ процедуры аннулирования (отзыва) сертификата, информация об аннулированном сертификате заносится в список аннулированных (отозванных) сертификатов.

Аннулирование (отзыв) сертификата по инициативе УЦ осуществляется с уведомлением Пользователя сетевого узла (владельца отозванного сертификата) с указанием обоснованных причин отзыва.

4.4.5 Приостановление действия сертификата

Приостановление действия сертификата осуществляется УЦ в следующих случаях:

- по заявлению Пользователя сетевого узла на приостановление действия сертификата;
- по инициативе УЦ в случае невыполнения Пользователя сетевого узла обязательств, предусмотренным Регламентом.

Заявление на приостановление действия сертификата представляет собой документ на бумажном носителе, заверенный собственноручной подписью Пользователя Узла (Приложение № 10).

При устном заявлении на приостановление действия сертификата Пользователя сетевого узла должен сообщить идентификационные данные, содержащиеся в сертификате.

При выполнении УЦ процедуры приостановления действия сертификата ключа подписи, информация о сертификате, действие которого приостановлено, заносятся в список аннулированных (отозванных) сертификатов.

Приостановление действия сертификата по инициативе УЦ осуществляется с уведомлением Пользователя сетевого узла (владельца отозванного сертификата) с указанием обоснованных причин приостановления.

Информация о прекращении действия сертификата ключа проверки электронной подписи должна быть внесена УЦ в реестр сертификатов в течение одного рабочего дня со дня наступления обстоятельств, повлекших за собой прекращение действия сертификата ключа проверки электронной подписи. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов.

4.4.6 Возобновление действия сертификата

Возобновление действия сертификата осуществляется УЦ по заявлению Пользователя сетевого узла на возобновление действия сертификата.

Заявление на возобновление действия сертификата представляет собой документ на бумажном носителе, заверенный собственноручной подписью Пользователя сетевого узла (Приложение № 11).

При выполнении УЦ процедуры возобновления действия сертификата, информация о сертификате, действие которого возобновлено, удаляется из списка аннулированных (отозванных) сертификатов.

4.5 Смена ключей электронной подписи Уполномоченного лица

Удостоверяющего центра

4.5.1 Сроки действия ключей электронной подписи Уполномоченного лица УЦ

- Срок действия закрытого ключа электронной подписи Уполномоченного лица УЦ составляет 12 месяцев.
- Срок действия открытого ключа проверки электронной подписи и соответствующего сертификата Уполномоченного лица УЦ составляет 24 месяца.
- Начало действия ключей электронной подписи Уполномоченного лица УЦ исчисляется с даты и времени начала действия соответствующего сертификата.

4.5.2 Плановая смена ключей электронной подписи Уполномоченного лица УЦ

- Плановая смена ключей электронной подписи Уполномоченного лица УЦ выполняется в соответствии со сроком действия и не позднее окончания срока действия текущего ключа электронной подписи Уполномоченного лица УЦ.
- Процедура плановой смены ключей электронной подписи Уполномоченного лица УЦ выполняется в порядке, определенном эксплуатационной документацией на средства УЦ.

4.5.3 Внеплановая смена ключей электронной подписи Уполномоченного лица Удостоверяющего центра

- Внеплановая смена ключей электронной подписи УЦ производится в случае компрометации или угрозы компрометации ключа электронной подписи Уполномоченного лица УЦ.
- Процедура по внеплановой смене ключей электронной подписи Уполномоченного лица УЦ выполняется в порядке, определенном эксплуатационной документацией на средства УЦ.
- При выполнении процедуры по внеплановой смене ключей электронной подписи Уполномоченного лица УЦ, сертификат ключа проверки электронной подписи, соответствующий скомпрометированному ключу ЭП УЦ, должен быть аннулирован (отозван) и занесен в список аннулированных (отозванных) сертификатов. Также должны быть проведены работы по внеплановой смене ключей электронной подписи пользователей, сертификаты которых созданы с использованием скомпрометированного ключа электронной подписи Уполномоченного лица УЦ.

4.6 Подтверждение подлинности электронной подписи Уполномоченного лица Удостоверяющего центра в созданных сертификатах

- УЦ осуществляет подтверждение подлинности электронной подписи Уполномоченного лица УЦ в созданных УЦ сертификатах по заявлению

Пользователя сетевого узла на подтверждение подлинности ЭП Уполномоченного лица УЦ в сертификате Пользователя сетевого узла (Приложение № 12).

- Обязательным приложением к заявлению на подтверждение подлинности электронной подписи Уполномоченного лица УЦ в сертификате пользователя является внешний носитель информации, содержащий файл сертификата, подвергающегося процедуре проверки, в формате PKCS#7 в кодировке Base64 (CER).
- Срок проведения работ по подтверждению подлинности электронной подписи Уполномоченного лица УЦ в созданном УЦ сертификате и предоставлению заключения о произведенной проверке составляет 10 (десять) рабочих дней с момента поступления в УЦ заявления Пользователя сетевого узла на подтверждение подлинности электронной подписи Уполномоченного лица УЦ в сертификате Пользователя.
- Результатом проведения работ по подтверждению подлинности электронной подписи Уполномоченного лица УЦ в сертификате пользователя является заключение УЦ, заверенное собственноручной подписью ответственного сотрудника и печатью УЦ.

4.7 Подтверждение подлинности электронной подписи пользователя в электронном документе

- Подтверждение подлинности электронной подписи в электронном документе осуществляется Удостоверяющим центром по обращению владельца сертификата (далее - Заявителя) на основании заявления на подтверждение подлинности электронной подписи в электронном документе (Приложение № 13).
- Заявление на подтверждение подлинности электронной подписи в электронном документе должно содержать информацию о дате и времени формирования электронной подписи в электронном документе.
- Бремя доказывания достоверности даты и времени формирования электронной подписи в электронном документе возлагается на заявителя.
- Обязательным приложением к заявлению на подтверждение электронной подписи в электронном документе является внешний носитель информации, содержащий электронный документ с электронной подписью в формате PKCS#7.
- Срок проведения работ по подтверждению подлинности электронной подписи в электронном документе составляет 10 (десять) рабочих дней с момента поступления заявления в Удостоверяющий центр.
- В ходе проведения работ по подтверждению подлинности электронной подписи в электронном документе Удостоверяющим центром может быть запрошена дополнительная информация.
- Результатом проведения работ по подтверждению подлинности электронной подписи в электронном документе является ответ в письменной форме, заверенный собственноручной подписью ответственного сотрудника и печатью Удостоверяющего центра.

5. Разрешение споров

- При рассмотрении спорных вопросов, связанных с настоящим Регламентом, стороны должны руководствоваться действующим законодательством Российской Федерации.
- Стороны должны принять все необходимые меры для того, чтобы в случае возникновения спорных вопросов решить их, в претензионном порядке.
- Сторона, получившая от другой стороны претензию, обязана в течение 20 (двадцати) рабочих дней удовлетворить заявленные в претензии требования или направить другой стороне мотивированный отказ с указанием оснований отказа.
- Все споры и разногласия между сторонами, в отношении данного Регламента, в том числе касающиеся его заключения, действия, исполнения, изменения, прекращения или действительности, по которым не было достигнуто соглашение, разрешаются в соответствии с действующим законодательством Российской Федерации.

6. Структура сертификата

Удостоверяющий центр создает ***усиленные неквалифицированные*** сертификаты, соответствующие международным рекомендациям ITU-T X.509 (далее - рекомендации X.509 версии 3)

6.1 Базовые поля сертификата

Наименование поля	***Описание***	***Содержание / Значение***
Version:	Версия формата X.509 сертификата	«V3»
SerialNumber:	Серийный номер сертификата	Уникальный номер сертификата
Signature:	Алгоритм подписи	ГОСТ Р 34.10 – 2012 256 (512 бит)
Issuer:	Идентифицирующие данные издателя сертификата	Согласно пункту 6.3 настоящего Регламента
Validity:	Даты начала и окончания действия сертификата	«Действителен с: дд.мм.ггг чч:мм:сс» «Действителен по: дд.мм.ггг чч:мм:сс»
Subject:	Идентифицирующие данные владельца сертификата	Согласно пункту 6.4 настоящего Регламента
SubjectPublicKeyInfo:	Ключ проверки ЭП владельца сертификата	Значение ключа проверки ЭП

6.2 Дополнения сертификата

Наименование поля	*Описание*	*Содержание/ Значение*
Key Usage:	Использование ключа	**В сертификатах Уполномоченного лица УЦКУ:** Электронная подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL) (f6) **В сертификатах пользователей:** Электронная подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
ExtendedKeyUsage:	Расширенное использование ключа	Набор объектных идентификаторов (OID), определяющих области применения сертификатов ключей проверки ЭП, описывающие юридическую сферу применения соответствующего сертификата
CertificatePolicies:	Политики сертификата	Класс средства электронной подписи
SubjectKeyIdentifier:	Идентификатор ключа субъекта	Идентификатор ключа ЭП владельца сертификата
AuthorityKey Identifier:	Идентификатор ключа издателя сертификата	Номер сертификата УЦ

Перечень объектных идентификаторов (OID), определяющих области применения сертификатов ключей проверки электронной подписи, создаваемых Удостоверяющим Центром, содержится в Приложении № 14 настоящего Регламента.

6.3 Структура данных поля Issuer (идентификационных данных Уполномоченного лица Удостоверяющего центра)

Наименование поля	***Описание***	***Содержание/ Значение***
Common Name, CN	Общее имя	Уполномоченное лицо УЦКУ Кузнецов Ю.В.
CountryName, C	Страна	RU
LocalityName, L	Наименование населенного пункта	Саратов
StateOrProvinceName, S	Наименование области	Саратовская
StreetAdress, Street	Адрес	пр. им. Петра Столыпина, д.10,12
OrganizationName, O	Наименование организации	ТФОМС Саратовской области
OrganizationUnit, OU	Подразделение	Управление информационных технологий
Title, T	Должность	Заместитель начальника управления
Email, E	Адрес электронной почты	kuznetsov@sartfoms.ru
OGRN	Основной государственный регистрационный номер (ОГРН)	1026403672591
INN	Идентификационный номер налогоплательщика (ИНН)	6455005067

6.4 Структура данных поля Subject (идентификационных данных владельцев сертификатов юридических лиц)

Наименование поля	***Описание***	***Содержание/ Значение***
Common Name, CN	Общее имя	Сокращенное наименование юридического лица
SureName	Фамилия	Фамилия уполномоченного представителя юридического лица
GivenName	Приобретенное имя	Имя и отчество (если имеется) уполномоченного представителя юридического лица (владельца сертификата)
CountryName, C	Страна	RU
LocalityName, L	Наименование населенного пункта	Город или населенный пункт места нахождения юридического лица
StateOrProvinceName, S	Наименование области	Субъект Российской Федерации места нахождения юридического лица
StreetAddress, Street	Адрес	Часть адреса места нахождения юридического лица, включающая наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения (если имеется)
Email, E	Адрес электронной почты	Адрес электронной почты владельца сертификата
OrganizationName, O	Наименование организации	Наименование юридического лица
OrganizationUnitName, OU	Подразделение организации	Наименование подразделения, сотрудником которого является уполномоченный представитель юридического лица (владелец сертификата)
Title, T	Должность	Наименование должности уполномоченного представителя юридического лица (владельца сертификата)
OGRN	Основной государственный регистрационный номер (ОГРН)	ОГРН юридического лица

INN	Идентификационный номер налогоплательщика (ИНН)	ИНН юридического лица
UnstructuredName	Неструктурированное имя	Наименование абонентского пункта юридического лица

7. Структура списка аннулированных (отозванных) сертификатов

Издаваемые Удостоверяющим центром списки аннулированных (отозванных) сертификатов должны соответствовать рекомендациям X.509. Все поля и дополнения, включаемые в список аннулированных (отозванных) сертификатов, должны быть заполнены в соответствии с рекомендациями X.509 версии 2.

Наименование поля	***Описание***	***Содержание/ Значение***
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	Атрибуты имени Удостоверяющего центра
Effective date	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
Next update	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
Revoked Certificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (Serial Number) 2. Время аннулирования или время обработки заявления на прекращение действия сертификата (Revokation Date) 3. Код причины отзыва сертификата (CRL Reason Code): «0» Не указана «1» Компрометация ключа «2» Компрометация ЦС «3» Изменение принадлежности «4» Сертификат заменен «5» Прекращение работы «6» Приостановление действия
Signature algorithm	Алгоритм подписи	ГОСТ Р 34.10 – 2012 256 (512 бит)
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.10 – 2012 256 (512 бит)

Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа электронной подписи Удостоверяющего центра, которым подписан СОС
CA Version	Версия сертификата издателя	Версия сертификата Удостоверяющего центра
CRL Number	Номер СОС	Порядковый номер СОС
CRL Next Publish	Следующая публикация СОС	дд.мм.гггг чч:мм:сс GMT

8. Требования к конфигурации ПО VipNet Client

На рабочем месте Участника Защищенной сети настройка ПО ViPNet Client производится согласно документу «*Программный комплекс ViPNet Client 4. Правила пользования*» и реализуется следующая общая политика безопасности:

- информационный обмен между Участниками производится только шифрованным виде, т.е. выполняется блокировка всего открытого IP-трафика;
- правила фильтрации открытой сети, настраиваются только для работы внутри корпоративной сети. Если рабочей станции требуется работать с внутренними корпоративными сетевыми ресурсами, то в настройках программы ViPNet Client должны быть произведены дополнительные настройки фильтров IP-пакетов открытой сети;
- правила доступа для пропуска трафика от адресатов защищенной сети должны разрешать работу только по разрешенным протоколам и портам;
- правами по модификации конфигурации сетевого узла обладает Администратор безопасности.

Основной функциональный состав абонентского пункта ПО ViPNet Client представлен в Таблице 1.

Таблица 1

Наименование	***Значение***	***Примечание***
Программное обеспечение ViPNet Client		
Драйвер сетевой защиты	✓	
ViPNet Client Монитор	✓	
MFTP	✓	
Деловая почта	✓	
Полномочия и настройки		
Подпись (сертификат)	✓	Рабочие ключи ЭП и сертификат изготавливаются в соответствии с порядком, определенным в Регламенте УЦКУ
Разрешенные связи	с Участниками Защищенной сети	

9. Порядок информационного взаимодействия в защищенной сети

9.1 Передача сведений

Передача сведений обеспечивается транспортным модулем ViPNet MFTP, входящим в состав ПАК защиты информации «ViPNet/ Транспортный модуль ViPNet. MFTP передает информацию в виде конвертов. Конверт формируется в одной из следующих программ: ViPNet Центр управления сетью, Деловая почта, Файловый обмен. Конверт состоит из тела конверта и заголовка. Тело конверта представляет собой файл с передаваемой информацией. В заголовок включена адресная информация (для правильной маршрутизации конвертов в сети), идентификаторы отправителя и получателей, и информация для расшифрования случайного ключа. На случайном ключе шифруется тело конверта, а случайный ключ шифруется на ключе обмена и помещается в заголовок.

9.2 Подтверждение приема/передачи передаваемых сведений

Подтверждение приема/передачи передаваемых сведений обеспечивается средствами ПО ViPNet Деловая почта, входящей в состав ПАК защиты информации «ViPNet», в соответствии с «*Руководством пользователя. ViPNet Деловая почта*».

9.3 Подтверждение достоверности и подлинности передаваемых сообщений

Подтверждение достоверности, подлинности и авторства передаваемых сведений обеспечивается средствами электронной подписи, предоставляемой ПО ViPNet Деловая почта, входящей в состав ПАК защиты информации «ViPNet», в соответствии с «*Руководством пользователя. ViPNet Деловая почта*».

9.4 Хранение сведений

Отправленные и полученные сведения сохраняются и могут быть перенесены на любые носители.

Стороны должны обеспечить защиту от несанкционированного доступа и непреднамеренного уничтожения и/или искажения учетных данных, содержащихся в электронных журналах регистрации электронных документов.

9.5 Хранение подписанных электронной подписью сведений

Все подписанные электронной подписью сведения должны храниться с электронной подписью в течение сроков, предусмотренных законодательством Российской Федерации, нормативными документами сторон, а в случае возникновения споров - до их разрешения.

Обязанности по организации архивов электронных документов возлагаются на каждую из Сторон, в части их касающейся.

Электронные архивы подлежат защите от несанкционированного доступа и непреднамеренного уничтожения и/или искажения.

9.6 Задание правил автопроцессинга в ПО ViPNet Деловая почта для обработки электронных документов, принимаемых и передаваемых в процессе защищенного обмена

Правила автопроцессинга определяют каталоги приема и передачи для соответствующего адресата защищенной сети ViPNet, используя которые участники документооборота обмениваются электронными документами:

- электронные документы, помещаются уполномоченным лицом отправителя в соответствующий получателю каталог передачи ПО ViPNet Деловая почта;
- электронные документы, помещенные уполномоченным лицом отправителя в каталог передачи в соответствии с правилом автопроцессинга ПО ViPNet Деловая почта и адресованные определенному получателю, автоматически отправляются получателю, при этом шифруются и подписываются электронной подписью отправителя;
- для контроля доставки исходящих электронных документов и результатах проверки электронной подписи в адрес отправителя направляется электронная квитанция о доставке, которая формируется в ПО ViPNet Деловая почта получателя на каждое входящее письмо и автоматически отправляется отправителю;
- входящие электронные документы, принятые ПО ViPNet Деловая почта автоматически расшифровываются и согласно правилам автопроцессинга сохраняются в каталог приема, соответствующий получателю. Проверка электронной подписи отправителя под принятым электронным документом производится автоматически в соответствии с заданным правилом автопроцессинга для данного получателя.

10.Порядок организации защищенного межсетевого информационного взаимодействия

10.1 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 межсетевом 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 определяют Координаторы, которые будут выполнять функции серверов-шлюзов при межсетевом взаимодействии сетей.

10.2 Порядок организации межсетевого защищенного информационного взаимодействия между ViPNet - сетями организаций

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

- в каждом 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 собственные 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;
- во всех ЦУСах и УКЦ сторонних организаций в соответствии с «*Руководством администратора. ViPNet [Центр управления сетью]*» и «*Руководством администратора. ViPNet [Удостоверяющий и ключевой центр]*» производится ввод и обработка (импорт) полученных данных

(начального экспорта), для установки связей своих узлов с узлами ЦУСов, предоставившими информацию. Далее в ЦУСах и УКЦ создается ответная информация (ответный экспорт) для ЦУСов, приславших первичную информацию, включая собственные 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 межсетевого 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 межсетевом взаимодействии, между узлами сетей Фонда и сторонних организаций можно осуществлять защищенный электронный документооборот.

После завершения процедуры установления защищенного информационного взаимодействия между ViPNet-сетью Фонда и сетями сторонних организаций подписывается Протокол установления межсетевого взаимодействия (Приложение №16).

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

В процессе функционирования защищенного информационного взаимодействия между сетями ViPNet Организаций в одной или нескольких сетях может потребоваться модификация межсетевого защищенного информационного взаимодействия, т.е. изменение состава узлов, участвующих в межсетевом защищенном взаимодействии, - добавление или удаление сетевого узла.

Порядок модификации межсетевого защищенного информационного взаимодействия между ViPNet - сетями Организаций предполагает выполнение следующих технологических и организационных мероприятий:
- при модификации защищенного информационного взаимодействия в какой-либо сети, администратор данной сети в своем ЦУСе производит соответствующие изменения в структуре связей, 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;
- 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 межсетевого защищенного взаимодействия между ЦУСами Организаций.

После рассылки каждым ЦУСом сформированных обновлений ключевой и справочной информации на свои узлы, применяется новая политика межсетевого взаимодействия.

10.4 Журнал изменений межсетевого защищенного информационного взаимодействия

При каждой модификации межсетевого защищенного информационного взаимодействия Администраторы безопасности заносят соответствующие записи в Журнал учета регистрационных файлов (лицензий сети) и межсетевого взаимодействия (экспорт, импорт) (Приложение №17).

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

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

- выбор типа межсетевого мастер–ключа, который будет использоваться для связи между сетями;
- выбор стороны-инициатора межсетевого взаимодействия, которая будет выпонять генерацию нового межсетевого мастер–ключа.
- выбор времени проведения смены межсетевого мастер-ключа и последующего обновления ключей шифрования для узлов своих сетей.

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

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.

После смены межсетевого мастер-ключа Администраторы сетей ViPNet и сторонних организаций должны занести соответствующие записи в Журнал учета регистрационных файлов (лицензий сети) и межсетевого взаимодействия (экспорт, импорт) (Приложение №17).

11.Приложения

1. Образец письма о подключении к системе защищенного обмена электронными документами и взаимодействия информационных систем в защищенной сети ОМС Саратовской области.
2. Заявка на подключение к системе защищенного обмена электронными документами и взаимодействия информационных систем сети ViPNet №602 по телекоммуникационным каналам связи.
3. Соглашение о присоединении к Регламенту Удостоверяющего Центра корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области для организации защищенного обмена электронными документами и взаимодействия информационных систем.
4. Доверенность на предоставление заявительных документов и получения ключей ЭП и сертификата ключа проверки ЭП Пользователя сетевого узла.
5. Заявление на регистрацию Пользователя сетевого узла.
6. Заявление на формирование Справочника сетевого узла.
7. Форма приказа «О допуске к работе в защищенной сети и предоставлении права владения сертификатами ключей проверки электронной подписи».
8. Заявление на изготовление сертификата ключа проверки электронной подписи Пользователя сетевого узла при генерации ключей подписей в УЦ.
9. Заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи Пользователя сетевого узла.
10. Заявление на приостановление действия сертификата ключа проверки электронной подписи Пользователя сетевого узла.
11. Заявление на возобновление действия сертификата ключа проверки электронной подписи Пользователя сетевого узла.
12. Заявление на подтверждение подлинности электронной подписи Уполномоченного лица УЦ в сертификате ключа проверки электронной подписи.
13. Заявление на подтверждение подлинности электронной подписи в электронном документе.
14. Перечень объектных идентификаторов (OID), определяющих области применения сертификатов ключей проверки ЭП, создаваемых УЦ.
15. Журнал учета изготовления и выдачи ключей под роспись.
16. Протокол установления межсетевого взаимодействия.
17. Журнал изменений.

Приложение № 1
к Регламенту

Образец письма

Директору
ТФОМС Саратовской области
Заречневу С.М.
им. Петра Столыпина пр., д. 10,12,
г. Саратов, 410012

О подключении к системе
защищенного обмена электронными документами
и взаимодействия информационных систем
в защищенной сети ТФОМС Саратовской области

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

Необходимое число сетевых узлов - ___

ViPNet Client приобретен самостоятельно

_____ _____
Должность руководителя подпись И.О.Фамилия

Приложение №2
к Регламенту

Заявка на подключение к системе защищенного обмена электронными документами и взаимодействия информационных систем сети ViPNet №602 по телекоммуникационным каналам связи			
Директору ТФОМС Саратовской области Заречневу С.М. от			
1. Полное наименование организации без сокращений (*на основании учредительных*			
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. ОГРН:			
8. КПП:			
9. Расчетный счет:			
10. БИК:			
11. Банк:			
12. ФИО руководителя:			
13. Должность руководителя:			
14. Действует на основании (*указать документ: устав, положение, доверенность или*			
15. Контактные телефоны			
16. Контактный E-mail			
Дата:		Подпись руководителя	М.П.

Приложение №3
к Регламенту

Соглашение №_____

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

г. Саратов «___»_____20__ г.

Территориальный фонд обязательного медицинского страхования Саратовской области, именуемый в дальнейшем «Фонд», в лице директора Заречнева Сергея Михайловича, действующего на основании Положения, с одной стороны, и _____, именуемый в дальнейшем «Пользователь УЦ», в лице _____, действующего на основании _____, с другой стороны, вместе именуемые «Стороны», на основании Федерального закона Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи», положений статьи 11 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и положений статей 428, 160 Гражданского Кодекса Российской Федерации в целях организации и осуществления защищенного обмена электронными документами и взаимодействия информационных систем с использованием средств защиты информации, заключили настоящее соглашение (далее - Соглашение) о нижеследующем:

1. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. В силу настоящего Соглашения Пользователь УЦ присоединяется к Регламенту Удостоверяющего центра корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области (далее - 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, использующих СКЗИ, соответствующие Требованиям к средствам электронной подписи, утвержденным приказом ФСБ Российской Федерации от 27.12.2011 № 796, для реализации функций электронной подписи (*создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи*) и обеспечивающих создание защищенной виртуальной сети на базе

общедоступной сети Интернет.

1.3. Соглашение регулирует отношения между Сторонами при организации и осуществлении защищенного обмена электронными документами и взаимодействия информационных систем в соответствии с Регламентом.

1.4. Соглашение определяет права и обязанности Сторон, возникающие при осуществлении взаимодействия в системе защищенного обмена электронными документами с учетом обеспечения информационной безопасности.

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

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1. Фонд является Администратором защищенной сети ViPNet № 602 и осуществляет все права, вытекающие из Регламента.

2.2. Фонд обязуется исполнять Регламент, в том числе своевременно и в полном объеме выполнять следующие обязанности:

- своевременно извещать Пользователя УЦ об изменениях и дополнениях, вносимых в Регламент или прекращении их действия;
- организовывать работу с криптографическими ключами Пользователя УЦ 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 УЦ, возникающие в соответствии с Регламентом.

2.3. Стороны признают, что:

2.3.1. Применяемые в системе защищенного обмена электронными документами сертифицированные средства криптографической защиты информации (далее - СКЗИ) обеспечивают аутентификацию, конфиденциальность, целостность и подлинность ЭД и достаточны для осуществления Сторонами обмена электронными документами с использованием общедоступных каналов связи, при условии использования не скомпрометированных ключей электронной подписи.

2.3.2. Электронная подпись в электронном документе признается равнозначной собственноручной подписи уполномоченных представителей Сторон, наделенных правом подписи соответствующих документов, и для этой электронной подписи соблюдены следующие условия:

- сертификат электронной подписи создан и выдан УЦ Фонда, сертификат уполномоченного лица которого действителен на день выдачи указанного сертификата;
- сертификат электронной подписи действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;
- имеется положительный результат проверки принадлежности владельцу сертификата электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания. Проверка осуществляется в соответствии с положениями Регламента и с использованием сертификата лица, подписавшего электронный документ;
- электронная подпись используется в соответствии со сведениями, указанными в сертификате (Приложение №14) с учетом ограничений, содержащихся в сертификате лица, подписывающего электронный документ (если такие ограничения установлены).

2.3.3. Удостоверенные корректными электронными подписями электронные документы, подтверждают Сторонам при защищенном обмене электронными документами:

- 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 электронными документами, удостоверенными корректной электронной подписью.

2.4.2. При проведении обмена электронными документами с использованием защищенного обмена электронными документами руководствоваться законодательством Российской Федерации, Регламентом, настоящим Соглашением и документацией на программные средства системы защищенного обмена электронными документами, включая средства криптографической защиты информации.

2.4.3. При компрометации ключей электронной подписи участников системы защищенного обмена электронными документами руководствоваться положениями, установленные Регламентом.

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 электронные документы участника системы защищенного обмена электронными документами в соответствии с настоящим Соглашением.

2.4.6. Осуществить подключение автоматизированного рабочего места Стороны к системе защищенного обмена электронными документами при выполнении Стороной необходимых условий, изложенных в Регламенте, а также корректировать настройки в случае изменения параметров подключения в соответствии с настоящим Соглашением.

2.4.7. Использовать автоматизированное рабочее место Стороны исключительно в целях, предусмотренных настоящим Соглашением.

2.4.8. Не вносить исправления, изменения или дополнения, а также не передавать третьим лицам средства электронной подписи, программное обеспечение и соответствующую техническую документацию.

2.4.9. Содержать в исправном состоянии компьютеры, участвующие в электронном взаимодействии, принимать организационные меры для предотвращения несанкционированного доступа к компьютерам, установленному на них программному обеспечению и средствам защиты информации, а также в помещения, в которых они установлены, не допускать появления на взаимодействующих компьютерах компьютерных вирусов.

2.4.10. Сторона, для которой сложились обстоятельства препятствующие возможности 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 с использованием программного продукта «VipNet», на время действия этих обстоятельств приостанавливается.

2.5. Сторона имеет право:

2.5.1. Отказывать другой Стороне в приеме/передаче электронных документов с указанием мотивированной причины отказа.

2.5.2. Приостанавливать обмен электронными документами при:

- несоблюдении Стороной требований к приему/передаче электронных документов 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 автоматизированных рабочих местах 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 электронных документов в случаях компрометации закрытых ключей электронной подписи.

2.5.4. В случае невозможности обмена электронными документами в системе защищенного обмена электронными документами 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 программных продуктов, объединенных под торговой маркой «ViPNet».

3.2. Стороны 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 электронной подписи, 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, 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. Электронные документы, подписанные некорректными электронными подписями, 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 электронных документов, принятых/переданных в системе защищенного обмена электронными документами, подписанных владельцем Сертификата ключа подписи Стороны.

5.3. Стороны не несут ответственность за возможные временные задержки исполнения и/или искажения электронных документов, возникающие по вине третьих лиц, предоставляющих услуги связи для использования в системе защищенного обмена электронными документами.

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

5.5. Сторона не несет ответственность за убытки, возникшие вследствие несвоевременного контроля другой Стороной электронных сообщений, подтверждающих получение и обработку электронных документов, не исполнения и не соблюдения мер обеспечения защиты от несанкционированного доступа.

5.6. Сторона не несет ответственности за ущерб, возникший вследствие разглашения пользователем другой Стороны собственного ключа электронной подписи, его утраты или его передачи, вне зависимости от причин, не уполномоченным лицам.

5.7. Сторона не несет ответственности за последствия изменения электронного документа, защищенного корректной электронной подписью, в том числе в случае использования ключей электронной подписи 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. КОНФИДЕНЦИАЛЬНОСТЬ

6.1. Стороны обязуются не разглашать сведения конфиденциального характера, полученные в процессе осуществления обмена электронными документами и взаимодействия информационных систем.

6.2. Стороны относят информацию к сведениям конфиденциального характера в порядке, установленным законодательством Российской Федерации

6.3. Порядок защиты и доступа к сведениям конфиденциального характера регламентируется соответствующими нормативными правовыми актами 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 заключается на неопределенный срок и вступает в силу со дня его подписания.

8.2. Изменения и дополнения к настоящему Соглашению оформляются в

письменной форме и действительны с момента подписания Сторонами.

8.3. Настоящее Соглашение может быть расторгнуто по инициативе любой из Сторон, о чем необходимо письменно уведомить другую Сторону не позднее, чем за 1 (один) месяц до дня его расторжения.

9. РЕКВИЗИТЫ СТОРОН

Фонд	**Пользователь УЦ**
Территориальный фонд обязательного медицинского страхования Саратовской области Юридический адрес: 410012, г. Саратов, им. Петра Столыпина пр., д. 10,12 Юридический адрес: 410012, г. Саратов, им. Петра Столыпина пр., д. 10,12 тел.: (8452) 65-30-50 факс: (8452) 65-30-50 *125 e-mail: general@sartfoms.ru	

10. ПОДПИСИ СТОРОН

Директор	_____
_____ **С.М. Заречнев**	_____ _____
мп	мп

Приложение №4
к Регламенту

Доверенность

на предоставление заявительных документов и получения ключей ЭП
и сертификата ключа проверки ЭП Пользователя сетевого узла

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 для регистрации, генерации ключей и изготовления сертификата ключа подписи своего полномочного представителя - Пользователя сетевого узла_____
(Ф.И.О. Пользователя сетевого узла)
2. Получить сертификат ключа электронной подписи Пользователя сетевого узла и иные документы.
3. Получить сформированный ключевой носитель, содержащий дистрибутив ключей Пользователя сетевого узла _____
(Ф.И.О. Пользователя сетевого узла)
4. Расписываться в копии сертификата ключа проверки электронной 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 сетевого узла _____ _____
подпись *И.О.Фамилия*

«____» _____ 20____ г.

_____ _____
Должность руководителя *подпись* *И.О.Фамилия*

МП

«____» _____ 20____ г.
дата подписания заявления

Приложение №5
к Регламенту

Заявление

на регистрацию Пользователя сетевого узла

_____
(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 сетевого узла на сетевом узле _____.

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 сетевого узла _____ _____
подпись *И.О.Фамилия*

«____» _____ 20__ г.

_____ _____
Должность руководителя *подпись* *И.О.Фамилия*

МП

«____» _____ 20____ г.
дата подписания заявления

Приложение №6
к Регламенту

Заявление

на формирование справочника сетевого узла

_____
(наименование Организации)

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит сформировать справочник сетевого узла для Пользователя:

(добавить, удалить) _____

_____

Пользователь сетевого узла _____ _____
подпись *И.О.Фамилия*

«____» _____ 20____ г.

_____ _____
Должность руководителя *подпись* *И.О.Фамилия*

МП

«____»_____ 20__ г.
дата подписания заявления

Приложение №7
к Регламенту

(Форма приказа)

ПРИКАЗ

_____ № _____

О допуске к работе в защищенной сети и предоставлении права владения сертификатами ключей проверки электронной подписи

В целях обеспечения юридической значимости электронных документов при осуществлении обмена документами в электронном виде и взаимодействие информационных систем в защищенной сети ViPNet №602 ТФОМС Саратовской области п р и к а з ы в а ю:

1. Создать группу по изучению правил работы со средством криптографической защиты информации (далее – СКЗИ) ViPNet и допустить после прохождения обучения к работе с СКЗИ ViPNet членов группы в составе:
руководителя организации *Иванова И.И*;
главного бухгалтера бухгалтерии *Петрова П.П.*;
специалиста-эксперта отдела ОМС *Сидорова С.С.*;

- -

2. Предоставить права владения сертификатами ключей проверки электронной подписи с полномочиями по подписанию электронных документов при осуществлении обмена документами в электронном виде и взаимодействие информационных систем в защищенной сети ViPNet №602 ТФОМС Саратовской области следующим сотрудникам < *наименование организации* >:

3.

№ п/п	Фамилия, инициалы	Должность	Структурное подразделение	Полномочия
1	2	3	4	5
1.	*Иванов И.И*	руководитель		Пользователь Руководитель
2.	*Петрова П.П.*	главный бухгалтер	бухгалтерия	Пользователь Главный бухгалтер
3.	*Сидорова С.С.*	специалист-эксперт	отдел ОМС	Пользователь
4.	. . . . .			

4. Контроль за исполнением приказа оставляю за собой.

_____ _____
Должность руководителя подпись И.О.Фамилия

ПРИМЕЧАНИЕ:

1. *Для «Полномочия» возможно указание следующих полномочий:*
Руководитель *- уполномоченное лицо юридического лица с правом первой подписи на основании учредительных документов или доверенности;*
Главный бухгалтер *- уполномоченное лицо юридического лица с правом второй подписи на основании учредительных документов или доверенности;*
Пользователь *– пользователь защищенной сети, аутентификация участников защищенной сети*

2. *Для каждого уполномоченного лица в таблице делается отдельная строка, в которой указываются все полномочия данного лица.*

Приложение №8
к Регламенту

Заявление

на изготовление сертификата ключа проверки электронной подписи Пользователя сетевого узла при генерации ключей подписей в УЦ

_____
(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 проверки электронной подписи своего уполномоченного представителя – Пользователя сетевого узла

_____
(фамилия, имя, отчество)

в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

Наименование поля	***Описание***	***Значение***
Common Name, CN	Общее имя	Сокращенное наименование юридического лица
SureName	Фамилия	Фамилия уполномоченного представителя юридического лица (владельца сертификата)
GivenName	Приобретенное имя	Имя и отчество (если имеется) уполномоченного представителя юридического лица (владельца сертификата)
CountryName, C	Страна	RU
LocalityName, L	Наименование населенного пункта	Город или населенный пункт места нахождения юридического лица
StateOrProvinceName, S	Наименование области	Субъект Российской Федерации места нахождения юридического лица
StreetAddress, Street	Адрес	Часть адреса места нахождения юридического лица, включающую наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения (если имеется)
Email, E	Адрес электронной почты	Адрес электронной почты владельца сертификата

OrganizationName, O	Наименование организации	Наименование юридического лица
OrganizationUnitName, OU	Подразделение организации	Наименование подразделения, сотрудником которого является уполномоченный представитель юридического лица (владелец сертификата)
Title, T	Должность	Наименование должности уполномоченного представителя юридического лица (владельца сертификата)
OGRN	Основной государственный регистрационный номер (ОГРН)	ОГРН юридического лица
INN	Идентификационный номер налогоплательщика (ИНН)	ИНН юридического лица
UnstructuredName	Неструктурированное имя	Наименование абонентского пункта юридического лица
Extended Key Usage	Расширенное использование ключа	Набор объектных идентификаторов (OID), определяющих области применения сертификатов ключей проверки ЭП, описывающие юридическую сферу применения соответствующего сертификата

Пользователь сетевого узла _____ _____
подпись *И.О.Фамилия*

«____» _____ 20____ г.

_____ _____
Должность руководителя подпись И.О.Фамилия

МП

«____» _____ 20__ г.
дата подписания заявления

Приложение №9
к Регламенту

Заявление

на аннулирование (отзыв) сертификата ключа проверки электронной подписи
Пользователя сетевого узла

_____
(наименование организации)

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит аннулировать (отозвать) сертификат ключа проверки электронной подписи своего уполномоченного представителя – Пользователя сетевого узла: _____, содержащий следующие идентификационные данные:
(фамилия, имя, отчество)

Наименование поля	***Описание***	***Значение***
SerialNumber, SN	Серийный номер	Серийный номер сертификата ключа подписи
Common Name, CN	Общее имя	Сокращенное наименование юридического лица
SureName	Фамилия	Фамилия уполномоченного представителя юридического лица (владельца сертификата)
GivenName	Приобретенное имя	Имя и отчество (если имеется) уполномоченного представителя юридического лица (владельца сертификата)
LocalityName, L	Наименование населенного пункта	Город или населенный пункт места нахождения юридического лица
Email, E	Адрес электронной почты	Адрес электронной почты владельца сертификата
OrganizationUnitName, OU	Подразделение организации	Наименование подразделения, сотрудником которого является уполномоченный представитель юридического лица (владелец сертификата)
INN	Идентификационный номер налогоплательщика (ИНН)	ИНН юридического лица
UnstructuredName	Неструктурированное имя	Наименование абонентского пункта юридического лица
CRL Reason Code	Код отзыва	Код причины отзыва сертификата «0» Не указана «1» Компрометация ключа «2» Компрометация ЦС «3» Изменение принадлежности «4» Сертификат заменен «5» Прекращение работы «6» Приостановление действия

Пользователь сетевого узла _____ _____
подпись *И.О.Фамилия*

«_____» _____ 20____ г.

_____ _____
Должность руководителя *подпись* *И.О.Фамилия*

МП

«_____» _____ 20__ г.
дата подписания заявления

Приложение №10
к Регламенту

Заявление

на приостановление действия Сертификат ключа проверки электронной подписи Пользователя сетевого узла

_____
(наименование Организации)

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит приостановить действие сертификата ключа подписи своего полномочного представителя – Пользователя сетевого узла: _____,
(фамилия, имя, отчество)

содержащего следующие идентификационные данные:

Наименование поля	***Описание***	***Значение***
SerialNumber, SN	Серийный номер	Серийный номер сертификата ключа подписи
Common Name, CN	Общее имя	Сокращенное наименование юридического лица
SureName	Фамилия	Фамилия уполномоченного представителя юридического лица (владельца сертификата)
GivenName	Приобретенное имя	Имя и отчество (если имеется) уполномоченного представителя юридического лица (владельца сертификата)
LocalityName, L	Наименование населенного пункта	Город или населенный пункт места нахождения юридического лица
Email, E	Адрес электронной почты	Адрес электронной почты владельца сертификата
OrganizationUnitName, OU	Подразделение организации	Наименование подразделения, сотрудником которого является уполномоченный представитель юридического лица (владелец сертификата)
INN	Идентификационный номер налогоплательщика (ИНН)	ИНН юридического лица
UnstructuredName	Неструктурированное имя	Наименование абонентского пункта юридического лица

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

Пользователь сетевого узла _____ _____
подпись *И.О.Фамилия*

«____» _____ 20____ г.

_____ _____
Должность руководителя *подпись* *И.О.Фамилия*

МП

«____» _____ 20__ г.
дата подписания заявления

ПРИМЕЧАНИЕ:
Приостановление действия сертификата может осуществляться по инициативе Владельца сертификата на период возможного длительного неисполнения обязанностей, связанных с подписанием ЭД.

Приложение №11
к Регламенту

Заявление

на возобновление действия сертификата ключа проверки электронной подписи
Пользователя сетевого узла

_____
(наименование Организации)

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит возобновить действие сертификата ключа проверки электронной подписи своего полномочного представителя – Пользователя сетевого узла _____
(фамилия, имя, отчество)

содержащий следующие идентификационные данные:

Наименование поля	***Описание***	***Значение***
SerialNumber, SN	Серийный номер	Серийный номер сертификата ключа подписи
Common Name, CN	Общее имя	Сокращенное наименование юридического лица
SureName	Фамилия	Фамилия уполномоченного представителя юридического лица (владельца сертификата)
GivenName	Приобретенное имя	Имя и отчество (если имеется) уполномоченного представителя юридического лица (владельца сертификата)
LocalityName, L	Наименование населенного пункта	Город или населенный пункт места нахождения юридического лица
Email, E	Адрес электронной почты	Адрес электронной почты владельца сертификата
OrganizationUnitName, OU	Подразделение организации	Наименование подразделения, сотрудником которого является уполномоченный представитель юридического лица (владелец сертификата)
INN	Идентификационный номер налогоплательщика (ИНН)	ИНН юридического лица
UnstructuredName	Неструктурированное имя	Наименование абонентского пункта юридического лица

_____ _____
Должность руководителя *подпись* *И.О.Фамилия*

МП

«____» _____ 20___ г.
дата подписания заявления

Приложение №12
к Регламенту

Заявление

на подтверждение подлинности электронной подписи Уполномоченного лица УЦ в сертификате ключа проверки электронной подписи

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

Просит подтвердить подлинность электронной подписи Уполномоченного лица удостоверяющего центра в изданном удостоверяющим центром сертификате ключа проверки электронной подписи Пользователя сетевого узла и установить его статус (действует / не действует) на основании предоставленных исходных данных:

1. Файл сертификата ключа проверки подписи на прилагаемом к заявлению внешнем носителе данных;
2. Время[1] (период времени) на момент наступления которого требуется установить статус сертификата: с «_____» по «_____».

_____ _____
Должность руководителя *подпись* *И.О.Фамилия*

МП

«____» _____ 20___ г.
дата подписания заявления

---

[1] *Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром.*

Приложение №13
к Регламенту

Заявление

на подтверждение подлинности электронной подписи в электронном документе

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

Просит подтвердить подлинность электронной подписи в электронном документе и предоставить информацию о статусе сертификата ключа проверки электронной подписи Пользователя сетевого узла (действовал / не действовал):
1. Файл электронного документа на прилагаемом к заявлению внешнем носителе данных;
2. Дата подписания документа электронной подписью: «____» _____ 20___г.»;
3. Значения полей сертификата:

Наименование поля	***Описание***	***Значение***
SerialNumber, SN	Серийный номер	Серийный номер сертификата ключа подписи
Common Name, CN	Общее имя	Сокращенное наименование юридического лица
SureName	Фамилия	Фамилия уполномоченного представителя юридического лица (владельца сертификата)
GivenName	Приобретенное имя	Имя и отчество (если имеется) уполномоченного представителя юридического лица (владельца сертификата)
LocalityName, L	Наименование населенного пункта	Город или населенный пункт места нахождения юридического лица
Email, E	Адрес электронной почты	Адрес электронной почты владельца сертификата
OrganizationUnitName, OU	Подразделение организации	Наименование подразделения, сотрудником которого является уполномоченный представитель юридического лица (владелец сертификата)
INN	Идентификационный номер налогоплательщика (ИНН)	ИНН юридического лица
UnstructuredName	Неструктурированное имя	Наименование абонентского пункта юридического лица

_____ _____
Должность руководителя *подпись* *И.О.Фамилия*

МП

«____» _____ 20__ г.
дата подписания заявления

Приложение №14
к Регламенту

Перечень

объектных идентификаторов (OID), определяющих области применения сертификатов ключей проверки ЭП, создаваемых УЦ

Объектный идентификатор	***Описание***	***Область правоотношений***
Базовые OID		
1.3.6.1.5.5.7.3.2	Проверка подлинности клиента	
1.3.6.1.5.5.7.3.4	Защищенная электронная почта	
Дополнительные OID из ветки OID УЦ		
1.2.643.3.164	Идентификация удостоверяющего центра корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области	Идентификация удостоверяющего центра корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области для организации юридической значимости защищенного обмена электронными документами и взаимодействия информационных систем путем формирования и утверждения перечня объектных идентификаторов областей применения сертификатов ключей проверки ЭП и включения перечня объектных идентификаторов в форму соглашения с пользователями
1.2.643.3.164.1	Уполномоченное лицо УЦКУ	Уполномоченное лицо, наделенное Удостоверяющим центром правом по заверению сертификатов ключей подписей и списков отозванных сертификатов
1.2.643.3.164.2	Пользователь абонентского пункта защищенной сети ViPNet №602	Уполномоченное лицо юридического лица с правом Аутентификации участников защищенной сети, проверки ЭП в ЭД (кроме сертификатов и списков отозванных сертификатов); невозможности отказа от ЭП в ЭД (кроме сертификатов и списков отозванных сертификатов); зашифрования закрытых и секретных ключей; зашифрования данных; согласования ключей
1.2.643.3.164.2.1	Руководитель	Уполномоченное лицо юридического лица с правом первой подписи на основании учредительных документов или доверенности
1.2.643.3.164.2.2	Главный бухгалтер	Уполномоченное лицо юридического лица с правом второй подписи на основании

Приложение № 15
к Регламенту

ЖУРНАЛ
поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации ключевых документов

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. сотрудника органа криптографической защиты, пользователя СКЗИ, производивших подключение (установку)	Дата подключения (установки) и подписи лиц, производивших подключение (установку)	Номера аппаратных средств, в которые установлены лил к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ произведших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Приложение №16
к Регламенту

ПРОТОКОЛ
установления межсетевого взаимодействия
«__» _____ 20___г. г. _____

1. Межсетевое взаимодействие устанавливается между сетями:

Номер сети	Наименование организации
№ _____	
№ _____	

2. Целью установления межсетевого взаимодействия является межсетевое 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 цифровой подписи, были произведены импорты справочников сети № ____ и сети № ___.

8. Смена межсетевых ключей, изменение состава сетевого узла, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствами взаимного экспорта/импорта, о чем администраторы защищенных сетей уведомляют друг друга с помощью программного обеспечения ViPNet 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 №17
к Регламенту

ЖУРНАЛ

учета регистрационных файлов (*лицензий сети*) и межсетевого взаимодействия (*экспорт, импорт*)

Дата	Тип изменяемой информации (лицензия, экспорт, импорт)	Номер и наименование сети, которой касаются изменения	Описание содержания файла несущего изменения	Подпись, фамилия администратора сети VipNet
1	2	3	4	5