

Обновление ViPNet Administrator с версии 2.8.x до версии 3.2.x

Приложение к документации ViPNet CUSTOM 3.2

1991–2012 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00006-05 90 11

Этот документ входит в комплект поставки программного обеспечения, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТеКС».

ViPNet является зарегистрированной торговой маркой программного обеспечения, разрабатываемого ОАО «ИнфоТеКС».

Все торговые марки и названия программ являются собственностью их владельцев.

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский пр., дом 1/23, строение 1

Тел: (495) 737-61-96 (hotline), 737-61-92, факс 737-72-78

Сайт компании «ИнфоТеКС»: <http://www.infotecs.ru>

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение.....	4
О документе	5
Для кого предназначен документ	5
Терминология документа	5
Соглашения документа.....	5
Обратная связь	7
Глава 1. Обновление ViPNet Administrator с версии 2.8.x до версии 3.2.x	8
Порядок проведения процедуры обновления	9
Подготовка к обновлению	11
Процесс обновления ViPNet Administrator.....	14
Формирование списков отозванных сертификатов.....	24
Обновление ключей пользователей, зарегистрированных на нескольких сетевых узлах	26
Приложение А. Глоссарий.....	28



Введение

О документе	5
Обратная связь	7

О документе

Настоящий документ описывает порядок обновления программного обеспечения ViPNet Administrator, установленного на рабочем месте администратора сети ViPNet, с версии 2.8.x до версии 3.2.x, а также содержит рекомендации по обновлению ключей пользователей, зарегистрированных на нескольких сетевых узлах.

Для кого предназначен документ

Документ предназначен для специалистов, имеющих квалификацию администратора сети ViPNet (подтвержденную соответствующим документом) и обладающих знаниями и опытом в области конфигурирования, эксплуатации и управления сетью ViPNet.

Терминология документа

Представленный документ ориентирован на терминологию, используемую в программе ViPNet Administrator версии 3.2.3 и выше. Отличия терминологии данной версии по сравнению с версиями 3.2.2 и ниже представлены в таблице.




Таблица 1. Различия терминологии

Термин ViPNet Administrator 3.2.2 и ниже	Термин ViPNet Administrator 3.2.3 и выше
Ключевая информация	Ключи
Справочно-ключевая информация	Справочники и ключи
Ключевой диск	Ключи пользователя
Ключевой набор	Ключи узла
Дистрибутив справочно-ключевой информации	Дистрибутив ключей

Соглашения документа

Соглашения данного документа представлены в таблице ниже.

Таблица 2. Условные обозначения

Указатель	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.

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте компании «ИнфоТеКС». По предложенным ссылкам можно найти ответы на многие вопросы, возникающие в процессе эксплуатации продуктов ViPNet.

- Описание комплекса ViPNet CUSTOM <http://www.infotecs.ru/products/line/custom.php>.
- Сборник часто задаваемых вопросов (FAQ) <http://www.infotecs.ru/support/faq/>.
- Законодательная база в сфере защиты информации <http://www.infotecs.ru/laws/>.
- Информация о решениях ViPNet <http://www.infotecs.ru/solutions/vpn/>.

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами компании «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Электронный адрес службы поддержки hotline@infotecs.ru.
- Форма запроса по электронной почте в службу поддержки <http://www.infotecs.ru/support/request/>.
- 8 (495) 737-6196 — «горячая линия» службы поддержки.
- 8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).



1

Обновление ViPNet Administrator с версии 2.8.x до версии 3.2.x

Порядок проведения процедуры обновления	9
Подготовка к обновлению	11
Процесс обновления ViPNet Administrator	14
Формирование списков отозванных сертификатов	24
Обновление ключей пользователей, зарегистрированных на нескольких сетевых узлах	26

Порядок проведения процедуры обновления

Процедура обновления включает в себя не только обновление программного обеспечения ViPNet Administrator непосредственно на рабочем месте администратора, но и полное обновление ключей на всех узлах защищенной сети. При этом обновление не затрагивает межсетевое взаимодействие, основанное на симметричных ключах шифрования (в процессе обновления индивидуальные симметричные межсетевые мастер-ключи (ИММК) не изменяются), что позволяет сохранить связь с узлами доверенных сетей ViPNet.



Примечание. Процесс обновления ViPNet Administrator на рабочем месте администратора головной и подчиненных сетей идентичен и соответствует порядку, описанному в данном документе.

Обновление программного обеспечения ViPNet Administrator следует производить согласно утвержденному графику. Для успешного проведения процедуры обновления требуется выполнить все действия из приведенного ниже списка.

Действие	Ссылка
1. Выполните подготовку к обновлению.	Подготовка к обновлению (на стр. 11)
2. На всех узлах сети ViPNet (кроме узла администратора) обновите программное обеспечение ViPNet Client и ViPNet Coordinator до версии 3.1.x и выше.	Документ «Обновление ПО ViPNet Client/Coordinator с версии 2.8.x до версии 3.1.x»
Программное обеспечение ViPNet Coordinator на узлах рекомендуется обновлять в последнюю очередь. Если на узлах программное обеспечение не будет обновлено или будет обновлено до версии ниже указанной, после обновления ViPNet Administrator работоспособность таких узлов и сети в целом может быть нарушена!	

3. На рабочем месте администратора обновите программное обеспечение ViPNet Client до версии 3.1.x и выше.
4. Выполните проверку функционирования программы ViPNet Client и проверьте защищенное соединение с узлами, с которыми связан сетевой узел администратора.
- Если связь не проверяется, приостановите обновление. Восстановите предыдущую версию программы ViPNet Client из резервной копии и повторите действия, указанные в п. 3 данного списка.
5. Выполните обновление программного обеспечения ViPNet Administrator до версии 3.2.x, после которого сформируйте и отправьте новые ключи ViPNet на все узлы защищенной сети.
- Если в сети ViPNet имеются пользователи, зарегистрированные на двух и более сетевых узлах, выполните обновление их ключей в соответствии с приведенным регламентом.
6. При наличии межсетевого взаимодействия сформируйте и отправьте в соответствующие доверенные сети ViPNet экспорт, предварительно выполнив в УКЦ смену межсетевых мастер-ключей и экспорт справочников (меню **Сервис > Экспорт справочников**).
- Смену межсетевых мастер-ключей следует производить только в том случае, если в доверенных сетях используется программное обеспечение ViPNet Administrator версии 3.x! Подробнее в разделе [Процесс обновления ViPNet Administrator](#) (на стр. 14).
- Документ «ViPNet Client Монитор. Руководство пользователя», глава «Встроенные средства коммуникации», раздел «Проверка соединения с сетевым узлом».
- [Процесс обновления ViPNet Administrator](#) (на стр. 14)
- [Обновление ключей пользователей, зарегистрированных на нескольких сетевых узлах](#) (на стр. 26)
- Документы «ViPNet Administrator Центр управления сетью. Руководство администратора» и «ViPNet Administrator Удостоверяющий и ключевой центр. Руководство администратора»
-

Подготовка к обновлению

Прежде чем начать обновление программного обеспечения ViPNet Administrator:

- 1 Внимательно прочтите настоящую инструкцию. Для успешного обновления, во избежание проблем, строго соблюдайте последовательность действий, указанных в документе.



Совет. К процессу обновления программного обеспечения следует подойти с максимальной ответственностью, контролируя все производимые действия на каждом из его этапов, особенно, если в данном процессе принимают участие несколько администраторов безопасности.

Если результат операций по какому-либо разделу данной инструкции не соответствует указанному, не выполняйте дальнейших действий, так как это может привести к нарушению работоспособности всей защищенной сети. При возникновении ошибки приостановите дальнейшую работу и обратитесь в службу технической поддержки компании «ИнфоТеКС» (см. «[Обратная связь](#)» на стр. 7).

- 2 Проинформируйте всех пользователей и администраторов сети ViPNet о планируемом обновлении и сроках его проведения.
- 3 Рекомендуйте пользователям сети расшифровать все сообщения программы «Деловая почта», включая архивные сообщения, во избежание их потери при возможных сбоях обновления.
- 4 Убедитесь, что в промежуток времени, отведенный на обновление, все пользователи сети ViPNet смогут выполнить вход в программу ViPNet Client или ViPNet Coordinator.
- 5 Убедитесь, что у каждого пользователя на узле имеется резервный набор персональных ключей (файл `AAAA.pk`, где `AAAA` — шестнадцатеричный идентификатор пользователя в защищенной сети). Если пользователь зарегистрирован на нескольких узлах, то его резервный набор ключей должен присутствовать на каждом из узлов.

Если у пользователя не окажется резервного набора персональных ключей, передайте ему соответствующий набор любым защищенным способом.

Внимание! Для автоматического обновления ключей пользователя на узле файл AAAA.pk должен находиться в папке по умолчанию, если это не противоречит требованиям безопасности организации. Папкой по умолчанию считается:

- C:\Program Files\InfoTeCS\ViPNet Client\station\abn_AAAA — при использовании ViPNet Client версии 2.8.x;
- C:\Program Files\InfoTeCS\ViPNet Client\d_station\abn_AAAA — при использовании ViPNet Client версии 3.x.



Если резервный набор персональных ключей пользователя будет отсутствовать в указанной папке, то обновление ключей, отправленное в процессе обновления программного обеспечения ViPNet Administrator, не вступит в действие и связь с узлом пользователя будет потеряна. Восстановить работоспособность узла в таком случае можно будет только при помощи дистрибутива ключей, сформированного в ViPNet Administrator версии 3.2.x, но с потерей всей зашифрованной корреспонденции пользователя в программе ViPNet Деловая почта.

- 6 Приостановите проведение работ, связанных с модификацией структуры защищенной сети (обработку импортов из других сетей, формирование и отправку экспортов в другие сети, регистрацию и удаление новых узлов сети и тому подобное), а также проведение работ по формированию и передаче пользователям дистрибутивов ключей ViPNet.
- 7 Если у вашей сети установлена связь с другой сетью ViPNet не на основе индивидуального симметричного межсетевого мастер-ключа (ИММК), то перейдите на его использование.

В обязательном порядке на рабочем месте администратора сети ViPNet также выполните следующие действия по подготовке к обновлению:

- 1 Сделайте резервную копию содержимого папки, в которой установлено программное обеспечение ViPNet Administrator версии 2.8.x. Настоятельно рекомендуется полностью сохранить папку InfoTeCS.
- 2 Убедитесь, что во вложенной папке \КС\Р_KEYS папки установки ViPNet Administrator нет файлов с расширением *.pk. При наличии файлов *.pk в указанной папке скопируйте их в любое место на диске, после чего передайте соответствующим пользователям любым защищенным способом.



Внимание! Эти файлы могут находиться в папке \КС\Р_KEYS в том случае, если по каким-либо причинам они не были переданы пользователям в составе

дистрибутивов ключей.

- 3 Удалите программное обеспечение ViPNet Client версии 2.8.x с сохранением всех пользовательских файлов и папок.
- 4 Проверьте наличие во вложенной папке `\SS\Station\abn_AAAA` файла `AAAA.pk`. Если этот файл отсутствует, перенесите его из папки с сохраненными файлами `*.pk` в указанную подпапку (см. п. 2 данного списка).

Процесс обновления ViPNet Administrator



Внимание! Приведенные ниже действия описывают обновление компонентов программного обеспечения ViPNet Administrator: ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр, установленных на одном сетевом узле.

Для обновления программного обеспечения ViPNet Administrator:

- 1 Двойным щелчком запустите программу установки `setup.exe`

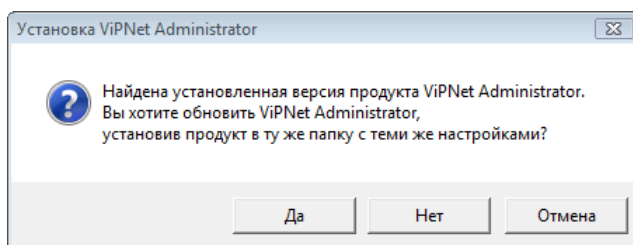


Рисунок 1: Сообщение о наличии ранее установленного программного обеспечения

- 2 В появившемся окне с сообщением о том, что обнаружена установленная ранее версия ViPNet Administrator, нажмите кнопку **Да**, чтобы начать обновление. При нажатии на кнопку **Нет** обновление не произойдет, и будет запущен мастер для установки программы в другую папку.
- 3 Дождитесь завершения процесса обновления.
- 4 При успешном окончании обновления перезагрузите компьютер.
- 5 Запустите УКЦ и следуйте указаниям мастера первичной инициализации.



Внимание! Ниже приведены действия, которые необходимо выполнить на отдельных страницах мастера. На остальных страницах рекомендуется оставить значения, предлагаемые по умолчанию. По завершении процесса обновления эти значения можно изменить в настройках УКЦ.

- 6 На странице **Выбор драйвера ODBC** выберите **Microsoft Access Driver (*.mdb)**.

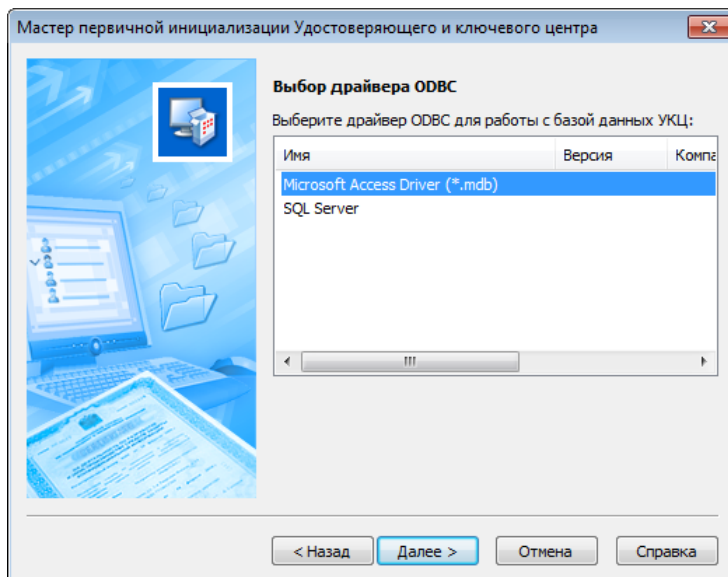


Рисунок 2: Выбор драйвера ODBC

- 7 На странице **Назначение администратора сети ViPNet** выберите пользователя (из числа зарегистрированных на данном узле), который будет выполнять функции администратора УКЦ.

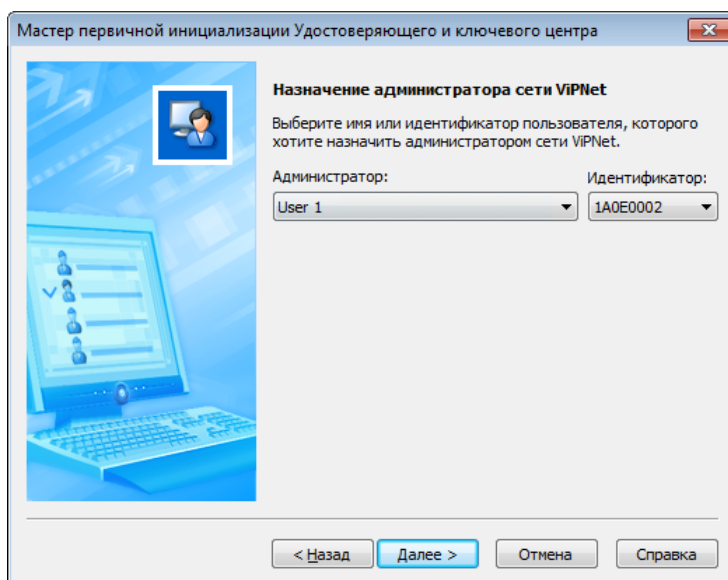


Рисунок 3: Выбор учетной записи администратора УКЦ

- 8 На странице **Пароль администратора сети ViPNet** выберите тип пароля для входа в УКЦ.

Рекомендуется выбрать тип **Собственный**.

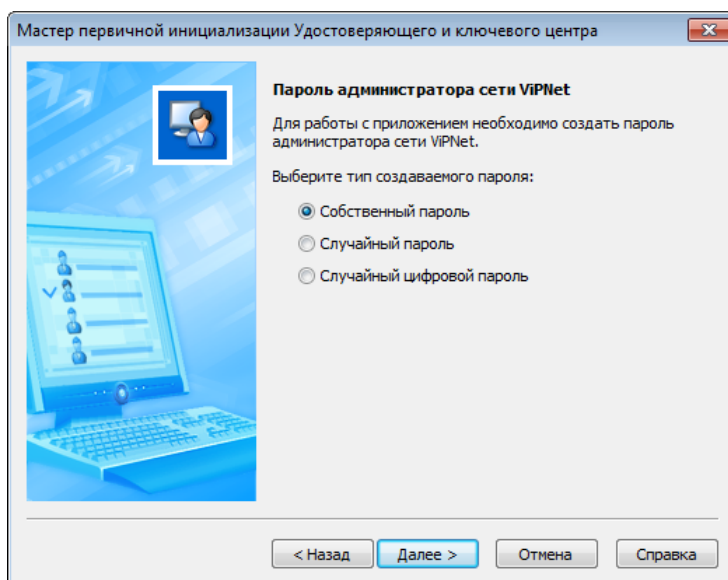


Рисунок 4: Выбор типа пароля администратора



Внимание! Запомните или запишите пароль! Без предварительного ввода пароля запуск УКЦ с текущей ключевой информацией будет невозможен. При утере восстановить данный пароль нельзя, вследствие чего потребуется заново устанавливать УКЦ и разворачивать сеть ViPNet с использованием новой ключевой информации.

- 9 На странице **База данных предыдущей версии УКЦ** в обязательном порядке установите флажок **Перенести ключевую информацию из обнаруженной базы данных в новую**.



Внимание! Если данное действие не будет выполнено, существующие ключи будут проигнорированы. Это приведет к нарушению работоспособности сети, так как невозможно будет произвести обновление ключей на сетевых узлах.

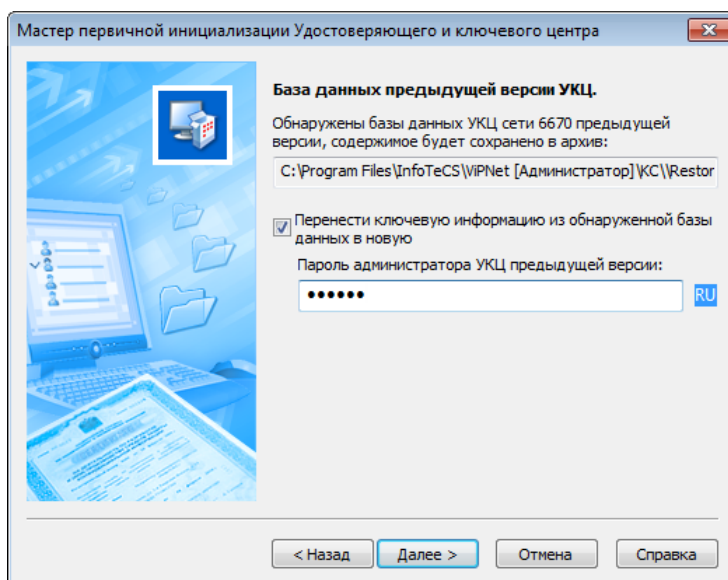


Рисунок 5: Настройка параметров работы с базой данных УКЦ предыдущей версии

По завершении работы мастера первичной инициализации произойдет запуск УКЦ.

- 10 Если до обновления в УКЦ использовалось несколько сертификатов администраторов (например, если было зарегистрировано несколько администраторов или для одного администратора было издано несколько сертификатов), то после запуска программы для каждого действительного сертификата каждого зарегистрированного администратора вручную сформируйте соответствующий список отозванных сертификатов (см. «[Список отозванных сертификатов \(СОС\)](#)»). Подробнее см. раздел [Формирование списков отозванных сертификатов](#) (на стр. 24).

В противном случае выполните просто проверку имеющегося СОС. Для этого в разделе **Удостоверяющий центр > Списки отозванных сертификатов > Своя сеть ViPNet** щелкните нужный СОС правой кнопкой мыши и в контекстном меню выберите пункт **Проверить**. Если СОС недействителен, обновите его с помощью пункта **Обновить** контекстного меню.

После выполнения какой-либо из вышеуказанных операций не формируйте обновления ключей.

- 11 Создайте новый пароль администратора сетевых узлов, входящих в группу **Вся сеть**.



Внимание! Пароль администратора сетевых узлов группы **Вся сеть**, который был задан в УКЦ версии 2.8.x, не переносится в УКЦ версии 3.2.x, поэтому его необходимо создать заново.

Данный пароль не является паролем для входа администратора в УКЦ.

Для этого:

- 11.1 В разделе **Ключевой центр** > **Своя сеть ViPNet** > **Сетевые группы** дважды щелкните по группе **Вся сеть** и на вкладке **Пароль администратора** нажмите кнопку **Создать пароль**.

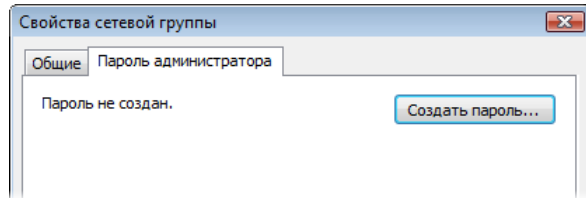


Рисунок 6: Просмотр пароля администратора

- 11.2 В окне **Пароль администратора** укажите тип пароля (рекомендуется использовать тип **Случайный**) и срок его действия, после чего нажмите кнопку **ОК**.

Максимальный срок действия пароля администратора сетевых узлов составляет 365 дней.

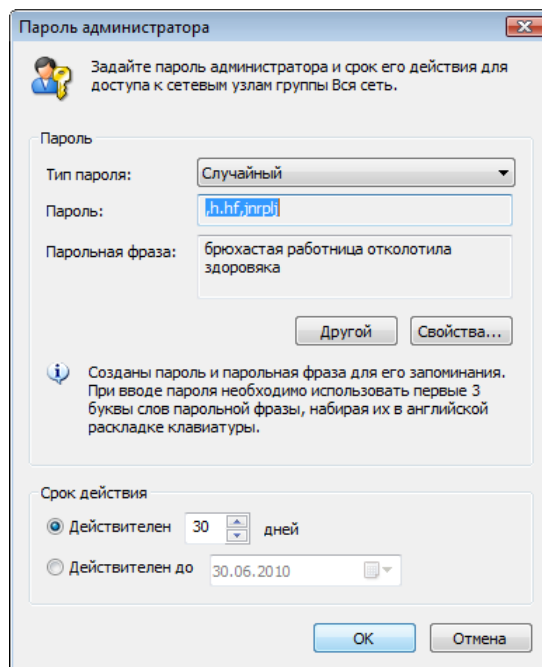


Рисунок 7: Указание пароля администратора и срока действия пароля

- 12 Завершите работу с УКЦ и запустите ЦУС.
- 13 В ЦУСе в меню **Службы** выберите пункт **Сформировать все справочники**.

- 14 Перенесите из ЦУСа в УКЦ файлы для создания ключей всех пользователей и ключей всех узлов. Для этого в ЦУСе в меню **Службы** выберите пункт **Файлы для создания ключей в УКЦ**, далее последовательно выберите пункты **Ключей пользователей** и **Ключей узлов**.



Внимание! Если в вашей сети есть координаторы с установленным программным обеспечением ViPNet Coordinator Linux, скопируйте из ЦУСа в УКЦ файлы для создания дистрибутивов таких координаторов. Для этого в меню **Службы** выберите пункт **Файлы для создания ключей в УКЦ** и далее **Дистрибутивов в полном объеме**. Выберите нужные координаторы, при этом категорически не рекомендуется копировать файлы для создания дистрибутивов других узлов.

- 15 Запустите УКЦ и приступите к созданию новых ключей пользователей и узлов. Прежде чем начать создание ключей, обязательно выполните следующие действия:
- В меню **Сервис** выберите пункт **Настройки**.
 - Если при создании ключей пользователей планируется формирование новых паролей пользователей сетевых узлов, в окне **Настройка** в разделе **Пароли** выполните настройку параметров создаваемых паролей.
 - При формировании ключей пользователей производится издание новых сертификатов открытого ключа подписи. Чтобы издание сертификатов происходило автоматически в соответствии с параметрами текущего шаблона сертификата, в окне **Настройка** в разделе **Сертификаты** в группе **Отображать сертификаты для редактирования** снимите флажок **При индивидуальном создании сертификатов**.
- 16 Создайте ключи пользователей. Для этого в разделе **Ключевой центр > Своя сеть ViPNet > Пользователи** выделите все записи пользователей и в контекстном меню выберите пункт **Ключи пользователя > Создать**. При создании ключей не рекомендуется изменять пароли пользователей ViPNet.



Внимание! При обновлении программного обеспечения ViPNet Administrator создание ключей пользователей должно производиться только один раз! Если для пользователя будет создано два и более набора ключей, после обновления ключей связь с узлом данного пользователя будет потеряна. Восстановить работоспособность узла можно будет только путем проведения первичной инициализации с использованием актуального дистрибутива ключей (файла *.dst). Однако следует учитывать, что вся зашифрованная корреспонденция в программе «Деловая почта» в таком случае будет утеряна.

17 Сформируйте ключи узлов. Для этого на панели инструментов нажмите кнопку

Создать ключи узлов  либо в меню **Сервис** выберите пункт **Автоматически создать > Ключи узлов**.



Внимание! Для координаторов с установленным программным обеспечением ViPNet Coordinator Linux сформируйте новые дистрибутивы ключей. Для этого в разделе **Ключевой центр > Своя сеть ViPNet > Сетевые узлы** выделите данные координаторы и в контекстном меню выберите пункт **Дистрибутивы ключей > Создать**.



Внимание! Убедитесь, что все предыдущие действия были произведены вами верно. Если вы считаете, что допустили какие-либо ошибки, следует удалить новую версию ViPNet Administrator, восстановить сохраненную копию версии 2.8.x и повторить все действия настоящей инструкции.

После выполнения п. 20 ваши действия станут необратимыми, поскольку на узлы защищенной сети будут отправлены новые ключи! Если в ходе выполнения предыдущих пунктов были допущены ошибки, то после принятия узлами обновленных ключей работоспособность защищенной сети может быть нарушена!

Восстановление функционирования сети будет возможно только с использованием дистрибутивов ключей, сформированных в ViPNet Administrator версии 3.2.x, но с потерей всей зашифрованной корреспонденции пользователей на узлах.

18 Перенесите ключи пользователей и ключи сетевых узлов из УКЦ в ЦУС.



Внимание! Если в вашей сети имеются пользователи, зарегистрированные на нескольких узлах, то перед переносом сделайте резервную копию ключей, сформированных для данных пользователей. Для этого скопируйте в любое защищенное место на компьютере соответствующие файлы `abn_АААА.ke` (где АААА — шестнадцатеричный идентификатор пользователя в защищенной сети) из вложенной папки `\КС\КЕУКЕУКЕ` папки установки ViPNet Administrator.

После переноса ключей пользователей в ЦУС указанные файлы из папки `\КС\КЕУКЕУКЕ` удаляются!

Данная операция необходима для того, чтобы впоследствии можно было получить и отправить ключи пользователей на сетевые узлы, тип коллектива на которых не является главным для этих пользователей (подробнее см. раздел [Обновление ключей пользователей, зарегистрированных на нескольких сетевых узлах](#) (на стр. 26)).

Для переноса:

- В разделе **Ключевой центр > Своя сеть ViPNet > Ключи > Ключи пользователей** выберите ключи всех пользователей и в контекстном меню выберите пункт **Перенести в ЦУС**.
- В разделе **Ключевой центр > Своя сеть ViPNet > Ключи > Ключи узлов** выберите все ключи сетевых узлов и в контекстном меню выберите пункт **Перенести в ЦУС**.



Внимание! Из УКЦ созданные для координаторов с программным обеспечением ViPNet Coordinator Linux дистрибутивы ключей перенесите в папку на диске. Для этого в разделе **Ключевой центр > Своя сеть ViPNet > Ключи > Дистрибутивы ключей** выделите дистрибутивы координаторов и в контекстном меню выберите команду **Перенести в папку**.

После этого защищенным способом передайте администраторам этих координаторов новые дистрибутивы ключей и сообщите дату их развертывания.

19 Перейдите в программу ЦУС.

20 Выполните отправку ключей с отсроченным вступлением в действие. Для этого в ЦУСе ознакомьтесь с сообщением о поступлении новых ключей пользователей и новых ключей узлов и в окне вопроса об отправке ключей нажмите кнопку **Да**. Выделите все узлы, на которые следует отправить обновления, и укажите отложенную дату проведения обновлений. Это гарантирует получение обновлений ключей всеми узлами защищенной сети до вступления этих обновлений в действие.

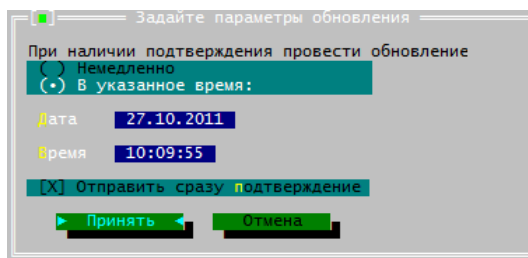


Рисунок 8: Указание даты и времени отправки обновлений

Рекомендуется указывать дату, на 2 дня (или более) превосходящую текущую дату. Установите дату ближайшего выходного дня (субботы или воскресенья) — если работа по обновлению проводится не позднее среды.

В течение рабочих дней до указанного выходного дня все узлы сети, на которых установлено программное обеспечение ViPNet Client или ViPNet Coordinator, должны функционировать, причем программное обеспечение ViPNet должно быть

запущено хотя бы один раз. Это необходимо для того, чтобы файлы обновлений поступили на узел.

Внимание! До наступления назначенной даты обновления администраторам безопасности сетей следует:

- Контролировать в ЦУСе в базе запросов и ответов процесс получения обновлений всеми сетевыми узлами, особенно координаторами.
- Если какие-либо узлы защищенной сети не получают обновления до назначенной даты, то после обновления ключей на других сетевых узлах связь с ними будет утрачена. В этом случае связь может быть восстановлена только вручную с помощью дистрибутива ключей (dst-файла), сформированного в ViPNet Administrator версии 3.2.x.
- Не изменять конфигурацию сети в ЦУСе (а именно не выполнять регистрацию новых сетевых узлов, пользователей, удаление имеющихся узлов, изменение связей и тому подобное) и не рассылать обновления.
- Не обрабатывать импорт, полученный из других сетей ViPNet.
- Не отправлять экспорт в другие сети ViPNet.



В результате при наступлении назначенной даты на включенных узлах обновления вступят в силу. При этом между включенными узлами установится связь на основе новых ключей.

На узлах, которые будут включены в первый рабочий день (или позднее) после назначенной даты, через 1–7 минут после включения и запуска программного обеспечения ViPNet произойдет обновление ключей и установится связь со всеми другими узлами сети, получившими и принявшими обновление.

Внимание! Если на сетевом узле предупреждение об обновлении ключей появилось в момент, когда запущена программа ViPNet Деловая почта, следует закрыть все файлы, открытые из вложений корреспонденции, завершить работу программы и выполнить прием обновления.



Если на сетевом узле в ходе приема обновления появится окно с предложением указать путь к файлу с резервным набором персональных ключей (имеется в виду файл AAAA.pk) или ввести пароль к нему, то следует указать путь к папке, в которой расположен данный файл, либо ввести соответствующий пароль. Данное окно не появится, если на узле файл AAAA.pk будет находиться в папке по умолчанию и пароль к нему совпадет с паролем пользователя.

При обновлении программного обеспечения ViPNet Administrator до версии 3.2.x связь с узлами других защищенных сетей ViPNet сохраняется, поскольку симметричные

межсетевые мастер-ключи не изменяются. Но после того как процесс обновления будет завершен, настоятельно рекомендуется сменить все межсетевые мастер-ключи, при условии, что в доверенных сетях уже используется программное обеспечение ViPNet Administrator версии 3.x. Это необходимо для перехода на более надежный алгоритм шифрования. Если в доверенных сетях используется программное обеспечение ViPNet Administrator версии 2.8.x, то данная операция не требуется. Однако стоит учесть, что взаимодействие с подобными доверенными сетями (использующими ViPNet Administrator версии 2.8.x или межсетевые мастер-ключи, созданные в программном обеспечении этой версии) будет существенно ограничено при зашифровании почтовой корреспонденции в приложениях ViPNet и при обмене служебной информацией. В дальнейшем (начиная с программного обеспечения ViPNet версии 4.x) взаимодействие с подобными доверенными сетями обеспечиваться не будет.

Информацию о том, как сменить межсетевой мастер-ключ можно найти в документе «ViPNet Administrator Удостоверяющий и ключевой центр. Руководство администратора».

Формирование списков отозванных сертификатов

В программе ViPNet Удостоверяющий и ключевой центр из состава программного обеспечения ViPNet Administrator версии 2.8.x независимо от количества зарегистрированных администраторов и количества сертификатов подписи у каждого из них, может быть сформирован и использоваться только один список отозванных сертификатов (СОС). В данный СОС в случае отзыва или приостановления действия попадают все сертификаты, изданные в УКЦ, независимо от того, каким администратором они были изданы и каким сертификатом администратора были заверены.

В УКЦ версии 3.2.x изменен порядок работы с СОС. Формирование СОС в новой версии осуществляется для каждого сертификата администратора, вследствие этого каждому сертификату администратора соответствует конкретный СОС.

В связи с данной функциональностью после обновления требуется для каждого действительного сертификата каждого зарегистрированного администратора вручную сформировать соответствующий СОС. В результате данной операции количество СОС должно стать равным количеству всех действительных в УКЦ сертификатов администраторов.

Чтобы сформировать нужное количество СОС, в УКЦ последовательно назначьте текущим каждый действительный сертификат каждого администратора, который не имеет соответствующего ему СОС.



Примечание. Если в УКЦ зарегистрировано несколько администраторов, то изменить текущий сертификат администратора можно при условии, что сам администратор является текущим.

Чтобы назначить текущим сертификат администратора:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в разделе **Администраторы** дважды щелкните по учетной записи текущего администратора.
- 2 В появившемся окне **Свойства администратора** на вкладке **Сертификаты** нажмите кнопку **Сертификаты**.

- 3 В окне **Сертификаты администратора** <имя администратора> в списке выберите сертификат, который должен стать текущим, и нажмите кнопку **Назначить текущим**.

После того как сертификат администратора будет выбран в качестве текущего, для него автоматически будет сформирован соответствующий СОС. В СОС будут помещены только сертификаты с отозванным и приостановленным действием, которые при издании были заверены сертификатом администратора, соответствующим этому СОС.



Внимание! Если операция по формированию СОС не будет выполнена (или СОС будут сформированы не для каждого действительного сертификата администратора), то после обновления ключей на узлах своей сети и после принятия экспорта в доверенных сетях ViPNet могут возникнуть проблемы с проверкой сертификатов пользователей.

Обновление ключей пользователей, зарегистрированных на нескольких сетевых узлах

Если в вашей сети существуют пользователи, зарегистрированные на нескольких сетевых узлах, то для корректного обновления ключей данных пользователей на всех узлах в процессе перехода программного обеспечения ViPNet Administrator на версию 3.2.x требуется выполнить ряд дополнительных действий.

После того как будет сделана резервная копия обновленных ключей пользователей, зарегистрированных на нескольких сетевых узлах (см. раздел [Процесс обновления ViPNet Administrator](#) (на стр. 14), п. 18), выполните следующие действия:

- 1 Поместите скопированные файлы `abn_АААА.ke` в подпапку `\КС\КЕУКЕУКЕ` папки установки ViPNet Administrator.



Внимание! Копирование файлов `abn_АААА.ke` в папку `\КС\КЕУКЕУКЕ` необходимо для того, чтобы сформированные ключи пользователя при переносе (см. п.3 данного списка) были перешифрованы на персональном ключе пользователя.

- 2 Перезапустите программу УКЦ.
- 3 В разделе **Ключевой центр > Своя сеть ViPNet > Ключи > Ключи пользователей** выберите появившиеся ключи пользователей и перенесите их в папку с помощью соответствующего пункта контекстного меню.
- 4 Перенесенные ключи (файлы `abn_АААА.ke`) по защищенному каналу отправьте пользователям, с указанием поместить их в подпапку `\ССС\key\` папки установки ViPNet Client на всех узлах, тип коллектива на которых не является для них главным. Поместить ключи в указанную папку пользователю следует до его аутентификации в программе ViPNet Client.

Данную операцию также может выполнить представитель пользователя (например, другой пользователь узла) при условии доверия к нему.

Внимание! Если на узле зарегистрирован один пользователь и его тип коллектива не является главным для этого пользователя, то файл `abn_АААА.ke` требуется поместить в подпапку `\ccc\key\` прежде чем будут высланы обновления ключей узлов (см. раздел [Процесс обновления ViPNet Administrator](#) (на стр. 14)).



Если на таком узле не окажется файла `abn_АААА.ke`, то связь с ним после обновления ключей будет потеряна, и восстановить работоспособность узла можно будет только с помощью дистрибутива ключей, сформированного в ViPNet Administrator версии 3.2.x, но с потерей всей зашифрованной корреспонденции пользователя в программе «Деловая почта».

В результате таким способом будут обновлены ключи пользователя, включая его закрытый ключ и сертификат, на всех узлах, на которых он зарегистрирован.



Глоссарий

С

Сертификат издателя

Сертификат, с помощью закрытого ключа которого подписывается другой сертификат.

Список отозванных сертификатов (СОС)

Список сертификатов, которые были отозваны администратором Удостоверяющего центра и на данный момент недействительны.

См. также: [Уполномоченное лицо \(администратор\) Удостоверяющего центра](#).