ТЕРРИТОРИАЛЬНЫЙ ФОНД
ОБЯЗАТЕЛЬНОГО МЕДИЦИНСКОГО СТРАХОВАНИЯ
ИРКУТСКОЙ ОБЛАСТИ

ПРИКАЗ

от 23.10.2026г. № 150

О внесении изменений в
Регламент Центра
администрирования сети ViPNet
№ 559 Территориального фонда
обязательного медицинского
страхования Иркутской области

Руководствуясь пунктом 1.6 Регламента Центра администрирования сети ViPNet № 559 Территориального фонда обязательного медицинского страхования Иркутской области, утвержденного ТФОМС Иркутской области 26.12.2023 года, пунктом 2.1 Соглашения о присоединении к Регламенту Центра администрирования сети ViPNet Территориального фонда обязательного медицинского страхования Иркутской области для организации защищенного обмена электронными документами и взаимодействия информационных систем,

п р и к а з ы в а ю:

1. Внести следующие изменения в Регламент Центра администрирования сети ViPNet № 559 Территориального фонда обязательного медицинского страхования Иркутской области, утвержденный Фондом 26.12.2023 года (далее – Регламент):

1.1. Пункт 8.3 Содержания Регламента дополнить новыми предложениями следующего содержания:

«Приложение № 7. Регламент смены мастер-ключей сети ViPNet № 559 ТФОМС Иркутской области для администратора безопасности

Приложение № 8. Порядок оповещения при компрометации ключей пользователя, ключей узла сетевого узла сети ViPNet № 559 ТФОМС Иркутской области».

1.2. В пункте 2.1 Регламента слова, следующие за текстом «Факс: 8 (3952) 34-16-58» исключить.

1.3. В пункте 2.5 Регламента первый абзац, включающий два дефиса, изложить в следующей редакции:

«В целях обеспечения функционирования Центра администрирования сети ViPNet № 559 Фонд к оказанию услуг администрирования сети ViPNet № 559 привлекает лиц, имеющих лицензии на оказание (выполнение) соответствующих услуг (работ) в рамках деятельности по технической защите конфиденциальной информации (Постановление Правительства РФ от 03.02.2012 г. № 79), в рамках

деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (Постановление Правительства РФ от 16.04.2012 г. № 313).».

1.4. В пункте 5.5. Регламента третий абзац изложить в новой редакции:

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

- при личном обращении к Администратору ЦАС ViPNet;
- по доверенному каналу с использованием СКЗИ ViPNet с использованием сервиса - «Деловая почта» ViPNet или встроенного механизма рассылки ключевой информации ViPNet;
- иным доверенным способом, согласно Правилам пользование продуктами ViPNet.».

1.5. Пункт 8.3. Регламента дополнить новыми абзацами следующего содержания:

«**Организационно-распорядительные документы:**

Неотъемлемой частью Регламента являются:

- Регламент смены мастер-ключей сети ViPNet № 559 ТФОМС Иркутской области для администратора безопасности (Приложение № 7 к Регламенту),
- Порядок оповещения при компрометации ключей пользователя, ключей узла сетевого узла сети ViPNet № 559 ТФОМС Иркутской области (Приложение № 8 к Регламенту).

Условия Приложения № 7 и Приложения № 8 к Регламенту подлежат исполнению Пользователем – Стороной, подписавшей Соглашение о присоединении к Регламенту Центра администрирования сети ViPNet Территориального фонда обязательного медицинского страхования Иркутской области для организации защищенного обмена электронными документами и взаимодействия информационных систем.

Руководителем или иным уполномоченным лицом Пользователя:

- утверждаются указанные организационно-распорядительные документы,
- назначается администратор безопасности.

1.6. Дополнить Регламент Приложением № 7 - Регламент смены мастер-ключей сети ViPNet № 559 ТФОМС Иркутской области для администратора безопасности (прилагается).

1.7. Дополнить Регламент Приложением № 8 - Порядок оповещения при компрометации ключей пользователя, ключей узла сетевого узла сети ViPNet № 559 ТФОМС Иркутской области (прилагается).

2. Пункт 1 настоящего приказа вступает в силу через 10 дней после даты размещения настоящего приказа на сайте www.irkoms.ru.

3. Начальнику отдела информационной безопасности ТФОМС Иркутской области – Ягомост А.С. обеспечить:

- размещение настоящего приказа на сайте www.irkoms.ru не позднее трех рабочих дней после дня его принятия;

- не позднее дня вступления в силу настоящего приказа известить Пользователей, подписавших Соглашение о присоединении к Регламенту Центра администрирования сети ViPNet Территориального фонда обязательного медицинского страхования Иркутской области для организации защищенного обмена электронными документами и взаимодействия информационных систем, о внесении изменений в Регламент.

Заместитель директора В.Ф. Вобликова

ПРИЛОЖЕНИЕ № 7

РЕГЛАМЕНТ

смены мастер-ключей сети ViPNet №559
ТФОМС Иркутской области для администратора безопасности

1. Общие Положения

Настоящий регламент устанавливает порядок смены мастер-ключей в сети ViPNet №559 ТФОМС Иркутской области для администратора безопасности.

Администратор безопасности – лицо, выполняющее функции администрирования средств защиты информации на автоматизированном рабочем месте.

Настоящий Регламент разработан исходя из положений документа «ViPNet Administrator 4 Руководство по смене мастер-ключей в сети ViPNet» Версия продукта: 4.x.

Настоящий Регламент доводится до администратора безопасности АРМ под подпись.

Регламент предназначен для администратора безопасности автоматизированных рабочих мест, на которых проходит смена мастер-ключей сети ViPNet №559 ТФОМС Иркутской области.

2. Определения и термины

ViPNet Administrator - 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. Предназначена для формирования и обновления ключей сетевых узлов ViPNet, а также для управления сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС) - 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 Удостоверяющего и ключевого центра;
- задание полномочий пользователей сетевых узлов ViPNet.

Администратор сети ViPNet - лицо, 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.

Администратор УКЦ - лицо, обладающее правом доступа к программе ViPNet Удостоверяющий и ключевой центр (УКЦ), отвечающее за создание ключей для сетевых узлов ViPNet, создание и обслуживание сертификатов ViPNet, обеспечение взаимодействия с доверенными сетями ViPNet. В сети ViPNet №559 ТФОМС Иркутской области администратор УКЦ это уполномоченное лицо, согласно Регламенту Центра администрирования сети ViPNet № 559 Территориального фонда обязательного медицинского страхования Иркутской области.

Ключ защиты - ключ, на котором шифруется другой ключ.

Ключ обмена - симметричный ключ, известный отправителю и получателю зашифрованной информации, которой обмениваются сетевые узлы ViPNet. Используется для зашифрования и расшифрования передаваемых данных.

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.

Ключи узла ViPNet - совокупность ключей, с использованием которых производится шифрование трафика, служебной информации и писем программы ViPNet Деловая почта.

Мастер-ключ - ключ, который администратор сети ViPNet использует для формирования симметричных ключей пользователей и узлов. В сети ViPNet формируется три вида мастер-ключей:

- мастер-ключ ключей обмена;
- мастер-ключ ключей защиты ключей обмена;
- мастер-ключ персональных ключей пользователей.

Мастер-ключ формируется с помощью датчика случайных чисел. Он хранится в программе ViPNet Удостоверяющий и ключевой центр в полной секретности, поскольку компрометация мастер-ключа приводит к компрометации всех ключей, сформированных на его основе.

Пароль пользователя - индивидуальный пароль пользователя для работы в приложениях ViPNet на сетевом узле ViPNet. Первоначально создается администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager. Этот пароль может быть изменен пользователем на сетевом узле ViPNet.

Полномочия пользователя - разрешения на определенные действия пользователей на сетевом узле ViPNet по изменению настроек некоторых программ ViPNet.

Администратор ЦУСа задает полномочия для всех пользователей сетевого узла ViPNet в свойствах ролей.

Пользователь ViPNet - лицо, которое использует программное обеспечение ViPNet и имеет ключи для работы с ним.

Резервный набор персональных ключей (РНПК) - набор из нескольких запасных персональных ключей, которые администратор УКЦ создает для пользователя. Имя

этого файла имеет маску AAAA.pk, где AAAA — идентификатор пользователя ViPNet в рамках своей сети. Используется для удаленного обновления ключей пользователя при их компрометации и при смене мастер-ключа персональных ключей.

Сетевой узел ViPNet - узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в управляющем ПО.

Сеть ViPNet - логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищенных узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Справочники и ключи - справочники, ключи узла и ключи пользователя.

3. Порядок действий

До смены мастер-ключей прочитайте настоящий Регламент полностью. При необходимости (будет описано в письме от администратора УКЦ), могут потребоваться действия, описанные в разделах: Предварительные действия на ViPNet Coordinator HW, Проверка наличия РНПК на сетевых узлах, возможные неполадки.

Смена мастер-ключей не влияет на межсетевые мастер-ключи. Для успешной смены мастер-ключей в сети ViPNet выполните все действия из приведенного ниже списка в указанной последовательности:

1. Необходимо получить письмо по Деловой почте от администратора УКЦ о предстоящей смене мастер-ключей с указанием периода смены мастер-ключей. Необходимо организовать наличие РНПК в соответствующей директории.

Способы организовать наличие РНПК:

– Необходимо получить РНПК от администратора УКЦ по доверенному каналу для всех узлов ViPNet;

– Заранее сохраненный РНПК необходимо переместить в соответствующую директорию, следуя правилам работы с РНПК.

Правила работы с РНПК! РНПК представляет собой файл с расширением *.pk. После первичной установки дистрибутивов ключей на сетевой узел, РНПК как правило находятся по адресам:

C:\Program Files (x86)\InfoTeCS\ViPNet Client или C:\ProgramData\InfoTeCS\ViPNet Client:

– \d_station\abn_AAAA.
– \user_AAAA\key_disk\dom.

После развертывания дистрибутива ключей *.dst на сетевом узле РНПК необходимо переместить на учтенный носитель (либо удалить РНПК) и в период смены мастер-ключей переместить в соответствующую директорию обратно. Сразу после удачной смены мастер-ключей также необходимо проконтролировать отсутствие РНПК, переместив его на учтенный носитель информации (либо удалить РНПК).

4. Предварительные действия на ViPNet Coordinator HW

До смены мастер-ключей в сети на ViPNet Coordinator HW необходимо выполнить:

– Соответствие паролей пользователей в УКЦ и на координаторе:

Если РНПК зашифрован на парольном ключе пользователя (выгружен вручную в файл и размещен на узле), то пароли в УКЦ и на координаторе должны совпадать. Поэтому необходимо убедиться, что для аутентификации пользователя на координаторе используется тот же пароль, что задан в УКЦ для пользователя узла. Если пароли не совпадают, то на координаторе для пользователя user необходимо задать тот же пароль, который задан в УКЦ. Измените пароль с помощью команды admin passwd.

- Установить актуальное ПО:

Для корректной смены мастер-ключей на координаторах должно быть установлено ПО последних версий. Обновите ПО до версии 4.3.2 (или 4.5.2) и выше. Обновление до 4.5.2 и выше возможно с версий не ниже 4.3.2 (4.3.3 для виртуализированного исполнения). Если вы обновляете ПО с более ранних версий, сначала обновите ПО до версии 4.3.2 (4.3.3).

См. «ViPNet Coordinator HW 4. Настройка с помощью командного интерпретатора», раздел «Обновление программного обеспечения».

- Провести проверку отсутствия не применившихся обновлений ключей:
  - Перейдите в режим администратора с помощью команды enable.
  - Перейдите в командную оболочку с помощью команды admin escape.
  - Введите команду: find /opt/vipnet/ccc/ -name "k*.*"

Если в командной строке появятся пути к файлам, это значит, что на вашем координаторе есть неприменившиеся обновления ключей. Чтобы исправить ситуацию, из ЦУСа заново отправьте справочники и ключи на координатор, и дождитесь, когда они примут статус Приняты. Затем повторите команду из предыдущего пункта для проверки успешности обновления.

- Обновление ПО на координаторах из кластера горячего резервирования:

При смене мастер-ключей для координаторов в кластере горячего резервирования изменения применяются только на активном узле кластера. На пассивном узле изменения применяются при последующем перезапуске службы mftp или при смене состояния кластера.

Поэтому после смены мастер-ключей может возникнуть ошибка удаленного обновления ПО на координаторах в кластере, если состояние кластера не менялось перед попыткой обновления ПО.

Для устранения ошибки удаленного обновления ПО после смены мастер-ключей, перезагрузите пассивный узел кластера горячего резервирования или перезапустите службу mftp на пассивном узле кластера, выполнив команды: #mftp stop #mftp start

- Создание резервной копии конфигурации координатора:

Для этого создайте частичную резервную копию, в которую не входят справочники и ключи.

После смены мастер-ключей и приема обновленных справочников и ключей отсутствует необходимость в информации о старых справочниках и ключах.

Чтобы создать копию текущей конфигурации координатора, используйте команду admin config save.

В случае непредвиденного сбоя вы сможете восстановить конфигурацию координатора с помощью сохраненной копии. После успешного обновления ключей на узле вы можете удалить созданные копии конфигурации.

5. Проверка наличия РНПК на сетевых узлах

РНПК предназначен для получения обновлений ключей при смене мастер-ключа персональных ключей и содержится в файле AAAA.pk, где <AAAA> — шестнадцатеричный номер пользователя в сети ViPNet. Поэтому перед сменой мастер-ключа персональных ключей необходимо обеспечить наличие РНПК на узлах.

ViPNet Coordinator HW. На ViPNet Coordinator HW можно проверить наличие РНПК, с помощью команды iplir show key-info:

– Если в выводе команды в секции Spare personals keys set info будет информация о ключах, это значит, что на координаторе есть РНПК.

– Также в выводе команды просмотрите дату создания мастер-ключей для параметра Master personal key date и проверьте, что она совпадает с датой последней смены мастер-ключей.

– Убедитесь, что идентификатор пользователя User ID совпадает для персональных ключей пользователя и для РНПК — в секциях Current personal key info и Spare personals keys set info соответственно.

Если на ViPNet Coordinator HW отсутствует РНПК, добавьте РНПК на сетевой узел:

1. В УКЦ сохраните РНПК сетевого узла в файл и скопируйте его на USB-носитель.
2. Войдите в режим администратора и импортируйте РНПК с USB-носителя с помощью команды: admin add spare keys

ViPNet Client for Windows. На компьютерах пользователей обеспечьте наличие файла РНПК *.pk по следующему пути в папке с названием продукта ViPNet, например в
C:\Program Files (x86)\InfoTeCS\ViPNet Client или C:\ProgramData\InfoTeCS\ViPNet Client:

– \d_station\abn_AAAA.

– \user_AAAA\key_disk\dom. Если файл *.pk расположен в этой папке, скопируйте файл в папку, указанную выше.

При необходимости создайте РНПК в УКЦ и передайте их на узлы пользователей.

6. Возможные неполадки

Не найдены или неверно указаны данные для аутентификации пользователя или запрошен пароль от РНПК. После смены мастер-ключей пароль пользователя не подходит при входе в программу ViPNet Монитор, а также при запросе пароля от РНПК. Это происходит, если пользователь ViPNet Client for Windows сменил пароль локально на узле, или если в УКЦ для пользователя была смена пароля после установки дистрибутива ключей на сетевом узле. Чтобы устранить неполадку, пользователю необходимо ввести пароль, выданный ему при последней установке дистрибутива ключей на узле. Чаще всего это пароль, заданный в УКЦ при выдаче пользователю первого дистрибутива ключей для развертывания сетевого узла. В случае если этот пароль забыт пользователем, выдайте новый дистрибутив ключей и установите его на узле пользователя.

На сетевом узле не найден РНПК. После обновления мастер-ключей при первом запуске программы ViPNet Монитор из состава ViPNet Client for Windows у пользователя может появиться сообщение об отсутствии файла РНПК на сетевом узле.

Чтобы устранить проблему:

1. Передайте пользователю РНПК, созданный до смены мастер-ключей. Убедитесь, что файл РНПК предназначен для данного пользователя. Для этого сравните идентификатор пользователя с идентификатором пользователя, используемого в названии файла РНПК, они должны совпадать.

2. Пользователю необходимо разместить файл РНПК AAAA.pk в папке \d_station\abn_AAAA, где <AAAA> — шестнадцатеричный идентификатор пользователя в сети ViPNet.

Ошибка отправки письма в программе ViPNet Деловая почта. После смены мастер-ключей в сети ViPNet на узле пользователя с программой ViPNet Деловая почта при попытке отправить письмо с электронной подписью появляется сообщение «Ключ не найден».

Для решения проблемы пользователю необходимо выбрать текущий сертификат, выпущенный вместе с новыми ключами. Как правило, это сертификат с самой поздней датой выпуска.

ПРИЛОЖЕНИЕ № 8

Порядок
оповещения при компрометации ключей пользователя,
ключей узла сетевого узла сети ViPNet №559 ТФОМС Иркутской области

1. Общие Положения

Настоящий Порядок оповещения при компрометации ключей пользователя, ключей узла сетевого узла сети ViPNet №559 ТФОМС Иркутской области устанавливает порядок оповещения при компрометации ключей пользователя, ключей узла или парольной информации сетевого узла ViPNet №559 ТФОМС Иркутской области для пользователей сети ViPNet №559 ТФОМС Иркутской области.

Пользователь сети ViPNet №559 ТФОМС Иркутской области (далее пользователь) - лицо, которое использует программное обеспечение ViPNet и имеет ключи для работы с ним.

Настоящий Порядок разработана исходя из положений ViPNet Удостоверяющий и ключевой центр 4 Руководства администратора (Версия продукта: 4.x).

Настоящий Порядок доводится до пользователя под подпись.

2. Определения и термины

Администратор УКЦ - лицо, обладающее правом доступа к программе ViPNet Удостоверяющий и ключевой центр (УКЦ), отвечающее за создание ключей для сетевых узлов ViPNet, создание и обслуживание сертификатов ViPNet, обеспечение взаимодействия с доверенными сетями ViPNet. В сети ViPNet №559 ТФОМС Иркутской области администратор УКЦ это уполномоченное лицо, согласно Регламенту Центра администрирования сети ViPNet № 559 Территориального фонда обязательного медицинского страхования Иркутской области.

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.

Ключи узла ViPNet - совокупность ключей, с использованием которых производится шифрование трафика, служебной информации и писем программы ViPNet Деловая почта.

Компрометация ключей - утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Пароль пользователя - индивидуальный пароль пользователя для работы в приложениях ViPNet на сетевом узле ViPNet. Первоначально создается администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager. Этот пароль может быть изменен пользователем на сетевом узле ViPNet.

Пользователь ViPNet - лицо, которое использует программное обеспечение ViPNet и имеет ключи для работы с ним.

Сетевой узел ViPNet - узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в управляющем ПО.

Сеть ViPNet - логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищенных узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

3. Порядок действий в случае компрометации ключей

Под компрометацией ключей узла, ключей пользователя, парольной информации понимается утрата доверия к тому, что используемые ключи или парольная информация обеспечивают безопасность информации (целостность, конфиденциальность, неотрекаемость). События, при которых ключи могут считаться скомпрометированными:

- посторонним лицам мог стать доступен файл дистрибутива ключей пользователя;
- посторонним лицам могло стать доступно съемное устройство с ключами пользователя;
- посторонние лица могли получить неконтролируемый физический доступ к ключам пользователя, хранящимся на компьютере;
- уволился пользователь, имевший доступ к паролям и ключам;
- съемное устройство с ключами вышло из строя, и не опровергнут тот факт, что это произошло в результате несанкционированных действий злоумышленника;
- обнаружены демаскирующие признаки взлома сетевого узла ViPNet;
- хранение пароля пользователя в открытом виде (в файле на узле ViPNet, на бумажном носителе в общем доступе);
- раскрытие пароля пользователя (например, при фишенговой атаке);

При обнаружении событий, при которых ключи или пароль пользователя могут считаться скомпрометированными, пользователю ViPNet, где используется ключи пользователя, ключи узла, необходимо незамедлительно уведомить о компрометации уполномоченных лиц:

- администратора УКЦ;
- администратора безопасности сети ViPNet – работник отдела информационной безопасности ТФОМС Иркутской области.

В уведомлении предоставить следующую информацию:

- Идентификационные данные скомпрометированных ключей узла, ключей пользователя;

- ФИО пользователя, который владел скомпрометированными ключом пользователя, ключом узла.

Администратор безопасности совместно с администратором УКЦ принимают решение считать или не считать ключи пользователя, ключи узла скомпрометированными.

При компрометации ключей узла, ключей пользователя необходимо провести расследование и зафиксировать обстоятельства происшествия, в том числе: сбор свидетельских показаний, сбор и анализ событий из журналов ViPNet, сбор и анализ журналов Windows (безопасности, приложений, журналов служб Windows, журналов командных интерпретаторов, например, PowerShell и др.), сбор и анализ событий из журналов средств защиты информации на сетевом узле ViPNet.