ViPNet Administrator

Руководство по смене мастер-ключей в сети ViPNet

infotecs

ФРКЕ.00109-07 90 08

Версия продукта 4.6.7

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 2 этаж

Телефон: +7 (495) 737-6192, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: https://infotecs.ru

Служба технической поддержки: hotline@infotecs.ru

Содержание

Введение **4**
О документе 4
Для кого предназначен документ 4
Соглашения документа 4
О программе 5
Обратная связь 5

Порядок действий **6**

Подготовка к смене мастер-ключей **8**
Копирование дистрибутивов ключей и РНПК из УКЦ 10
Предварительные действия на координаторах ПАК ViPNet Coordinator HW и ViPNet Coordinator for Linux 10
Проверка наличия РНПК на сетевых узлах 12
Установка последней версии ПО на мобильных клиентах с ОС Android и iOS 14

Смена мастер-ключей **14**
Смена мастер-ключей в ViPNet Administrator 3.2 14
Смена мастер-ключей в ViPNet Administrator 4.6 15

Обновление ключей на узлах после смены мастер-ключей **16**
Обновление ключей узлов после смены мастер-ключей в ViPNet Administrator 3.2 16
Обновление ключей узлов после смены мастер-ключей в ViPNet Administrator 4.6 17
Обновление персонального ключа пользователей, использующих внешнее устройство для аутентификации на сетевых узлах ПАК ViPNet Coordinator HW 18

Возможные неполадки и способы их устранения **19**
Не найдены или неверно указаны данные для аутентификации пользователя или запрошен пароль от РНПК 19
На сетевом узле не найден РНПК 20
Не устанавливается новый дистрибутив ключей после смены мастер-ключей при использовании ViPNet Administrator версии 4.6.1 20
Ошибка отправки письма в программе ViPNet Деловая почта 20

Глоссарий **21**

Введение

О документе

В документе указан порядок действий администратора сети ViPNet при смене мастер-ключей в сети ViPNet под управлением программного обеспечения ViPNet Administrator версий 3.2 и 4.6, для различных сетевых узлов приведены особенности обновления ключей, которые следует учесть, чтобы избежать возможных неполадок.

Перед сменой мастер-ключей в сети ViPNet рекомендуется полностью прочитать данный документ.

Для кого предназначен документ

Данный документ предназначен для администраторов сетей ViPNet, ответственных за смену мастер-ключей в своей сети. Предполагается, что читатель данного руководства предварительно прошел курс обучения «Администрирование системы защиты информации ViPNet» в учебном центре ОАО «ИнфоТеКС» http://edu.infotecs.ru/learning/ и сдал экзамен в рамках итоговой аттестации.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	**Внимание!** Указывает на обязательное для исполнения или следования действие или информацию.
	**Примечание.** Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	**Совет.** Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

О программе

ПО ViPNet Administrator® предназначено для администрирования сетей ViPNet (см. глоссарий, стр. 23) и состоит из двух компонентов:

- ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 21).
- ViPNet Удостоверяющий и ключевой центр (УКЦ) (см. глоссарий, стр. 21).

Программа ViPNet Центр управления сетью предназначена для формирования структуры защищенной сети ViPNet, настройки параметров сетевых узлов, регистрации пользователей на сетевых узлах и управления объектами сети.

Программа ViPNet Удостоверяющий и ключевой центр предназначена для издания и обслуживания сертификатов ключа проверки электронной подписи. Она выполняет функции удостоверяющего центра и предоставляет ключи, необходимые для работы в сети ViPNet.

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС»:

- Информация о продуктах ViPNet https://infotecs.ru/product/.
- Информация о решениях ViPNet https://infotecs.ru/resheniya/.
- Часто задаваемые вопросы https://infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet https://infotecs.ru/forum/.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ОАО «ИнфоТеКС»:

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба технической поддержки: hotline@infotecs.ru.

  Форма для обращения в службу технической поддержки через сайт https://infotecs.ru/support/request/.

  Консультации по телефону для клиентов с расширенной схемой технической поддержки: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется политикой ответственного разглашения https://infotecs.ru/disclosure.php.

Порядок действий

При формировании персональных ключей пользователей, а также ключей обмена и ключей защиты, входящих в состав ключей узлов, используются соответствующие мастер-ключи (см. глоссарий, стр. 22):

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

Указанные мастер-ключи создаются при первичной инициализации программы ViPNet Удостоверяющий и ключевой центр и хранятся на компьютере с УКЦ в полной секретности, поскольку компрометация мастер-ключа приводит к компрометации всех ключей, сформированных на его основе. С течением времени должна проводиться смена всех мастер-ключей.

Если произошла компрометация пользователя сети вследствие утраты доверия к его резервному набору персональных ключей, то необходимо сменить мастер-ключ персональных ключей. Остальные мастер-ключи в данном случае менять необязательно.

Смена мастер-ключей не влияет на межсетевые мастер-ключи. Подробнее о смене межсетевых мастер-ключей см. в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

Для успешной смены мастер-ключей в сети ViPNet выполните все действия из приведенного ниже списка в указанной последовательности.

Таблица 3. Порядок действий при смене мастер-ключей

	Действие	Ссылка
☐	Ознакомьтесь с документом полностью.	
☐	Обновите ПО ViPNet Administrator до версии 4.6.3 или выше.	
☐	Проинформируйте всех пользователей и администраторов сети ViPNet о планируемом обновлении ключей и сроках его проведения.	Подготовка к смене мастер-ключей (на стр. 8)
☐	Перед обновлением ключей на сетевых узлах проверьте наличие резервного набора персональных ключей (РНПК) (см. глоссарий, стр. 23).	Проверка наличия РНПК на сетевых узлах (на стр. 12)
☐	Сохраните дистрибутивы ключей, созданные до смены мастер-ключей, для всех узлов своей сети.	Копирование дистрибутивов ключей и РНПК из УКЦ (на стр. 10)
☐	Выполните подготовку координаторов ПАК ViPNet Coordinator HW или ViPNet Coordinator for Linux.	Предварительные действия на координаторах ПАК ViPNet Coordinator HW и ViPNet Coordinator for Linux (на стр. 10)
☐	Отправьте последнюю рекомендованную версию на мобильные клиенты со следующим ПО: • ViPNet Client for Android; • ViPNet Client for iOS.	Установка последней версии ПО на мобильных клиентах с ОС Android и iOS (на стр. 14)
☐	Отправьте на сетевые узлы с ПО ViPNet Client for Windows и ViPNet Coordinator for Windows версию 4.3.3, 4.3.4 или 4.5.1 и выше.	Подробнее см. документ «ViPNet Центр управления сетью. Руководство администратора», главу «Управление сетью ViPNet», раздел «Отправка обновлений на сетевые узлы», подраздел «Обновление программного обеспечения»
☐	Проведите смену мастер-ключей с помощью ПО ViPNet Administrator той версии, которая используется в вашей сети.	Смена мастер-ключей в ViPNet Administrator 3.2 (на стр. 14) Смена мастер-ключей в ViPNet Administrator 4.6 (на стр. 15)

	Действие	Ссылка
☐	Создайте новые ключи для всех пользователей и передайте их в ЦУС. И только после этого создайте и передайте в ЦУС ключи для всех узлов. В УКЦ создайте новые дистрибутивы ключей для сетевых узлов со следующим ПО или ПАКами: • ПО ViPNet Client for Android версии ниже 2.12.1; • ПО ViPNet Client for iOS версии ниже 2.9.12; • ПО ViPNet Terminal; • ПАК ViPNet Coordinator HW версии ниже 4.2; • ПАК ViPNet Coordinator HW или узлов с ПО ViPNet Coordinator for Linux, работающих в режиме кластера горячего резервирования. Затем передайте дистрибутивы ключей пользователям или администраторам этих сетевых узлов.	Обновление ключей узлов после смены мастер-ключей в ViPNet Administrator 3.2 (на стр. 16) Обновление ключей узлов после смены мастер-ключей в ViPNet Administrator 4.6 (на стр. 17)
☐	Если на сетевых узлах ПАК ViPNet Coordinator HW пользователи используют для аутентификации персональный ключ, сохраненный на внешнем устройстве, обновите эти ключи с помощью создания новых дистрибутивов ключей.	Обновление персонального ключа пользователей, использующих внешнее устройство для аутентификации на сетевых узлах ПАК ViPNet Coordinator HW (на стр. 18)
☐	Для сетевых узлов, на которых возникли неполадки при обновлении ключей после смены мастер-ключей, в УКЦ выдайте новые дистрибутивы ключей и передайте их пользователям или администраторам для установки на сетевых узлах.	Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», главу «Управление ключевой структурой ViPNet», раздел «Работа с дистрибутивами ключей», подраздел «Создание дистрибутивов ключей».

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Подготовка к смене мастер-ключей

Перед сменой мастер-ключей выполните следующие действия:

- Выберите промежуток времени 5-10 дней, в течение которых вы будете проводить смену мастер-ключей.

  В этот выбранный период в сети ViPNet не рекомендуется выполнять следующие действия:

  - обрабатывать межсетевую информацию;
  - изменять структуру сети;
  - менять способ аутентификации пользователям сетевых узлов;
  - рассылать обновления CRL.

- Проинформируйте всех пользователей и администраторов сети ViPNet о планируемом обновлении ключей и сроках его проведения.
- Рекомендуйте пользователям расшифровать все сообщения программы ViPNet Деловая почта, включая архивные сообщения. После того как на узлах будут установлены ключи, созданные на основе новых мастер-ключей, зашифрованные на старых ключах сообщения невозможно будет прочитать.

  После смены мастер-ключей и обновления ключей на узлах пользователи могут зашифровать письма. Подробнее о том, как выполнить шифрование и расшифрование писем, см. документ «ViPNet Деловая почта. Руководство пользователя», главу «Электронная подпись», раздел «Шифрование и расшифрование писем».

- Рекомендуйте пользователям, использующим ПО ViPNet SafeDisk-V, создать резервную копию ключей контейнера данных. Таким образом, в случае неудачной смены мастер-ключей и установки нового дистрибутива ключей на узле будет возможно восстановить доступ к защищенной информации, находящейся в файле контейнера ViPNet SafeDisk-V, с помощью резервной копии ключей контейнера.
- Совместно с администраторами сетевых узлов проконтролируйте, что у каждого пользователя на узле имеется резервный набор персональных ключей (РНПК) (см. Проверка наличия РНПК на сетевых узлах на стр. 12). Если пользователь зарегистрирован на нескольких узлах, то его РНПК должен присутствовать на каждом из узлов. Если у пользователя не окажется резервного набора персональных ключей, создайте и передайте ему соответствующий набор доверенным способом.

  Без РНПК новые ключи на узлах не вступят в действие.

- Убедитесь в достаточном количестве лицензий для выпуска новых сертификатов пользователей.

Примечание. После смены мастер-ключей в процессе создания ключей пользователей или дистрибутивов ключей будут выпущены новые сертификаты пользователей.

При необходимости заранее обеспечьте достаточное количество лицензий на максимальное число сертификатов пользователей ViPNet, обратившись в ОАО «ИнфоТеКС» для обновления лицензии на сеть ViPNet, заполнив форму на сайте https://infotecs.ru/personal-offer/.

- Для своевременного применения обновлений ключей с отложенной датой, устанавливаемой в ЦУСе при отправке справочников и ключей, попросите пользователей сообщить заданные

часовой пояс и время на их сетевых узлах. Эти значения понадобятся, чтобы вычислить время отложенного применения обновлений ключей. Для личного удобства при выборе узлов для отправки отложенного обновления вы можете в ЦУСе сохранить отчет о структуре сети в файл *.html и посмотреть, какие узлы зарегистрированы на координаторах.

Копирование дистрибутивов ключей и РНПК из УКЦ

Перед сменой мастер-ключей создайте дистрибутивы ключей для сетевых узлов, зарегистрированных в роли «Деловая почта», и сохраните дистрибутивы ключей и РНПК в отдельную папку (отличающуюся от папки по умолчанию). Эти дистрибутивы ключей могут понадобиться, если кто-то из пользователей не расшифрует письма в программе ViPNet Деловая почта. Установка дистрибутива ключей, созданного до смены мастер-ключа персональных ключей, на узле пользователя позволит расшифровать письма программы ViPNet Деловая почта и восстановить к ним доступ.

Примечание. Если вы меняли пароль пользователя в УКЦ или пользователь сетевого узла сменил пароль локально на узле, то при входе в программу ViPNet Деловая почта пароль пользователя может не подойти. Пользователю необходимо ввести пароль, выданный ему при выдаче последнего дистрибутива ключей. Чаще всего это пароль, выданный при выпуске первого дистрибутива ключей для развертывания сетевого узла.

После восстановления доступа к письмам программы ViPNet Деловая почта в УКЦ выдайте дистрибутив ключей, сформированный на новых мастер-ключах, для обновления ключей на узле.

Предварительные действия на координаторах ПАК ViPNet Coordinator HW и ViPNet Coordinator for Linux

До смены мастер-ключей в сети на координаторах ПАК ViPNet Coordinator HW и ViPNet Coordinator for Linux выполните следующие действия и проверки:

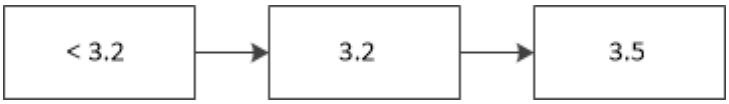
- Для корректной смены мастер-ключей на координаторах должно быть установлено ПО последних версий.
- Если координаторы объединены в кластеры горячего резервирования, на координаторах необходимо обновить ПО до следующих версий:
  - ViPNet Coordinator HW до версии 4.2.4 и выше.

- ViPNet Coordinator for Linux до версии 4.2.5 и выше.

После смены мастер-ключей обновление ключей на координаторах из кластера горячего резервирования выполняется удаленно с помощью отправки ключей из ЦУСа.

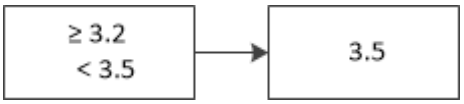
Если на координаторах установлена версия ПО ниже указанных, после смены мастер-ключей обновление ключей на координаторах из кластера горячего резервирования выполняется вручную с помощью дистрибутива ключей.

- Если на ViPNet Coordinator HW установлено ПО другой версии, выполните одно из действий:
  - Если установлено ПО более ранней версии, чем 3.2, последовательно обновите его сначала до версии 3.2, а затем до версии 3.5.



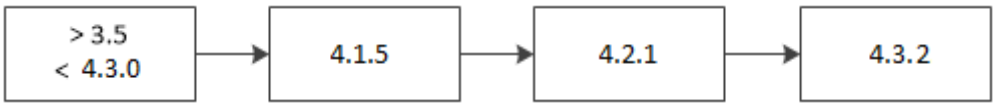
    Подробнее см. документ «Программно-аппаратный комплекс ViPNet Coordinator HW 3. Руководство администратора», раздел «Обновление программного обеспечения, справочников и ключей».

  - Если установлено ПО версии 3.2 или более поздней версии, но более ранней, чем 3.5, обновите его до версии 3.5.



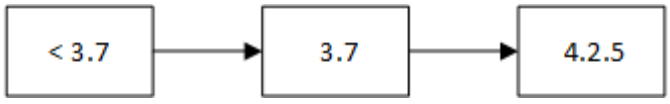
    Подробнее см. документ «Программно-аппаратный комплекс ViPNet Coordinator HW 3. Руководство администратора», раздел «Обновление программного обеспечения, справочников и ключей».

  - Если установлено ПО более поздней версии, чем 4.0, но более ранней, чем 4.3.2, обновите его сначала до версии 4.1.5, затем до версии 4.2.1, и наконец до версии 4.3.2.



  - Подробнее см. документ «ViPNet Coordinator HW 4. Настройка с помощью командного интерпретатора», раздел «Обновление программного обеспечения».

- Если на ViPNet Coordinator for Linux установлено ПО более ранней версии, чем 3.7, последовательно обновите его сначала до версии 3.7, а затем до версии 4.2.5 или выше при условии, что дистрибутив ОС Linux входит в список поддерживаемых для соответствующей версии.



- Убедитесь, что для аутентификации пользователя на ViPNet Coordinator HW используется тот же пароль, что задан в программе ViPNet Удостоверяющий и ключевой центр для пользователя узла ViPNet Coordinator HW.
- На ViPNet Coordinator HW проверьте, что у вас отсутствуют неприменившиеся обновления ключей. Для этого выполните следующие действия:

- Перейдите в режим администратора с помощью команды `enable`.
- Перейдите в командную оболочку ОС Linux с помощью команды `admin escape`.
- Введите команду:

  ```
  find /opt/vipnet/ccc/ -name "k*.*"
  ```

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

- На ViPNet Coordinator for Linux проверьте, что у вас отсутствуют неприменившиеся обновления ключей. Для этого выполните команду:

  ```
  find /opt/vipnet/ccc/ -name "k*.*"
  ```

  В случае неприменившихся обновлений ключей повторите действия в ЦУСе как описано в пункте выше.

- Создайте резервную копию конфигурации координатора ПАК ViPNet Coordinator HW или ViPNet Coordinator for Linux. 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.

  Подробнее о создании копии текущей конфигурации VPN координатора см. документ «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», раздел «Управление копиями конфигурации VPN». А также для ViPNet Coordinator for Linux описание команды iplir config save см. в документе «ViPNet Coordinator for Linux. Справочное руководство по командам».

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

Проверка наличия РНПК на сетевых узлах

РНПК предназначен для получения обновлений ключей и содержится в файле `AAAA.pk`, где `<AAAA>` — шестнадцатеричный номер пользователя в сети ViPNet.

Обеспечьте наличие РНПК на компьютерах пользователей и координаторах. Необходимо обеспечить присутствие файла РНПК `*.pk` на сетевых узлах с ОС Microsoft Windows и Linux по следующему пути в папке с названием продукта ViPNet:

- ОС Microsoft Windows:
  - `\d_station\abn_AAAA`;

- \user_AAAA\key_disk\dom.

- ОС Linux: /etc/vipnet/d_station/abn_AAAA.

При необходимости создайте РНПК в УКЦ и передайте их на узлы пользователей. О том, как создать, сохранить и передать пользователю файл с РНПК, см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

На ПАК ViPNet Coordinator HW вы можете проверить, что у вас есть 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 вашем 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.

На сетевом узле с ПО ViPNet Coordinator for Linux проверьте, что у вас есть РНПК, вручную в папке /etc/vipnet/d_station/abn_AAAA.

Если же на ПАК ViPNet Coordinator HW или на сетевом узле с ПО ViPNet Coordinator for Linux нет РНПК, то выполните следующие действия:

1 В УКЦ сохраните РНПК сетевого узла в файл и скопируйте его на USB-носитель.

Примечание. На координаторах ViPNet Coordinator for Linux начиная с версии 4.2.5 вы можете добавить файл РНПК с USB-носителя на сетевой узел.

---

2 Добавьте РНПК на сетевой узел. Для этого выполните следующие действия:

- На сетевом узле ПАК ViPNet Coordinator HW войдите в режим администратора и импортируйте РНПК с USB-носителя с помощью команды:

  admin add spare keys

- На ViPNet Coordinator for Linux переместите файл РНПК вручную с помощью команды:

  recrypt_pks [t] <абсолютный путь к файлу iplirpsw> <абсолютный путь к файлу РНПК с расширением *.pk> [<абсолютный путь, по которому будет размещен файл РНПК>]

  По умолчанию файл iplirpsw расположен в каталоге /etc.

  Чтобы проверить соответствие вашего пароля пользователя ViPNet паролю, который задал администратор сети ViPNet, укажите ключ -t при выполнении команды. Если пароли различаются, появится сообщение об ошибке. В таком случае запросите пароль у администратора сети ViPNet.

  Например:

  recrypt_pks /etc/iplirpsw /home/user/0001.pk /etc/ViPNet/d_station/abn_0001/0001.pk

  Подробнее см. документ «ViPNet Coordinator for Linux. Подготовка к работе», раздел «Порядок добавления РНПК».

Установка последней версии ПО на мобильных клиентах с ОС Android и iOS

Для корректного обновления ключей на мобильных клиентах отправьте на сетевые узлы последнюю рекомендованную версию ПО ViPNet Client for Android и ViPNet Client for iOS. Подробнее см. документ «ViPNet Центр управления сетью. Руководство администратора», главу «Управление сетью ViPNet», раздел «Отправка обновлений на сетевые узлы», подраздел «Обновление программного обеспечения».

Начиная с версий ПО ViPNet Client for Android 2.12.1 и ViPNet Client for iOS 2.9.12, отправьте обновления ключей на сетевые узлы удаленно из ЦУСа. В более ранних версиях обновления ключей нужно устанавливать вручную, если произошла смена мастер-ключей в сети.

Смена мастер-ключей

Смена мастер-ключей в ViPNet Administrator 3.2

Перед сменой мастер-ключей с помощью ПО ViPNet Administrator 3.2 убедитесь, что во вложенной папке `\KC\P_KEYS` папки установки программы ViPNet Удостоверяющий и ключевой центр нет файлов с резервными наборами персональных ключей (файлов с расширением `*.pk`). При наличии файлов `*.pk` в указанной папке скопируйте их на диск и передайте соответствующим пользователям доверенным способом.

Примечание. Эти файлы могут находиться в папке `\KC\P_KEYS` в том случае, если по каким-либо причинам они не были переданы пользователям в составе дистрибутивов ключей.

Для смены мастер-ключей выполните следующие действия:

1 Создайте резервную копию текущей конфигурации программы.

Подробнее см. документ «ViPNet Administrator Удостоверяющий и ключевой центр 3.2. Руководство администратора», главу «Административные функции», раздел «Создание и восстановление резервных копий конфигурации программы», подраздел «Создание резервной копии текущей конфигурации».

2 В окне программы на панели навигации перейдите в раздел **Ключевой центр** > **Своя сеть ViPNet** > **Ключи** > **Мастер-ключи**.

3 Поочередно щелкните каждый из трех мастер-ключей правой кнопкой мыши и в контекстном меню выберите пункт **Сменить**.

Примечание. Если произошла компрометация пользователя сети вследствие утраты доверия к его резервному набору персональных ключей, то необходимо сменить мастер-ключ персональных ключей. Остальные мастер-ключи в данном случае менять необязательно.

---

4 В появившемся окне предупреждения о последствиях смены мастер-ключа установите флажок **Сменить ключ <название мастер-ключа>** и нажмите кнопку **Продолжить**.

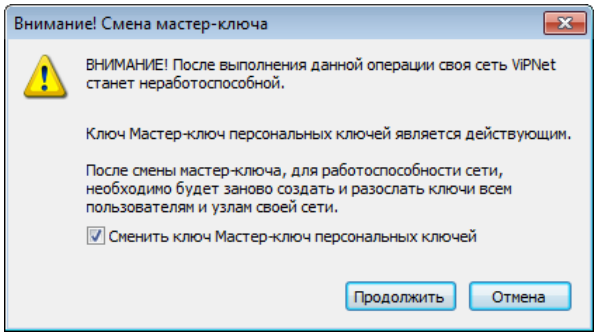


Рисунок 1. Предупреждение при смене мастер-ключа

5 В окне с запросом ввести пароль введите пароль для учетной записи администратора УКЦ.

В результате будет произведена смена мастер-ключей.

Смена мастер-ключей в ViPNet Administrator 4.6

Для смены мастер-ключей выполните следующие действия:

1 В окне программы ViPNet Удостоверяющий и ключевой центр на панели навигации перейдите в представление **Ключевой центр** и выберите раздел **Моя сеть** > **Мастер-ключи**.

2 Поочередно щелкните каждый из трех мастер-ключей правой кнопкой мыши и в контекстном меню выберите пункт **Сменить**.

3 В появившемся окне с предупреждением о последствиях смены мастер-ключа установите флажок **Сменить <название мастер-ключа>** и нажмите кнопку **Продолжить**.

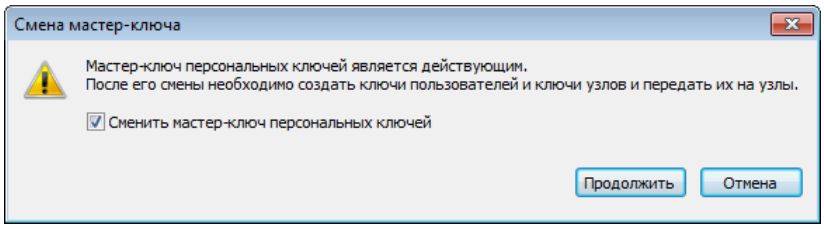


Рисунок 2. Предупреждение при смене мастер-ключа

4 В окне с запросом ввести пароль введите пароль для учетной записи администратора УКЦ.

В результате будет произведена смена мастер-ключей.

Обновление ключей на узлах после смены мастер-ключей

Обновление ключей узлов после смены мастер-ключей в ViPNet Administrator 3.2

После смены мастер-ключей выполните следующие действия:

1 В УКЦ создайте ключи пользователей и передайте их в ЦУС.

2 В УКЦ создайте ключи узлов и передайте их в ЦУС.

3 Если в вашей сети есть программно-аппаратные комплексы ViPNet Coordinator HW, создайте новые дистрибутивы ключей и выполните локальное обновление ключей на этих сетевых узлах. См. документ «ViPNet Administrator. Удостоверяющий и ключевой центр 3.2. Руководство администратора», главу «Управление ключевой структурой ViPNet», раздел «Работа с дистрибутивами ключей», подраздел «Создание дистрибутивов ключей».

Внимание! Для паролей пользователей сетевых узлов ViPNet Coordinator HW при обновлении ключей, рассылаемых через ViPNet Центр управления сетью версии 3.2.9 или 3.2.10, используйте следующие наборы символов:

- строчные и заглавные латинские буквы (a-z, A-Z);
- цифры (0-9).

Если для паролей пользователей вы используете другие символы (например, спецсимволы — точка, запятая и так далее), то обновление ключей не будет выполнено.

---

4 Из ЦУСа отправьте обновления ключей с отсроченной датой вступления в действие (см. документ «ViPNet Центр управления сетью 3.2. Руководство администратора», главу «Управление сетью»).

   Пока не истек срок назначенного обновления, в УКЦ и ЦУС желательно не производить никаких действий. Если же что-то было изменено, то в ЦУС все обновления необходимо отсылать с более поздней датой, чем дата, указанная для обновления ключей.

5 С помощью журнала запросов и ответов в ЦУСе проконтролируйте процесс принятия новых ключей на узлах.

6 Если обновление было принято не всеми пользователями, по необходимости выполните обновление ключей на их узлах вручную. Для этого сформируйте новый дистрибутив ключей и установите его на узле пользователя. О том, как установить дистрибутив ключей на узле пользователя см. документацию на соответствующее ПО ViPNet.

Обновление ключей узлов после смены мастер-ключей в ViPNet Administrator 4.6

После смены мастер-ключей выполните следующие действия:

1 В УКЦ создайте и передайте в ЦУС новые ключи для всех пользователей.

2 В УКЦ создайте и передайте в ЦУС ключи для всех узлов.

   Из ЦУСа отправьте на узлы ключи с отложенной датой применения (см. документ «ViPNet Центр управления сетью. Руководство администратора», главу «Управление сетью ViPNet», раздел «Отправка обновлений на сетевые узлы»).

   При этом обновить ключи путем удаленной отправки ключей из ЦУСа невозможно на сетевых узлах со следующим ПО или ПАКами в следующих случаях:

   - ПАК ViPNet Terminal (ранее — ViPNet ThinClient):
     - на сетевом узле было произведено обновление ПО ViPNet Terminal с версии 3.4 или ниже до более поздней версии;
     - справочники, ключи и настройки были импортированы на сетевой узел с помощью файла `*.vbe`, созданного в ПО ViPNet Terminal версии 3.4 или ниже;
     - для аутентификации пользователя на сетевом узле используется устройство.
   - ПАК ViPNet Coordinator HW:
     - установлено программное обеспечение версии ниже 4.2.4;
     - пароль пользователя ПАКа был изменен локально и отличается от пароля, заданного для пользователя в УКЦ.

- Координаторы работают в режиме кластера горячего резервирования со следующими версиями ПО:
  - ViPNet Coordinator HW версии ниже 4.2.4;
  - ViPNet Coordinator for Linux версии ниже 4.2.5.
- ПО ViPNet Client for Android и ViPNet Client for iOS:
  - установлено ПО ViPNet Client for Android версий ниже 2.12.1;
  - установлено ПО ViPNet Client for iOS версий ниже 2.9.12;
  - если для пользователей задан минимальный уровень полномочий (см. глоссарий, стр. 23).

В этих случаях создайте для них новые дистрибутивы ключей и передайте их доверенным способом пользователям узлов или администраторам координаторов.

Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», главу «Управление ключевой структурой ViPNet», раздел «Работа с дистрибутивами ключей», подраздел «Создание дистрибутивов ключей».

3. Совместно с администратором ЦУСа проконтролируйте процесс приема новых ключей на узлах.
4. Если обновление было принято не всеми пользователями, при необходимости выполните обновление ключей на их узлах вручную. Для этого сформируйте новый дистрибутив ключей и установите его на узле пользователя.

   При необходимости за более подробной информацией об обновлении ключей на сетевых узлах обратитесь к документации на соответствующие продукты ViPNet.
5. Если пользователь зарегистрирован на нескольких сетевых узлах, сформируйте новый дистрибутив ключей для каждого из узлов и установите их на узлах.

Обновление персонального ключа пользователей, использующих внешнее устройство для аутентификации на сетевых узлах ПАК ViPNet Coordinator HW

Чтобы обновить персональный ключ пользователя на внешнем устройстве, которое используется пользователем для аутентификации на сетевом узле ПАК ViPNet Coordinator HW, выполните следующие действия:

1 Убедитесь, что в настройках создания дистрибутивов ключей в УКЦ установлен флажок **Выбор способа аутентификации в мастере выдачи дистрибутива ключей**.

   Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», главу «Управление ключевой структурой ViPNet», раздел «Работа с дистрибутивами ключей», подраздел «Настройка параметров создания дистрибутивов ключей».

2 Подключите внешнее устройство к компьютеру с УКЦ.

3 Запустите мастер создания нового дистрибутива ключей, заменив персональный ключ на внешнем устройстве.

   Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», главу «Управление ключевой структурой ViPNet», раздел «Работа с дистрибутивами ключей», подраздел «Создание дистрибутивов ключей».

4 Передайте внешнее устройство администратору координатора ПАК ViPNet Coordinator HW.

Возможные неполадки и способы их устранения

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 на клиенте или координаторе с ОС Windows сменил пароль локально на узле, либо если в УКЦ для пользователя была смена пароля после установки дистрибутива ключей на сетевом узле.

Чтобы устранить неполадку, сообщите пользователю, что необходимо для входа в программу ViPNet Монитор или при запросе пароля от РНПК ввести пароль, выданный пользователю 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 ПО ViPNet Client и ViPNet Coordinator для ОС Windows у пользователя может появиться сообщение об отсутствии файла РНПК на сетевом узле. Для этого выполните следующие действия:

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.

Не устанавливается новый дистрибутив ключей после смены мастер-ключей при использовании ViPNet Administrator версии 4.6.1

Если вы используете ПО ViPNet Administrator версии 4.6.1 и после смены мастер-ключей при установке нового дистрибутива ключей на сетевой узел появилось сообщение об ошибке, повторно выдайте дистрибутив ключей и установите его на узле.

Примечание. Для устранения неполадки обновите версию ПО ViPNet Administrator до версии 4.6.3 или выше.

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 следующее сообщение:

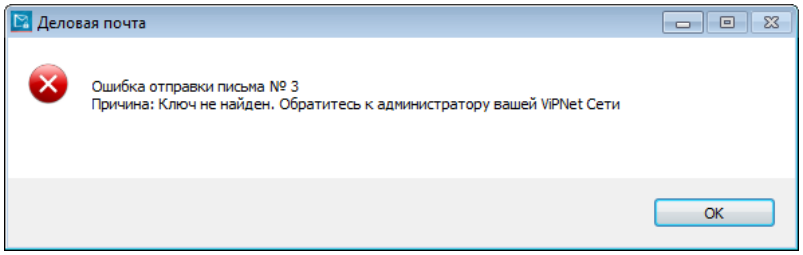


Рисунок 3. Сообщение об ошибке при отправке письма

Для решения проблемы пользователю необходимо выбрать в качестве текущего сертификат, выпущенный вместе с новыми ключами. Как правило, это сертификат с самой поздней датой выпуска. Подробнее см. документ «ViPNet Деловая почта 4. Руководство пользователя».

Глоссарий

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. Администратор УКЦ формирует и обновляет ключи для сетевых узлов ViPNet, а также управляет сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

ViPNet Центр управления сетью — 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.

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.

Ключ защиты

Ключ, на котором шифруется другой ключ.

Ключ обмена

Симметричный ключ, известный отправителю и получателю зашифрованной информации, которой обмениваются 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 администратора УКЦ

Пароль для входа в программу ViPNet Удостоверяющий и ключевой центр.

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 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 устройствами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Справочники и ключи

Справочники, ключи узла и ключи пользователя.