



НОВЫЕ ВОЗМОЖНОСТИ ViPNet Administrator 4.6

Приложение к документации ViPNet



© ОАО «ИнфоТеКС», 2019

ФРКЕ.00109-07 90 02

Версия продукта 4.6.7

Этот документ входит в комплект поставки продукта ViPNet, 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 зарегистрированным товарным знаком ОАО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

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.....	6
О документе.....	7
Для кого предназначен документ	7
Соглашения документа.....	7
Обратная связь.....	8
 Глава 1. Общие изменения в программном обеспечении ViPNet Administrator 4.6.....	9
Архитектура.....	10
Структура программы ViPNet Центр управления сетью	10
Механизм взаимодействия компонентов ПО ViPNet Administrator	11
Поддерживаемые операционные системы	13
Терминология	14
Роли сетевых узлов	16
Названия и назначение ролей.....	16
Состав ролей.....	17
Функции, перенесенные из ViPNet Центр управления сетью 3.2 в ViPNet	
Удостоверяющий и ключевой центр 4.6.....	19
Выделение ViPNet CSP в отдельную программу	22
Графический интерфейс.....	23
Система лицензирования	25
Увеличение минимальной допустимой длины паролей	28
Локализация интерфейса.....	29
Обновление документации и справки	30
 Глава 2. Новые возможности программы ViPNet Центр управления сетью 4.6	31
Создание сети ViPNet.....	33
Добавление сетевого узла.....	34
Управление защищенными DNS-серверами.....	36
Управление уровнем полномочий пользователя на координаторе	37
Объединение сетевых узлов и пользователей в группы	38
Связи между объектами сети.....	40
Формирование таблиц маршрутизации.....	41
Назначение адресов.....	42
Настройка подключения через межсетевой экран	44
Изменения в настройке параметров роли «Terminal».....	46

Туннелирование	47
Организация межсетевого взаимодействия	49
Отправка обновлений программного обеспечения на узлы	51
Обновление справочников и ключей при смене координатора узла.....	53
Работа с журналами событий	54
Настройка параметров безопасности сетевых узлов	56
Создание отчетов о структуре сети и лицензионных ограничениях	58
Глава 3. Новые возможности программы ViPNet Удостоверяющий и ключевой центр 4.6.....	61
Сертификаты и ключи электронной подписи.....	62
Создание ключей электронной подписи.....	62
Сроки действия сертификатов	63
Плановая смена ключа электронной подписи администратора.....	64
Обработка запросов на сертификаты со сроком действия ключа электронной подписи 3 года	65
Сохранение ключей электронной подписи в файл.....	66
Добавление информации о центрах регистрации в издаваемые сертификаты пользователей.....	67
Работа с сертификатами пользователей.....	68
Задание срока действия CRL в часах	70
Работа с большими списками	71
Ключи пользователей, ключи сетевых узлов и дистрибутивы ключей	72
Создание ключей пользователей и ключей сетевых узлов	72
Выдача дистрибутивов ключей.....	73
Создание и передача резервных наборов персональных ключей (РНПК).....	74
Обработка запросов на дистрибутивы ключей вручную	75
Настройка параметров аутентификации пользователя.....	75
Новые способы аутентификации пользователя	76
Выдача паролей пользователей	77
Компрометация ключей пользователя	79
Распаковка ключей и дистрибутивов ключей	79
Отказ от использования обновлений ключей узлов	79
Учет ключей ДСДР	80
Административные функции.....	82
Отказ от использования нескольких учетных записей администратора	82
Смена пароля администратора и ключа защиты УКЦ	83
Удаление паролей администраторов сетевых узлов.....	84
Новая система оповещений в программе ViPNet Удостоверяющий и ключевой центр	85

Организация межсетевого взаимодействия	86
Передача сертификатов администраторов и CRL в доверенную сеть	87
Автоматический режим работы	87
Реализация системного журнала событий	89
Резервное копирование конфигурации сети	90
Обмен данными с программой ViPNet Publication Service	92
Приложение А. Глоссарий	93



Введение

О документе	7
Обратная связь	8

О документе

Данный документ содержит описание основных изменений и новых функциональных возможностей программного обеспечения [ViPNet Administrator](#) (см. глоссарий, стр. 93) версии 4.6.7, в частности его компонентов [ViPNet Центр управления сетью \(ЦУС\)](#) (см. глоссарий, стр. 93) и [ViPNet Удостоверяющий и ключевой центр \(УКЦ\)](#) (см. глоссарий, стр. 93), по сравнению с версией 3.2.12.

Для кого предназначен документ

Данный документ предназначен для технических специалистов, партнеров ОАО «ИнфоТекС» и администраторов сетей ViPNet®.

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.

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>.

1

Общие изменения в программном обеспечении ViPNet Administrator 4.6

Архитектура	10
Поддерживаемые операционные системы	13
Терминология	14
Роли сетевых узлов	16
Функции, перенесенные из ViPNet Центр управления сетью 3.2 в ViPNet Удостоверяющий и ключевой центр 4.6	19
Выделение ViPNet CSP в отдельную программу	22
Графический интерфейс	23
Система лицензирования	25
Увеличение минимальной допустимой длины паролей	28
Локализация интерфейса	29
Обновление документации и справки	30

Архитектура

Принципиальные архитектурные отличия программного обеспечения [ViPNet Administrator](#) (см. глоссарий, стр. 93) версии 4.6.7 от версии 3.2.12 заключаются в следующем:

- изменена структура программы ViPNet Центр управления сетью (см. [Структура программы ViPNet Центр управления сетью](#) на стр. 10);
- изменен механизм взаимодействия программ ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр (см. [Механизм взаимодействия компонентов ПО ViPNet Administrator](#) на стр. 11).

Структура программы ViPNet Центр управления сетью

Структура программы [ViPNet Центр управления сетью \(ЦУС\)](#) (см. глоссарий, стр. 93) версии 4.6.7 по сравнению с версией 3.2.12 показана на схеме ниже.



Рисунок 1. Структура программы версии 3.x и 4.x

В отличие от программы ViPNet Центр управления сетью версии 3.2.12, программа ViPNet Центр управления сетью версии 4.6.7 состоит из двух взаимосвязанных программных компонентов: серверного и клиентского приложений. При этом для организации многопользовательского режима работы к серверному приложению может подключаться несколько клиентских приложений, что позволяет:

- снизить нагрузку на компьютер администратора и управлять структурой сети ViPNet с нескольких рабочих мест;
- распределить обязанности по администрированию больших сетей между несколькими администраторами;
- повысить надежность и работоспособность сети в целом.

Серверное приложение ViPNet Центр управления сетью представляет собой набор служб, которые осуществляют чтение и запись информации в базу данных SQL (см. [Механизм взаимодействия компонентов ПО ViPNet Administrator](#) на стр. 11) и обеспечивают взаимодействие с клиентским приложением. Серверное приложение и база данных могут быть установлены на разные компьютеры.

Клиентское приложение обеспечивает удобный графический интерфейс для управления структурой [сети ViPNet](#) (см. глоссарий, стр. 97) и свойствами сетевых объектов. Оно может быть установлено на одном компьютере с серверным приложением, на удаленном компьютере или на нескольких компьютерах, если управление сетью ViPNet осуществляется с нескольких рабочих мест.

Механизм взаимодействия компонентов ПО ViPNet Administrator

На схеме ниже представлены схемы взаимодействия программ, входящих в состав программного обеспечения (ПО) ViPNet Administrator версий 3.2.12 и 4.6.7.

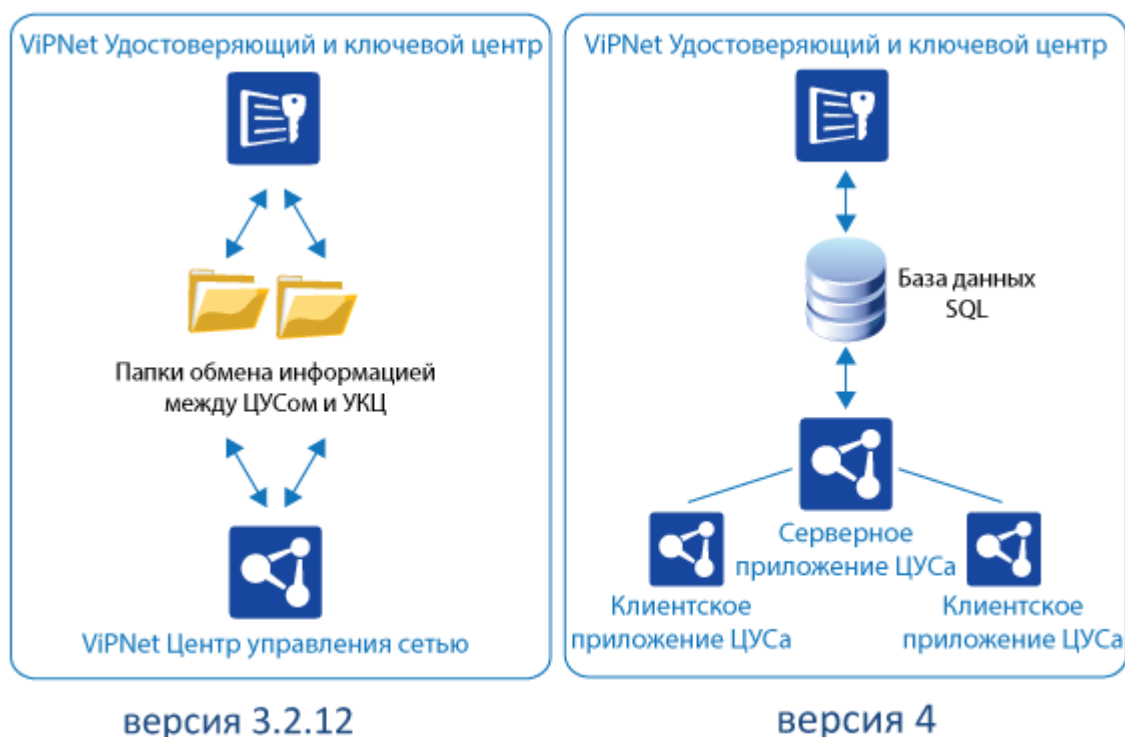


Рисунок 2. Механизмы взаимодействия разных версий ЦУСа и УКЦ

В ПО ViPNet Administrator версии 3.2.12 взаимодействие между двумя его компонентами — программой [ViPNet Центр управления сетью](#) (ЦУС) (см. глоссарий, стр. 93) и программой [ViPNet Удостоверяющий и ключевой центр](#) (УКЦ) (см. глоссарий, стр. 93) — осуществляется при помощи папок на диске (или сетевых папок):

- \For NCC — для размещения файлов, предназначенных для обработки в ЦУСе;

- \From NCC — для размещения файлов, обработанных в ЦУСе.

Неудобство такой схемы заключается в том, что в некоторых случаях могут возникать конфликты во время обращения к файлам на диске. Кроме того, скорость работы с файлами при обработке большого количества информации может быть низкой.

В ПО ViPNet Administrator версии 4.6.7 программы ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр независимо друг от друга обращаются к базе данных SQL, в которой хранится вся информация о структуре и настройках сети ViPNet. При этом изменения, выполненные в одной программе, незамедлительно применяются в другой, а для случая, когда программы пытаются одновременно внести изменения в базу данных, реализована функция блокировки их действий (например, когда в УКЦ создаются ключи, в ЦУСе нельзя изменить структуру сети).

Такой механизм взаимодействия компонентов ПО ViPNet Administrator повышает надежность работы программ и их устойчивость к различным сбоям.

В качестве базы данных SQL вы можете использовать:

- экземпляр SQL-сервера, который может быть автоматически создан во время установки серверного приложения ЦУСа (в состав ПО ViPNet Administrator версии 4.6.7 включена программа Microsoft SQL Server 2014 Express);
- существующий экземпляр SQL-сервера, установленный на локальный или удаленный компьютер и имеющий определенные параметры

Подробную информацию об использовании SQL-сервера см. в документе «ViPNet Administrator. Руководство по установке», в главе «Установка программного обеспечения ViPNet Administrator», в разделе «Информация для администраторов SQL».

Поддерживаемые операционные системы

Программа ViPNet Центр управления сетью версии 3.2.12 является DOS-приложением и может быть установлена только на компьютер с 32-разрядной операционной системой Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 или Windows 7.

В связи с изменениями в архитектуре ПО ViPNet Administrator версии 4.6.7 (см. [Архитектура](#) на стр. 10) и распространением операционных систем новых версий, теперь для программ ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр поддерживаются следующие операционные системы:

- Windows 7 (32/64-разрядная);
- Windows Server 2008 R2 (64-разрядная);
- Windows 8 (32/64-разрядная);
- Windows Server 2012 (64-разрядная);
- Windows 8.1 (32/64-разрядная);
- Windows Server 2012 R2 SP1 (64-разрядная);
- Windows 10 (32/64-разрядная).

Подробную информацию о системных требованиях см. в документе «ViPNet Administrator. Руководство по установке», в главе «Введение», в разделе «Системные требования».

Терминология

В связи с переработкой функциональности и логики работы ПО ViPNet Administrator версии 4.6.7 по сравнению с версией 3.2.12 изменились некоторые термины и названия элементов интерфейса, содержащие эти термины. Кроме того, некоторые термины приведены в соответствие с Федеральным законом №63-ФЗ «Об электронной подписи» от 06 апреля 2011 года.

Основные изменения в терминологии представлены в следующей таблице.

Таблица 3. Отличия терминологии ViPNet Administrator 3.2.12 и 4.6.7

Термин в ViPNet Administrator 3.2.12	Термин в ViPNet Administrator 4.6.7	Комментарий
Абонентский пункт	Клиент	
Адресные справочники	Справочники	
Владелец сертификата	Владелец сертификата ключа проверки электронной подписи (владелец сертификата)	
Группа СУ (сетевая группа)	Группа узлов	Группа узлов, в отличие от сетевой группы, предназначена только для логического объединения узлов (см. Объединение сетевых узлов и пользователей в группы на стр. 38). Объединение узлов в группы позволяет оптимизировать процессы создания связей между сетевыми узлами и отправки справочников, ключей и обновлений ПО ViPNet на узлы.
Закрытый ключ	Ключ электронной подписи (ключ ЭП)	
Импорт	Входящая межсетевая информация	
Ключевая дискета (3.2.2 и ниже)	Ключи пользователя	
Ключевой набор (3.2.2 и ниже)	Ключи узла	
Коллектив	Нет	

Термин в ViPNet Administrator 3.2.12	Термин в ViPNet Administrator 4.6.7	Комментарий
Нет	Группа пользователей	Группа пользователей предназначена для объединения пользователей, задания связей с другими пользователями или группами пользователей (см. Объединение сетевых узлов и пользователей в группы на стр. 38). Группа пользователей является аналогом типа коллектива, в котором зарегистрировано несколько пользователей.
Отзыв сертификата	Аннулирование сертификата	
Открытый ключ	Ключ проверки электронной подписи (ключ проверки ЭП)	
Подпись	Электронная подпись (ЭП)	
Прикладная задача	Роль	
Сервер-маршрутизатор	Координатор	В интерфейсе программы ViPNet Центр управления сетью термин «Сервер-маршрутизатор» был изменен на «Координатор». Однако координаторы по-прежнему выполняют функцию сервера-маршрутизатора почтовых и служебных конвертов.
Сертификат открытого ключа подписи пользователя	Сертификат ключа проверки электронной подписи (сертификат)	
Список отозванных сертификатов (COC)	Список аннулированных сертификатов (CRL)	
Тип коллектива	Нет	В программе ViPNet Центр управления сетью 4.6.7 понятие используется только во внутренней логике работы программы. При межсетевом взаимодействии с сетью на базе ViPNet Administrator 3.2.12 типы коллектива отображаются в ЦУСе доверенной сети.
Экспорт	Исходящая межсетевая информация	

Роли сетевых узлов

В ПО ViPNet Administrator версии 3.2.12 возможность использования какой-либо функциональности ПО ViPNet на сетевом узле определяется прикладными задачами. В ПО ViPNet Administrator версии 4.6.7 прикладные задачи называются ролями. В связи с переработкой функциональности и логики работы ПО ViPNet Administrator изменились названия и назначение некоторых ролей (см. [Названия и назначение ролей](#) на стр. 16), а также были реализованы новые роли и удалены устаревшие роли (см. [Состав ролей](#) на стр. 17).

Подробно о добавлении ролей на сетевые узлы см. в документе «ViPNet Центр управления сетью. Руководство администратора», в главе «Настройка параметров сетевых узлов», в разделе «Добавление ролей на сетевые узлы», полный список ролей и описание их особенностей — в документе «ViPNet Центр управления сетью. Руководство администратора», в приложении «Роли сетевых узлов».

Названия и назначение ролей

Роли сетевых узлов, названия которых были изменены в ПО ViPNet Administrator версии 4.6.7, перечислены в таблице ниже.

Таблица 4. Старые и новые названия ролей сетевых узлов в ПО ViPNet Administrator

Идентификатор роли	Название в версии 3.2.12	Название в версии 4.6.7
0000	Деловая почта	Business Mail
0004	Центр управления сетью	Network Control Center
0005	Диспетчер	Dispatcher
000C	Центр управления политиками	Policy Manager
0017	Защита трафика	VPN-клиент
001A	Сервер IP-адресов	Программный VPN-координатор
001D	Центр регистрации	Registration Point
001E	Секретный диск	SafeDisk
0020	КриптоСервис	CryptoService
002C	Web-шлюз	Web Gate
0032	ViPNet Cluster	Cluster Windows
0038	Сервис публикации	Publication Service
0047	Сервер мониторинга	StateWatcher

Идентификатор роли	Название в версии 3.2.12	Название в версии 4.6.7
0048	КриптоСервис Linux	CryptoService Linux

Помимо названия, изменились особенности использования для роли «Terminal». В ПО ViPNet Administrator версии 3.2.12 задать параметры для программного обеспечения ViPNet Terminal можно только индивидуально для каждого клиента, на который добавлена роль «Terminal». В ПО ViPNet Administrator версии 4.6.7 задать эти параметры можно как индивидуально, так и централизованно, то есть сразу для всех клиентов с ролью «Terminal».

В ПО ViPNet Administrator версии 4.6.7 название параметра функции сервера открытого Интернета в свойствах ролей для различных модификаций координаторов переименовано в защищенный интернет-шлюз.

Состав ролей

В ПО ViPNet Administrator версии 4.6.7 добавлены следующие новые роли сетевых узлов:

- «Сервер DNS» и «Сервер WINS» — позволяют централизованно задавать список серверов DNS или WINS, используемых пользователями сети ViPNet для подключения к корпоративным ресурсам через Интернет.

В сетях ViPNet, работающих под управлением ПО ViPNet Administrator версии 3.2.12, список корпоративных серверов DNS или WINS можно задать только вручную на каждом сетевом узле, редактируя файл `dns.txt`.

- «Обмен сообщениями и файлами» — позволяет разрешать использование встроенных средств коммуникации на защищенном узле. С помощью этой роли можно защитить сетевые узлы от получения нежелательных сообщений и файлов, а также запретить отдельным сетевым узлам обмен сообщениями и файлами.

В сетях ViPNet, работающих под управлением ПО ViPNet Administrator версии 3.2.12, ограничений на использование встроенных средств коммуникации на узлах сети ViPNet нет.

- «Client for Linux» — позволяет установить ПО ViPNet Client for Linux для защиты IP-трафика на клиентах с ОС Linux.
- «Connect» — позволяет использовать на защищенном узле программу ViPNet Connect. Пользователи этой программы могут звонить друг другу и обмениваться мгновенными текстовыми сообщениями.
- «Coordinator HW50 A», «Coordinator HW50 B», «Coordinator HW1000 C», «Coordinator HW1000 D», «Coordinator HW5000» — позволяют развернуть координаторы на базе соответствующих программно-аппаратных комплексов.
- «Coordinator IG10», «Coordinator IG10 A/B», «Coordinator IG100 A/B» — позволяет развернуть координатор соответствующих вариантов исполнения ПАК ViPNet Coordinator IG10 и ПАК ViPNet Coordinator IG100.

- «Coordinator KB2000» и «Coordinator KB5000» — позволяют развернуть координатор на базе соответствующих вариантов исполнения ПАК ViPNet Coordinator.
- «StateWatcher SHW1000» и «StateWatcher SHW2000» — позволяют развернуть сервер системы мониторинга ViPNet StateWatcher на базе соответствующих ПАК StateWatcher SHW.
- «StateWatcher VA» — позволяет развернуть сервер системы мониторинга ViPNet StateWatcher на базе виртуального устройства Statewatcher VA.
- «xF100», «xF1000», «xF1000 C», «xF1000 D», «xF5000», «xF-VA» — позволяют развернуть координатор на базе соответствующих вариантов исполнения ПАК ViPNet xFirewall.
- «Failover xF100» — позволяет развернуть кластер горячего резервирования на базе ПАК ViPNet xFirewall 100.
- «IPS100», «IPS1000», «IPS1000 C», «IPS1000 D», «IPS5000» и «IPS-VA» — позволяют использовать систему предотвращения вторжений (IPS) для соответствующих вариантов исполнения ПАК ViPNet xFirewall.
- «ConServer» — позволяет установить серверное ПО для организации групповых чатов с помощью клиентского приложения ViPNet Connect.
- «CPNs» (Customer Push Notification Server) — позволяет развернуть серверное ПО для рассылки push-уведомлений на устройства с ViPNet Connect.
- «QSS Server», «QSS Point» и «QSS Phone» — позволяют развернуть сетевые узлы на базе продуктов ViPNet QSS Server, ViPNet QSS Point и ViPNet QSS Phone соответственно для сети с квантовым распределением ключей.

В связи с неактуальностью из ПО ViPNet Administrator версии 4.6.7 удалены следующие роли: «Удостоверяющий и ключевой центр», «Агент мониторинга», «Сервер TSP/OCSP», «Security Gateway», «VPN-Координатор KB2», «Координатор HW110», «Координатор HW100R», «Координатор HW100R advanced», а также ряд ролей, позволявших использовать на сетевом узле программу ViPNet Client со специальными настройками («Терминал Навигатор», «ИСУ Магистраль» и другие).

Функции, перенесенные из ViPNet Центр управления сетью 3.2 в ViPNet Удостоверяющий и ключевой центр 4.6

Несколько функций, которые выполняются в программе ViPNet Центр управления сетью 3.2.12, перенесены в программу ViPNet Удостоверяющий и ключевой центр 4.6.7, а именно:

1 Назначение права электронной подписи.

Администратор программы ViPNet Удостоверяющий и ключевой центр может разрешить или запретить использование [электронной подписи](#) (см. глоссарий, стр. 98). Если использование электронной подписи разрешено, то в процессе формирования дистрибутива ключей или новых ключей пользователя создается [сертификат ключа проверки электронной подписи](#) (см. глоссарий, стр. 97).

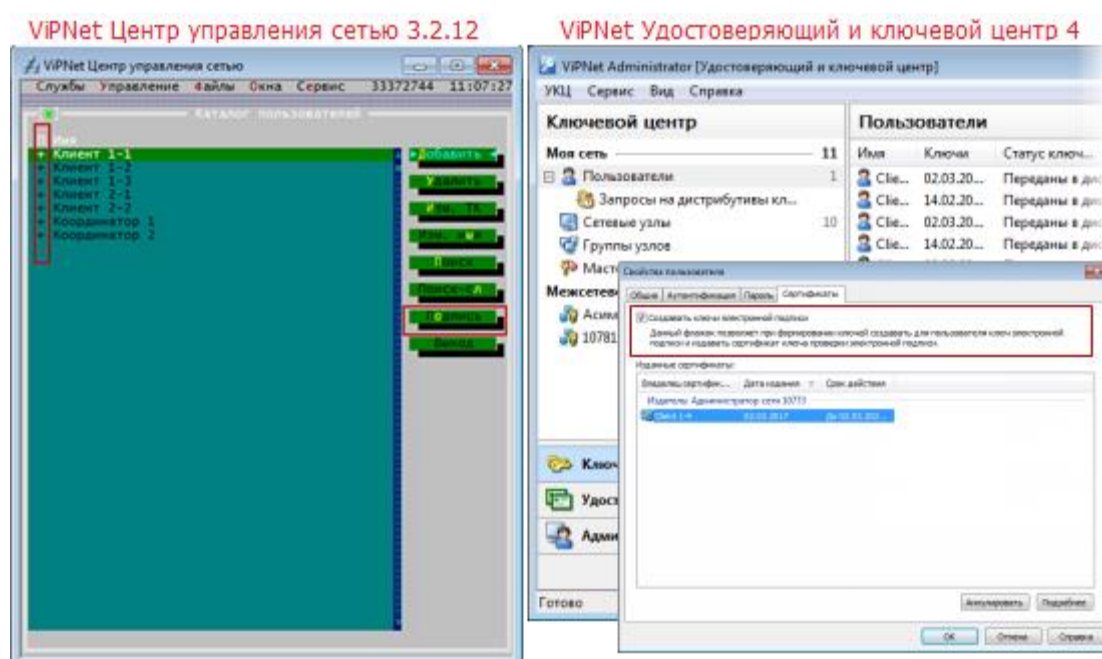


Рисунок 3. Назначение права электронной подписи

2 Выбор узлов для рассылки [списков аннулированных сертификатов](#) (см. глоссарий, стр. 97).

Рассылка списков аннулированных сертификатов в случае их изменения осуществляется согласно заданному в программе ViPNet Удостоверяющий и ключевой центр списку сетевых узлов. На все остальные сетевые узлы обновленные списки аннулированных сертификатов отправляются в комплексах CRL. При первом запуске программы ViPNet Удостоверяющий и ключевой центр список рассылки пуст, и вы можете самостоятельно его сформировать.

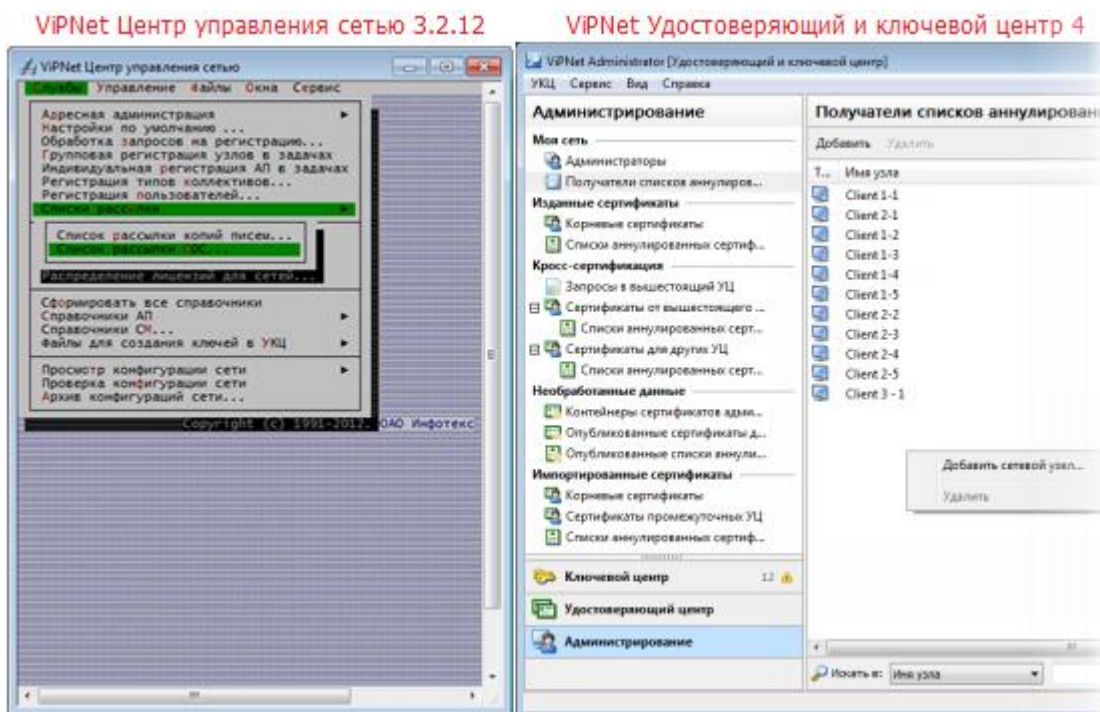


Рисунок 4. Настройка рассылки списков аннулированных сертификатов

3 Компрометация ключей (см. глоссарий, стр. 95).

Все операции при компрометации ключей пользователя или сетевого узла выполняются в программе ViPNet Удостоверяющий и ключевой центр.

В программе ViPNet Удостоверяющий и ключевой центр версии 3.2 действия в случае компрометации выполнялись отдельно для ключей пользователя и ключей сетевого узла. Теперь вы можете считать скомпрометированными только ключи пользователя. При этом, когда ключи пользователя считаются скомпрометированными, автоматически изменяются вариант персонального ключа пользователя и вариант ключей всех узлов, на которых зарегистрирован пользователь.

После этого на основе измененных вариантов ключей создаются новые ключи пользователя и ключи сетевых узлов, на которых он зарегистрирован. Операция создания ключей при компрометации удалена. Также теперь при компрометации ключей пользователя требуется создавать ключи для узлов, имеющих связь с узлом скомпрометированного пользователя.

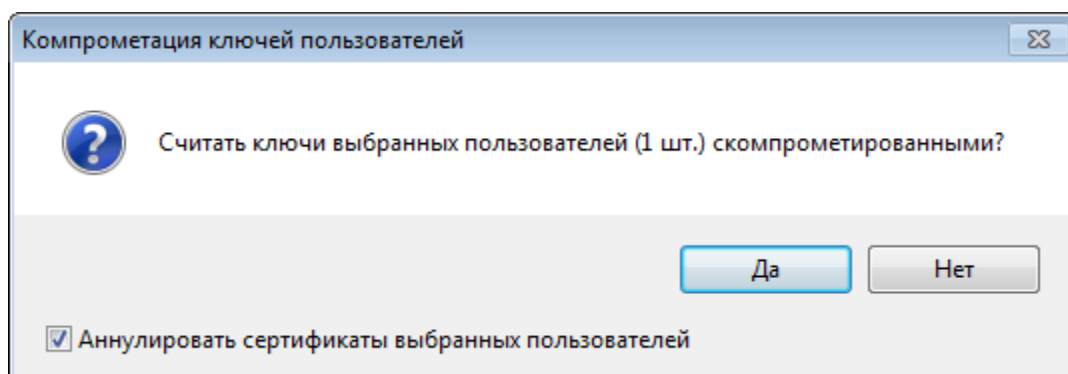


Рисунок 5. Компрометация ключей пользователя вместе с компрометацией ключей его узла

Также реализована возможность изменения варианта персонального ключа пользователя и ключей узла в случае неявной компрометации ключей (если нет фактов, подтверждающих компрометацию ключей, но есть подозрение, что злоумышленник получил доступ к ним) или планово в соответствии с регламентом политики безопасности организации.

Подробно о процедуре компрометации см. в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», в главе «Управление ключевой структурой ViPNet», в разделе «Компрометация ключей».

Выделение ViPNet CSP в отдельную программу

В состав программы ViPNet Удостоверяющий и ключевой центр версии 3.2.12 входит криптопровайдер ViPNet CSP. Вместе с программой ViPNet Удостоверяющий и ключевой центр версии 4.6.7 также устанавливается криптопровайдер ViPNet CSP, однако теперь он представляет собой отдельную программу, что позволяет обновлять его независимо от программы ViPNet Удостоверяющий и ключевой центр.

Графический интерфейс

В отличие от программы ViPNet Центр управления сетью версии 3.2.12, текстовый интерфейс которой оформлен с использованием символов псевдографики, программа ViPNet Центр управления сетью версии 4.6.7 имеет новый интуитивно понятный графический интерфейс пользователя, который значительно упрощает работу с программой.

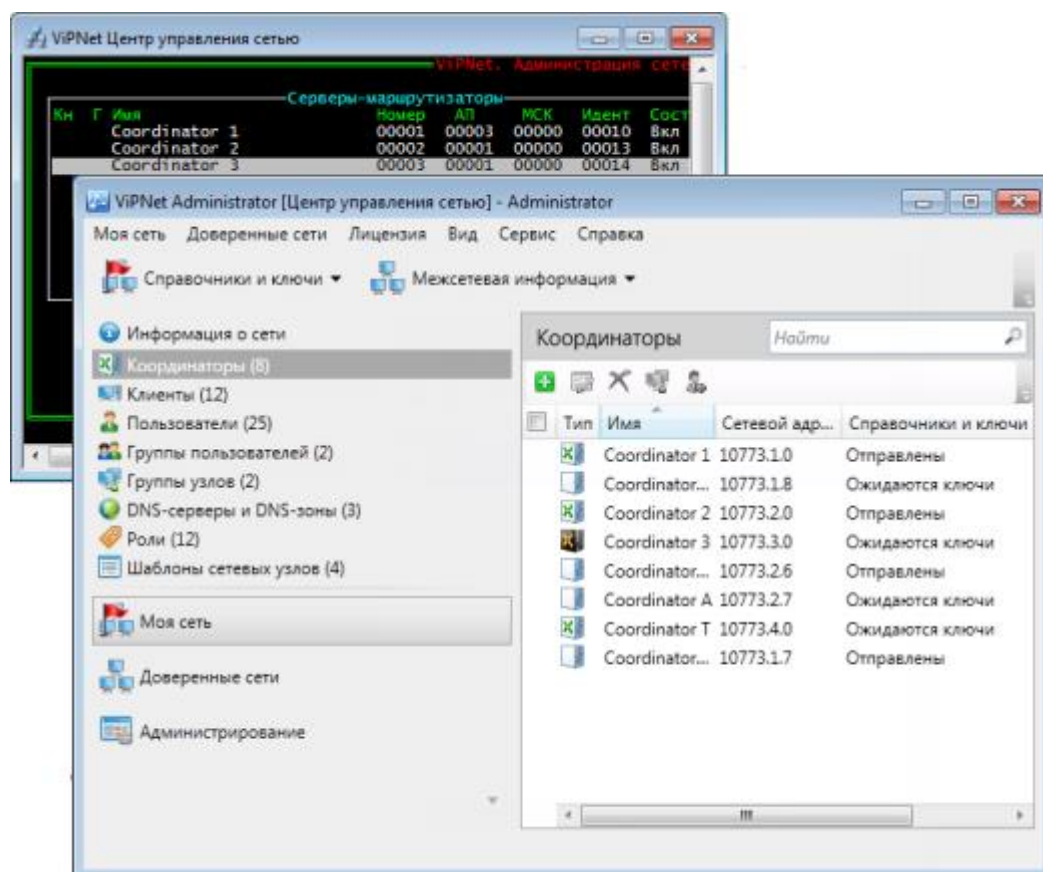


Рисунок 6. Сравнение интерфейса программы ViPNet Центр управления сетью версий 3.2.12 и 4.6.3

В главном окне программы ViPNet Центр управления сетью версии 4.6.7 реализовано три представления, в каждом из которых логически сгруппированы следующие функции:

- В представлении **Моя сеть** осуществляется работа с объектами своей сети ViPNet.
- В представлении **Доверенные сети** выполняются действия по установлению [межсетевого взаимодействия с другими сетями](#) (см. глоссарий, стр. 95).
- В представлении **Администрирование** осуществляется работа с журналами событий и учетными записями администраторов.

Графический интерфейс пользователя программы ViPNet Удостоверяющий и ключевой центр версии 4.6.7 также переработан по сравнению с версией 3.2.12.

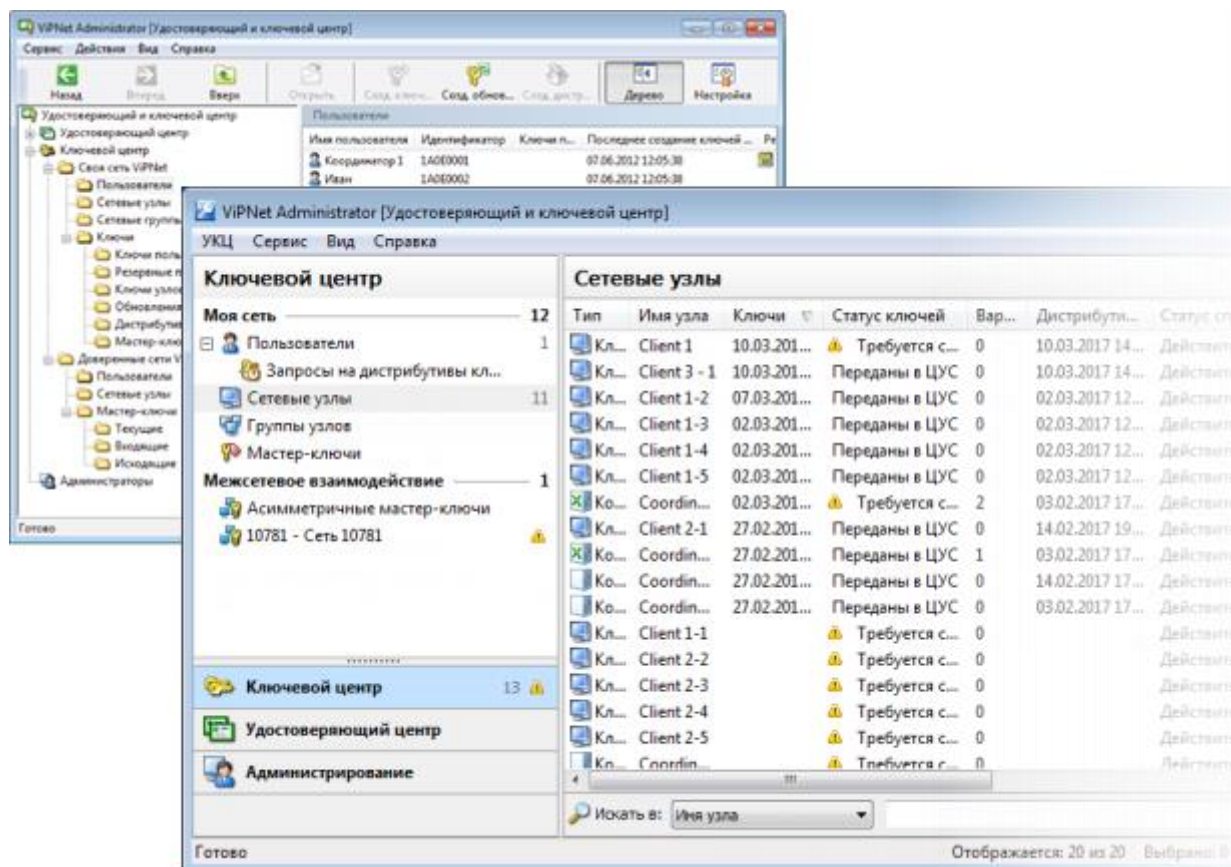


Рисунок 7. Сравнение интерфейса программы ViPNet Удостоверяющий и ключевой центр версий 3.2.12 и 4.6.4

Главное окно программы ViPNet Удостоверяющий и ключевой центр версии 4.6.7 содержит три представления, каждое из которых объединяет следующие функции:

- В представлении **Ключевой центр** осуществляется управление ключевой структурой ViPNet.
- В представлении **Удостоверяющий центр** выполняются действия с сертификатами.
- В представлении **Администрирование** осуществляется работа с учетными записями и сертификатами администраторов своей сети.

Система лицензирования

Лицензия для развертывания сети под управлением ПО ViPNet Administrator версии 3.2.12 предоставляется в двух файлах: `infotecs.re` и `infotecs.reg`. Для начала работы с ПО ViPNet Administrator версии 3.2.12 эти файлы необходимо разместить в папках с установленными программами ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр.

Лицензия для развертывания сети под управлением ПО ViPNet Administrator версии 4.6.7 может предоставляться в одном из следующих файлов: `*.itcslic` либо `infotecs.reg`. Чтобы начать работу с ПО ViPNet Administrator версии 4.6.7, при первом запуске серверного приложения ЦУСа требуется указать файл лицензии (подробнее см. в документе «ViPNet Administrator. Руководство по установке», в главе «Начало работы», в разделе «Первый запуск программы ViPNet Центр управления сетью»).

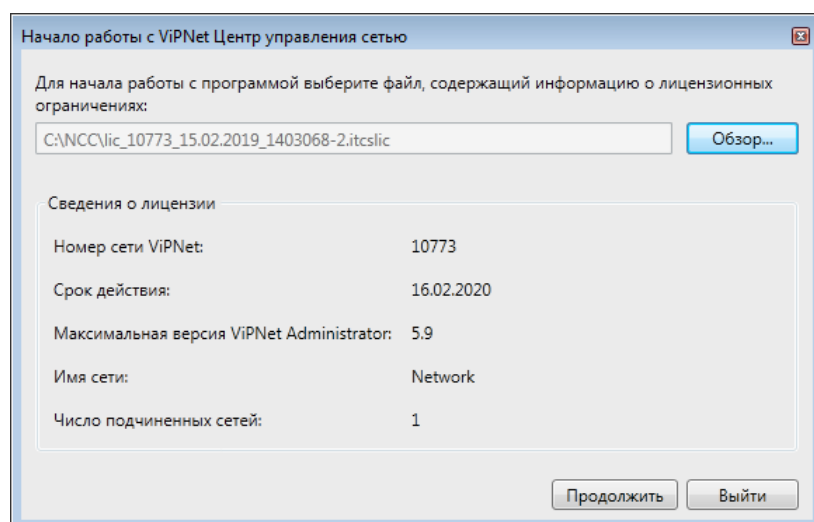


Рисунок 8. Указание пути к файлу лицензии

Кроме того, в системе лицензирования произошли следующие изменения:

- Файл лицензии ограничивает не количество клиентов и координаторов сети ViPNet, а число ролей, которое вы можете добавить на узлы вашей сети. Таким образом ограничивается число программ ViPNet, которое вы можете устанавливать на сетевые узлы.
- Добавлена возможность управления версиями отдельных компонентов ViPNet. Файл лицензии может включать в себя дополнительные ограничения для ролей по версии и периоду использования устанавливаемого программного обеспечения. Например, для одного узла с ролью «VPN-клиент» можно выбрать установку программы ViPNet Client последней версии и с индивидуальным периодом использования. На остальных узлах с той же ролью можно использовать программу ViPNet Client предыдущей версии в течение общего срока действия лицензии.

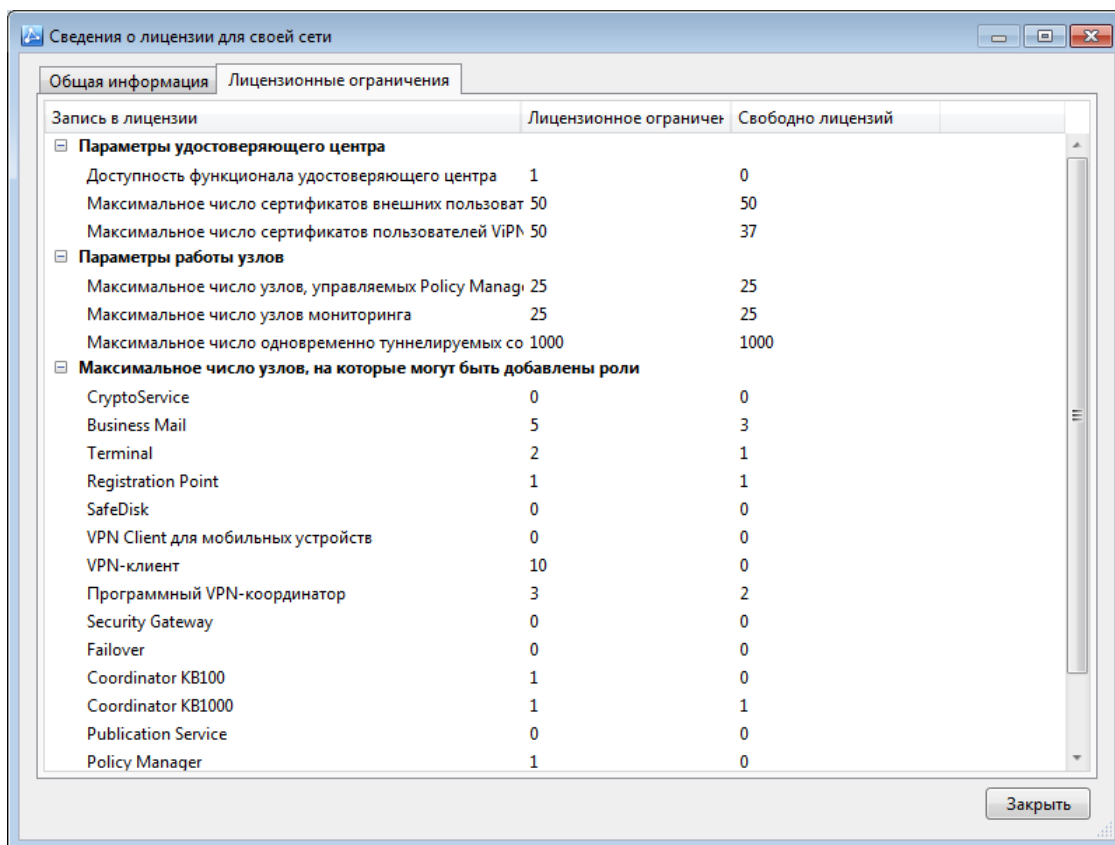


Рисунок 9. Просмотр информации о лицензионных ограничениях

- Лицензия не только ограничивает количество сертификатов, которое может быть издано в УКЦ, но и может полностью исключать функции удостоверяющего центра (при этом соответствующие элементы интерфейса не отображаются). Впоследствии вы можете разблокировать функции удостоверяющего центра, обновив лицензию.

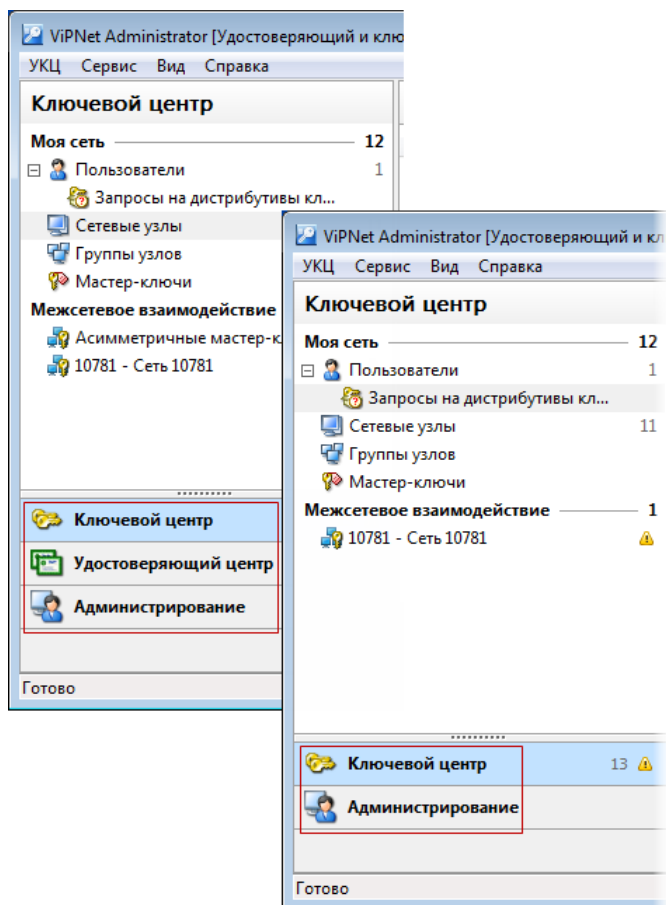


Рисунок 10. Изменение интерфейса программы ViPNet Удостоверяющий и ключевой центр при блокировании функций удостоверяющего центра

Увеличение минимальной допустимой длины паролей

В соответствии с требованиями безопасности минимальная допустимая длина паролей, задаваемых для пользователей и администраторов в программе ViPNet Удостоверяющий и ключевой центр 4.6.7, а также формируемых для администраторов в программе ViPNet Центр управления сетью увеличена до 8 символов. При попытке задания пароля, состоящего из меньшего числа символов, появляется предупреждение.

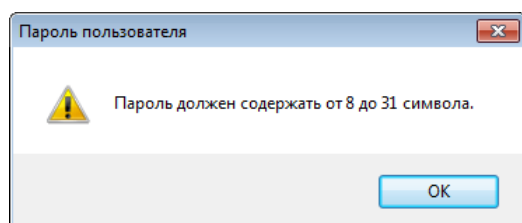


Рисунок 11. Предупреждение о недостаточной длине пароля

Локализация интерфейса

Программы ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр версии 3.2.12 доступны только на русском языке.

Программа ViPNet Удостоверяющий и ключевой центр версии 4.6.7 доступна как на русском языке, так и английском. Для каждой локализации предусмотрен отдельный установочный файл.

Серверное и клиентское приложение программы ViPNet Центр управления сетью версии 4.6.7 также доступны на русском и английском языках. Язык интерфейса серверного приложения выбирается при установке программы.

При установке клиентского приложения пользователем выбирается язык только для программы установки. Язык интерфейса клиентского приложения определяется автоматически при подключении к серверному приложению и совпадает с языком, выбранным для серверного приложения. Чтобы изменить язык клиентского приложения, вам необходимо переустановить серверное приложение и выбрать нужный язык.

Подробную информацию об установке программ см. в документе «ViPNet Administrator. Руководство по установке», в главе «Установка программного обеспечения ViPNet Administrator».

Обновление документации и справки

Документация и справка для программ Центр управления сетью и ViPNet Удостоверяющий и ключевой центр версии 4.6.7 полностью переработаны, а также переведены на английский язык. При этом акцент был сделан на описании основных сценариев работы с программами.

В комплект поставки программного обеспечения ViPNet Administrator версии 4.6.7 входят следующие документы:

- «ViPNet Administrator. Руководство по установке».
- «ViPNet Administrator. Руководство по обновлению с версии 3.2.x до версии 4.x».
- «ViPNet Administrator. Руководство по миграции программного обеспечения на другой компьютер».
- «ViPNet Administrator. Быстрый старт».
- «ViPNet Центр управления сетью. Руководство администратора».
- «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».
- «ViPNet Administrator. Руководство по смене мастер-ключей в сети ViPNet».
- «ViPNet CSP. Руководство пользователя».
- «Развертывание сети с помощью ViPNet Administrator 4.x. Руководство администратора».
- «Новые возможности ViPNet Administrator. Приложение к документации ViPNet».
- «Печать сертификатов. Приложение к документации ViPNet».
- «ViPNet Administrator. Лицензионные соглашения на компоненты сторонних производителей».

2

Новые возможности программы ViPNet Центр управления сетью 4.6

Создание сети ViPNet	33
Добавление сетевого узла	34
Управление защищенными DNS-серверами	36
Управление уровнем полномочий пользователя на координаторе	37
Объединение сетевых узлов и пользователей в группы	38
Связи между объектами сети	40
Формирование таблиц маршрутизации	41
Назначение адресов	42
Настройка подключения через межсетевой экран	44
Изменения в настройке параметров роли «Terminal»	46
Туннелирование	47
Организация межсетевого взаимодействия	49
Отправка обновлений программного обеспечения на узлы	51

Обновление справочников и ключей при смене координатора узла	53
Работа с журналами событий	54
Настройка параметров безопасности сетевых узлов	56
Создание отчетов о структуре сети и лицензионных ограничениях	58

Создание сети ViPNet

В программе ViPNet Центр управления сетью версии 3.2.12 процесс создания структуры сети ViPNet включает следующие этапы:

- 1 Создание структуры сетевого уровня, то есть создание координаторов и клиентов, групп сетевых узлов, межсерверных каналов между координаторами.
- 2 Регистрация сетевых узлов в прикладных задачах.
- 3 Регистрация типов коллективов на сетевых узлах и группах сетевых узлов, определение связей между типами коллективов.
- 4 Регистрация пользователей в типах коллективов.

В программе ViPNet Центр управления сетью версии 4.6.7 существует два способа создания структуры сети ViPNet:

- 1 Использование мастера, который позволяет создать необходимое количество сетевых узлов ViPNet и пользователей, задать связи между узлами и между пользователями.
- 2 Создание координаторов, клиентов и пользователей вручную (см. [Добавление сетевого узла](#) на стр. 34).

В этом случае процесс создания сети включает следующие этапы:

- 2.1 Создание и настройка координаторов, в том числе выбор ролей, задание IP-адресов или DNS-имен, параметров [межсетевого экрана](#) (см. глоссарий, стр. 95), настройка [туннелирования](#) (см. глоссарий, стр. 97). На каждом создаваемом узле можно автоматически создать одноименного пользователя.

- 2.2 Создание и настройка клиентов по аналогии с созданием и настройкой координаторов.

- 2.3 Создание межсерверных каналов, создание связей между сетевыми узлами.

Автоматически создаются связи между координаторами, образующими межсерверные каналы, между координаторами, работающими в режиме VPN-сервера и их клиентами и координаторами с отключенным режимом работы VPN-сервера, между ЦУСом и другими узлами. Такие связи нельзя удалить.

- 2.4 Создание пользователей и добавление их на сетевые узлы, создание связей между пользователями.

Таким образом, в программе ViPNet Центр управления сетью версии 3.2.12 существует четкое разделение на сетевой и прикладной уровни администрирования, соответствующие настройки выполняются в независимых окнах программы.

В программе ViPNet Центр управления сетью версии 4.6.7 процесс создания сети состоит в последовательном создании сетевых объектов, причем различные настройки этих объектов можно выполнить непосредственно при их создании. Создание связей между сетевыми объектами в программе новой версии упростилось благодаря отсутствию типов коллективов. Подробнее см. в документе «ViPNet Центр управления сетью. Руководство администратора», в разделе «Начало работы с программой ViPNet Центр управления сетью».

Добавление сетевого узла

В программе ViPNet Центр управления сетью версии 3.2.12 для добавления клиента (абонентского пункта) или координатора требуется выполнить следующие действия:

- 1 Создать сетевой узел (клиент или координатор) в окне **ViPNet. Администрация сетевого уровня**.
- 2 Если создаваемый сетевой узел является координатором, то требуется создать межсерверные каналы для обмена служебной информацией с другими координаторами.
- 3 Зарегистрировать узел в нужных прикладных задачах.
- 4 Создать на сетевом узле тип коллектива, если он не был создан автоматически при создании сетевого узла.
- 5 Задать связи созданного типа коллектива с другими типами коллективов.
- 6 Создать одного или несколько пользователей в типе коллектива, который зарегистрирован на новом сетевом узле.

В программе ViPNet Центр управления сетью версии 4.6.7 появилась возможность создать координатор с отключенными функциями VPN-сервера — без функций сервера IP-адресов и транспортного сервера, который позволит уменьшить нагрузку на вычислительные ресурсы координатора. Для этого при создании координатора, требуется выбрать соответствующий режим работы и указать координатор, который будет выполнять функции VPN-сервера.

Координатор без функций VPN-сервера не рассылает информацию о других узлах, его необходимо регистрировать на другом координаторе и на него нельзя добавить клиенты. Вы можете использовать его для туннелирования и в качестве межсетевого экрана.

В программе ViPNet Центр управления сетью версии 4.6.7 для добавления сетевого узла требуется выполнить следующие действия:

- 1 Создать клиент или координатор, нажав соответствующую кнопку на панели инструментов и указав имя нового узла.

Если создаваемый сетевой узел является клиентом или координатором без функций VPN-сервера, то требуется указать координатор, который будет выполнять функции сервера IP-адресов и транспортного сервера для этого сетевого узла.

При создании сетевого узла можно автоматически создать для него одноименного пользователя.

- 2 В окне свойств узла выполнить следующие настройки:
 - Создать связи с другими сетевыми узлами.
 - Добавить роли узла и задать свойства ролей, такие как уровень полномочий пользователя.
 - Задать IP-адреса узла и параметры межсетевого экрана.

- Задать список защищенных DNS- и WINS-серверов, которые требуется использовать на узле. В качестве защищенных DNS- и WINS-серверов можно использовать сетевые узлы, на которые добавлены соответствующие роли.
- Если создаваемый сетевой узел является координатором, выполняющим функции VPN-сервера, создать межсерверные каналы, задать адреса туннелируемых узлов, параметры межсетевого экрана клиентов, для которых данный координатор будет назначен сервером IP-адресов.

3 Добавить на новый сетевой узел одного или несколько пользователей, задать их связи с другими пользователями.

Таким образом, в программе ViPNet Центр управления сетью версии 3.2.12 для создания сетевого узла нужно выполнить ряд действий в независимых окнах программы, соблюдая определенную последовательность. Из-за этого создание сетевого узла занимает довольно много времени и может вызвать затруднения у неопытного администратора.

В программе ViPNet Центр управления сетью версии 4.6.7 все настройки сетевого узла выполняются в одном окне. Пользователи регистрируются непосредственно на сетевых узлах, а не в типах коллективов, что упрощает управление структурой сети.

Кроме того, в программе ViPNet Центр управления сетью версии 4.6.7 есть возможность создавать шаблоны с настройками параметров сетевых узлов. При создании узлов можно просто выбрать шаблоны, настройки из которых будут применены к узлам. Это позволяет упростить процесс создания большого количества сетевых узлов с похожими параметрами.

Подробную информацию см. в документе «ViPNet Центр управления сетью», в разделе «Настройка параметров сетевых узлов».

Управление защищенными DNS-серверами

Мобильные клиенты ViPNet и другие узлы могут одновременно использовать публичные и корпоративные DNS-серверы. При нахождении пользователя в публичной сети DNS-запрос о разрешении доменного имени корпоративного ресурса мог быть отправлен на незащищенные публичные DNS-серверы, создавая возможность атак, направленных на подмену запрашиваемых ресурсов. В программе ViPNet Центр управления сетью версии 4.6.7, чтобы запросы корпоративных ресурсов отправлялись только на защищенные DNS-серверы, вы можете настроить доменные зоны, которые будут обслуживаться только выделенными защищенными DNS-серверами. В этом случае запросы корпоративных ресурсов, отправленные на публичные DNS-серверы, будут блокироваться.

Если в вашей сети ViPNet несколько DNS-серверов, не взаимодействующих между собой и обслуживающих отдельные доменные зоны, такие DNS-серверы вы можете добавить в разные группы DNS-серверов (см. глоссарий, стр. 94) и задать для каждой группы список доменных зон.

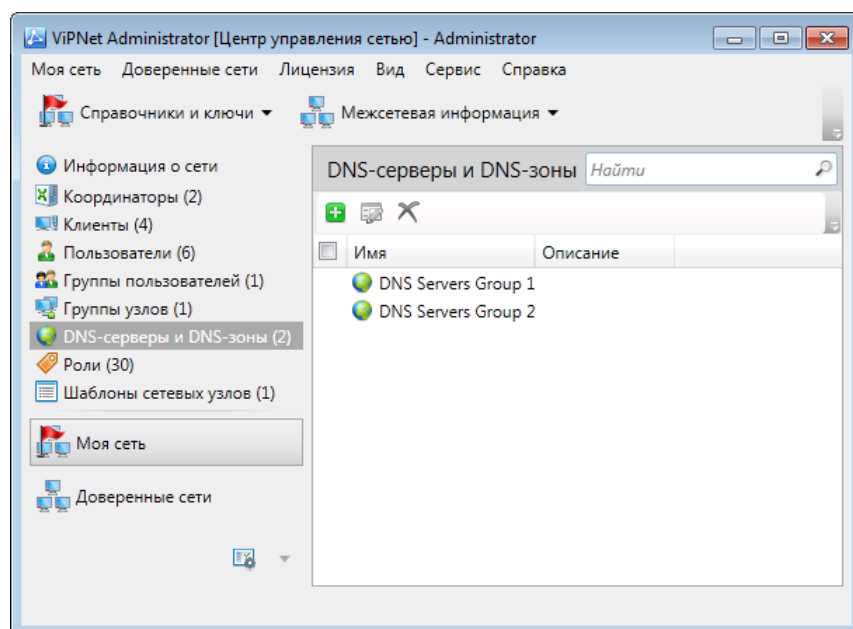


Рисунок 12. Создание списка защищенных DNS-серверов и доменных зон

Подробную информацию см. в документе «ViPNet Центр управления сетью», в разделе «Настройка защищенных DNS-серверов».

Управление уровнем полномочий пользователя на координаторе

В программе ViPNet Центр управления сетью версии 3.2 была возможность задать уровень полномочий для пользователя координатора с программным обеспечением ViPNet Coordinator for Windows. Для этого нужно было добавить на координатор прикладную задачу «Защита трафика» и указать в этой прикладной задаче уровень полномочий пользователя.

В программе ViPNet Центр управления сетью версии 4.6.7 вы можете задать уровень полномочий для пользователя координатора в свойствах роли «Программный VPN-координатор».

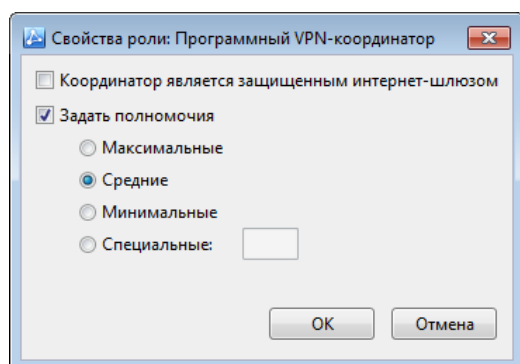


Рисунок 13. Настройка уровня полномочий для роли «Программный VPN-координатор»

Объединение сетевых узлов и пользователей в группы

В программе ViPNet Центр управления сетью версии 3.2.12 [сетевые узлы](#) (см. глоссарий, стр. 97) можно объединять в сетевые группы и создавать для каждой группы типы коллектива. Если сетевые узлы связаны на уровне типов коллектива, они могут устанавливать друг с другом защищенное соединение.

В программе ViPNet Центр управления сетью версии 4.6.7 сетевые узлы можно объединять в группы узлов. Логическое объединение узлов в группы узлов в версии 4.6.7 предназначено для задания паролей администраторов узлов ViPNet, оптимизации процессов создания связей между сетевыми узлами и отправки справочников, ключей и обновлений ПО ViPNet на узлы.

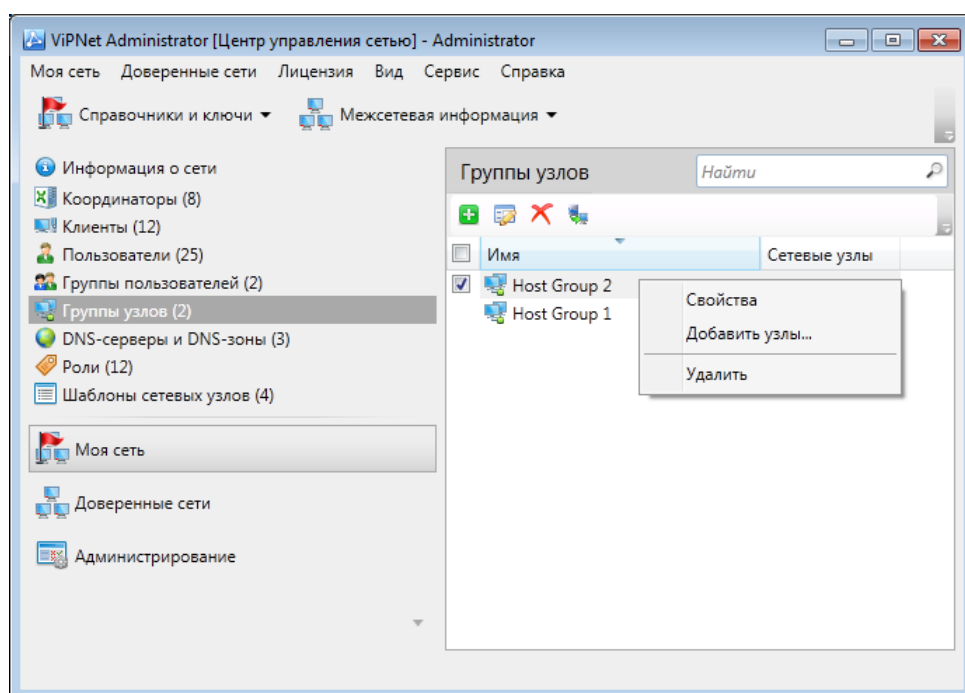


Рисунок 14. Группы сетевых узлов

Кроме того, в программе ViPNet Центр управления сетью 4.6.7 реализована возможность объединения пользователей в группы, что упрощает управление связями между пользователями (см. [Связи между объектами сети](#) на стр. 40).

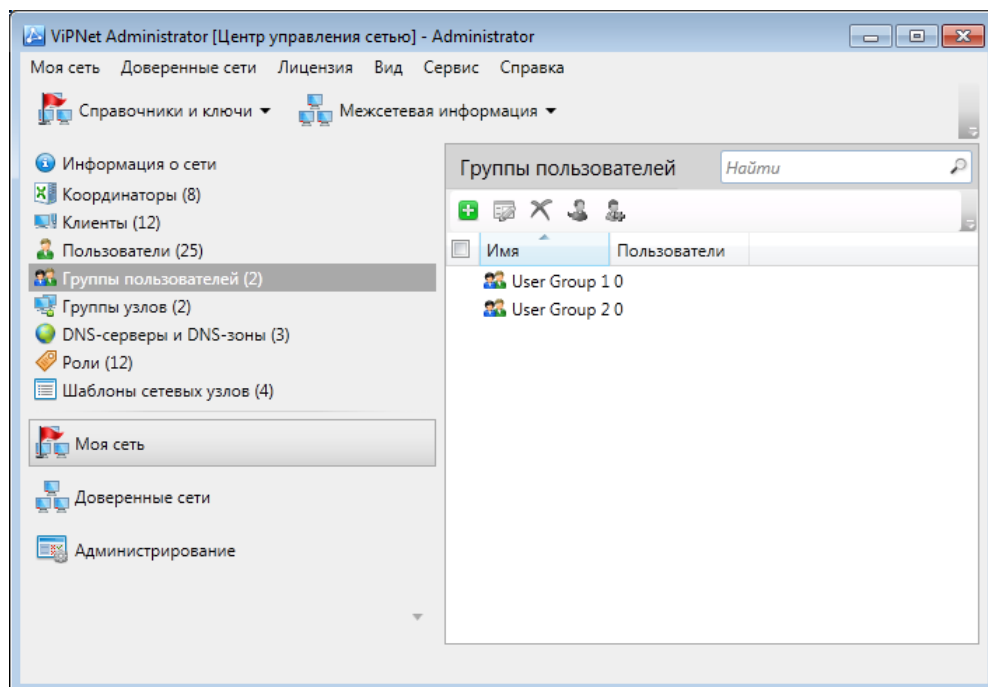


Рисунок 15. Группы пользователей

Связи между объектами сети

В ViPNet Центр управления сетью версии 3.2.x объекты [сети](#) (см. глоссарий, стр. 97) связаны между собой на уровне типов коллективов (ТК). В программе ViPNet Центр управления сетью версии 4.x образуются связи других видов, при этом во внутренних механизмах работы программы связи между ТК остаются. При конвертации данных ЦУСа 3.2.x появляются связи между [узлами сети](#) (см. глоссарий, стр. 97), связи между ТК преобразуются в связи следующего типа:

- связи между пользователями;
- связи между пользователями и группами пользователей.

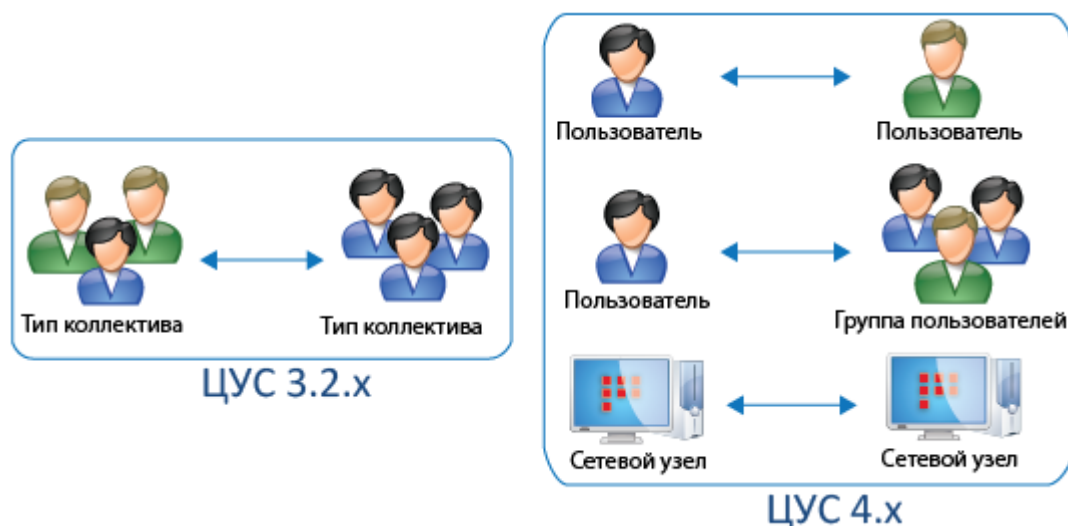


Рисунок 16: Сравнение связей в разных версиях ЦУСа

Если пользователь связан с группой пользователей, в программе ViPNet Деловая почта он может адресовать зашифрованные сообщения всем пользователям этой группы на определенном сетевом узле или отдельным участникам группы. При добавлении пользователя в группу автоматически создается связь между пользователем и этой группой.

Более подробно о преобразовании связей при обновлении с версии 3.2.12 до версии 4.6.7 см. в документе «ViPNet Administrator. Руководство по обновлению с версии 3.2.x до версии 4.x», в главе «Обновление с версии 3.2.x до версии 4.x», в разделе «Особенности преобразования связей при конвертации».

Формирование таблиц маршрутизации

При работе с программой ViPNet Центр управления сетью требуется формирование таблиц маршрутизации, согласно которым происходит процесс выбора оптимального пути для передачи данных. В версии 3.2.12 для формирования таблиц маршрутизации нужно выполнять специальную команду.

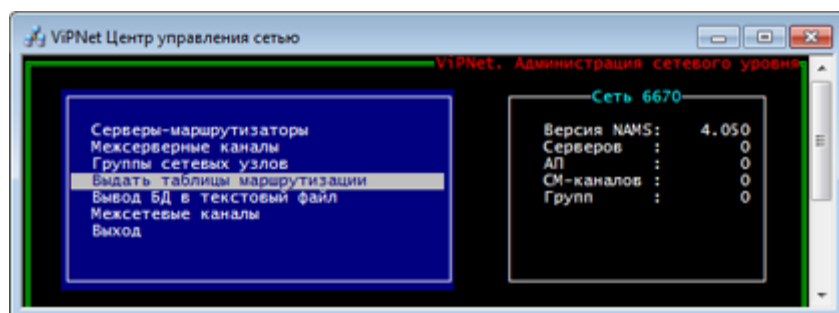


Рисунок 17: Создание таблиц маршрутизации в версии 3.x

В версии 4.6.7 формирование таблиц маршрутизации выполняется автоматически при формировании справочников.

Назначение адресов

Для того чтобы сетевые узлы ViPNet могли устанавливать соединения друг с другом, должны быть известны их IP-адреса или DNS-имена.

В программе ViPNet Центр управления сетью версии 3.2.12 IP-адреса узлов во внешних сетях можно было задавать при групповой регистрации сетевых узлов в прикладных задачах «Сервер IP-адресов» (для координаторов) и «Защита трафика» (для клиентов), а также в окне **Управление внешними адресами** (для всех объектов сети ViPNet).

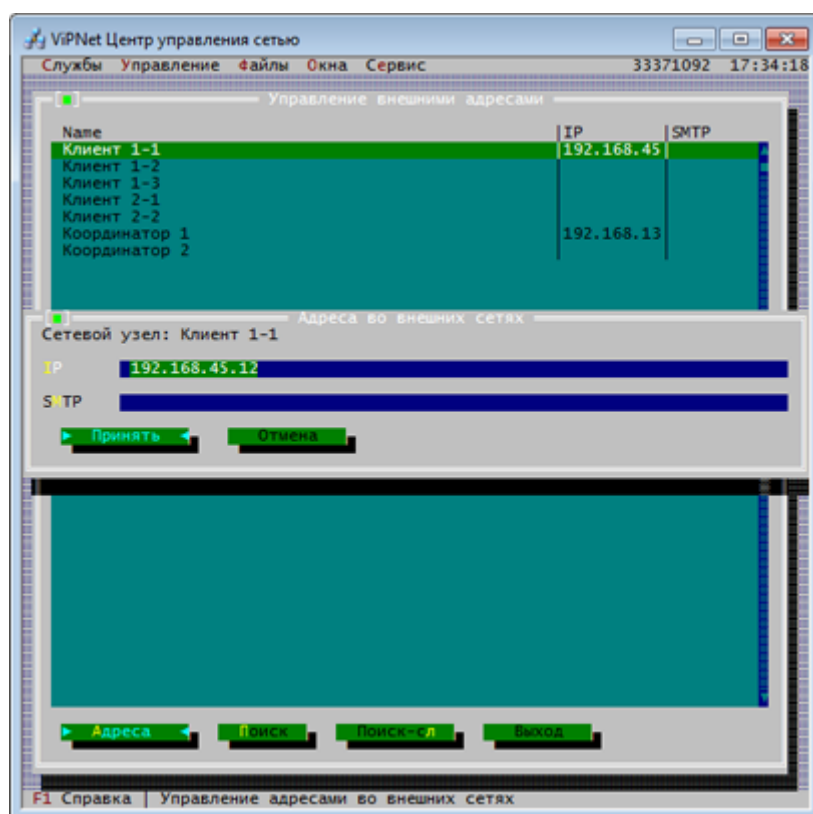


Рисунок 18. Задание адресов сетевых узлов в ViPNet Центр управления сетью 3.2.12

В программе ViPNet Центр управления сетью версии 4.6.7 IP-адреса, DNS-имена и SMTP-адреса назначаются в окне свойств выбранного клиента или координатора.

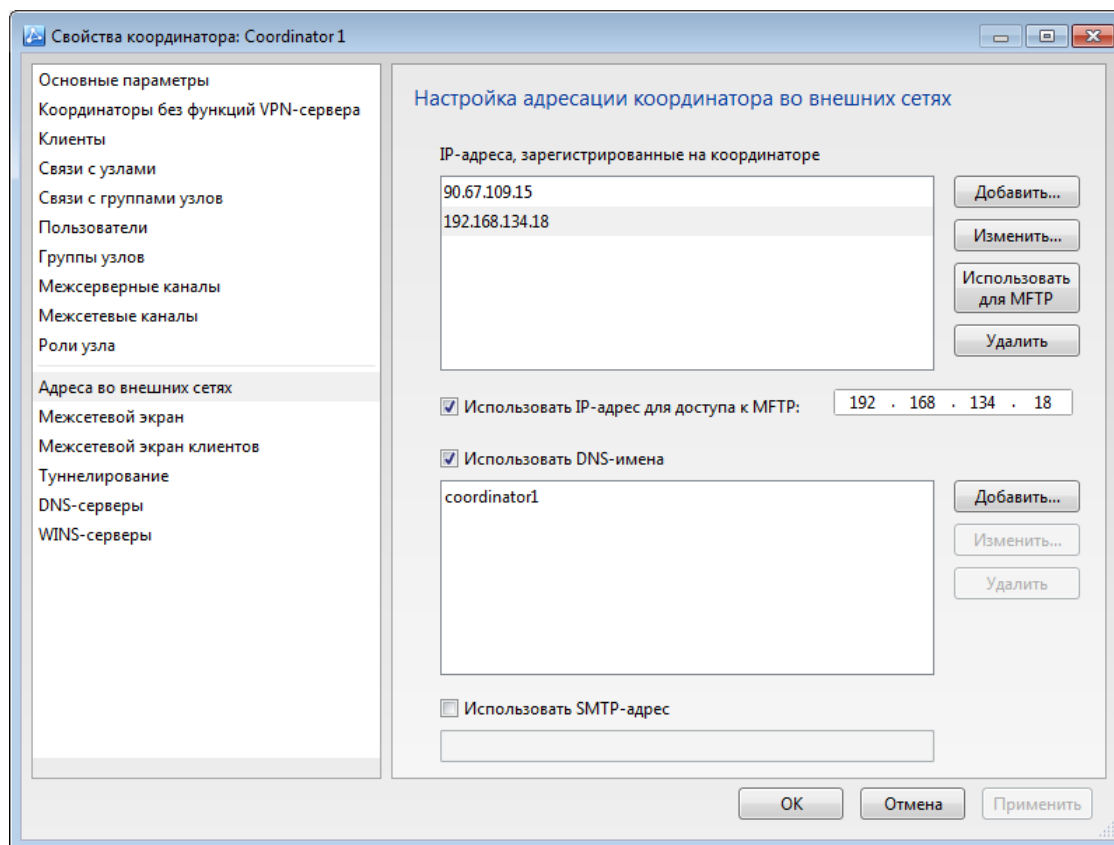


Рисунок 19. Задание адресов и DNS-имен сетевого узла

Настройка подключения через межсетевой экран

Если клиент или координатор не имеет прямого подключения к внешней сети, для него требуется задать настройки подключения через [межсетевой экран](#) (см. глоссарий, стр. 95), который установлен между сетевым узлом и внешней сетью.

Настройка межсетевого экрана в ViPNet Центр управления сетью версии 3.2.12 осуществляется при групповой регистрации сетевых узлов в прикладных задачах «Сервер IP-адресов» (для координатора и клиентов, для которых данный координатор является [сервером IP-адресов](#) (см. глоссарий, стр. 97)) и «Защита трафика» (для клиентов) путем добавления специальных строк.

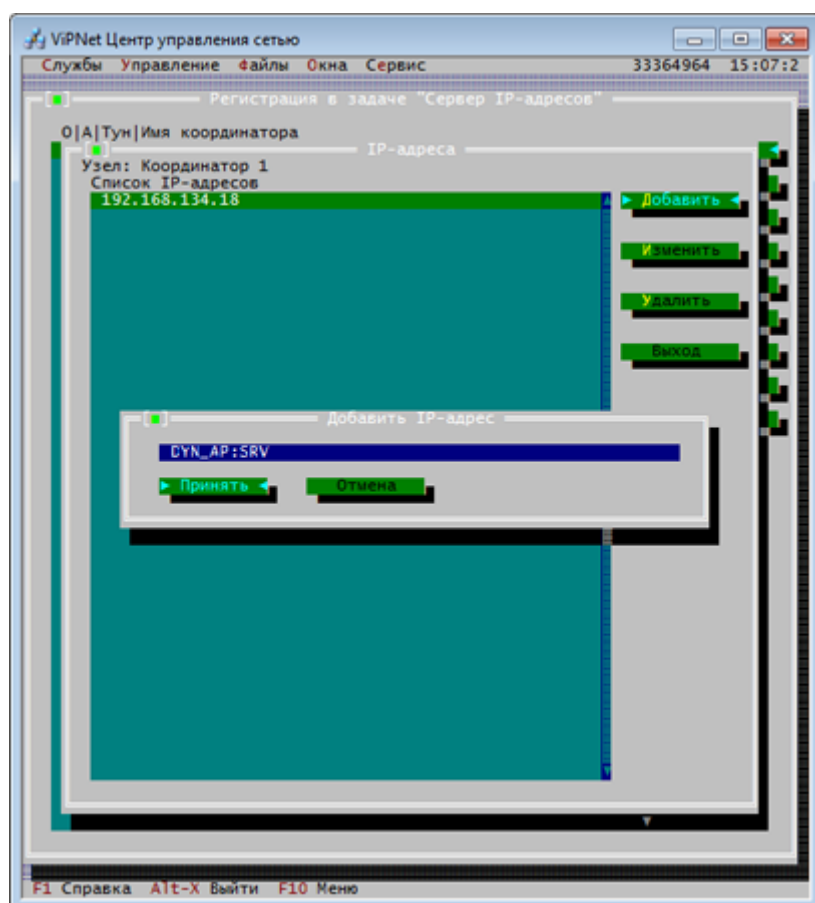


Рисунок 20. Настройка межсетевого экрана в ViPNet Центр управления сетью 3.2.12

В ViPNet Центр управления сетью версии 4.6.7 настройка межсетевого экрана осуществляется в окне свойств выбранного сетевого узла. При этом в окне свойств координатора можно настроить межсетевой экран как самого координатора, так и клиентов, для которых данный координатор является сервером IP-адресов.

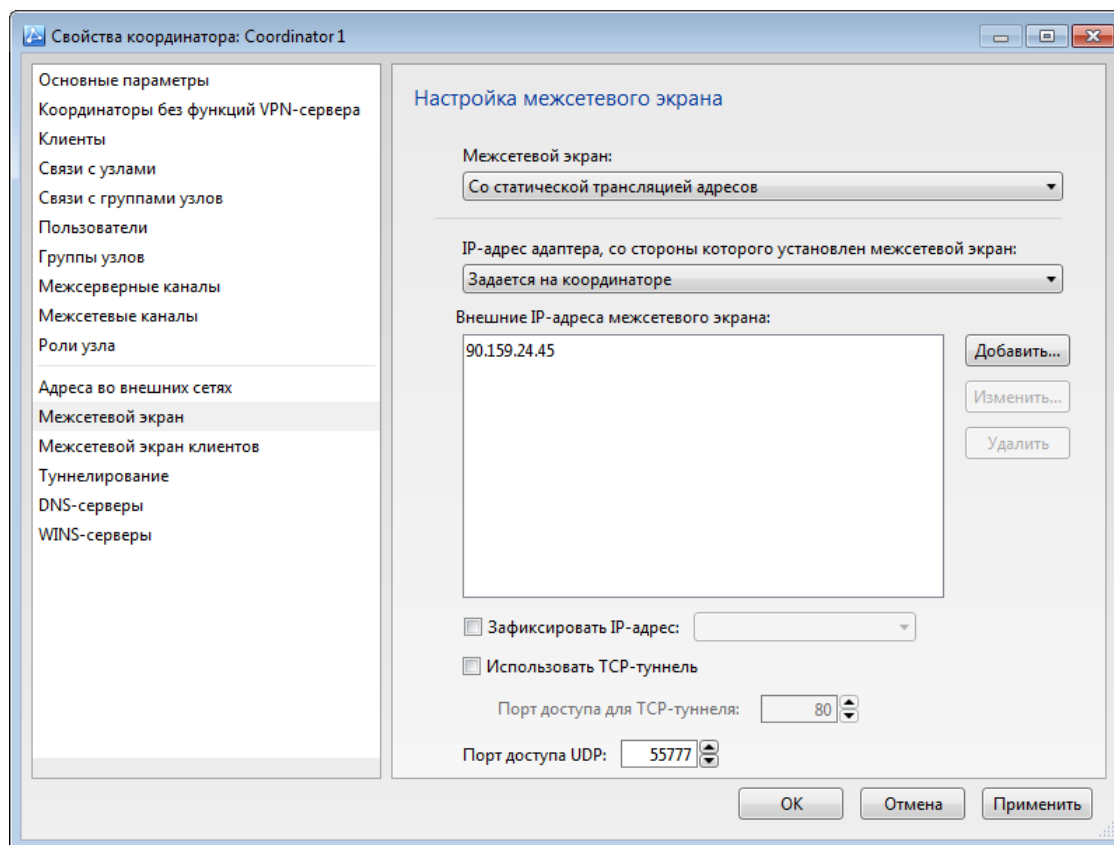


Рисунок 21. Настройка межсетевого экрана в программе ViPNet Центр управления сетью 4.6

Теперь в настройках подключения к внешней сети для координатора в случае недоступности передачи IP-пакетов по протоколу UDP вы можете установить TCP-туннель. Использование TCP-туннеля может быть настроено при подключении через межсетевой экран со статической трансляцией адресов, а также при подключении без использования межсетевого экрана.

Изменения в настройке параметров роли «Terminal»

Раньше с помощью ПО ViPNet Administrator можно было задать только несколько стандартных параметров узла с ролью «Terminal». Остальные настройки выполнялись непосредственно на узле в программе ViPNet Terminal.

Теперь с помощью ПО ViPNet Administrator вы можете задавать все параметры узла с ролью «Terminal», которые поддерживаются программным обеспечением ViPNet Terminal.

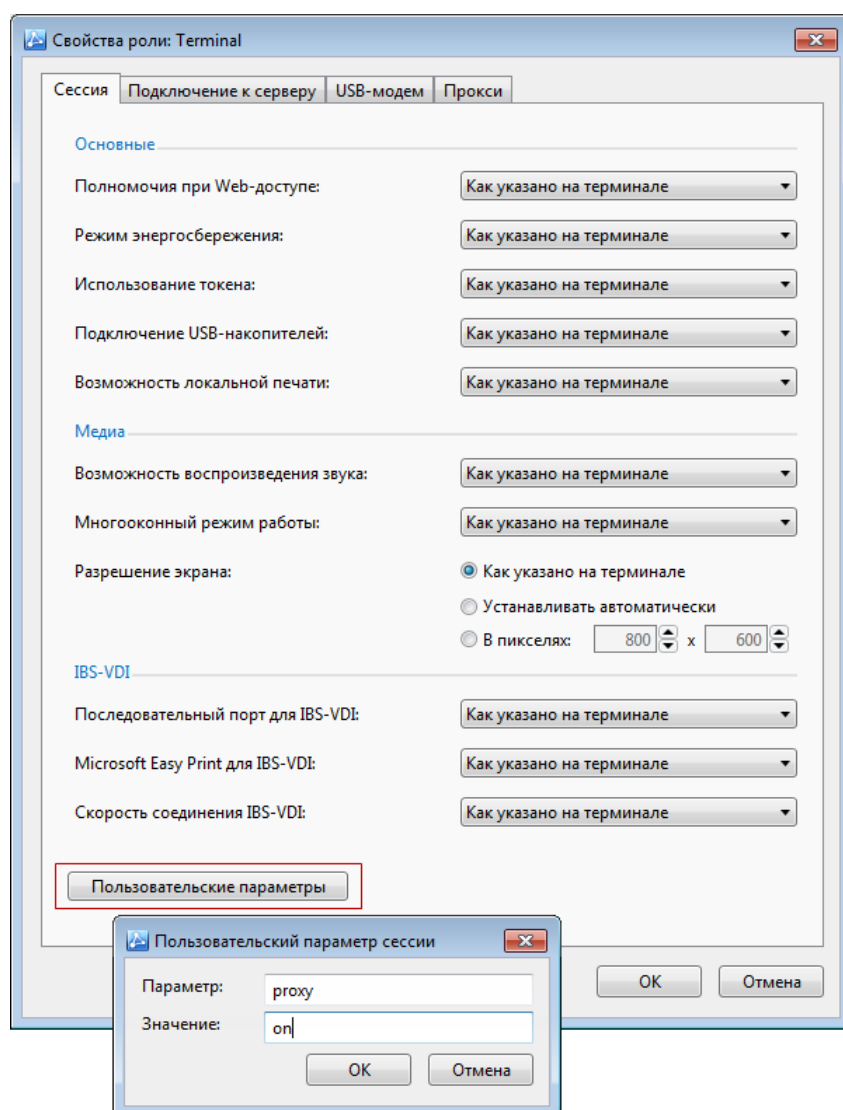


Рисунок 22. Настройка дополнительных параметров терминала

Туннелирование

Технология [туннелирования](#) (см. глоссарий, стр. 97) применяется в том случае, если требуется защитить соединения с участием [открытых узлов](#) (см. глоссарий, стр. 96) при передаче данных через Интернет или другие публичные сети.

Чтобы настроить туннелирование в ViPNet Центр управления сетью версии 3.2.12, нужно задать туннелируемые адреса координатора в формате `S:<туннелируемые адреса>` в прикладной задаче «Сервер IP-адресов». Здесь же можно указать и число соединений, которые координатор может туннелировать одновременно.

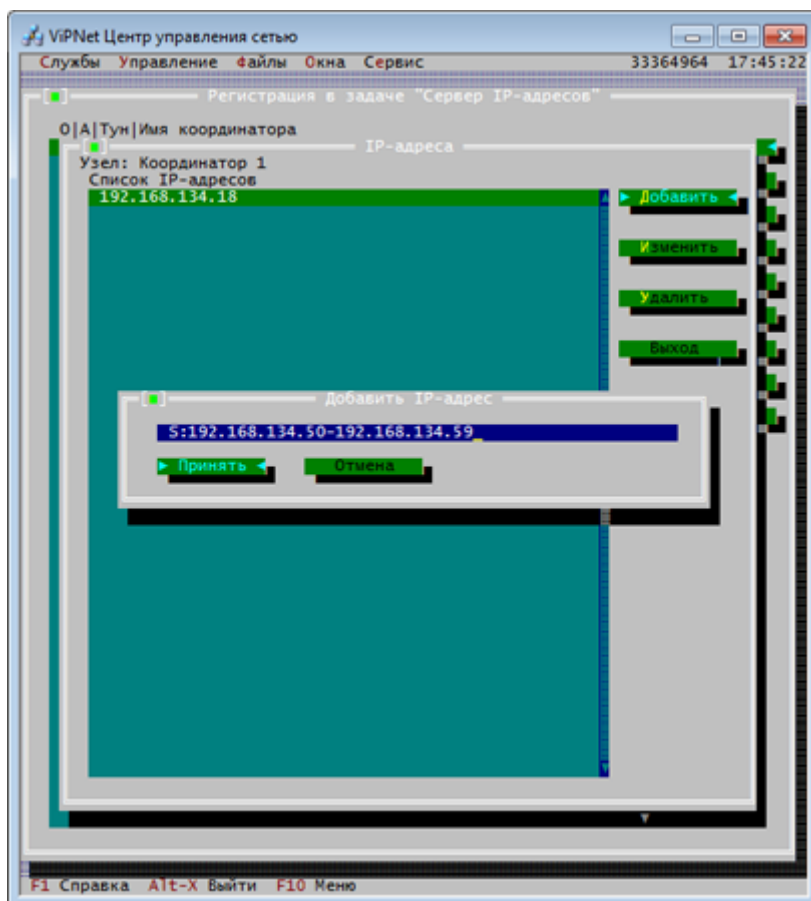


Рисунок 23. Настройка туннелирования в ViPNet Центр управления сетью 3.2.12

В ViPNet Центр управления сетью версии 4.6.7 настройка туннелирования осуществляется в окне свойств выбранного координатора. Здесь можно указать IP-адреса или диапазоны адресов туннелируемых узлов, а также задать число соединений, которые координатор может туннелировать одновременно.

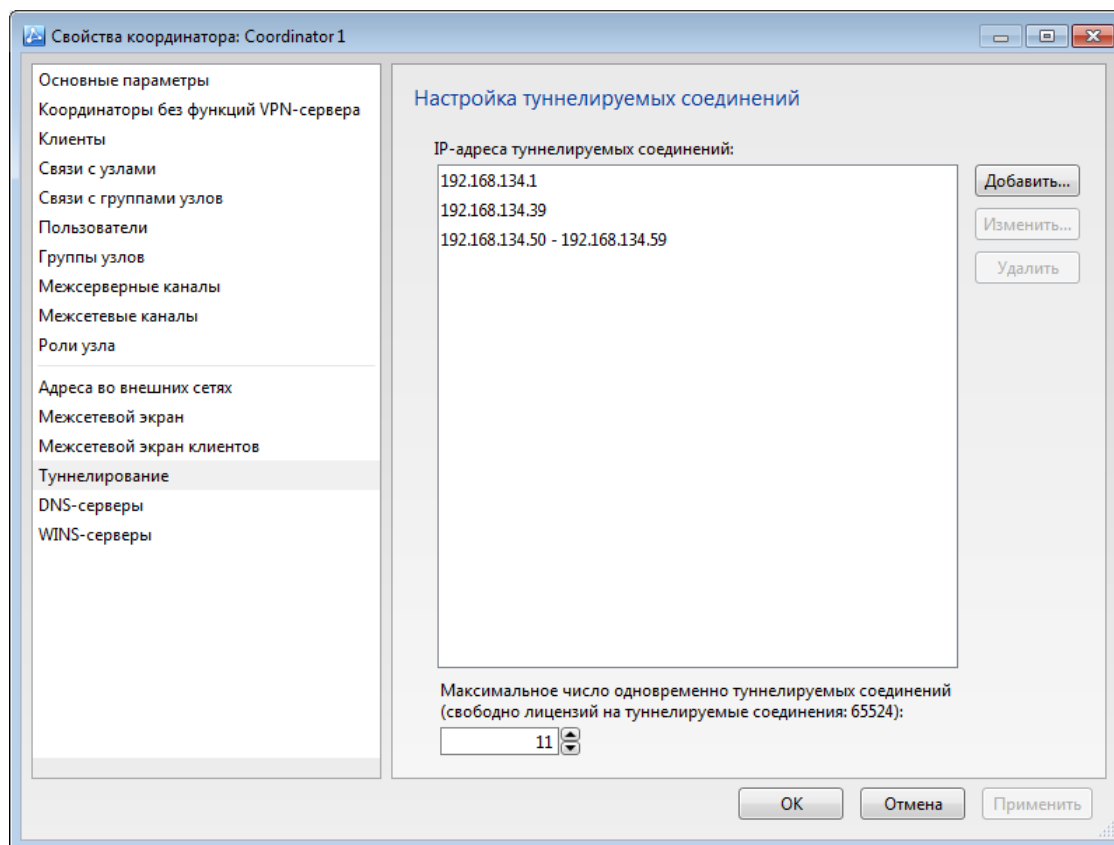


Рисунок 24. Настройка туннелирования

Организация межсетевого взаимодействия

Алгоритм организации [межсетевого взаимодействия](#) (см. глоссарий, стр. 95) в программе ViPNet Центр управления сетью версии 4.6.7 по сравнению с версией 3.2.12 не изменился и выполняется в несколько этапов:

- 1 Создание файла межсетевой информации и [межсетевого мастер-ключа](#) (см. глоссарий, стр. 95) в своей сети.
- 2 Прием межсетевой информации и создание файла с ответной межсетевой информацией в [доверенной сети](#) (см. глоссарий, стр. 94).
- 3 Прием ответной межсетевой информации в своей сети.

Однако в программе ViPNet Центр управления сетью версии 4.6.7 стало значительно проще организовать межсетевое взаимодействие по следующим причинам:

- Все действия выполняются в мастере **Установка межсетевого взаимодействия**.
- Межсетевая информация, используемая для организации взаимодействия, представлена не набором файлов, а одним файлом в формате LZN, в который включены данные о связях между объектами своей и доверенной сетей. Этот файл не требуется распаковывать и помещать в определенную папку, нужно просто указать путь к нему в мастере установки.
- Межсетевая информация может быть создана сразу для нескольких доверенных сетей и отправлена группе доверенных сетей за одно действие.
- Межсетевые мастер-ключи могут быть импортированы в программу ViPNet Удостоверяющий и ключевой центр из любой папки на жестком диске или внешнем носителе. То есть при загрузке межсетевых мастер-ключей администратору доверенной сети больше не требуется помещать файл с межсетевым мастер-ключом в подпапку `.\import` папки, где установлена программа ViPNet Удостоверяющий и ключевой центр.

В программе ViPNet Центр управления сетью версии 3.2.12 для организации межсетевого взаимодействия связи устанавливаются между типами коллектива.

В программе ViPNet Центр управления сетью версии 4.6.7 связи задаются между пользователями своей и доверенной сетей, и эти связи должны быть подтверждены администратором доверенной сети, с которой устанавливается межсетевое взаимодействие. Подтвердить или отклонить предложенные связи можно при обработке межсетевой информации (подтверждение всех связей) или при редактировании свойств пользователя, с которым предлагается установить связь (выборочное подтверждение или отклонение связей).

Если связь между пользователями своей и доверенной сетей больше не нужна, в версии 3.2.12 такую связь можно только запретить. В версии 4.6.7:

- Администратор своей сети может запретить устанавливать взаимодействие с тем или иным пользователем своей сети. В этом случае администратор доверенной сети не сможет предложить связи с этим пользователем.
- Если подтвержденная связь между пользователями своей и доверенной сетей больше не нужна, ее можно удалить. При необходимости связь между данными пользователями можно будет снова установить.

Подробнее об организации межсетевого взаимодействия см. в документе «ViPNet Центр управления сетью. Руководство администратора», в главе «Межсетевое взаимодействие».

Отправка обновлений программного обеспечения на узлы

Программа ViPNet Центр управления сетью позволяет централизованно рассылать обновления программного обеспечения ViPNet на сетевые узлы.

В программе ViPNet Центр управления сетью версии 3.2.12 администратор выбирает архивы с обновлением программного обеспечения. Если имя архива указано неверно или выбран архив, не соответствующий обновляемому программному обеспечению, то архив будет выслан, но обновление не произойдет или будет выполнено с ошибкой.

В программе ViPNet Центр управления сетью версии 4.6.7 подготовка и отправка обновления программного обеспечения на узлы ViPNet осуществляется посредством мастера обновления программного обеспечения. В процессе подготовки требуется загрузить файл с обновлением в базу данных SQL, которая предназначена для работы с данными ViPNet Administrator. При загрузке выполняется проверка соответствия загружаемого файла выбранному типу программного обеспечения (на основании содержимого файла обновления или его имени), что позволяет снизить вероятность возникновения ошибок при обновлении.

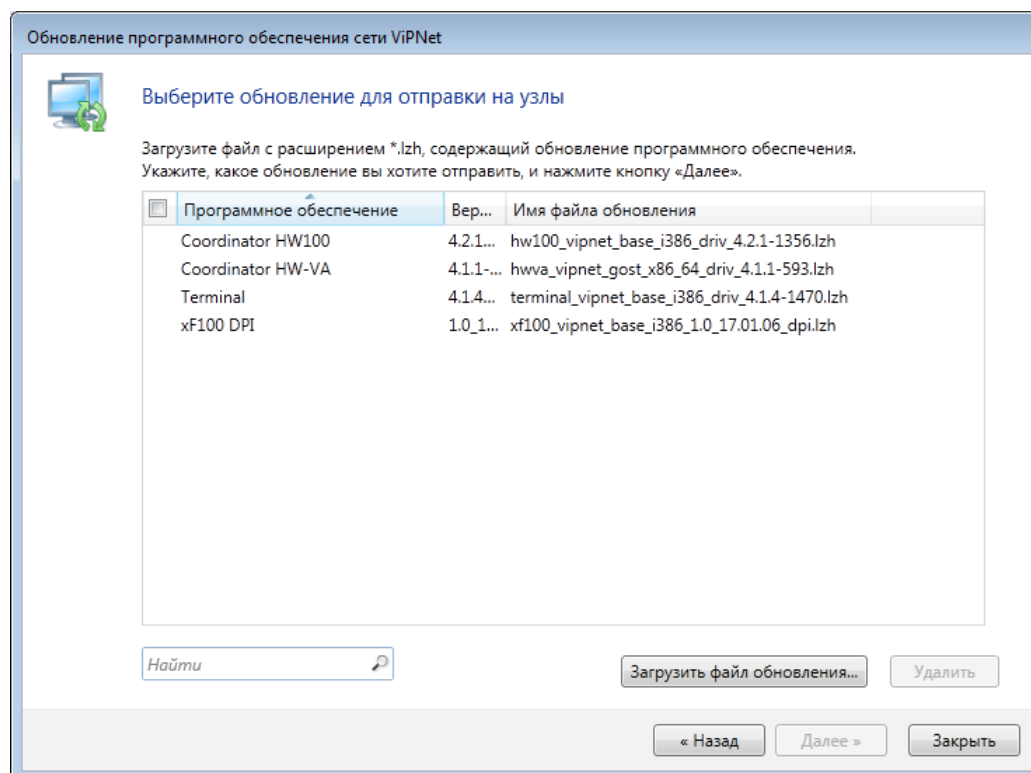


Рисунок 25. Загрузка и выбор обновлений ПО

Если обновление выбранного программного обеспечения отправляется впервые, в списке отображаются все клиенты или координаторы, в зависимости от типа обновления. При последующей отправке обновлений выбранного типа в списке отображаются сетевые узлы, на которые данный тип обновления отправлялся ранее. Список узлов для отправки обновления доступен для редактирования.

Обновление справочников и ключей при смене координатора узла

В программе ViPNet Центр управления сетью версии 3.2.12 нельзя было сменить координатор клиента сети ViPNet. Однако это может быть необходимо, например, если нужно включить клиент в сегмент сети, относящийся к другому координатору. В программе ViPNet Центр управления сетью версии 4.6.7 вы можете сменить координатор любого клиента сети ViPNet, в том числе клиента, являющегося ЦУСом, а также сменить координатор для координатора, не выполняющего функции сервера IP-адресов и транспортного сервера.

При смене координатора для обычного клиента и координатора без функций VPN-сервера доставка обновления справочников и ключей на этот узел производится автоматически. Доставку обновления обеспечивает старый координатор узла, который используется еще в течение некоторого времени после смены. Время использования старого координатора задается в настройках программы.

При смене координатора для клиента, являющегося ЦУСом, на этом узле и его координаторе необходимо установить новые дистрибутивы ключей вручную.

Работа с журналами событий

В программе ViPNet Центр управления сетью версии 3.2.12 вы можете просмотреть журнал запросов и ответов. В программе ViPNet Центр управления сетью версии 4.6.7 ведется аналогичный журнал транспортных конвертов, а также журнал аудита.

В журналах транспортных конвертов администратор ЦУСа может просмотреть историю отправленных на сетевые узлы обновлений (справочников и ключей, программного обеспечения), а также принятых запросов на сертификаты от центра регистрации и пользователей сетевых узлов. Для разбора конфликтных ситуаций реализована возможность просмотра содержимого конвертов.

В журналах аудита фиксируется информация о действиях, которые выполняют администраторы в процессе управления сетью ViPNet. Можно просматривать несколько журналов, которые содержат информацию о различных группах событий: изменение настроек программы ViPNet Центр управления сетью, изменение свойств объектов сети, вход и выход администраторов из программы и так далее. Благодаря ведению подробного журнала аудита обеспечивается прозрачность работы каждого из администраторов и возможность отследить источник тех или иных изменений.

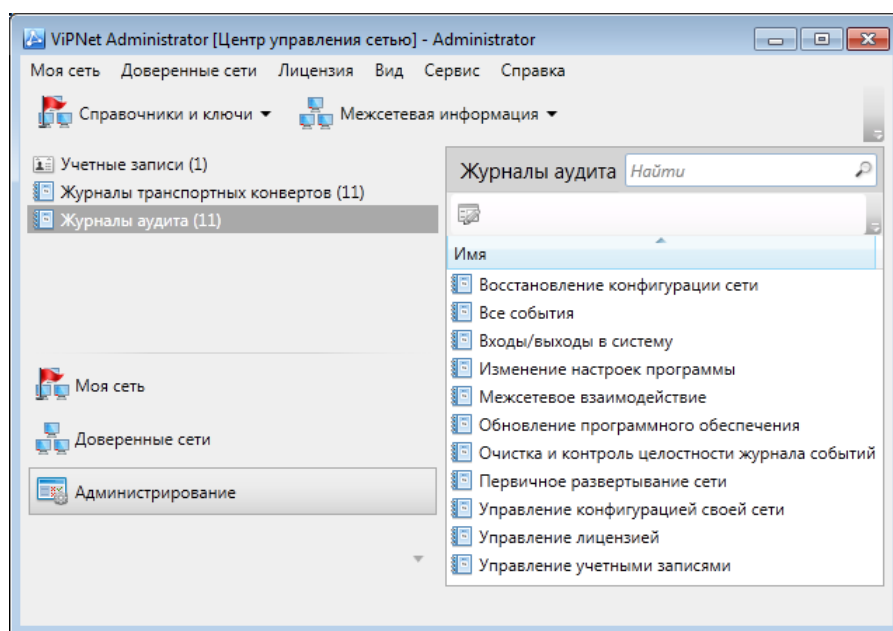


Рисунок 26. Работа с журналами событий

В настройках программы ViPNet Центр управления сетью версии 4.6.7 можно задать время хранения записей в журнале аудита в диапазоне от 7 до 365 дней. Записи с истекшим временем хранения автоматически удаляются из журналов. Также можно задать время хранения записей в журнале транспортных конвертов в диапазоне от 1 до 365 дней.

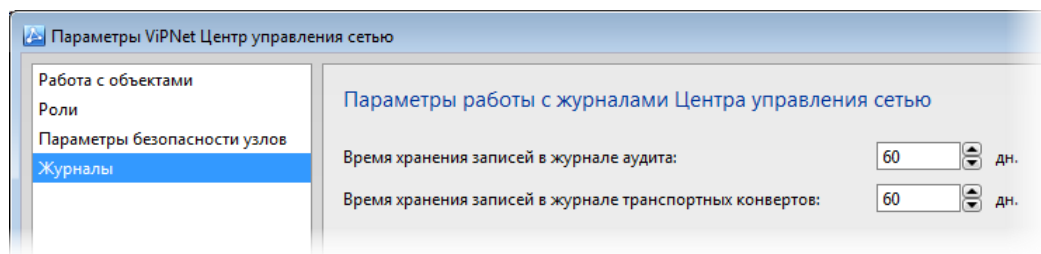


Рисунок 27. Настройка времени хранения записей в журналах

Настройка параметров безопасности сетевых узлов

В программе ViPNet Центр управления сетью версии 4.6.7 можно централизованно настроить следующие параметры безопасности сетевых узлов:

- Шифрование данных.

Администратор сети ViPNet может централизованно задавать алгоритм шифрования исходящего IP-трафика сетевых узлов и писем, отправляемых пользователями сетевых узлов с помощью программы ViPNet Деловая почта.

- Отключение брандмауэра Windows при запуске программ ViPNet Client и ViPNet Coordinator.

Если для фильтрации IP-трафика, который проходит через узлы ViPNet, используются сетевые экраны, встроенные в программы ViPNet Client и ViPNet Coordinator, на данных узлах необходимо отключить брандмауэр Windows. В противном случае между встроенным сетевым экраном и брандмауэром Windows могут возникнуть конфликты, влекущие за собой проблемы с доступом в сеть. Раньше отключение брандмауэра Windows происходило автоматически при запуске программ ViPNet Client и ViPNet Coordinator, и администратор не мог изменить данную настройку. Теперь в случае необходимости использования брандмауэра Windows администратор может отменить его автоматическое отключение.

- Сохранение пароля пользователя программы ViPNet Client и ViPNet Coordinator.

Раньше данный параметр администратор сети ViPNet настраивал в программах ViPNet Client и ViPNet Coordinator. Теперь его можно задать в программе ViPNet Центр управления сетью и

передать сразу на все узлы, на которых используются программы ViPNet Client или ViPNet Coordinator, в составе дистрибутива ключей или обновления справочников.

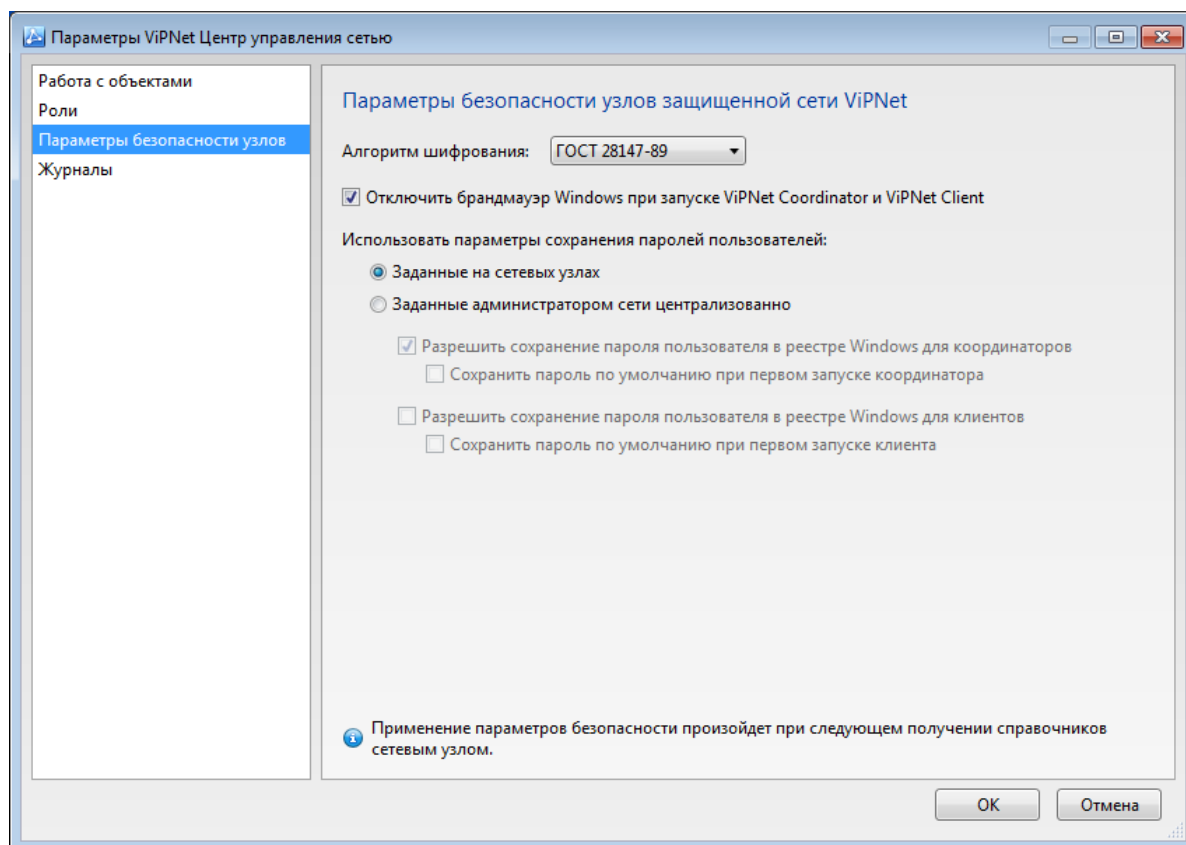


Рисунок 28: Настройка параметров безопасности сетевых узлов

Создание отчетов о структуре сети и лицензионных ограничениях

В программе ViPNet Центр управления сетью версии 3.2 вы могли просмотреть отчет о структуре сети с помощью меню **Службы > Просмотр конфигурации сети**.

В программе ViPNet Центр управления сетью версии 4.6.7 вы можете создать и сохранить отчет структуре сети ViPNet в формате XML или HTML для просмотра или использования в сторонних программах. В данных отчета информация о сети представлена в иерархическом виде, отображены все имеющиеся координаторы, клиенты и пользователи, а также информация о связях узлов и пользователей и назначенных ролях.

Структура сети 10773

- ⊕ Развернуть все ⊖ Свернуть все
- ⊖ **Координатор Coordinator 1 (2A15000A)**
- ⊖ Роли
 - Программный VPN-координатор (0018)
 - Обмен сообщениями и файлами (0059)
 - DNS-Сервер (005A)
 - ⊖ Пользователи
 - ⊖ Coordinator 1 (2A150002)
 - ⊖ Связи с пользователями
 - Client 2-1 (2A150004)
 - Client 2-2 (2A150006)
 - ⊖ Связи с узлами
 - Client 1-1 (2A15000C)
 - Client 1-2 (2A15000E)
 - Client 2-1 (2A15000D)
 - Client 2-2 (2A15000F)
 - Client 3 (2A150010)
 - Coordinator 2 (2A15000B)
 - ⊖ Узлы
 - ⊖ Клиент Client 1-1 (2A15000C)
 - ⊖ Роли
 - Network Control Center (0004)
 - Policy Manager (000C)
 - VPN-клиент (0017)
 - Publication Service (0038)
 - Обмен сообщениями и файлами (0059)
 - ⊕ Пользователи
 - ⊕ Связи с узлами
 - ⊕ Клиент Client 1-2 (2A15000E)
 - ⊕ Клиент Client 3 (2A150010)
- ⊕ **Координатор Coordinator 2 (2A15000B)**

Рисунок 29. Просмотр отчета о структуре сети ViPNet в формате HTML

Также в программе ViPNet Центр управления сетью версии 4.6.7 вы можете создать и сохранить в файл формата CSV следующие отчеты об использовании лицензий:

- Отчет об общем количестве лицензий на различные компоненты сети ViPNet, а также о количестве свободных и использованных лицензий в вашей сети.

- Если ваш ЦУС является головным в иерархической системе сетей ViPNet, вы можете создать отчет о распределении лицензионных ограничений, в котором содержатся сведения о том, сколько лицензий на различные компоненты сети используется в главной и подчиненных сетях ViPNet.

3

Новые возможности программы ViPNet Удостоверяющий и ключевой центр 4.6

Сертификаты и ключи электронной подписи	62
Ключи пользователей, ключи сетевых узлов и дистрибутивы ключей	72
Административные функции	82

Сертификаты и ключи электронной подписи

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 по сравнению с версией 3.2.12 появились новые возможности и изменились некоторые сценарии работы с сертификатами и ключами электронной подписи.

Создание ключей электронной подписи

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 вы можете издавать сертификаты по различным алгоритмам электронной подписи, в том числе по алгоритму ГОСТ Р 34.10-2012.



Примечание. Для издания сертификатов по алгоритму ГОСТ Р 34.10-2012 требуется использование сертифицированной ФСБ программы ViPNet CSP версии не ниже 4.0.

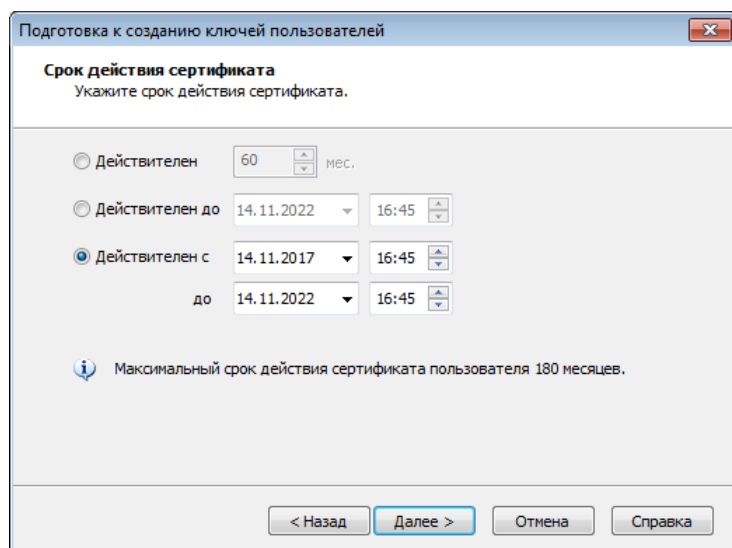
Поскольку каждый алгоритм электронной подписи реализуется конкретным криптопровайдером, в УКЦ предусмотрена возможность выбора криптопровайдера. То есть теперь при издании сертификата администратора или при создании шаблона сертификата для издания сертификата пользователя, требуется выбрать криптопровайдер, который определит алгоритм электронной подписи.

Рисунок 30. Настройка параметров ключа электронной подписи

Сроки действия сертификатов

В соответствии с требованиями Приказа ФСБ РФ № 796 от 27 декабря 2011 года срок действия ключа проверки электронной подписи не должен превышать срок действия соответствующего [ключа электронной подписи](#) (см. глоссарий, стр. 95) более чем на 15 лет. По этой причине в программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 срок действия сертификатов администраторов УКЦ увеличен с 6 лет до 16 лет, срок действия сертификатов пользователей, издаваемых в УКЦ, — с 5 лет до 15 лет.

Срок действия сертификатов задается в процессе их издания. Для сертификатов пользователей, издаваемых в УКЦ, вы можете задать начало и окончание срока действия.



Подготовка к созданию ключей пользователей

Срок действия сертификата
Укажите срок действия сертификата.

☐ Действителен 60 мес.

☐ Действителен до 14.11.2022 16:45

☒ Действителен с 14.11.2017 16:45 до 14.11.2022 16:45

Максимальный срок действия сертификата пользователя 180 месяцев.

< Назад Далее > Отмена Справка

Рисунок 31. Задание срока действия сертификата пользователя

Сертификат администратора УКЦ используется для подписания издаваемых сертификатов пользователей, и вступление его в действие по истечении какого-либо времени после издания недопустимо. Поэтому при издании сертификата администратора УКЦ вы можете задать только срок окончания его действия.

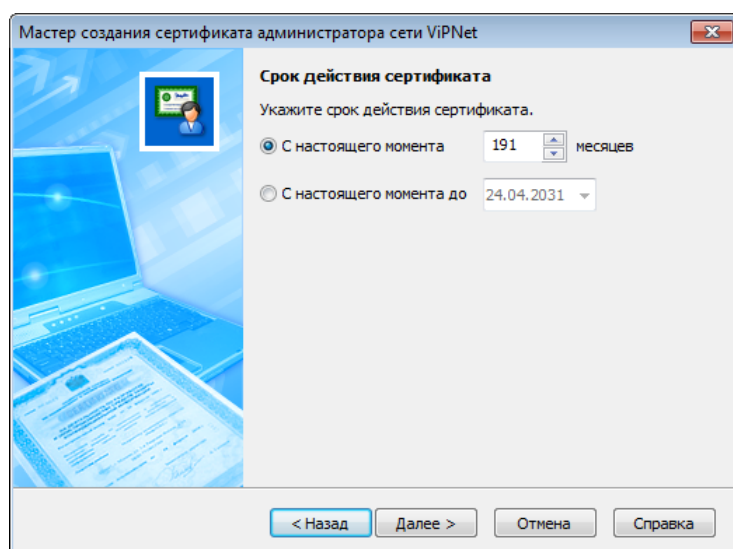


Рисунок 32. Настройка срока действия сертификата администратора

Плановая смена ключа электронной подписи администратора

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 появилась функция плановой смены ключа электронной подписи администратора. Период плановой смены ключа электронной подписи зависит от места хранения ключа электронной подписи. При хранении ключа электронной подписи в файле на компьютере либо на внешнем устройстве, которое не поддерживает алгоритм ГОСТ Р 34.10-2001/2012, его плановая смена должна производиться каждые 15 месяцев. Если ключ электронной подписи хранится на устройстве с поддержкой ГОСТ Р 34.10-2001/2012 (был непосредственно сформирован на нем), то период плановой смены ключа составляет 3 года.

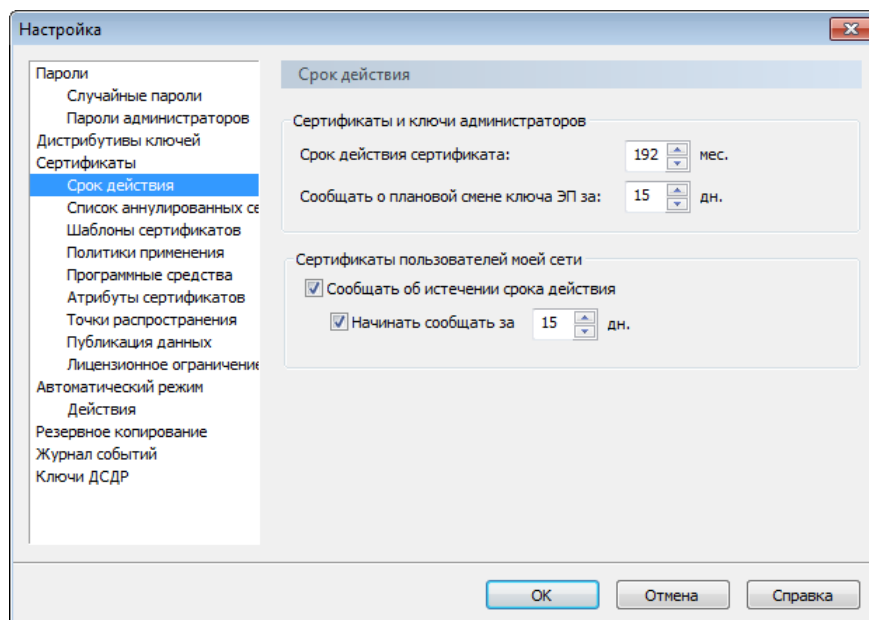


Рисунок 33. Настройка плановой смены ключа электронной подписи администратора

По истечении периода плановой смены производится оповещение. В настройках программы вы можете задать количество дней, за которое оповещение должно быть произведено. Во время плановой смены администратор должен создать новый ключ электронной подписи и получить новый [сертификат ключа проверки электронной подписи](#) (см. глоссарий, стр. 97). В противном случае издание сертификатов пользователей в программе станет невозможным.

Обработка запросов на сертификаты со сроком действия ключа электронной подписи 3 года

В УКЦ могут поступать запросы на сертификаты, в которых задан срок действия ключа электронной подписи 3 года. Такой срок действия в запросе указывается в том случае, если ключ электронной подписи при формировании запроса создается на устройстве с аппаратной поддержкой криптографических алгоритмов (например, eToken GOST). В программе ViPNet Удостоверяющий и ключевой центр версии 3.2.12 при обработке таких запросов заданный срок действия ключа электронной подписи не учитывался и в сертификате задавался срок 1 год. В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 в сертификат переносится срок действия ключа электронной подписи из запроса при условии, что сертификат издается больше чем на 3 года. Если сертификат издается на срок, меньший чем 3 года, то срок действия ключа будет равен сроку действия сертификата, и расширения со сроком действия ключа в этом случае в сертификате не будет.

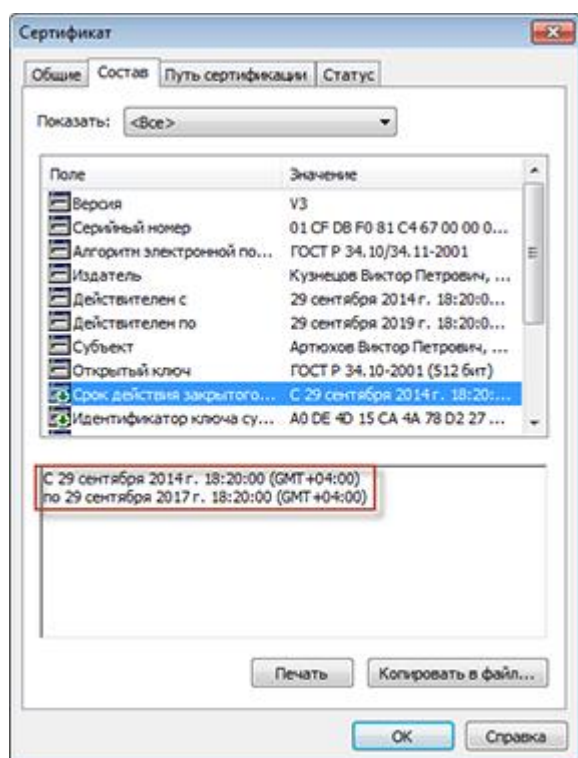


Рисунок 34. Возможность издания сертификатов со сроком действия ключа электронной подписи больше 1 года

Сохранение ключей электронной подписи в файл

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 появилась возможность создать и сохранить ключи электронной подписи в отдельный файл. Отдельный файл с ключами электронной подписи может потребоваться, например, в том случае, если у пользователя нет в наличии внешнего устройства, но при этом ему необходимо получить ключи электронной подписи в виде отдельного файла на съемном диске, а не в составе ключей или дистрибутива ключей.



Примечание. Контейнер ключей электронной подписи в виде отдельного файла требуется при работе в программе ViPNet CryptoFile и при развертывании службы ViPNet CA Web Service.

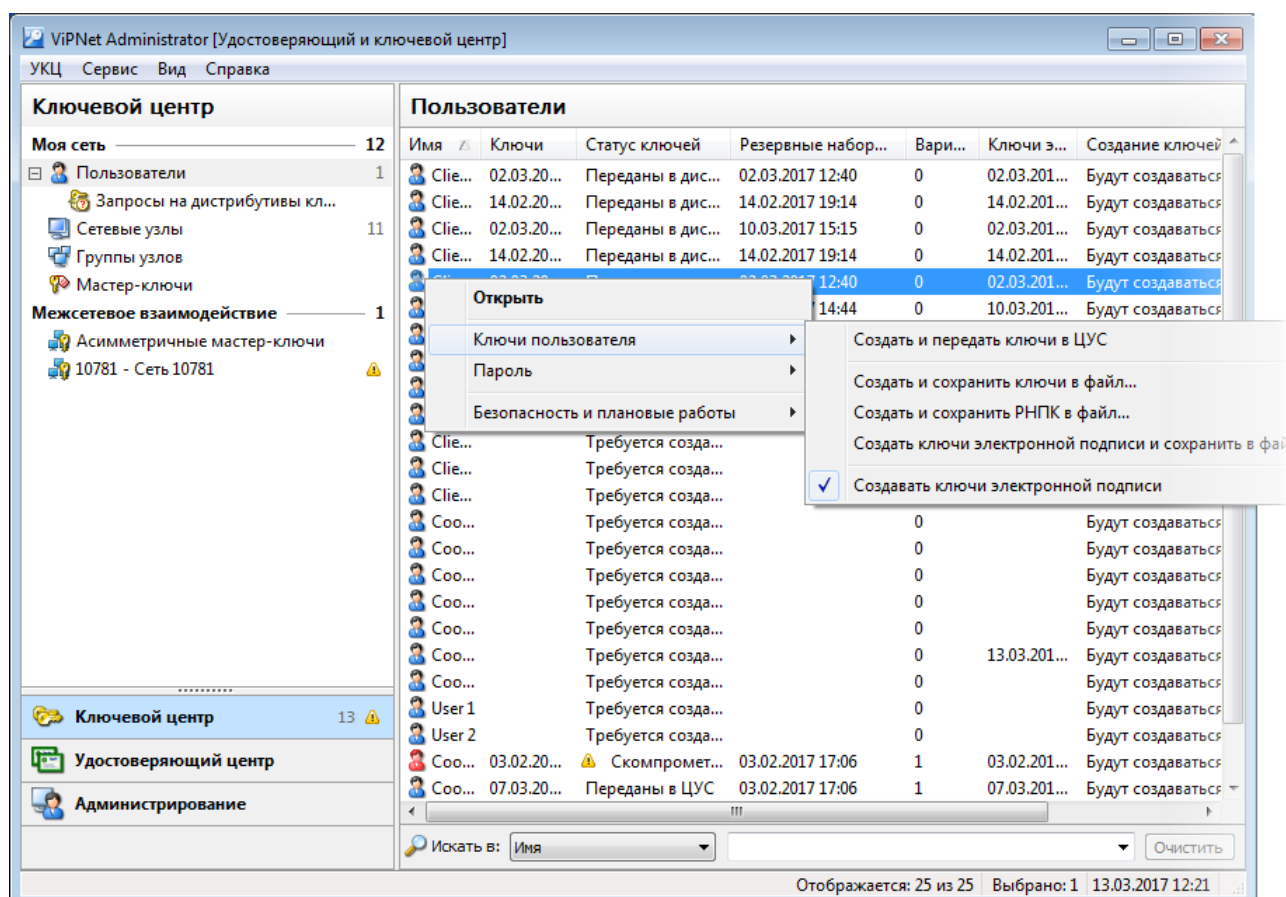


Рисунок 35. Возможность сохранения ключа ЭП и ключа проверки ЭП пользователя в файл

Создать и сохранить ключи электронной подписи в файл можно только в том случае, если они не создавались ранее в составе дистрибутива ключей или ключей пользователя. При сохранении ключи электронной подписи зашифровываются на [пароле, заданном для пользователя в УКЦ](#) (см. глоссарий, стр. 96).

Добавление информации о центрах регистрации в издаваемые сертификаты пользователей

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 реализована возможность включать в сертификаты, издаваемые по запросам из центров регистрации, информацию об этих центрах — имя и серийный номер сертификата администратора [центра регистрации](#) (см. глоссарий, стр. 98).

Информация о центре регистрации, по запросу из которого был издан сертификат, может потребоваться при возникновении конфликтных ситуаций, связанных с использованием сертификата, особенно в том случае, если в [удостоверяющем центре](#) (см. глоссарий, стр. 98)

функционирует большое количество центров регистрации и невозможно быстро установить, в каком из них этот сертификат был выдан.

Чтобы информация о центрах регистрации добавлялась в издаваемые сертификаты, в настройках программы требуется установить соответствующий флажок. Информация о центрах регистрации будет представлена в сертификатах в отдельных [расширениях](#) (см. глоссарий, стр. 96).

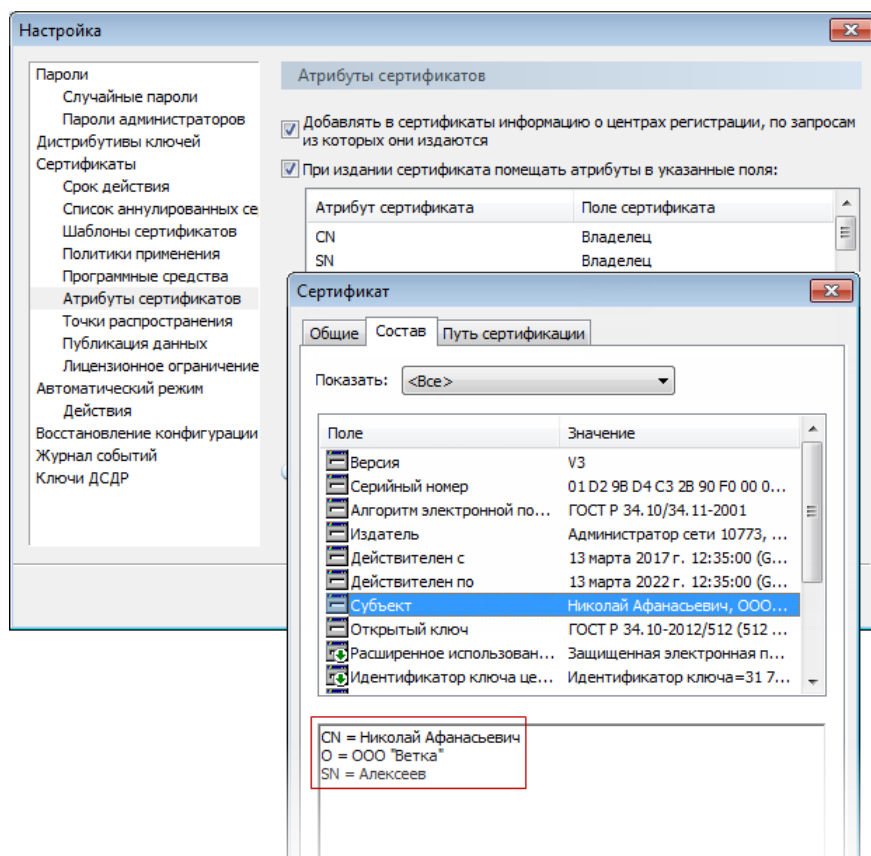


Рисунок 36. Добавление информации о центре регистрации в сертификаты пользователей

Работа с сертификатами пользователей

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 появились следующие изменения в работе с сертификатами пользователей:

- При просмотре изданных сертификатов теперь могут отображаться столбцы с дополнительной информацией о фамилии, приобретенном имени (отчестве), ОГРН и СНИЛС владельцев сертификатов. Это удобно, если администратору нужно найти необходимый сертификат по дополнительной информации, когда он не может быть найден по основным полям, например, по имени владельца. Чаще всего такие случаи могут возникать, когда сертификат выдан не конкретному лицу, а организации.

По умолчанию в разделах сертификатов новые столбцы скрыты, при необходимости их можно добавить. Чтобы производить поиск сертификатов по информации из новых столбцов, они

должны отображаться в разделе со списком сертификатов. В противном случае, сертификаты можно будет искать только по столбцам с основной информацией.

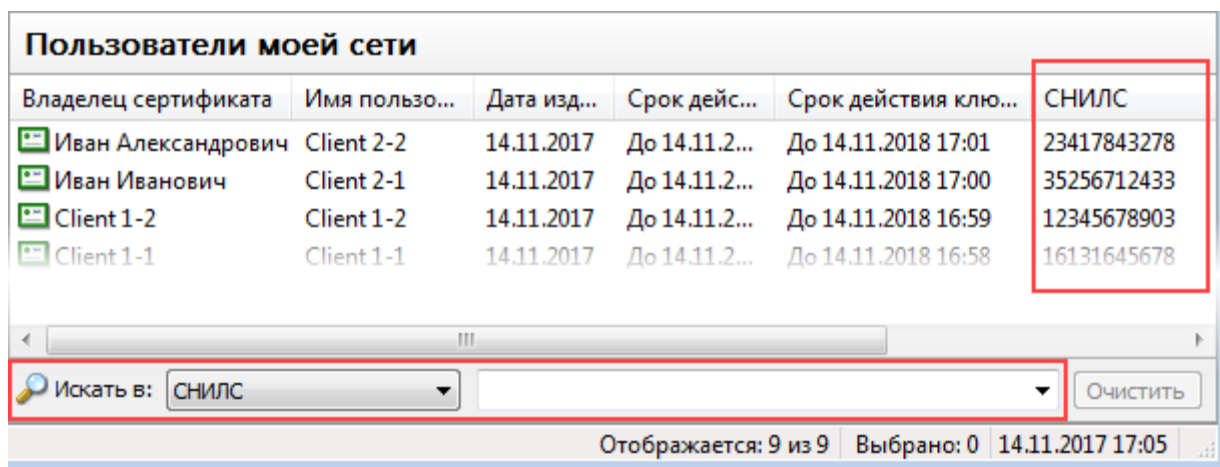


Рисунок 37. Возможность поиска сертификатов по дополнительным полям

- Сертификаты пользователей, удаленных из сети ViPNet, перемещаются в специальный раздел **Изданные сертификаты > Пользователи, удаленные из моей сети**. В случае необходимости администратор сети может аннулировать, приостановить действие или возобновить действие сертификатов таких пользователей.

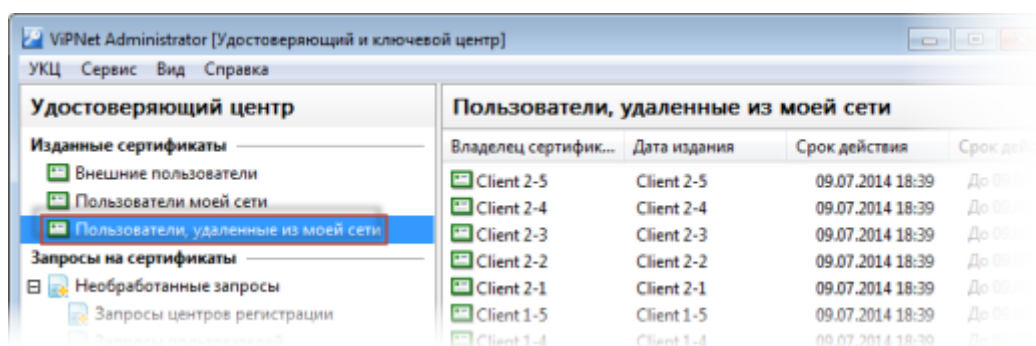


Рисунок 38. Сертификаты пользователей, удаленных из сети ViPNet

- При необходимости можно распечатать сразу нескольких сертификатов пользователей. Также реализована возможность печати сертификата на нескольких листах и оптимизировано расположение текста полей сертификата на распечатанной странице.

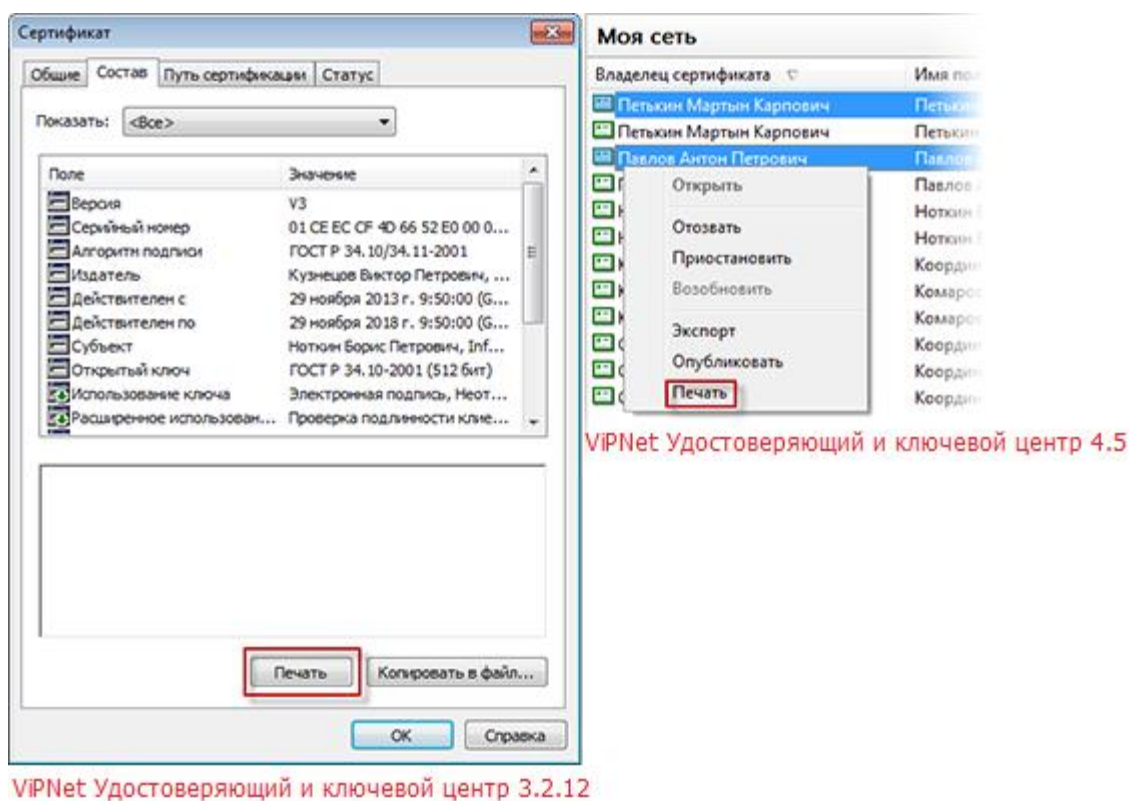


Рисунок 39. Возможность отправки на печать нескольких сертификатов

Задание срока действия CRL в часах

В настройках программы ViPNet Удостоверяющий и ключевой центр версии 3.2.12 можно задать срок действия списка аннулированных сертификатов только в днях. В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 вы можете задать данный срок и в часах. Например, если в вашей организации срок действия списка аннулированных сертификатов ограничен несколькими часами. Также появилась возможность указать время оповещения об истечении срока действия CRL в часах.

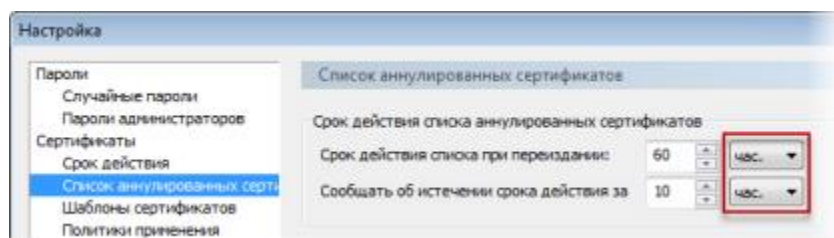



Рисунок 40. Срок действия CRL в часах

Работа с большими списками

При запуске программы ViPNet Удостоверяющий и ключевой центр версии 3.2.12 списки сертификатов пользователей, а также удовлетворенных и отклоненных запросов на сертификаты загружаются из базы данных полностью. Например, если такой список содержит более миллиона объектов, для его загрузки потребуется большой объем оперативной памяти на компьютере с УКЦ.

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 работа с такими списками оптимизирована, и каждый раз загружается фиксированное количество объектов из списка — 100 объектов. В строке состояния главного окна программы при этом отображается, сколько всего объектов данного типа содержится в базе данных. Просмотреть остальные объекты списка можно только путем их поиска с помощью строки поиска .

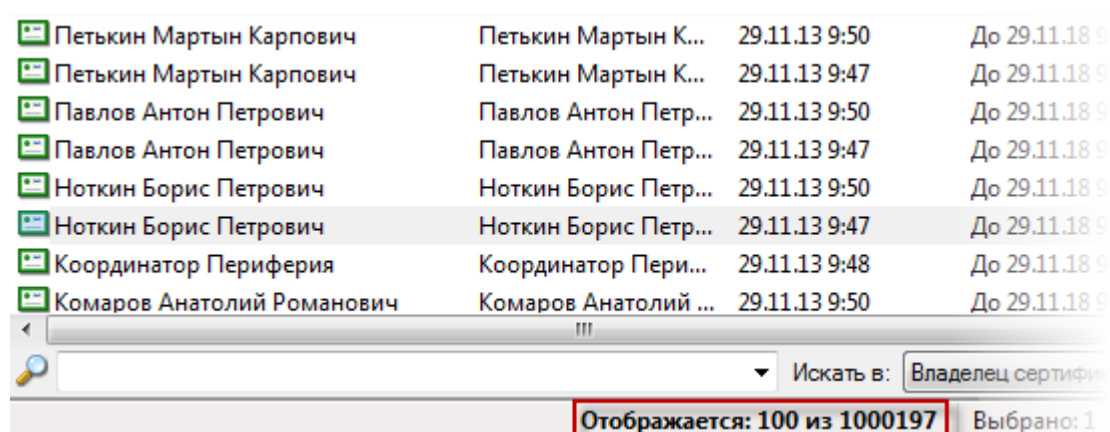


Рисунок 41. Отображение информации о количестве загруженных объектов в строке состояния

Ключи пользователей, ключи сетевых узлов и дистрибутивы ключей

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 по сравнению с версией 3.2.12 появились новые возможности и изменились некоторые сценарии работы с ключами пользователей, ключами сетевых узлов и дистрибутивами ключей.

Создание ключей пользователей и ключей сетевых узлов

В программе ViPNet Удостоверяющий и ключевой центр 3.2.12 можно создавать ключи узлов, ключи пользователей и дистрибутивы ключей только после их формирования в ЦУСе и отправки в УКЦ справочников (файлов связей), даже если справочники, переданные ранее, актуальны. В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 реализована возможность повторно создавать ключи и дистрибутивы ключей без необходимости передачи справочников из ЦУСа.

В новой версии программы отображается дата создания ключей сетевых узлов, дистрибутивов ключей и списка аннулированных сертификатов.

Теперь вы также можете просмотреть статусы ключей, статусы списка аннулированных сертификатов и статусы справочников ЦУС и выполнить сортировку по статусу ключей или по статусам справочников ЦУС, например, чтобы найти узлы, для которых требуется создать ключи или сформировать справочники в ЦУС.

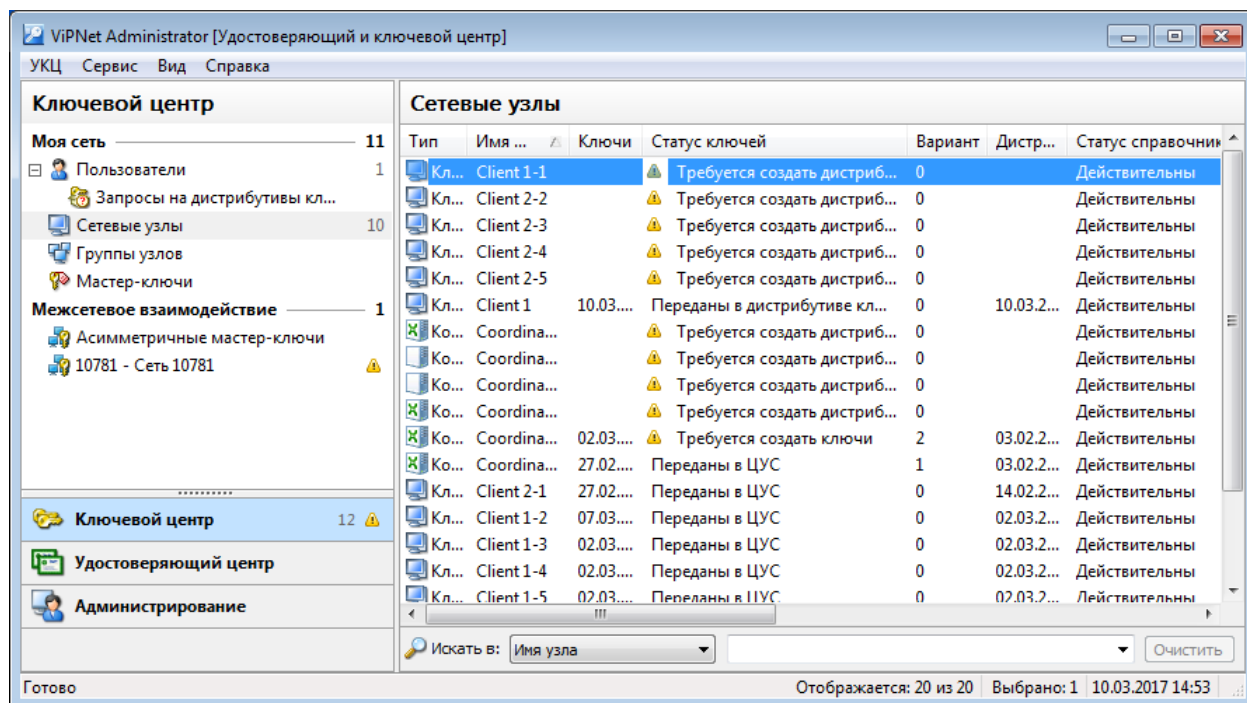


Рисунок 42. Отображение статусов ключей сетевых узлов и дистрибутивов

Выдача дистрибутивов ключей

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 процедура создания дистрибутивов ключей изменилась по сравнению с версией 3.2:

- Теперь дистрибутивы ключей сразу после создания автоматически сохраняются программой в заданную папку, и от администраторов УКЦ больше не требуется выполнять это действие вручную.

В связи с этим в представлении **Ключевой центр** на панели навигации был удален раздел **Сетевые узлы > Дистрибутивы**, из контекстного меню сетевых узлов была удалена группа команд **Дистрибутивы ключей** и была добавлена команда **Выдать новый дистрибутив ключей** для создания дистрибутивов ключей.

- Если на сетевом узле зарегистрировано несколько пользователей, теперь в мастере подготовки к выдаче новых дистрибутивов вы можете выбрать, кому из пользователей узла нужно выдать дистрибутив ключей, при этом не создавать еще один дистрибутив и не издавать дополнительный сертификат.
- Теперь в мастере создания дистрибутива ключей вы можете выбрать способ аутентификации пользователей в ПО ViPNet на узлах.
- Теперь вы можете выбирать способ сохранения ключей электронной подписи пользователей в мастере создания дистрибутивов. Например, если вы создаете дистрибутивы ключей сразу для нескольких узлов, и для части пользователей требуется сохранить ключи электронной подписи на внешние устройства, а для остальных — поместить в дистрибутив ключей.

В связи с изменением процедуры выдачи дистрибутивов ключей в программе ViPNet Удостоверяющий и ключевой центр окне **Настройка** был добавлен раздел **Дистрибутивы ключей**. В этом разделе вы можете задать папку для сохранения дистрибутивов ключей, а также включить функцию выбора способа аутентификации пользователей и способа сохранения ключей электронной подписи пользователей.

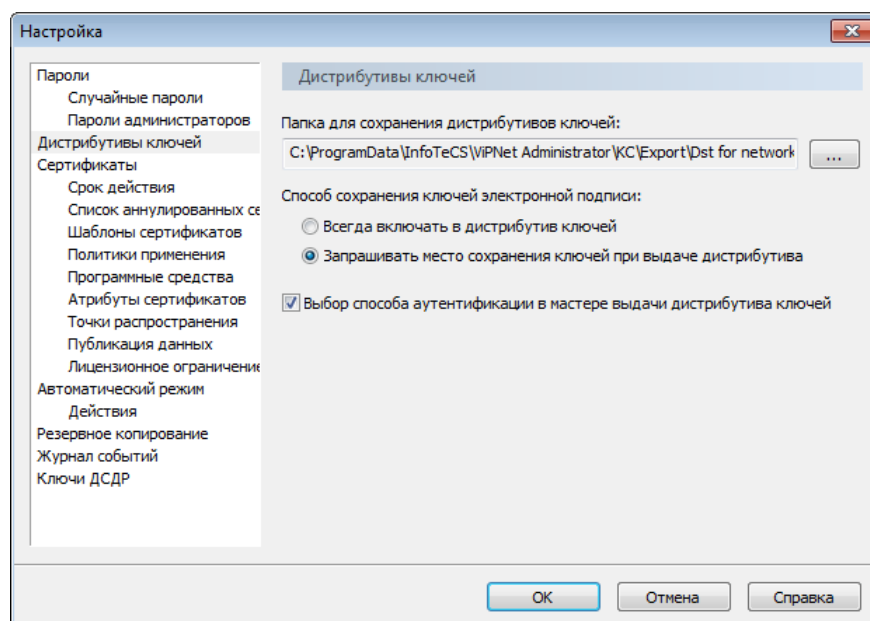


Рисунок 43. Настройка параметров выдачи дистрибутивов ключей

Создание и передача резервных наборов персональных ключей (РНПК)

В программе ViPNet Удостоверяющий и ключевой центр 4.6.7 появилась возможность создавать ключи пользователя вместе с **резервным набором персональных ключей (РНПК)** (см. глоссарий, стр. 96) и сохранять их в один файл.

Создание РНПК вместе с ключами пользователя может потребоваться перед проведением операции компрометации или при создании ключей пользователя после смены мастер-ключа в сети, если по каким-то причинам у пользователя нет резервного набора, либо если указанные операции были проведены некорректно.

Для упрощения работы с РНПК в новой версии нет необходимости в настройке параметров их создания. Теперь в набор всегда входит 20 персональных ключей, и минимальное число ключей, которые должны оставаться неиспользованными, всегда равно 1.

Обработка запросов на дистрибутивы ключей вручную

В программе ViPNet Удостоверяющий и ключевой центр версии 3.2.12 обработка запросов на дистрибутивы ключей, созданных в программе ViPNet Registration Point, выполнялась автоматически, без участия администратора УКЦ.

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 появилась возможность просмотреть и обработать такие запросы вручную (удовлетворить или отклонить). Кроме того, при соответствующих настройках программы в случае удовлетворения запроса на дистрибутив ключей можно отредактировать поля издаваемого сертификата с помощью мастера.

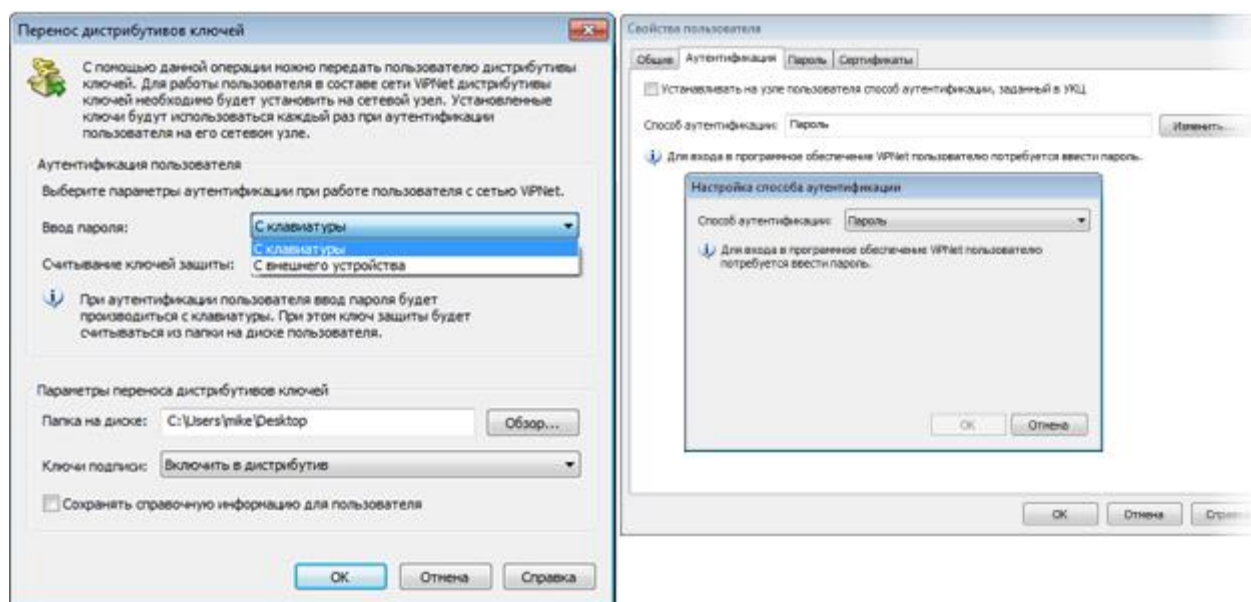
Таким образом, теперь администратор УКЦ может контролировать создание дистрибутивов. Это особенно важно потому, что в ЦУСе, через который запросы передаются в УКЦ, отсутствует фильтрация и контроль запросов.

Способ обработки запросов на дистрибутивы ключей задается в настройках автоматического режима работы программы (см. [Автоматический режим работы](#) на стр. 87).

Настройка параметров аутентификации пользователя

В программе ViPNet Удостоверяющий и ключевой центр версии 3.2.12 способ аутентификации пользователя в программном обеспечении ViPNet на сетевых узлах задавался при переносе дистрибутива ключей в папку и зависел от выбранного способа ввода пароля, а также от места хранения ключей защиты.

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 выбор способа аутентификации пользователя не связан с переносом дистрибутива ключей в папку и осуществляется в окне свойств пользователя либо при выдаче дистрибутива ключей (см. [Выдача дистрибутивов ключей](#) на стр. 73).



ViPNet Центр управления сетью 3.2.12

ViPNet Удостоверяющий и ключевой центр 4

Рисунок 44. Выбор способа аутентификации пользователя

Новые способы аутентификации пользователя

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 изменились способы аутентификации, которые вы можете выбрать для пользователей сетевых узлов.

В версиях 4.x невозможно задать способ аутентификации с вводом пароля с внешнего устройства (**Пароль на устройстве**), поскольку этот способ больше не отвечает требованиям безопасности.

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 введены два новых способа аутентификации пользователя:

- Аутентификация с помощью внешнего устройства, на котором сохранены сертификат ключа проверки электронной подписи и соответствующий **ключ электронной подписи** (см. глоссарий, стр. 95).

При использовании этого способа аутентификации сертификат ключа проверки электронной подписи может быть издан не только в УКЦ, но в стороннем **удостоверяющем центре** (см. глоссарий, стр. 98). Если до начала работы с ПО ViPNet у пользователя уже имеется внешнее устройство с сертификатом, изданным сторонним удостоверяющим центром, то для пользователя может быть задан тип аутентификации с помощью этого устройства.

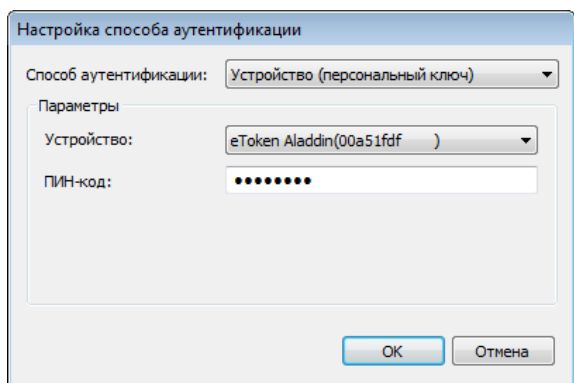


Рисунок 45. Задание способа аутентификации с помощью внешнего устройства

- Аутентификация по сертификату.

При использовании этого способа аутентификации для входа в программу пользователю требуется контейнер ключей и сертификат ключа проверки электронной подписи. Данный способ аутентификации используется, если у пользователей организации уже имеются сертификаты, изданные сторонним удостоверяющим центром, и ключи электронной подписи хранятся на компьютерах пользователей либо в защищенном хранилище организации. Также за счет использования данного способа аутентификации может быть настроена аутентификация пользователя по одному сертификату в ОС Windows, ПО ViPNet и других специализированных программах.

При настройке данного способа аутентификации администратору УКЦ не требуется контейнер ключей электронной подписи пользователя, за счет этого обеспечивается защита ключей от доступа третьих лиц.

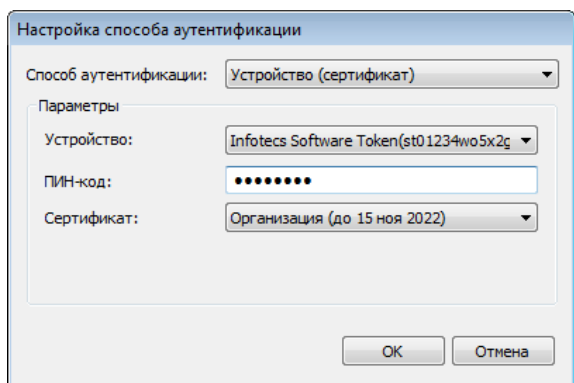


Рисунок 46. Настройка аутентификации по сертификату

Выдача паролей пользователей

По требованиям безопасности в программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 реализована функция печати паролей пользователей на специальных ПИН-конвертах, в которых пароли содержатся в запечатанной части. За счет этого обеспечивается защищенная передача паролей пользователям и исключается доступ к паролям посторонних лиц.

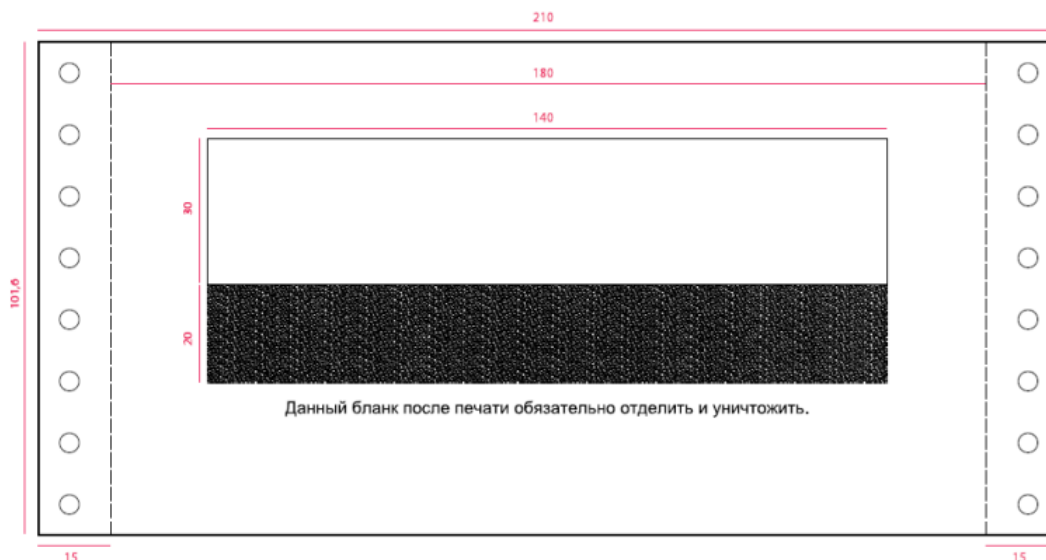


Рисунок 47. Внешний вид стандартного ПИН-конверта, размеры указаны в миллиметрах

Возможность выдачи пароля в файле осталась. Только теперь пароль сохраняется в графическом виде в файле *.xps. При этом вы должны обеспечить защиту пароля, выдаваемого в файле, самостоятельно с помощью организационных мер.

Вы задаете способ выдачи паролей пользователей в окне **Настройка** в разделе **Пароли**. В зависимости от заданного способа по завершении создания дистрибутивов ключей (см. [Выдача дистрибутивов ключей](#) на стр. 73) или по вашей команде производится сохранение паролей в файл или их отправка на печать.

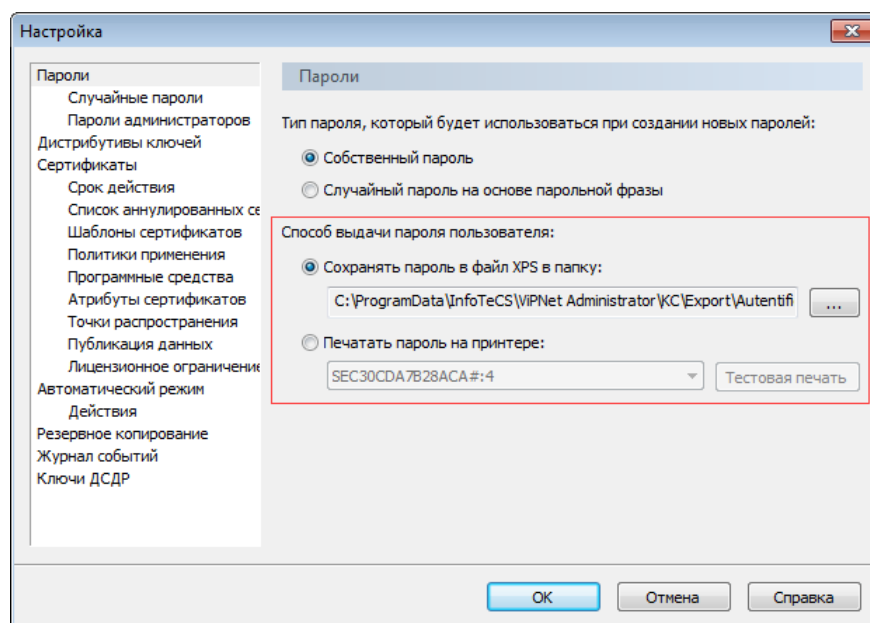


Рисунок 48: Настройка способа выдачи паролей пользователей

Компрометация ключей пользователя

В программе ViPNet Удостоверяющий и ключевой центр 3.2.12 действия в случае компрометации выполнялись отдельно для ключей пользователя и ключей сетевого узла. Теперь они объединены в единую процедуру. При этом, когда ключи пользователя считаются скомпрометированными, автоматически изменяются вариант персонального ключа пользователя и вариант ключей всех узлов, на которых зарегистрирован пользователь. После этого на основе измененных вариантов ключей создаются новые ключи пользователя и ключи сетевых узлов, на которых он зарегистрирован.

Также реализована возможность изменения варианта персонального ключа пользователя и ключей узла в случае неявной компрометации ключей (если нет фактов, подтверждающих компрометацию ключей, но есть подозрение, что злоумышленник получил доступ к ним) или планоно в соответствии с регламентом политики безопасности организации.

Распаковка ключей и дистрибутивов ключей

В программе ViPNet Удостоверяющий и ключевой центр версии 3.2.12 можно было выполнить распаковку ключей или дистрибутивов ключей. В связи с невостребованностью данных операций, в программе версии 4.6.7 они были исключены.

Отказ от использования обновлений ключей узлов

В программе ViPNet Удостоверяющий и ключевой центр версии 3.2.12 для доставки на узлы [CRL](#) (см. глоссарий, стр. 97), сертификатов администраторов, аутентификационных данных пользователя и служебной информации по узлу использовались обновления ключей узлов.

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 обновления ключей узлов не используются, при этом:

- CRL и сертификаты администраторов передаются на узлы в комплектах CRL.
- Аутентификационная информация и служебная информация по узлу передается в составе ключей узла.

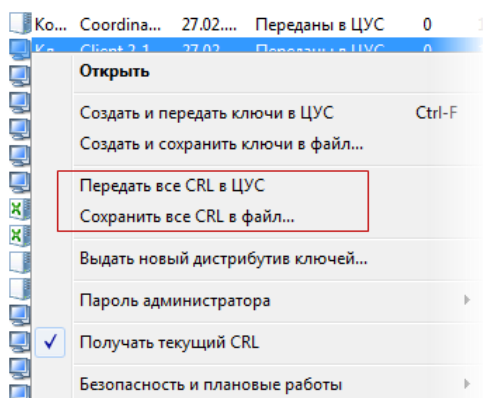


Рисунок 49. Передача CRL на узлы сети вместо обновлений ключей узлов

Эти изменения сделаны для того, чтобы отделить информацию для работы в PKI-инфраструктуре от информации для работы в VPN-сети и передавать ее в составе разных объектов.

Учет ключей ДСДР

Если в сети ViPNet в качестве координаторов используются программно-аппаратные комплексы (ПАК) ViPNet Coordinator KB2 (узлы с ролями «Coordinator KB100», «Coordinator KB1000», «Coordinator KB2000» и «Coordinator KB5000») или ViPNet L2 (узлы с ролями «L2-10G» и «L2-100G»), для выработки ключей шифрования IP-трафика, передаваемого между ПАКами ViPNet Coordinator KB2 (или ViPNet L2), используются ключи ДСДР, формируемые сторонней уполномоченной организацией. При получении и перед вводом в действие комплекты ключей ДСДР в обязательном порядке регистрируются в программе ViPNet Удостоверяющий и ключевой центр — задается серия ключей и каждому координатору присваивается номер комплекта ключей.

В ViPNet Удостоверяющий и ключевой центр версии 3.2.13 на узлах ПАК ViPNet Coordinator KB2 срок действия ключей ДСДР не учитывался и истекал без каких-либо оповещений и предупреждений. Несвоевременная регистрация новых ключей ДСДР и смена ключей ДСДР приводили к простоя в работе узлов ПАК ViPNet Coordinator KB2.

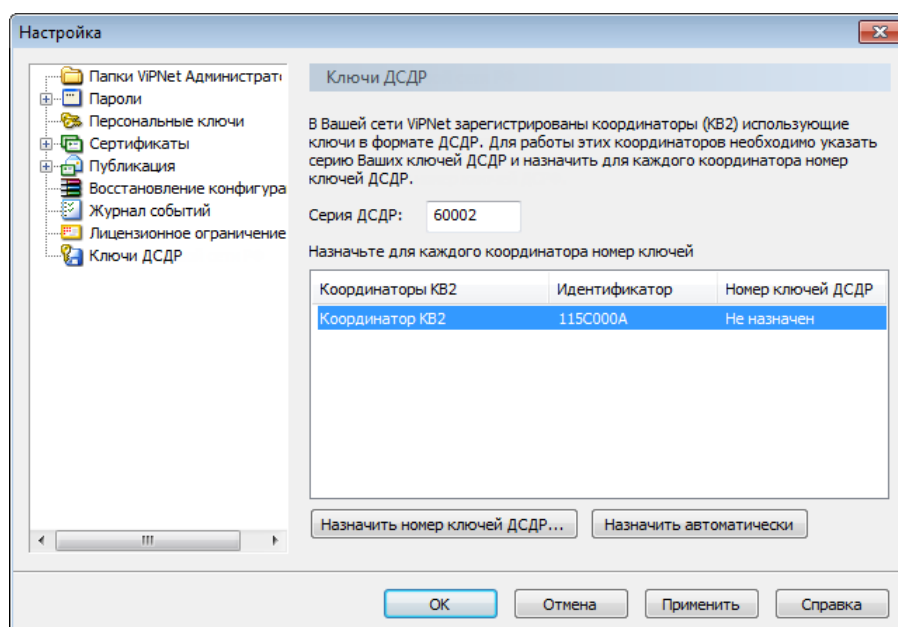


Рисунок 50. Настройка работы с ключами ДСДР в УКЦ версии 3.x

В ViPNet Удостоверяющий и ключевой центр версии 4.6.7 появилась возможность зарегистрировать до двух серий ключей ДСДР одновременно. По истечении срока действия текущей серии ключей ДСДР автоматически будет использована следующая серия. Это исключает время простоя в работе узлов ПAK ViPNet Coordinator KB2 (или ViPNet L2) при несвоевременной регистрации новых ключей ДСДР за счет следующих настроек:

- контроля сроков действия ключей ДСДР для узлов ПAK ViPNet Coordinator KB2 (или ViPNet L2);
- настройки оповещения об окончании срока действия ключей ДСДР;
- автоматической смены ключей ДСДР при регистрации двух серий ключей ДСДР.

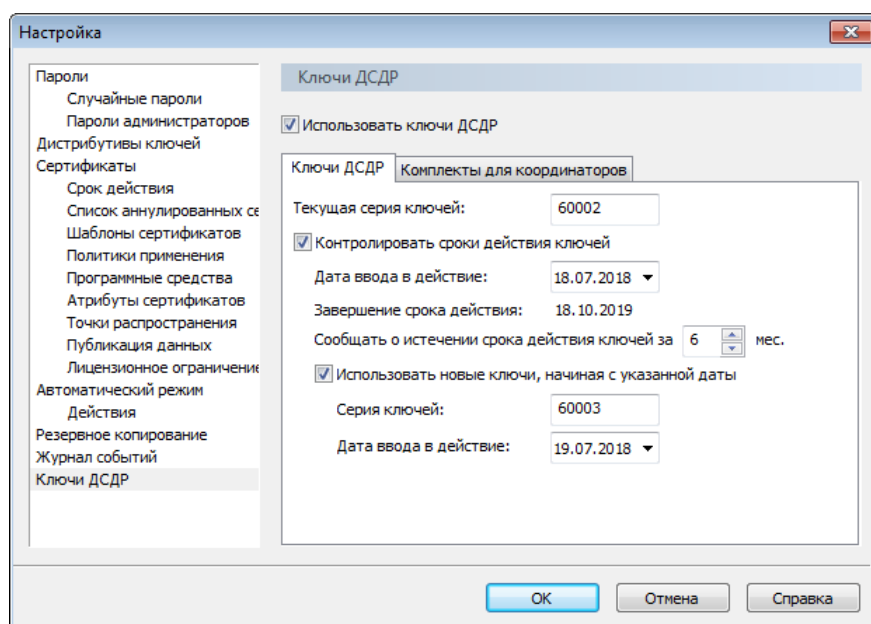


Рисунок 51. Настройка контроля срока действия ключей ДСДР

Административные функции

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 по сравнению с версией 3.2.12 появились новые возможности и изменились некоторые сценарии администрирования.

Отказ от использования нескольких учетных записей администратора

В программе ViPNet Удостоверяющий и ключевой центр версии 3.2.12 можно использовать несколько учетных записей администраторов. Однако это может быть затруднительно по следующим причинам:

- С увеличением количества администраторов повышается сложность надежного хранения сертификатов и ключей электронной подписи этих администраторов. В случае утери ключа электронной подписи одного из администраторов или удаления его учетной записи происходит потеря доверия ко всей цепочке сертификатов, изданных с использованием сертификата этого администратора. Аннулирование, проверка и обновление сертификатов пользователей после этого невозможна.
- Организационно усложняется процедура обновления списков аннулированных сертификатов (CRL). Для обновления CRL необходимо физическое присутствие администратора, сертификату которого соответствует данный CRL. Если администратор по тем или иным причинам недоступен (например, находится в отпуске), другой администратор, поставив его в известность, должен войти в УКЦ с использованием пароля отсутствующего администратора и обновить CRL. Однако передача индивидуальной конфиденциальной информации крайне нежелательна из соображений безопасности.
- При наличии нескольких учетных записей администратора УКЦ списков аннулированных сертификатов (CRL) тоже несколько. При этом у каждого CRL после его публикации на внешней точке доступа имеется собственный адрес. Собственный адрес необходим, поскольку для проверки разных сертификатов пользователей нужно скачивать разные CRL.

По этим причинам в программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 функция создания нескольких учетных записей администратора была заблокирована. Тем не менее, если в вашей сети ранее были созданы несколько учетных записей администратора, при переходе на версию 4.6.7 они продолжают нормально функционировать.

Смена пароля администратора и ключа защиты УКЦ

При работе с программой ViPNet Удостоверяющий и ключевой центр версии 3.2.12 в целях обеспечения безопасности рекомендуется менять пароль администратора и ключ защиты УКЦ не реже одного раза в год. При этом никаких уведомлений о необходимости их смены не предусмотрено.

В программе ViPNet Удостоверяющий и ключевой центр 4.6.7 по истечении 6 месяцев со дня начала действия пароля администратора и ключа защиты УКЦ вы будете получать уведомление о необходимости их смены (см. [Новая система оповещений в программе ViPNet Удостоверяющий и ключевой центр](#) на стр. 85). Просмотреть информацию о сроках смены ключа защиты УКЦ, пароля администратора, а также ключа электронной подписи администратора вы можете в представлении **Администрирование** в разделе **Администраторы**.

Кроме того, в программе ViPNet Удостоверяющий и ключевой центр 4.6.7 выполнены следующие доработки:

- Сменить ключ защиты УКЦ можно не только с помощью меню **УКЦ**, но с помощью соответствующей кнопки в окне просмотра свойств администратора.

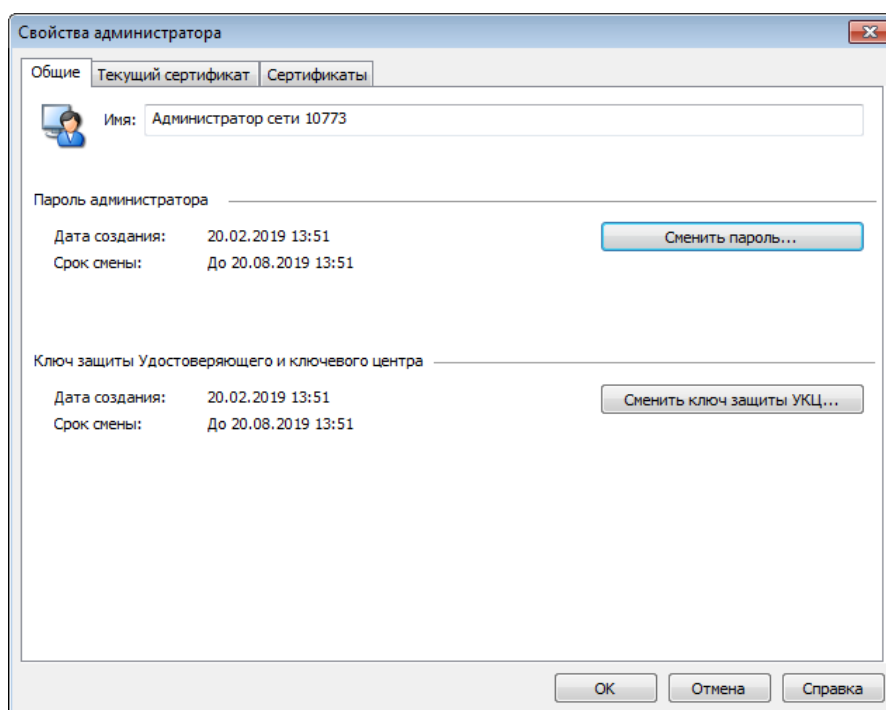


Рисунок 52. Смена ключа защиты УКЦ

- Для повышения уровня безопасности при смене [пароля администратора УКЦ](#) (см. глоссарий, стр. 96) требуется указывать текущий пароль.

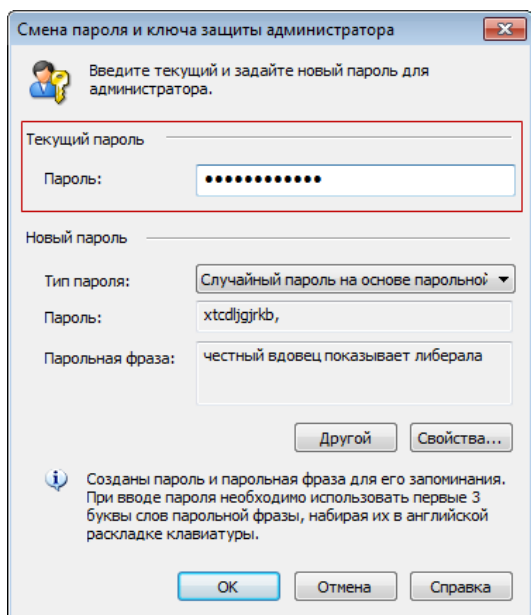


Рисунок 53. Задание текущего пароля администратора УКЦ

- С целью повышения безопасности паролей пользователей, администраторов сетевых узлов и администратора УКЦ отменена возможность использовать случайный цифровой пароль.

Удаление паролей администраторов сетевых узлов

В программе ViPNet Удостоверяющий и ключевой центр версии 3.2.12 пароль администратора можно было только сменить. В программе версии 4.6.7 появилась возможность удаления (сброса) [паролей администраторов сетевых узлов](#) (см. глоссарий, стр. 96). Данная операция может потребоваться в том случае, если пароль искажен или недействителен и если не требуется создавать вместо него новый пароль (менять пароль). Удалить пароли администраторов можно одновременно для нескольких выбранных узлов.

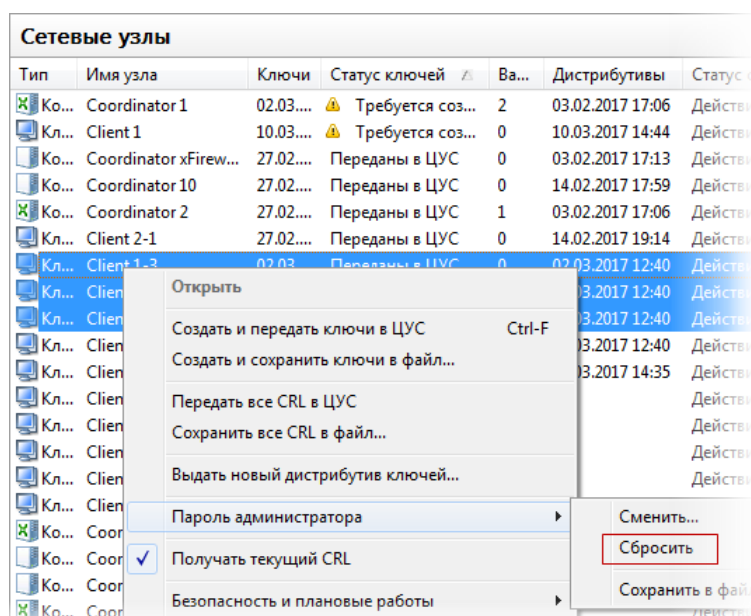


Рисунок 54. Возможность сброса паролей администраторов сетевых узлов и групп узлов



Примечание. Стоит учитывать, что без пароля администратора на сетевом узле невозможно выполнить расширенные настройки ПО ViPNet.

Новая система оповещений в программе ViPNet Удостоверяющий и ключевой центр

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 реализована новая система оповещений администратора о необходимости проведения тех или иных операций. Если требуется, чтобы администратор выполнил некоторые важные операции, например, создал ключи для пользователя, обновил CRL (см. глоссарий, стр. 97) или обработал поступивший запрос на сертификат, то на панели навигации главного окна программы появятся значки оповещений . Значок оповещения будет рядом с названием того представления, с объектами которого требуется выполнить нужные операции. Рядом со значком будет указано количество операций, которое нужно выполнить. Количество операций также будет указано напротив разделов данного представления.

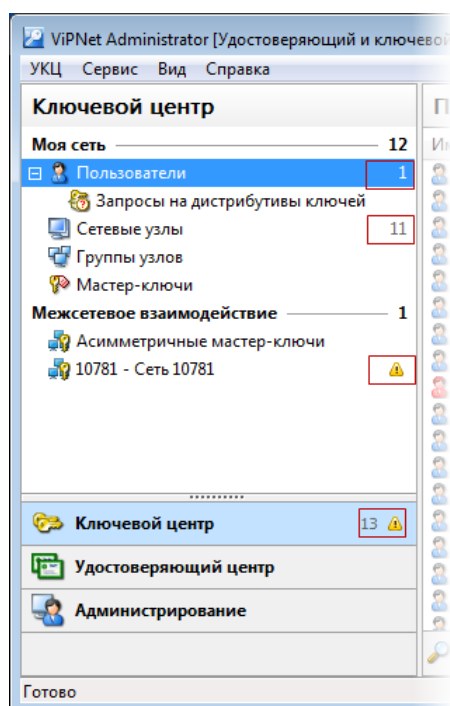


Рисунок 55. Оповещения о необходимости проведения важных операций

Организация межсетевого взаимодействия

В программе ViPNet Удостоверяющий и ключевой центр 3.2.12 для организации межсетевого взаимодействия использовались три типа межсетевых мастер-ключей: индивидуальные симметричные межсетевые мастер-ключи, универсальные симметричные межсетевые мастер-ключи и асимметричные межсетевые мастер-ключи.

Для обеспечения более высокого уровня безопасности межсетевого взаимодействия в программе ViPNet Удостоверяющий и ключевой центр 4.6.7 вы можете использовать только асимметричные и индивидуальные симметричные межсетевые мастер-ключи. Универсальные межсетевые мастер-ключи больше не поддерживаются и удаляются при конвертации базы данных УКЦ в процессе миграции с версии 3.2.12.



Внимание! Перед тем как обновить программу ViPNet Удостоверяющий и ключевой центр с версии 3.2.12 до версии 4.6.7, необходимо отменить использование универсального межсетевого мастер-ключа и перейти на использование индивидуальных межсетевых мастер-ключей. Если этого не сделать, переход на версию 4.6.7 вызовет нарушение связи между узлами доверенных сетей на время организации нового межсетевого взаимодействия.

Передача сертификатов администраторов и CRL в доверенную сеть

В программе ViPNet Administrator 3.2.12 сертификаты администраторов и списки аннулированных сертификатов передаются в доверенную сеть в едином контейнере сертификатов. В программе ViPNet Удостоверяющий и ключевой центр 4.6.7 при обработке контейнера сертификатов можно выбрать отдельные сертификаты и соответствующие им списки аннулирования для применения.



Примечание. В программе ViPNet Удостоверяющий и ключевой центр 4.6.7 нельзя импортировать сертификат без соответствующего списка аннулированных сертификатов и наоборот.

Кроме того, в новой версии программы списки аннулированных сертификатов могут обновляться в автоматическом режиме работы УКЦ. При этом они передаются в доверенные сети сразу после обновления вместе с корневым сертификатом издателя.

Автоматический режим работы

В программе ViPNet Удостоверяющий и ключевой центр версии 3.2.12 автоматические операции выполняются в случайном порядке, и параллельно с ними можно производить операции вручную. Вследствие этого могут возникать различные конфликты. Например, могут одновременно создаваться ключи узлов по команде администратора и обновления ключей узлов по расписанию либо при автоматической обработке запросов на сертификаты могут производиться действия с сертификатом издателя. Такие конфликты могут стать причиной сбоя в работе программы. Кроме того, в программе версии 3.2.12 автоматические операции выполняются в фоновом режиме, и администратор может узнать об их выполнении только из журнала событий.

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 выполнены следующие доработки автоматического режима:

- Формируется очередь операций для выполнения в автоматическом режиме, и блокируются возможности выполнения любых действий администратора вручную. Это позволяет избежать одновременного выполнения нескольких операций и предотвратить возникновение конфликтов и сбоев.
- Расширен список операций, которые могут выполнять в автоматическом режиме. Теперь автоматически могут создаваться ключи узлов, импортироваться списки аннулированных сертификатов (CRL) из доверенных сетей и CRL, загруженные сервисом публикации из точек распространения других удостоверяющих центров и другие. Также в автоматическом режиме программы выполняется создание резервных копий конфигурации сети ViPNet.
- Настройки автоматических операций в новой версии программы могут быть произведены в процессе первичной инициализации УКЦ либо в настройках программы в разделе **Автоматический режим > Действия**, а также настройка автоматического создания резервных копий — в разделе **Восстановление конфигурации**.

- Все автоматические операции отображаются в специальном окне, что позволяет администратору УКЦ легко отслеживать ход их выполнения.

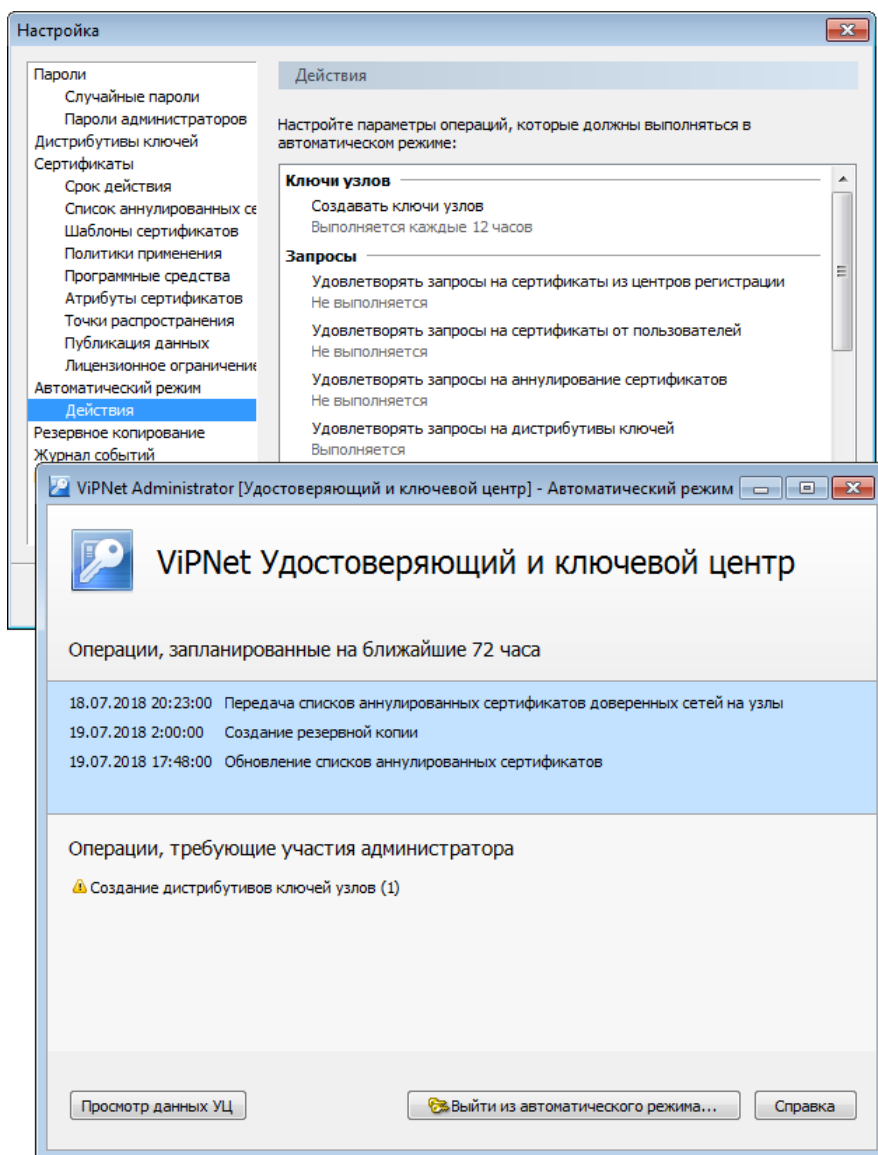


Рисунок 56. Использование автоматического режима работы УКЦ

- Появилась возможность просмотра изданных сертификатов пользователей и их параметров. Это позволяет администратору УКЦ отслеживать, какие сертификаты издаются в автоматическом режиме по запросам.

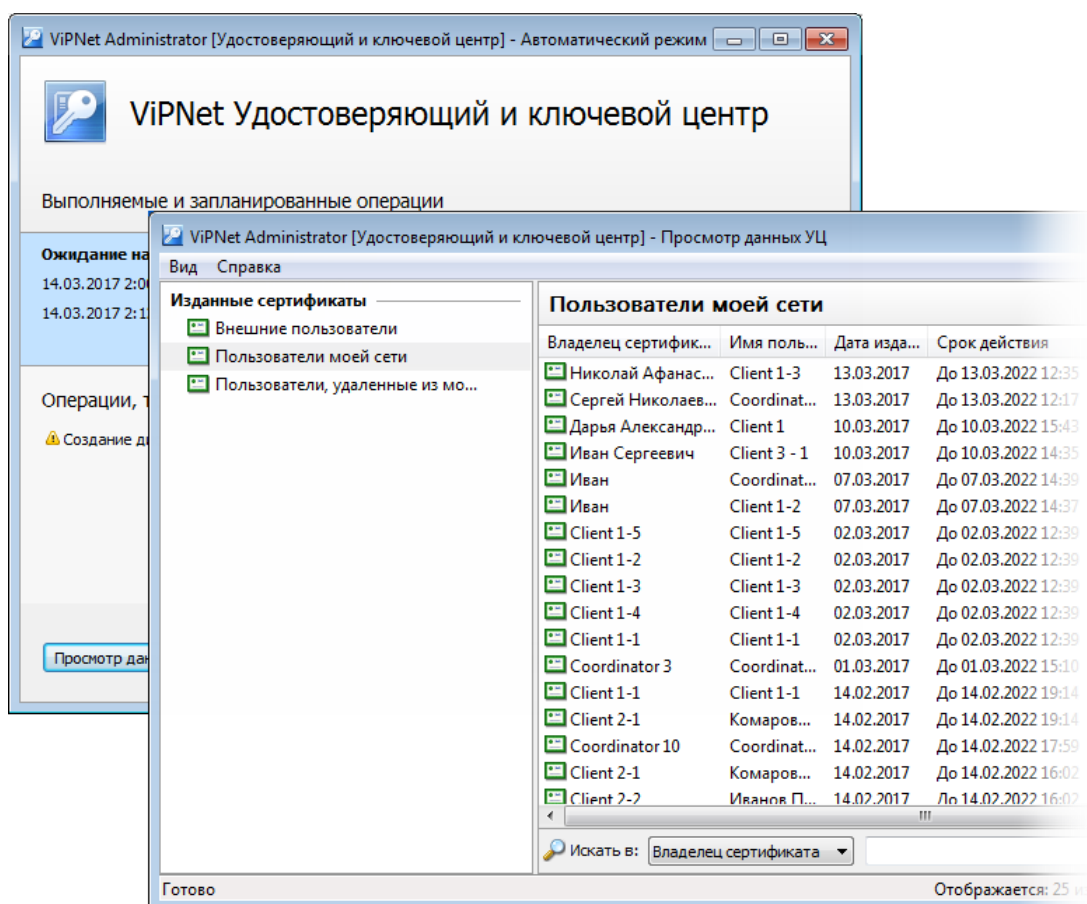


Рисунок 57. Возможность просмотра изданных сертификатов при работе в автоматическом режиме

Подробную информацию об автоматическом режиме работы УКЦ см. в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», в главе «Режимы работы в программе ViPNet Удостоверяющий и ключевой центр».

Реализация системного журнала событий

В программе ViPNet Удостоверяющий и ключевой центр версии 3.2.12 журнал событий был организован непосредственно в самой программе. В новой версии программы регистрация событий, возникающих в процессе работы УКЦ, осуществляется в системном журнале Windows, который защищен от модификации и удаления обычным пользователем, не имеющим прав администратора операционной системы.

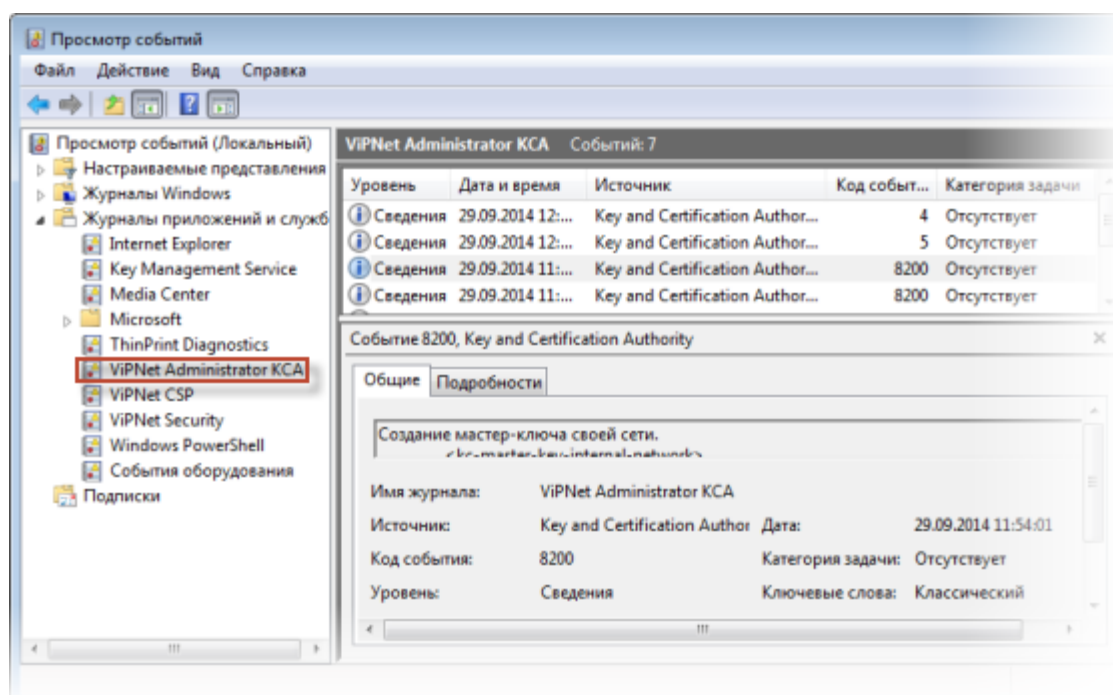


Рисунок 58. Системный журнал событий УКЦ

Подробную информацию о работе с журналом событий см. в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», в главе «Административные функции», в разделе «Работа с журналом событий».

Полный перечень событий УКЦ, регистрируемых в журнале событий см. в приложении документа «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

Резервное копирование конфигурации сети

В программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 выполнена доработка функциональных возможностей резервного копирования конфигурации сети, а именно:

- Появилась возможность создания и восстановления резервных копий конфигурации сети в случае, если база данных SQL и программа ViPNet Удостоверяющий и ключевой центр установлены на разных компьютерах. При таком размещении требуется настроить в программе доступ к папке, в которую помещаются резервные копии на компьютере с базой данных. При правильной настройке резервная копия, созданная на компьютере с базой данных, автоматически перемещается на компьютер с УКЦ в папку `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore`. При восстановлении конфигурации резервная копия, выбранная в УКЦ, автоматически копируется на компьютер с базой данных. Таким образом, теперь создание и восстановление резервных копий конфигурации доступны всегда, независимо от способа размещения программы и базы данных.
- Появилась возможность настроить автоматическое создание резервных копий — с определенной периодичностью (от 1 до 31 дней) и в любое время суток. При переходе УКЦ в

автоматический режим создание резервных копий конфигурации будет включено в список выполняемых операций в этом режиме.

В программе ViPNet Удостоверяющий и ключевой центр версии 3.2.12 автоматически создавать резервные копии конфигурации сети ViPNet можно только при выходе из программы. Это не всегда удобно для администратора, особенно в случае работы с большими сетями, создание резервной копии конфигурации которых может занимать продолжительное время.

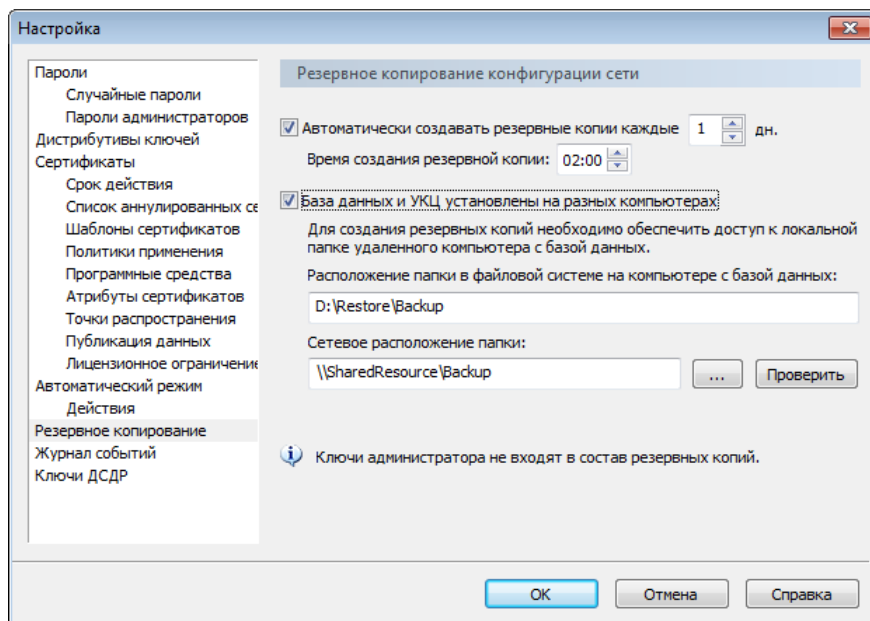


Рисунок 59. Автоматическое создание резервных копий конфигурации по расписанию

- Изменился состав файла резервной копии конфигурации сети. Теперь в него не включаются следующие данные:
 - информация о файлах, полученных и отправленных сетевыми узлами (хранится в специальной базе);
 - справочники и ключи узлов (всегда могут быть созданы в текущей конфигурации сети).

Это позволяет значительно сократить время, необходимое для создания резервной копии конфигурации сети и последующего восстановления конфигурации сети из резервной копии.

- Появилась возможность восстановить конфигурацию сети, используя резервную копию, созданную в программе ViPNet Удостоверяющий и ключевой центр версии 3.2.12.

В версии 3.2.12 в случае возникновения проблем в сети после обновления ПО ViPNet Administrator для восстановления конфигурации сети с помощью программы ViPNet Удостоверяющий и ключевой центр определенной версии могла использоваться только резервная копия, которая была создана в УКЦ той же версии. В случае несовпадения версий восстановление было невозможно.

Обмен данными с программой ViPNet Publication Service

В программе ViPNet Удостоверяющий и ключевой центр версии 3.2.12 обмен данными с программой [ViPNet Publication Service](#) (см. глоссарий, стр. 93) осуществляется через те же папки, которые используются для обмена данными с программой ViPNet Центр управления сетью.

В связи с тем, что в программе ViPNet Удостоверяющий и ключевой центр версии 4.6.7 обмен данными осуществляется посредством базы данных SQL и задавать папки обмена данными с ViPNet Центр управления сетью не нужно, теперь для обмена данными с программой ViPNet Publication Service требуется отдельно назначать папки (в том числе и папки на сетевых дисках).

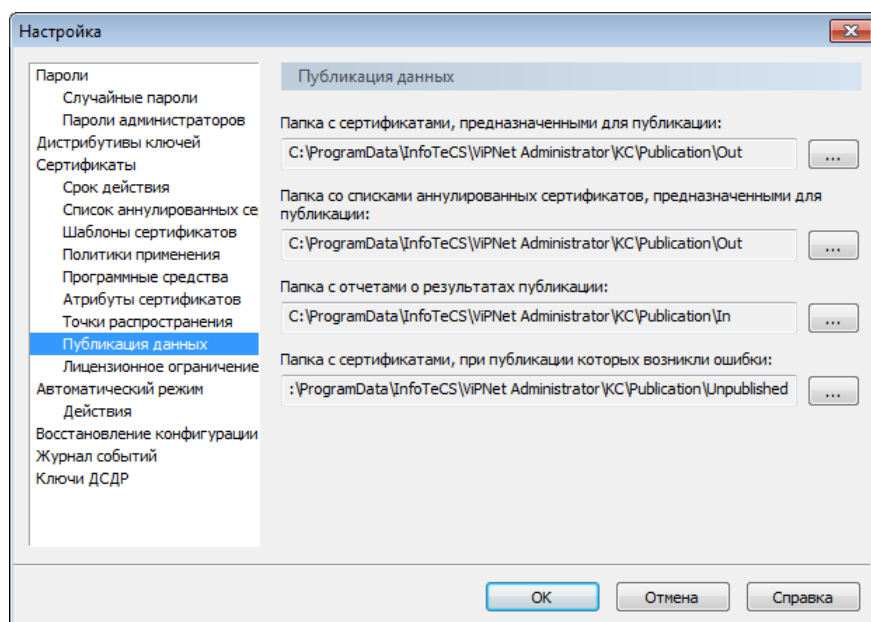


Рисунок 60. Настройка папок обмена данными с ViPNet Publication Service

Кроме того, в программе ViPNet Удостоверяющий и ключевой центр версии 3.2.12 импорт сертификатов издателей и CRL, опубликованных сторонними удостоверяющими центрами и полученных из программы ViPNet Publication Service, выполнялся автоматически, без участия администратора УКЦ. В новой версии программы появилась возможность управлять импортом вручную. Это позволяет администратору УКЦ фильтровать данные и импортировать только те данные, которые необходимы для дальнейшей рассылки на сетевые узлы. При этом сертификаты издателей могут быть импортированы только вручную, а списки аннулированных сертификатов — как вручную, так и автоматически.



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 Policy Manager

Программа, которая входит в состав программного комплекса ViPNet. Предназначена для централизованного управления политиками безопасности узлов защищенной сети ViPNet.

ViPNet Publication Service

Программное обеспечение для публикации сертификатов пользователей, издателей (администраторов) и списков отозванных сертификатов в общедоступных хранилищах данных.

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.

Адреса видимости

IP-адреса, виртуальные или реальные, по которым данный узел видит остальные узлы сети ViPNet и по которым приложения отправляют свой трафик.

Вышестоящий удостоверяющий центр

Удостоверяющий центр, который является вышестоящим по отношению к другому удостоверяющему центру в иерархической системе доверительных отношений между удостоверяющими центрами. При этом может быть подчиненным по отношению к третьему удостоверяющему центру, если не является головным.

Группа DNS-серверов

Совокупность списка доменных зон и списка закрепленных за ними DNS-серверов.

Доверенная сеть

Сеть ViPNet, с узлами которой узлы своей сети ViPNet осуществляют защищенное взаимодействие.

Доменная зона (DNS-зона)

Группа имен системы DNS, входящая в конкретный домен или поддомены более низких уровней, находящаяся под одним административным управлением и обслуживаемая одним или несколькими DNS-серверами.

Защищенный DNS-сервер

Защищенный внутренний DNS-сервер организации, который является защищенным узлом сети или туннелируется координатором ViPNet и входит в группу DNS-серверов.

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Ключ электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом электронной подписи называется закрытый ключ, который является секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Компрометация ключей

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

Межсетевая информация

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

Межсетевое взаимодействие

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

Межсетевой мастер-ключ

Ключ, служащий для формирования ключей обмена между сетевыми узлами разных сетей ViPNet.

Межсетевой экран

Устройство на границе локальной сети, служащее для предотвращения несанкционированного доступа из одной сети в другую. Межсетевой экран проверяет весь входящий и исходящий IP-трафик, после чего принимается решение о возможности дальнейшего направления трафика к пункту назначения. Межсетевой экран обычно осуществляет преобразование внутренних адресов в адреса, доступные из внешней сети (выполняет NAT).

Обновление справочников и ключей

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

Открытый интернет (Защищенный интернет-шлюз)

Технология, реализованная в программном обеспечении ViPNet. При подключении к интернету узлы локальной сети изолируются от сети ViPNet, а при работе в сети ViPNet — от интернета, что обеспечивает защиту от возможных сетевых атак извне без физического отключения компьютеров от локальной сети.

Начиная с версии ПО ViPNet Administrator ЦУС 4.6.3, технология «Открытый Интернет» называется «Защищенный интернет-шлюз».

Открытый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Пароль администратора сетевого узла ViPNet

Пароль для входа на сетевом узле ViPNet в режим администратора, в рамках которого становятся доступны дополнительные возможности настройки приложений ViPNet. Пароль администратора сетевого узла ViPNet может быть создан администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр.

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.

Расширения сертификата ключа проверки электронной подписи

Дополнительные атрибуты сертификата, такие как использование ключа, политики сертификата, базовые ограничения, ограничения имени и другие. Расширение может быть критичным или некритичным. Система, использующая сертификаты, должна отвергать сертификат, если она встретила критичное расширение, которое не в состоянии распознать; однако некритичные расширения могут игнорироваться, если они не распознаются. Каждое расширение сертификата должно иметь соответствующий идентификатор объекта (OID).

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.

Роль

Некоторая функциональность сетевого узла, предназначенная для решения целевых и служебных задач сети ViPNet. Роль используется в лицензировании сети с помощью файла лицензии и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

Роли могут иметь атрибуты в виде количественных характеристик и полномочий, которые также влияют на функциональность.

Набор ролей для каждого сетевого узла задается администратором сети ViPNet в программе ViPNet Центр управления сетью.

Сервер IP-адресов

Функциональность координатора, обеспечивающая регистрацию, рассылку и предоставление информации о состоянии защищенных узлов.

Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

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).

Список аннулированных сертификатов (CRL)

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

Туннелирование

Технология, позволяющая защитить соединения между узлами локальных сетей, которые обмениваются информацией через интернет или другие публичные сети, путем инкапсуляции и шифрования трафика этих узлов не самими узлами, а координаторами, которые установлены на

границе их локальных сетей. При этом установка программного обеспечения ViPNet на эти узлы необязательна, то есть туннелируемые узлы могут быть как защищенными, так и открытыми.

Удостоверяющий центр

Организация, осуществляющая выпуск сертификатов ключей проверки электронной подписи, а также сертификатов другого назначения.

Центр регистрации

Компонент удостоверяющего центра. Центру регистрации делегируется часть функций удостоверяющего центра: регистрация пользователей, предоставление пользователям сертификатов ключа проверки электронной подписи, изданных в удостоверяющем центре, и выполнение других операций.

Цепочка сертификации

Упорядоченная последовательность сертификатов, соответствующая иерархии издателей этих сертификатов. Сертификат считается действительным, если цепочка сертификации полна (то есть завершается корневым сертификатом) и все входящие в нее сертификаты также действительны.

Электронная подпись

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.