Центр инноваций
и информационных
технологий

Федеральная нотариальная палата

УТВЕРЖДЕН
Приказом Директора
Фонда «Центр инноваций
и информационных технологий»
(№ 01-01.4/25 от 23 июня 2025 г.)

РЕГЛАМЕНТ ПОДКЛЮЧЕНИЯ УЧАСТНИКА ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ К ЗАЩИЩЕННОЙ СЕТИ ФОНДА «ЦЕНТР ИННОВАЦИЙ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ» VipNet №4995

МОСКВА

2025

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Авторизованный партнёр	– юридическое лицо имеющее действующие партнёрские обязательства перед Фондом и имеющее право продавать ПАК и ПО для работы с защищённой сетью ViPNet №4995
ЕИС	– единая информационная система нотариата.
ФНП	– Федеральная нотариальная плата, оператор и собственник ЕИС.
Интернет	– информационно-телекоммуникационная сеть «Интернет».
Ключевой дистрибутив	– файл или набор файлов, создаваемых индивидуально для каждого сетевого узла защищенной сети VipNet, содержащий адресные справочники, ключи криптографического преобразования, данные о лицензиях и другие сведения, необходимые для настройки, первичного запуска и последующей работы сетевого узла защищенной сети VipNet, а также перечень разрешенных для взаимодействия сетевых узлов защищенной сети VipNet и порядок взаимодействия с ними
ПАК	– программно-аппаратный комплекс.
ПК	– программный комплекс.
ПО	– программное обеспечение.
РНПК	– резервный набор персональных ключей.
Средство криптографической защиты информации (СКЗИ)	– программно-аппаратный комплекс или программное обеспечение VipNet, сертифицированные ФСБ России на соответствие требованиям по безопасности информации, предъявляемым к средствам криптографической защиты информации.
Участник электронного взаимодействия	– государственные органы, органы местного самоуправления, а также организации, осуществляющие обмен информацией с Фондом в электронной форме.
Фонд	– Фонд «Центр инноваций и информационных технологий».
ViPNet Client	– ПО, реализующее на рабочем месте пользователя или сервере функцию VPN-клиента и межсетевого экрана.
ViPNet Coordinator	– ПАК, выполняющий функции универсального сервера виртуальной защищённой сети ViPNet.
VPN	– технология, позволяющая обеспечить одно или несколько защищенных сетевых соединений (логическую сеть) поверх другой сети.
Компрометация	– утрата доверия к используемому в целях обеспечения безопасности информации ключу.

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Регламент подключения участника электронного взаимодействия к защищенной сети Фонда «Центр Инноваций и информационных технологий» (далее – Фонд) ViPNet №4995 (далее – защищенная сеть ViPNet №4995) разработан во исполнение требований следующих нормативных правовых и локальных актов:

– Основы законодательства Российской Федерации о нотариате;

– Федерального закона от 27.07.2006 № 149–ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказа Федеральной службы безопасности Российской Федерации от 10.07.2014 года № 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»;

– Приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации 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»;

– Модели угроз безопасности информации информационной системы «Единая информационная система нотариата» от 2022 года;

1.2. Настоящий регламент определяет единый для защищенной сети ViPNet №4995 порядок подключения, отключения и эксплуатации СКЗИ.

2. ПОРЯДОК ПОДКЛЮЧЕНИЯ СКЗИ

2.1. Порядок подключения СКЗИ участников электронного взаимодействия к защищённой сети ViPNet №4995 включает в себя следующие этапы:

– приобретение участником электронного взаимодействия за свой счет СКЗИ;

– формирование ответственными лицами Фонда ключевого дистрибутива и передача его уполномоченному представителю компании партнера или уполномоченному представителю участника электронного взаимодействия;

– передача ключевого дистрибутива участнику электронного взаимодействия;

– настройка и подключение СКЗИ участника электронного взаимодействия к защищенной сети ViPNet №4995.

2.2. Запрещается использовать и подключать к защищённой сети ViPNet №4995 СКЗИ, не имеющие действующие сертификаты соответствия ФСБ России по безопасности информации.

2.3. Юридическое лицо – участник информационного взаимодействия должно иметь собственный индивидуальный защищенный канал для взаимодействия с сетью ViPNet №4995.

Запрещается взаимодействовать с сервисами ФНП, через один защищенный канал конкретного юридического лица разными юридическими лицами.

Участник информационного взаимодействия, подключаясь к защищенной сети ViPNet №4995 в соответствии с положениями настоящего Регламента, гарантирует использование индивидуального защищенного канала для взаимодействия с сетью ViPNet №4995 самостоятельно и в своих интересах без предоставления (передачи) какой-либо возможности использования канала другому (другим) юридических и/или иным лицам любой организационно-правовой формы и формы собственности, в том числе вне зависимости от характера правовых и иных взаимоотношений между такими лицами, включая, но не ограничиваясь взаимозависимым (аффилированным) лицам.

В случае выявления (установления) факта использования юридическим и/или иным лицом защищенного канала для взаимодействия с защищённой сетью ViPNet №4995 участника информационного взаимодействия Фонд оставляет за собой право ограничить, приостановить или прекратить возможность взаимодействия соответствующего участника информационного взаимодействия с защищённой сетью ViPNet №4995.

3. ПРИОБРЕТЕНИЕ ПК (ИЛИ ПАК) VIPNET

3.1. Для подключения к защищённой сети ViPNet №4995 участнику электронного взаимодействия необходимо за свой счет приобрести сертифицированный (ФСБ России и ФСТЭК России) СКЗИ класса защищённости не ниже КС1, с лицензией для защищенной сети ViPNet №4995.

3.2. Для приобретения СКЗИ, а также услуг по их сопровождению участнику электронного взаимодействия необходимо обратиться к авторизованному партнеру:

1) ООО «НЕОДАТА», Тел: 8 (499) 753-63-03, Моб. 8 (903) 587-78-72, web-сайт: www.neodata.info, e-mail: 4995@neodata.info.

2) ООО НТЦ «Фобос-НТ», Тел: 8 (4862) 76-03-56, Моб. 8-910-304-45-00, e-mail: minakov@fobos-nt.ru, сайт: www.fobos-nt.ru

4. ФОРМИРОВАНИЕ И ПЕРЕДАЧА КЛЮЧЕВОГО ДИСТРИБУТИВА

4.1. Для формирования ключевого дистрибутива участнику электронного взаимодействия необходимо заполнить и направить авторизованному партнёру заполненную форму заявки на подключение к защищенной сети VipNet №4995 (далее - заявка) (Приложение 1).

4.2. При получении сведений, указанных в п. 4.1, ответственные лица авторизованного партнёра принимают решение о возможности формирования ключевого дистрибутива, посредством направления в Фонд заявки на адрес электронной почты: vipnet@fciit.ru.

В случае если сведения, указанные в п. 4.1, предоставлены не в полном объеме, ответственные лица авторизованного партнёра или Фонда имеют право:

– запросить у участника электронного взаимодействия сведения, необходимые для формирования ключевого дистрибутива;

– отказать в формировании ключевого дистрибутива, до момента предоставления участником электронного взаимодействия сведений, указанных в п. 4.1.

4.3. После поступления в Фонд заявки и обновления лицензии для защищенной сети VipNet №4995 на приобретенное участником электронного взаимодействия СКЗИ, указанное в заявке, ответственные лица Фонда в течение 3 (трех) рабочих дней осуществляют рассмотрение заявки.

4.4. В случае принятия решения о возможности формирования ключевого дистрибутива ответственные лица Фонда:

– формируют ключевой дистрибутив;

– размещают ключевой дистрибутив на оптическом носителе информации;

– помещают оптический носитель с ключевым дистрибутивом в бумажный конверт и запечатывают;

– после изготовления ключевого дистрибутива ответственные лица Фонда направляют сообщение о возможности его получения на указанный в заявке адрес электронной почты участника электронного взаимодействия или представителя авторизованного партнёра;

– передают запечатанный конверт уполномоченному представителю участника электронного взаимодействия или представителю авторизованного партнёра.

4.5. Передача ключевого дистрибутива осуществляется ответственными лицами Фонда на руки руководителю или доверенному лицу участника электронного взаимодействия (при предъявлении им паспорта и доверенности на получение ключевой информации по форме согласно приложению 4 к настоящему Регламенту) в соответствии с действующим законодательством Российской Федерации.

4.6. Выдача ключевого дистрибутива осуществляется ответственными лицами Фонда:

– адрес выдачи: г. Москва, ул. Долгоруковская, д.9;

– время выдачи: рабочие дни с 09:00 до 13.00 и с 14:00 до 17:00 (пятница до 16:45).

Для своевременного получения ключевого дистрибутива необходимо заблаговременно позвонить по телефону +7 (495)730-57-05 доб.: 13-39 или 13-32 и согласовать время прибытия в Фонд.

4.7. Срок хранения невостребованных ключевых дистрибутивов составляет 3 (три) месяца со дня исполнения заявки на подключение. По истечение указанного срока невостребованные ключевые дистрибутивы подлежат уничтожению.

5. НАСТРОЙКА И ПОДКЛЮЧЕНИЕ СКЗИ

5.1. Для подключения к защищенной сети ViPNet №4995 участник электронного взаимодействия самостоятельно осуществляет первичную настройку СКЗИ согласно инструкциям производителя, размещенным в сети Интернет по адресу: https://infotecs.ru.

6. ТЕХНИЧЕСКОЕ СОПРОВОЖДЕНИЕ И ЭКСПЛУТАЦИЯ

6.1. При подключении СКЗИ участника электронного взаимодействия к защищенной сети ViPNet №4995 Фонд оказывает техническое сопровождение ТОЛЬКО защищённого канала на безвозмездной основе.

В рамках технического сопровождения защищённого канала Фонд не оказывает следующие услуги:

– монтаж и коммутацию оборудования;

– техническую поддержку оборудования VipNet;

– иные мероприятия по сопровождению, требующие непосредственного доступа к оборудованию.

6.2. Фонд НЕ НЕСЕТ ответственности за:

– правильность эксплуатации СКЗИ участником информационного взаимодействия;

– достоверность передаваемой участником информационного взаимодействия посредством СКЗИ информации;

– своевременность передачи участником информационного взаимодействия посредством СКЗИ информации;

– обеспечение конфиденциальности, передаваемой участником информационного взаимодействия посредством СКЗИ информации, в случае неправильной настройки участником информационного взаимодействия СКЗИ или нарушения требований эксплуатационной документации на СКЗИ.

6.3. Участник электронного взаимодействия НЕСЕТ ответственность за:

– полноту и достоверность информации, представленной в заявке;

– соблюдение требований по учету, хранению и обращению в отношении принадлежащих ему СКЗИ и ключевого дистрибутива к ним (в том числе места эксплуатации СКЗИ по адресу, указанному в заявке);

– администрирование и сопровождение принадлежащих ему СКЗИ;

– поддержание в актуальном состоянии принадлежащих ему СКЗИ, в том числе обновление до актуальной версии программного обеспечения и обновление аппаратных платформ по рекомендации производителя;

– своевременное отключение от защищенной сети ViPNet №4995 принадлежащих ему СКЗИ на которые истек срок действия сертификата соответствия ФСБ России на соответствие требованиям по безопасности информации;

– несанкционированное подключение защищаемых с использованием сетевых узлов защищенной сети VipNet №4995 сегментов локальной вычислительной сети к открытым каналам связи;

– своевременное оповещение Фонда об изменении условий эксплуатации, принадлежащих ему СКЗИ, об изменении контактов лиц ответственных за эксплуатацию СКЗИ, наименования участника электронного взаимодействия, в том числе в связи с его реорганизацией, как юридического лица, об изменении адреса места эксплуатации СКЗИ, а также о ремонте и об обновлении СКЗИ;

– достоверность передаваемой посредством СКЗИ информации;

– своевременную передачу посредством СКЗИ информации.

6.4. Участник электронного взаимодействия обязуется не предпринимать попытки взлома, заражения вредоносными программным обеспечением и иных противоправных действий в отношении сетевых узлов защищенной сети VipNet №4995 и подключенных к ним средств вычислительной техники.

6.5. По вопросам получения технического сопровождения, эксплуатируемого участником электронного взаимодействия СКЗИ в защищенной сети VipNet №4995, необходимо обратиться к авторизованному партнёру, реализовавшему сертификат технической поддержки.

6.6. По вопросам технического сопровождения защищенного канала связи необходимо обращаться в Фонд по адресу: vipnet@fciit.ru.

7. ПОРЯДОК ПЛАНОВОЙ СМЕНЫ МАСТЕР-КЛЮЧЕЙ

7.1. Плановая смена мастер-ключей в защищенной сети VipNet №4995 осуществляется Фондом в соответствии с требованиями эксплуатационно-технической документации на СКЗИ и рекомендациями производителя с периодичностью не реже одного раза в 15 месяцев.

7.2. Плановая смена мастер-ключей в защищенной сети VipNet №4995 проводится в IV квартале каждого года. Период смены мастер-ключей может быть изменен. Информация о точном периоде проведения плановой смены мастер-ключей в защищенной сети VipNet №4995 размещается не позднее чем за 2 (два) месяца до даты начала смены мастер-ключей:

– на официальном сайте Фонда в сети Интернет https://fciit.ru в разделе «Новости»;

– в официальном письме фонда, направленном на адреса электронных почт участников электронного взаимодействия, указанных в заявках на подключение к защищенной сети VipNet №4995.

7.3. В целях минимизации рисков потери доступа к защищенной сети VipNet №4995, в период плановой смены мастер-ключей, для её успешного проведения участнику электронного взаимодействия, при эксплуатации принадлежащего ему СКЗИ необходимо выполнить следующие условия:

7.3.1. При эксплуатации ПАК VipNet Coordinator HW.

7.3.1.1. Иметь в наличии актуальный сертификат активации сервиса прямой или совместной технической поддержки производителя, на принадлежащий ему ПАК VipNet Coordinator HW уровня «Расширенный»;

7.3.1.2. Иметь в наличии (актуальную) поддерживаемую производителем аппаратную платформу ПАК VipNet Coordinator HW. Информация об актуальных версиях поддерживаемых аппаратных платформ размещена в сети Интернет на сайте производителя https://infotecs.ru.

В случае если аппаратная платформа, эксплуатируемого ПАК VipNet Coordinator HW, не поддерживается необходимо обратиться к авторизованному партнёру, указанному в пункте 3 настоящего регламента, осуществившего его поставку, для:

1) приобретения нового ПАК VipNet Coordinator HW, в состав которого входит актуальная аппаратная платформа;

2) модернизации текущей аппаратной платформы, входящей в состав эксплуатируемого ПАК VipNet Coordinator HW (при наличии такой возможности у производителя).

После получения от авторизованного партнёра, указанного в пункте 3 настоящего регламента, нового или модернизированного ПАК VipNet Coordinator HW и поступления в Фонд обновления лицензии для защищенной сети VipNet №4995 на него, необходимо обратиться в Фонд по адресу электронной почты: vipnet@fciit.ru для выпуска и получения ключевого дистрибутива. Получение ключевого дистрибутива осуществляется в соответствии с пунктом 4 настоящего регламента.

7.3.1.3. Иметь в наличии установленную последнюю, сертифицированную версию программного обеспечения на ПАК VipNet Coordinator HW. Информация о сертифицированной версии программного обеспечения размещена в сети Интернет на сайте производителя https://infotecs.ru.

В случае если текущая версия установленного программного обеспечения на ПАК VipNet Coordinator HW не соответствует рекомендованной производителем, необходимо обратиться необходимо обратиться к авторизованному партнёру, указанному в пункте 3 настоящего регламента, для ее приобретения и последующего обновления.

7.3.1.4. Обеспечить наличие РНПК на ПАК VipNet Coordinator HW.

7.3.2. При эксплуатации ПО VipNet Client.

7.3.2.1. Иметь в наличии установленную последнюю сертифицированную версию программного обеспечения на ПО VipNet Client. Информация о последней сертифицированной версии программного обеспечения размещена в сети Интернет на сайте производителя https://infotecs.ru.

В случае если текущая версия установленного программного обеспечения на ПО VipNet Client не соответствует версии, рекомендованной производителем, необходимо обратится к авторизованному партнёру, указанному в пункте 3 настоящего регламента для ее приобретения и последующего обновления.

7.3.2.2. Обеспечить наличие файла с РНПК на сервере с установленным ПО VipNet Client.

7.3.3. В случае отсутствия РНПК необходимо обратиться в Фонд по адресу электронной почты: vipnet@fciit.ru для его выпуска и получения. Получение РНПК осуществляется в соответствие с п.4 настоящего регламента.

7.3.4. Обеспечить доступность ПАК VipNet Coordinator HW или сетевого узла с установленным ПО VipNet Client в течение всего периода смены мастер-ключей в рабочие дни с 09:00 до 18:00 по Московскому времени. В случае подключения к защищенной сети VipNet №4995 с использованием кластера горячего резервирования обеспечить доступность обеих нод кластера.

7.3.5. После успешной смены мастер-ключей шифрование информации будет осуществляться на новых мастер-ключах.

7.3.6. Если после смены мастер-ключей доступ сетевого узла участника электронного взаимодействия к защищенной сети VipNet №4995 потерян, необходимо обратиться в Фонд по адресу электронной почты: vipnet@fciit.ru для выпуска и получения нового ключевого дистрибутива.

Получение ключевого дистрибутива осуществляется в соответствии с пунктом 4 настоящего регламента.

8. ПОРЯДОК ОБНОВЛЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ

8.1. Для обновления ключевой информации, с целью минимизации рисков отказа в работе принадлежащего участнику электронного взаимодействия СКЗИ, необходимо иметь действующий сертификат активации сервиса прямой или совместной технической поддержки производителя на принадлежащее ему СКЗИ.

Участник электронного взаимодействия обращается в Фонд (по адресу электронной почты: vipnet@fciit.ru) и в письменной форме сообщает о своём желании произвести замену ключевой информации. К письму необходимо приложить заполненную форму заявки на обновление ключевой информации участника электронного взаимодействия защищенной сети ViPNet №4995 (Приложение 2).

8.2. Срок рассмотрения заявки составляет 3 (три) рабочих дня с момента подачи. При положительном решении Администратор сети ViPNet №4995 связывается с контактным лицом участника электронного взаимодействия и согласовывает технологическое окно для проведения работ по замене ключевой информации.

8.3. Участникам электронного взаимодействия, эксплуатирующим для подключения к защищенной сети VipNet №4995 программный комплекс, необходимо помимо заявки сформировать на рабочем месте запрос на обновление ключевой информации согласно инструкциям производителя, размещенным в сети Интернет по адресу: https://infotecs.ru.

8.4. Для участников электронного взаимодействия, эксплуатирующих для подключения к защищенной сети ViPNet №4995 программно-аппаратный комплекс, замена ключевой информации инициируется Администратором сети ViPNet №4995.

9. ПОРЯДОК ОБНОВЛЕНИЯ СЕРТИФИКАТА ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

9.1. Для обновления сертификата технической поддержки участнику электронного взаимодействия необходимо обратиться к авторизованному партнёру, указанному в пункте 3 настоящего Регламента.

10. ПОРЯДОК ОТКЛЮЧЕНИЯ ОТ ЗАЩИЩЕННОЙ СЕТИ ФОНДА «ЦЕНТР ИННОВАЦИЙ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ» VIPNET №4995

10.1. Участники электронного взаимодействия, которые не производили ни одного подключения к инфраструктуре Фонда через защищенный канал ViPNet сети №4995 (бездействовали) на протяжении 3 (трех) месяцев и более будут отключены.

Для возобновления доступа необходимо предоставить заполненную анкету, содержащую актуальную информацию, и получить вновь сформированный ключевой дистрибутив согласно пункту 4 настоящего Регламента

11. ПОРЯДОК ДЕЙСТВИЙ ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕВОЙ ИНФОРМАЦИИ

11.1. Ключевая информация пользователя ViPNet-сети №4995 может считаться скомпрометированной в следующих случаях:

– посторонним лицам мог стать доступным файл ключевого дистрибутива;

– посторонним лицам мог стать доступным съемный носитель с паролем доступа к ключевой информации;

– посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящийся на компьютере;

– уволился пользователь, имевший доступ к ключевой информации.

11.2. В случае компрометации ключевой информации участник электронного взаимодействия обязан прекратить работу на своём узле и незамедлительно сообщить об этом в порядке, установленном в Приложении 3 к настоящему Регламенту.

Приложение 1.

ЗАЯВКА НА ПОДКЛЮЧЕНИЕ К СЕТИ №4995

АНКЕТА УЧАСТНИКА ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ

ИНФОРМАЦИЯ О ПОЛЬЗОВАТЕЛЕ ЗАЩИЩЕННОЙ СЕТИ VIPNET №4995			
1.	**Полное наименование** (в соответствии с учредительными документами)		
2.	**Сокращенное наименование** (в соответствии с учредительными документами)		
3.	**Адрес в пределах места нахождения** (в соответствии ЕГРЮЛ)		
4.	**Фактический адрес** (адрес эксплуатации СКЗИ):		
5.	**ИНН**		
6.	**ОГРН**		
7.	**Телефон:**		
8.	**Адрес электронной почты** (для отправки официальных уведомлений в части работы сети №4995)		
9.	**Контакты технического специалиста, осуществляющего установку СКЗИ**	**Должность**	
		Ф.И.О.	
		№телефона	
		Адрес электронной почты	
10.	**Контакты технического специалиста, ответственного за эксплуатацию СКЗИ**	**Должность**	
		Ф.И.О.	
		№телефона	
		Адрес электронной почты	
11.	**Выбранный продукт ViPNet (ПК/ПАК)** (указывать вместе с сертификатами технической поддержки)		
12.	**Использование режима кластера горячего резервирования (для ПАК)*** (при использовании ПАК VipNet Coordinator)		
13.	**Количество (шт.)**		

ВСЕ ПОЛЯ ОБЯЗАТЕЛЬНЫ ДЛЯ ЗАПОЛНЕНИЯ!

*для создания кластера на VipNet Coordinator HW 100, HW 50, HW 10 необходимо дополнительно приобретать отдельную роль **failover 100**

Схемы взаимодействия Фонда с участниками электронного взаимодействия

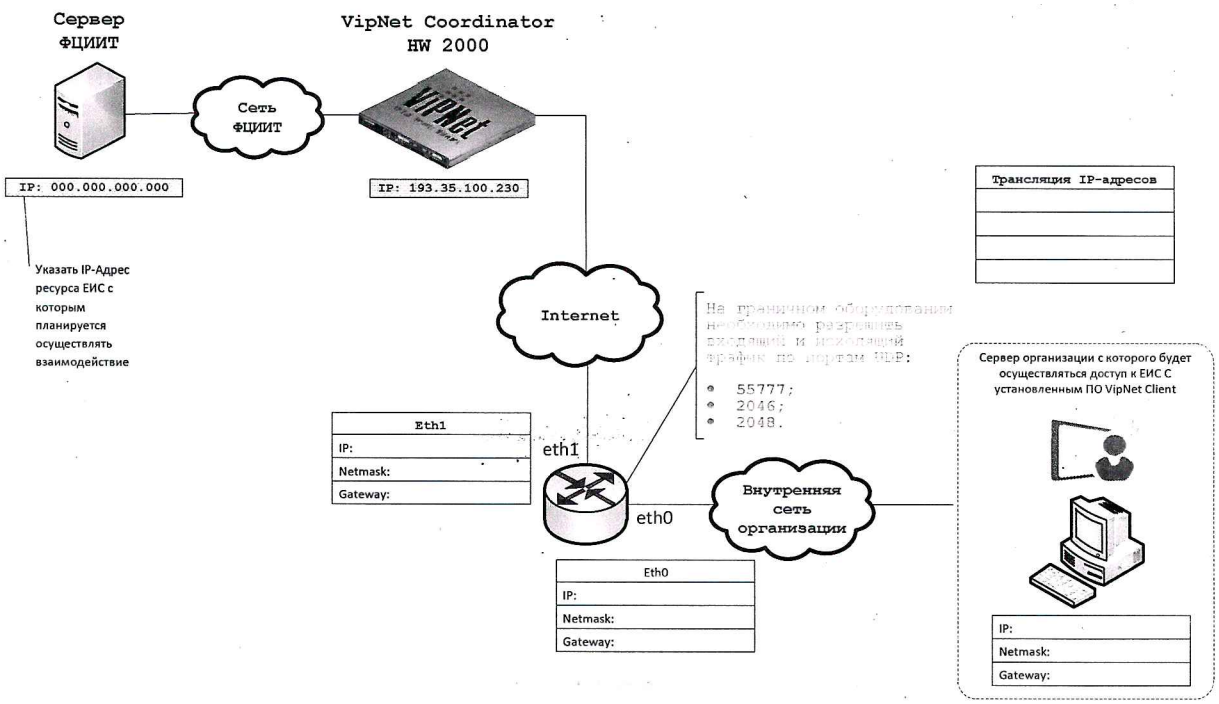
1) Схема взаимодействия при подключении программно-аппаратного комплекса

	IP	Mask:	GW:
**Eth1:	000.000.000.000	000.000.000.000	000.000.000.000
***Eth0:	000.000.000.000	000.000.000.000	000.000.000.000
Сервер организации с которого будет осуществляться доступ к ЕИС	000.000.000.000 000.000.000.001 000.000.000.002 Допускается указывать не более 3(трёх) ip-адресов	000.000.000.000 000.000.000.000 000.000.000.000	000.000.000.000 000.000.000.000 000.000.000.000

**Eth1 – внешний IP адрес организации (статический)
***Eth0 – внутренняя сеть организации

2) Схема взаимодействия при подключении программного комплекса

ЭЛЕКТРОННОЕ ВЗАИМОДЕЙСТВИЕ ПРИ ИСПОЛЬЗОВАНИИ ПО VipNet Client



	IP	Mask:	GW:
**Eth1:	000.000.000.000	000.000.000.000	000.000.000.000
***Eth0:	000.000.000.000	000.000.000.000	000.000.000.000
Сервер организации с которого будет осуществляться доступ к ЕИС	000.000.000.000	000.000.000.000	000.000.000.000

**Eth1 – внешний IP адрес организации (статический)
***Eth0 – внутренняя сеть организации

Приложение 2

ЗАЯВКА
на обновление ключевой информации участника электронного взаимодействия сети ViPNet №4995

1.	Полное наименование организации	
2.	ИНН	
3.	Телефон:	
4.	ID сетевого узла	
5.	Эксплуатируемый продукт ViPNet (ПК/ПАК)	
6.	Количество (шт.)	
7.	ФИО и контакты технического специалиста, осуществляющего обслуживание СКЗИ	

КОМПРОМЕТАЦИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЯ.

В случае компрометации ключевой информации пользователя участнику электронного взаимодействия необходимо:

1. Незамедлительно прекратить работу на своём узле и обратиться в Фонд (по адресу электронной почты: vipnet@fciit.ru) и в письменной форме сообщить об этом.

В письме необходимо указать:

– Тема – **Компрометация ключевой информации** ;

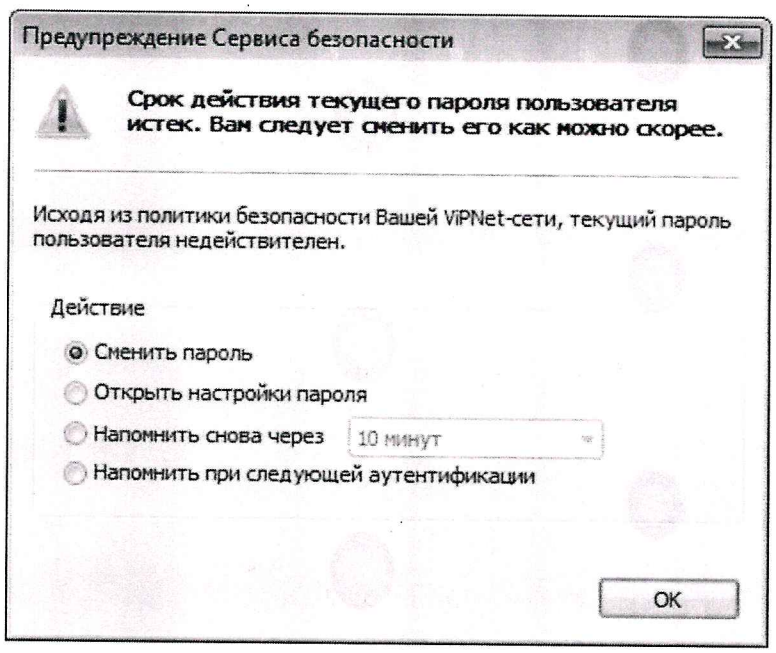
– Идентификатор узла в формате 0xAAAABBBB;

– Контактные данные для связи (номер стационарного или мобильного телефона)

2. Сотрудники Фонда, ответственные за подключение к защищенной сети VipNet №4995 производят необходимые работы по замене ключей, после которых на компьютере пользователя будет произведен перезапуск ПО ViPNet Client.

3. На ПК пользователя в ПО ViPNet Client появится диалоговое окно, в котором участнику электронного взаимодействия необходимо будет указать путь до РНПК (Путь по умолчанию: *C:\ProgramData\Infotecs\<идентификатор сетевого узла в формате AAAABBBB >\d_station\abn_XXXX\XXXX.pk*) и ввести пароль пользователя.

4. После успешного обновления на узле, появится диалоговое окно с информацией о том, что текущий пароль истёк и его следует сменить. Для смены пароля необходимо выбрать пункт «Открыть настройки пароля» и установить новый пароль (рис. 1).



(рис.1)

В случае, если файл РНПК отсутствует на компьютере, необходимо запросить новый дистрибутив с ключевой информацией в Фонде.

Приложение 4

ДОВЕРЕННОСТЬ
на выполнение действий от лица организации
№

г. _____ « _____ » _____ 20 ____ г.
(место) *(число)* *(месяц)* *(год)*

_____
(дата прописью)

Настоящей доверенностью _____

_____
(полное и сокращенное наименование организации)

ИНН _____ ОГРН _____
(номер ИНН) (номер ОГРН)

местонахождение _____

_____
(адрес организации в соответствии с учредительными документами)

в лице _____
(должность руководителя организации)

_____
(Ф.И.О. руководителя организации)

действующего на основании _____
(номер и дата документа)

уполномочивает _____
(должность и Ф.И.О. уполномоченного лица)

_____
(должность и Ф.И.О. уполномоченного лица)

паспорт гражданина РФ _____ _____ выдан _____ г.
(серия) (номер) (дата выдачи)

_____

_____
(наименование органа, выдавшего документ, код подразделения)

Совершать следующие действия:

1. Получать в «Фонде центр инноваций и информационных технологий» дистрибутивы ключей для защищенной сети VipNet №4995.

2. Расписываться в соответствующих учетных формах, предназначенных для исполнения поручения, определённого настоящей доверенностью

Настоящая доверенность выдана без права передоверия и действительна по _____
(срок действия доверенности)

Собственноручную подпись _____ _____ удостоверяю.
(подпись) (Ф.И.О. уполномоченного лица)

_____ _____ _____
(должность руководителя) (подпись руководителя) (Ф.И.О. руководителя)

М.П.