



ViPNet Удостоверяющий и ключевой центр 4

Руководство администратора

Версия продукта: 4.6.11



© АО «ИнфоТеКС», 2024

ФРКЕ.00109-08 32 02

Версия продукта 4.6.11, документ обновлён 05.03.2025

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 АО «ИнфоТеКС».

ViPNet[®] является зарегистрированным товарным знаком АО «ИнфоТеКС».

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

АО «ИнфоТеКС»

127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение.....	10
О документе.....	11
Для кого предназначен документ	11
Соглашения документа.....	11
О программе	12
Что нового в версии 4.6.11.....	13
Системные требования	14
Комплект поставки	15
Обратная связь.....	16
 Глава 1. Общие сведения	17
Назначение программы ViPNet Удостоверяющий и ключевой центр.....	18
Лицензионные ограничения.....	20
Отсутствие лицензии на выполнение функций удостоверяющего центра.....	21
Расширение лицензии для работы программы в роли удостоверяющего центра	22
Просмотр лицензионного ограничения	23
Настройка оповещения о достижении лицензионного ограничения	24
Взаимодействие с программой ViPNet Центр управления сетью.....	25
Взаимодействие с программой ViPNet Registration Point	27
Взаимодействие с программой ViPNet Publication Service.....	28
Совместимость с программным обеспечением ViPNet	29
 Глава 2. Начало работы с программой ViPNet Удостоверяющий и ключевой центр	30
Установка и первичная инициализация программы ViPNet Удостоверяющий и ключевой центр.....	31
Запуск и завершение работы программы.....	33
Подключение к SQL-серверу при запуске программы	34
Интерфейс программы ViPNet Удостоверяющий и ключевой центр	36
Представление «Ключевой центр».....	38
Представление «Удостоверяющий центр»	39
Представление «Администрирование»	40
 Глава 3. Режимы работы в программе ViPNet Удостоверяющий и ключевой центр.....	42
Режимы работы УКЦ	43
Работа в автоматическом режиме	45
Настройка автоматического режима.....	48

Особенности работы в автоматическом режиме.....	50
Глава 4. Управление ключевой структурой ViPNet.....	51
Ключевая структура ViPNet.....	52
Симметричные ключи в ПО ViPNet.....	52
Асимметричные ключи в ПО ViPNet	53
Работа с дистрибутивами ключей	55
Когда следует создавать дистрибутивы ключей?	55
Особенности создания дистрибутивов ключей.....	56
Настройка параметров создания дистрибутивов ключей	57
Создание дистрибутивов ключей.....	58
Создание дистрибутивов ключей по запросам из центра регистрации	62
Создание дистрибутива ключей для ПАК ViPNet Coordinator KB.....	63
Работа с ключами узлов	65
Когда следует создавать ключи узлов?.....	65
Особенности создания ключей узлов.....	65
Настройка автоматического создания ключей узлов	66
Создание и передача ключей узлов в ЦУС	67
Создание и сохранение ключей узлов в файл.....	67
Работа с ключами пользователей	69
Когда следует создавать ключи пользователей?	69
Особенности создания ключей пользователей	69
Настройка создания ключа электронной подписи и ключа проверки электронной подписи для пользователей сети ViPNet.....	70
Создание и передача ключей пользователей в ЦУС.....	72
Создание и сохранение ключей пользователей в файл	73
Создание и сохранение ключей электронной подписи пользователя в файл.....	75
Работа с резервными наборами персональных ключей.....	77
Когда следует создавать резервные наборы персональных ключей?	77
Создание и сохранение резервных наборов персональных ключей в файл	78
Правила передачи резервных наборов персональных ключей	79
Действия в случае компрометации ключей.....	80
Действия в случае компрометации ключей пользователя	80
Изменение вариантов персонального ключа пользователя и ключей узла.....	82
Действия при утрате резервного набора персональных ключей пользователя	85
Действия в случае компрометации ключа электронной подписи пользователя.....	85
Действия в случае компрометации ключей администратора УКЦ	86
Работа с мастер-ключами.....	88
Смена мастер-ключей защиты и обмена	88

Смена мастер-ключа персональных ключей	90
Глава 5. Просмотр и изменение свойств объектов сети ViPNet	93
Задание способа аутентификации пользователя.....	94
Просмотр свойств пользователя.....	98
Просмотр свойств сетевого узла.....	100
Просмотр свойств группы узлов.....	101
Глава 6. Управление паролями пользователей и администраторов сетевых узлов ViPNet	102
Смена паролей пользователей ViPNet	103
Выдача паролей пользователей	105
Настройка способа выдачи паролей пользователей	106
Настройка печати паролей пользователей	106
Создание и смена пароля администратора сетевого узла или группы узлов.....	110
Сброс пароля администратора сетевого узла.....	113
Сохранение паролей администраторов сетевых узлов.....	115
Настройка оповещений об истечении срока действия паролей администраторов сетевых узлов и групп узлов.....	116
Настройка типа создаваемых паролей	118
Настройка параметров случайных паролей	119
Глава 7. Организация межсетевого взаимодействия.....	121
Порядок организации межсетевого взаимодействия.....	122
Типы межсетевых мастер-ключей.....	124
Создание межсетевых мастер-ключей	126
Экспорт межсетевого мастер-ключа	128
Импорт межсетевого мастер-ключа.....	130
Ввод в действие и прекращение использования межсетевого мастер-ключа	132
Импорт контейнеров сертификатов администраторов доверенных сетей ViPNet	133
Смена межсетевого мастер-ключа.....	136
Удаление межсетевого мастер-ключа.....	138
Экспорт межсетевой информации.....	139
Экспорт межсетевой информации вручную	139
Глава 8. Управление сертификатами.....	140
Издание сертификатов	141
Особенности издания сертификатов.....	142
Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ	143
Издание сертификатов по запросам от пользователей своей сети ViPNet	149

Издание сертификатов по запросам, поступившим из центра регистрации	151
Издание сертификатов по запросам от внешних пользователей.....	153
Настройка параметров издания сертификатов	156
Создание и изменение шаблонов сертификатов.....	156
Настройка списка политик применения сертификата	163
Настройка добавления информации о центрах регистрации в сертификаты пользователей	165
Настройка распределения атрибутов сертификатов.....	166
Настройка оповещения об истечении срока действия сертификатов пользователей	168
Настройка обработки поля ИНН	169
Издание квалифицированных сертификатов	171
Требования к изданию квалифицированных сертификатов	171
Дополнительные атрибуты имени в квалифицированных сертификатах разных видов субъектов.....	173
Настройка параметров издания квалифицированных сертификатов	175
Аннулирование, приостановление действия, возобновление действия сертификатов ..	179
По запросу из центра регистрации	180
По инициативе администратора УКЦ.....	180
Просмотр запросов и сертификатов.....	183
Просмотр запроса на сертификат.....	183
Просмотр сертификатов	185
Просмотр истории сертификатов	188
Экспорт сертификатов	189
Форматы экспорта сертификатов	190
Проверка сертификатов	192
Печать сертификатов	193
Настройка количества сертификатов, отображаемых в окне программы	194
Глава 9. Работа со списками аннулированных сертификатов	195
Общие сведения о списках аннулированных сертификатов	196
Обновление списков аннулированных сертификатов.....	197
Настройка автоматического обновления CRL	197
Обновление CRL вручную.....	198
Настройка срока действия CRL.....	199
Распространение списков аннулированных сертификатов	200
Передача CRL через список рассылки.....	201
Настройка автоматической передачи CRL	202
Передача CRL на узлы вручную	204

Просмотр списков аннулированных сертификатов	206
Экспорт списков аннулированных сертификатов в файл.....	208
Экспорт одного CRL в файл.....	208
Экспорт всех CRL в файл.....	208
Управление временем обновления и публикации CRL.....	210
Глава 10. Публикация сертификатов и списков аннулированных сертификатов	211
Взаимодействие с сервисом публикации	212
Организация взаимодействия с сервисом публикации.....	213
Передача данных для публикации вручную	213
Импорт данных, опубликованных сторонними удостоверяющими центрами	214
Настройка параметров публикации данных	215
Настройка папок обмена с программой ViPNet Publication Service	215
Настройка списка точек распространения.....	216
Глава 11. Установление доверительных отношений с другими удостоверяющими центрами.....	220
Общая информация.....	221
Установление доверительных отношений с вышестоящим или подчиненным удостоверяющим центром.....	223
Создание запроса на сертификат к вышестоящему удостоверяющему центру.....	224
Импорт сертификатов администраторов, полученных из вышестоящего удостоверяющего центра.....	227
Импорт списков аннулированных сертификатов, полученных из вышестоящего удостоверяющего центра.....	228
Импорт сертификата, выданного вышестоящим удостоверяющим центром.....	229
Просмотр запроса на сертификат к вышестоящему удостоверяющему центру	231
Установление доверительных отношений с равнозначным удостоверяющим центром.....	233
Создание запроса на кросс-сертификат	234
Издание кросс-сертификата по запросу.....	236
Экспорт кросс-сертификата	239
Просмотр запроса на кросс-сертификат.....	240
Установление доверительных отношений с удостоверяющим центром Минкомсвязи России	242
Глава 12. Работа с данными администратора программы ViPNet Удостоверяющий и ключевой центр.....	243
Управление учетной записью администратора	244
Отказ от использования нескольких учетных записей администратора	244
Удаление учетной записи администратора.....	244

Смена текущей учетной записи администратора	245
Просмотр и изменение данных об администраторе	248
Управление ключами электронной подписи и сертификатом администратора	250
Издание сертификата администратора	250
Выбор текущего сертификата администратора	256
Плановая смена ключа электронной подписи и сертификата администратора	257
Настройка оповещений о плановой смене ключа электронной подписи и сертификата администратора	259
Просмотр контейнера ключей подписи администратора	259
Смена пароля администратора	261
Смена ключа защиты УКЦ	263
Глава 13. Административные функции	265
Работа с резервными копиями конфигураций сети	266
Создание резервной копии текущей конфигурации	267
Редактирование списка резервных копий	268
Восстановление конфигурации	269
Настройка параметров создания резервных копий	271
Изменение места хранения резервных копий, используемого по умолчанию	273
Работа с журналом событий	274
Просмотр событий в журнале событий	274
Настройка параметров журнала событий	274
Проверка текущих данных	278
Проверка текущих данных вручную	281
Учет ключей ДСДР	282
Приложение А. Возможные неполадки	286
Не удается войти в программу ViPNet Удостоверяющий и ключевой центр	286
Не удается посмотреть пароль, сохраненный в файле	287
Не удается выполнить обновление списка аннулированных сертификатов	288
Приложение В. История версий	290
Что нового в версии 4.6.9 R3	290
Что нового в версии 4.6.10	291
Что нового в версии 4.6.9 R2	291
Что нового в версии 4.6.9 R1	291
Что нового в версии 4.6.7	293
Что нового в версии 4.6.6	294
Что нового в версии 4.6.5	294

Что нового в версии 4.6.4.....	295
Что нового в версии 4.6.3.....	300
Что нового в версии 4.6.2.....	303
Что нового в версии 4.5	309
Что нового в версии 4.4	312
Что нового в версии 4.3	318
Что нового в версии 4.2	321
Что нового в версии 4.1	327
Что нового в версии 4.0	328
Приложение С. Внешние устройства	331
Общие сведения	331
Список поддерживаемых внешних устройств.....	332
Алгоритмы и функции, поддерживаемые внешними устройствами	335
Приложение D. Получение CRL из локальных точек распространения	337
Подготовка файла crl-update-settings.ini.....	340
Пример составления файла crl-update-settings.ini	342
Приложение E. Региональные настройки	343
Региональные настройки в Windows	344
Приложение F. Перечень событий УКЦ, регистрируемых в журнале событий Windows	348
Приложение G. Основы криптографии.....	353
Симметричное шифрование	354
Асимметричное шифрование.....	356
Сочетание симметричного и асимметричного шифрования.....	357
Сочетание хэш-функции и асимметричного алгоритма электронной подписи	359
Приложение H. Термины и сокращения	361
Приложение I. Изменения в документации.....	372



Введение

О документе	11
О программе	12
Что нового в версии 4.6.11	13
Системные требования	14
Комплект поставки	15
Обратная связь	16

О документе

Настоящий документ является подробным руководством по настройке и использованию программы ViPNet[®] Удостоверяющий и ключевой центр (далее — УКЦ). При его изучении рекомендуется дополнительно ознакомиться с остальной документацией из комплекта поставки (см. [Комплект поставки](#)). Это позволит получить общее представление об основных понятиях и структуре сети ViPNet и составить более полную картину взаимодействия УКЦ с программой [ViPNet Центр управления сетью \(ЦУС\)](#).

Для кого предназначен документ

Данное руководство предназначено для администраторов сетей ViPNet[®], отвечающих за организацию работы программы ViPNet Удостоверяющий и ключевой центр — [администраторов УКЦ](#).

Предполагается, что читатель данного руководства предварительно прошел курс обучения в [учебном центре ИнфоТеКС](#), знаком с технологией ViPNet и имеет представление о базовых понятиях в области криптографии (см. [Основы криптографии](#)), а также об [инфраструктуре открытых ключей PKI](#).

Соглашения документа

Обозначение	Описание
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская ее, нажмите вторую
Меню > Команда	Последовательность элементов или действий
Код	Имя файла, путь, фрагмент кода или команда в командной строке



Примечание. В документе могут присутствовать снимки интерфейса из предыдущих версий продукта. Поэтому некоторые элементы интерфейса, которые не влияют на понимание текста, могут выглядеть не так, как в продукте.

О программе

Программа ViPNet Удостоверяющий и ключевой центр (далее — УКЦ) является составной частью программного обеспечения ViPNet Administrator[®], которое используется для администрирования сетей ViPNet.

Программа ViPNet Удостоверяющий и ключевой центр предназначена для управления ключевой структурой сети ViPNet, а также для выполнения функций удостоверяющего центра — издания и обслуживания [сертификатов ключа проверки электронной подписи](#).

Что нового в версии 4.6.11

- Поддержка ViPNet CSP 4.4.8
- Поддержка Windows 11 и Windows Server 2022

Системные требования

Требования к компьютеру для установки программы ViPNet Удостоверяющий и ключевой центр:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Оперативная память — не менее 1 Гбайт (при использовании 64-разрядных версий ОС Microsoft Windows — не менее 2 Гбайт).
- Свободное место на жестком диске — не менее 20 Гбайт.
- Операционная система — Windows Server 2012 R2 (64-разрядная), Windows 10 (32/64-разрядная), Windows Server 2016, Windows Server 2019, Windows 11, Windows Server 2022.

Для операционной системы должен быть установлен самый последний пакет обновлений.

Дополнительные требования:

- Для возможности сохранения паролей пользователей в файлы на компьютере должен быть установлен виртуальный принтер Microsoft XPS Document Writer. Данный принтер по умолчанию присутствует в операционной системе Windows 10 (32/64-разрядная). Если используется операционная система Windows Server 2012 R2 SP1 или Windows Server 2016, виртуальный принтер следует устанавливать вручную (см. [Не удается посмотреть пароль, сохраненный в файле](#)).
- При печати паролей пользователей ViPNet на ПИН-конвертах рекомендуется использовать:
 - Специализированные принтеры для печати ПИН-конвертов или аналогичные матричные принтеры модели OKI ML5100FB.
 - Стандартные четырехслойные ПИН-конверты с расширенным полем для секретной информации.

Комплект поставки

Программа ViPNet Удостоверяющий и ключевой центр поставляется в составе программного обеспечения ViPNet Administrator совместно с программой ViPNet Центр управления сетью.

В комплект поставки программного обеспечения ViPNet Administrator входит:

- Установочный файл серверного приложения ViPNet Центр управления сетью.
- Установочный файл клиентского приложения ViPNet Центр управления сетью.
- Приложения сторонних производителей, необходимые для работы компонентов программы ViPNet Центр управления сетью.
- Установочный файл программы ViPNet Удостоверяющий и ключевой центр.
- Документация в формате PDF:
 - «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».

Обратная связь

Контактная информация

- Единый многоканальный телефон:
+7 (495) 737-6192,
8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба поддержки: hotline@infotecs.ru.
Форма для обращения в службу поддержки через сайт.
Телеграм-канал поддержки: t.me/vhd21
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

- [О продуктах ViPNet.](#)
- [О решениях ViPNet.](#)
- [Часто задаваемые вопросы.](#)
- [Форум пользователей продуктов ViPNet.](#)

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов компании ИнфоТеКС регулируется [политикой ответственного разглашения](#).

1

Общие сведения

Назначение программы ViPNet Удостоверяющий и ключевой центр	18
Лицензионные ограничения	20
Взаимодействие с программой ViPNet Центр управления сетью	25
Взаимодействие с программой ViPNet Registration Point	27
Взаимодействие с программой ViPNet Publication Service	28
Совместимость с программным обеспечением ViPNet	29

Назначение программы ViPNet Удостоверяющий и ключевой центр

Программу ViPNet Удостоверяющий и ключевой центр условно можно разделить на два компонента: ключевой центр и удостоверяющий центр. Схематично данное деление представлено на рисунке ниже.



Рисунок 1. Условное деление УКЦ на компоненты

При работе УКЦ в роли ключевого центра осуществляется:

- Формирование **мастер-ключей**, в том числе **межсетевых мастер-ключей**, необходимых для установления взаимодействия с доверенными сетями.
- Создание ключей для объектов сети ViPNet на основе данных, поступающих из программы ViPNet Центр управления сетью. Данные ключи используются программным обеспечением ViPNet для организации безопасного обмена конфиденциальной информацией.

При работе УКЦ в роли удостоверяющего центра осуществляется:

- Издание сертификатов ключа проверки электронной подписи по запросам, поступающим от пользователей сети ViPNet либо из центров регистрации (узлов с программным обеспечением **ViPNet Registration Point**).



Примечание. Издание сертификатов может осуществляться на базе алгоритма стандарта ГОСТ Р 34.10-2012. С описанием алгоритма можно ознакомиться в [RFC 7836](#).

При необходимости сертификаты подписи могут быть изданы в формате **квалифицированных**.

- Аннулирование выпущенных сертификатов, приостановление и возобновление их действия.
- Формирование [сертификата администратора](#), [списков аннулированных сертификатов](#) и их распространение в своей и доверенных сетях.
- Создание запросов на проведение кросс-сертификации с другими удостоверяющими центрами либо издание кросс-сертификатов (см. [Издание кросс-сертификата по запросу](#)).
- Импорт корневых сертификатов и CRL из доверенных сетей ViPNet и других удостоверяющих центров.
- Другие стандартные операции, связанные с работой удостоверяющего центра.

Криптографические функции выполняются программой ViPNet CSP, которая устанавливается автоматически вместе с УКЦ. Программа ViPNet CSP позволяет создавать ключи электронной подписи, формировать и проверять электронную подпись. Подробнее о функциях программы ViPNet CSP см. в документе «ViPNet CSP. Руководство пользователя».

Лицензионные ограничения

Работа программы ViPNet Удостоверяющий и ключевой центр (так же как и программы ViPNet Центр управления сетью) регулируется лицензией, информация о которой содержится в файле *.itcslic или infotecs.reg. Файл с лицензией указывается администратором при запуске ЦУСа (см. документ «ViPNet Administrator. Руководство по установке») и становится доступен для УКЦ при его подключении к SQL-серверу при первичной инициализации.

Лицензией может быть ограничена функциональность программы ViPNet Удостоверяющий и ключевой центр как удостоверяющего центра. Лицензия регулирует количество сертификатов, которые могут быть изданы в УКЦ для [пользователей сети ViPNet](#) и [внешних пользователей](#). Она может допускать издание ограниченного или неограниченного количества сертификатов, либо не разрешать издание сертификатов. Функциональность УКЦ как ключевого центра лицензией не ограничивается.

Если лицензия на издание сертификатов ограничена, и в процессе работы с программой количество изданных сертификатов станет равным максимальному, издание нового сертификата будет невозможно, о чем будет указано в специальном сообщении.

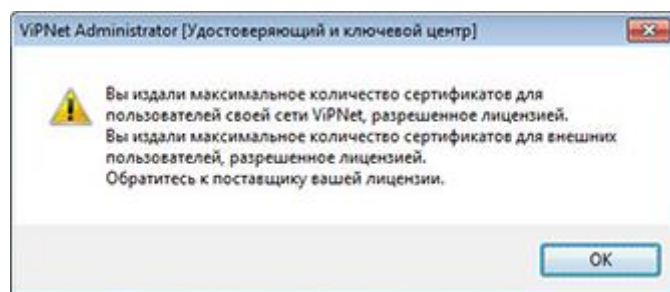


Рисунок 2. Сообщение об издании максимального числа сертификатов, разрешенного лицензией

Указанное сообщение может появляться заранее, а не при достижении максимального количества изданных сертификатов, если выполнена соответствующая настройка (см. [Настройка оповещения о достижении лицензионного ограничения](#)). Данное сообщение также будет появляться каждый раз при запуске программы и проверке текущих данных. В этом случае чтобы продолжить издание сертификатов, потребуется расширение лицензии — увеличение максимально допустимого количества издаваемых сертификатов.

Если в лицензии издание сертификатов запрещено, УКЦ будет выполнять только функции ключевого центра.

Чтобы узнать содержание предоставленной лицензии, следуйте указаниям раздела [Просмотр лицензионного ограничения](#). Для расширения лицензии обратитесь к представителю компании ИнфоТеКС и закажите новую лицензию, дополнительно сообщив ему номер вашей сети ViPNet и желаемые параметры новой лицензии. Чтобы узнать номер сети, в УКЦ в меню **Справка** выберите пункт **О программе**. После обработки запроса на расширение лицензии вы получите новый файл *.itcslic или infotecs.reg.

Ввод в действие полученной лицензии осуществляется в программе ViPNet Центр управления сетью (см. документ «ViPNet Центр управления сетью. Руководство администратора»). После ввода в действие новой лицензии в ЦУСе в УКЦ будет использоваться расширенная лицензия.

Отсутствие лицензии на выполнение функций удостоверяющего центра

При отсутствии в программе ViPNet Удостоверяющий и ключевой центр лицензии на выполнение функций удостоверяющего центра:

- В интерфейсе программы скрыто представление **Удостоверяющий центр** и другие элементы интерфейса, служащие для выполнения функций удостоверяющего центра.

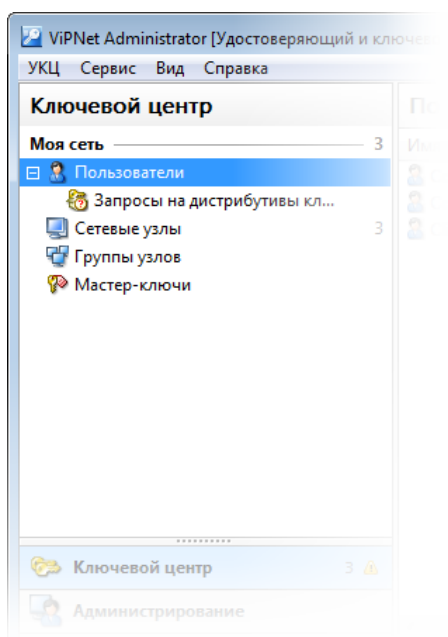


Рисунок 3. Интерфейс программы ViPNet Удостоверяющий и ключевой центр при отсутствии функциональности удостоверяющего центра

- Не издается корневой сертификат администратора.
- Не производится загрузка сертификатов и проверка ключей подписи в ходе запуска программы.
- Не производятся проверки статуса списков аннулированных сертификатов (CRL) и сертификатов администраторов, в связи с чем не отображаются соответствующие оповещения.
- Справочники сертификатов администраторов и CRL игнорируются при импорте межсетевой информации.
- Ключи узлов не содержат справочники сертификатов администраторов и CRL.
- Не производится отправка CRL на узлы сети.

- Для пользователей не создаются ключ электронной подписи и ключ проверки электронной подписи (см. [Настройка создания ключа электронной подписи и ключа проверки электронной подписи для пользователей сети ViPNet](#)) и не издаются сертификаты ключа проверки электронной подписи.

Чтобы добавить функциональность удостоверяющего центра в программу ViPNet Удостоверяющий и ключевой центр, обратитесь в ИнфоТеКС и расширьте вашу лицензию (см. [Расширение лицензии для работы программы в роли удостоверяющего центра](#)).

Расширение лицензии для работы программы в роли удостоверяющего центра

Если у вас отсутствует лицензия на работу программы в роли удостоверяющего центра, эту функциональность можно добавить, расширив лицензию. Для этого выполните следующие действия:

- 1 Обратитесь в ИнфоТеКС и получите новый файл лицензии *.itcslic или infotecs.reg (см. [Лицензионные ограничения](#)).
- 2 Введите в действие полученную лицензию в программе ViPNet Центр управления сетью (см. документ «ViPNet Центр управления сетью. Руководство администратора»).
- 3 Перезапустите программу ViPNet Удостоверяющий и ключевой центр.



Примечание. Если при вводе в действие новой лицензии программа ViPNet Удостоверяющий и ключевой центр запущена, на панели уведомлений появится всплывающая подсказка о том, что программу необходимо перезапустить.

- 4 При запуске программы появится окно мастера создания сертификата администратора сети ViPNet. Следуя инструкциям мастера, издайте корневой сертификат администратора (см. [Издание сертификата администратора](#)).

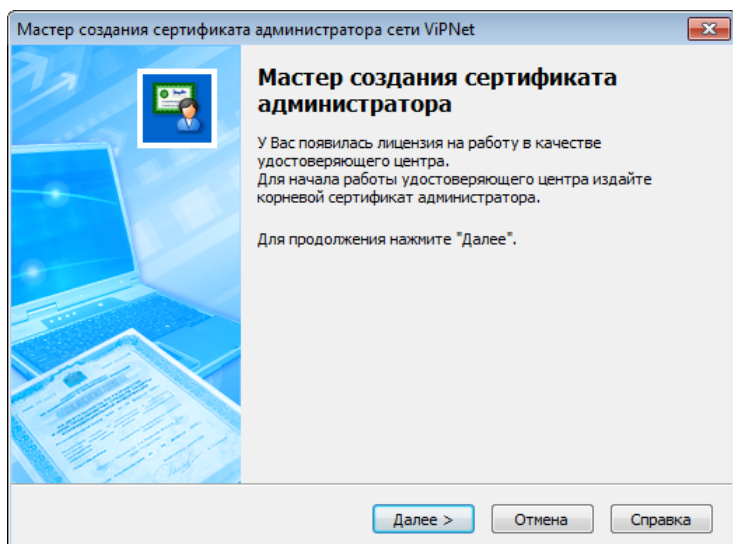


Рисунок 4. Первый запуск ViPNet Удостоверяющий и ключевой центр после расширения лицензии для работы в роли удостоверяющего центра

После издания сертификата администратора в главном окне программы ViPNet Удостоверяющий и ключевой центра появится представление **Удостоверяющий центр** и другие элементы интерфейса, необходимые для выполнения функций удостоверяющего центра.

Просмотр лицензионного ограничения

Чтобы ознакомиться с лицензией на работу программы ViPNet Удостоверяющий и ключевой центр в роли удостоверяющего центра:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Лицензионное ограничение**.

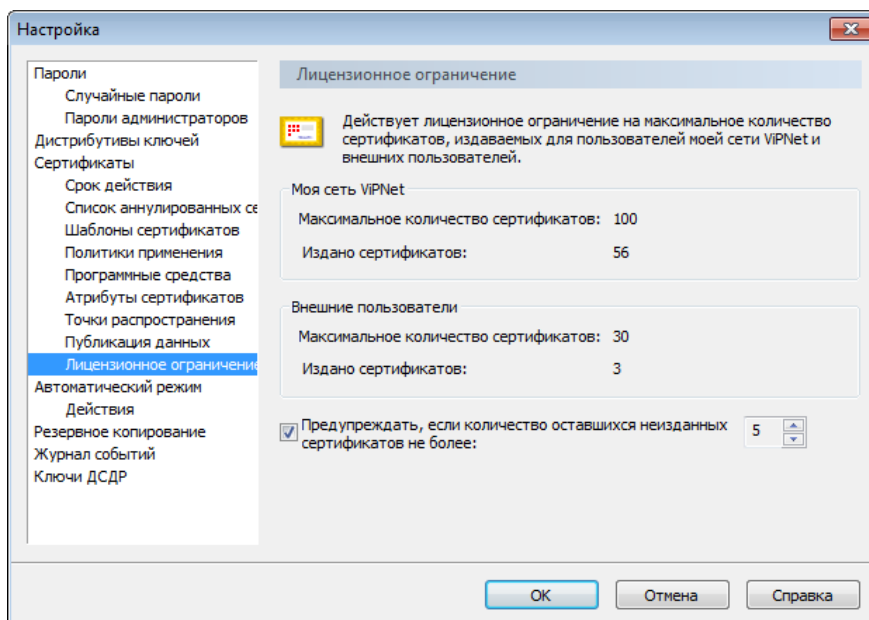


Рисунок 5. Просмотр лицензии

3 В разделе **Лицензионное ограничение** просмотрите следующие сведения:

- В группе **Моя сеть ViPNet**:
 - максимальное количество сертификатов, которые лицензия позволяет издать в программе для пользователей сети ViPNet;
 - количество уже изданных сертификатов.
- В группе **Внешние пользователи**:
 - максимальное количество сертификатов, которые лицензия позволяет издать в программе для внешних пользователей ViPNet по запросам из центров регистрации (узлов с программным обеспечением ViPNet Registration Point);
 - количество уже изданных сертификатов для данной категории пользователей.

Настройка оповещения о достижении лицензионного ограничения

Чтобы сообщение о достижении максимального количества издаваемых сертификатов, разрешенного лицензией, появлялось заранее, в настройках программы в разделе **Лицензионное ограничение** установите флажок **Предупреждать, если количество оставшихся неизданных сертификатов не более:** и в поле справа введите количество оставшихся неизданных сертификатов, при достижении которого пользователю будет выдаваться сообщение. По умолчанию флажок установлен, сообщение будет появляться, когда останется 5 неизданных сертификатов.

Взаимодействие с программой ViPNet Центр управления сетью

Программа ViPNet Центр управления сетью (далее — ЦУС) предназначена для формирования структуры сети ViPNet, задания основных параметров сетевых узлов и пользователей, а также для централизованной отправки ключей, справочников и программного обеспечения на узлы развернутой сети.

Данные о структуре и объектах сети ViPNet, формируемые в ЦУСе, используются в программе ViPNet Удостоверяющий и ключевой центр для создания ключей. Созданные ключи впоследствии передаются через ЦУС на сетевые узлы. Кроме этого, через ЦУС также производится обмен запросами на сертификаты и изданными сертификатами между Удостоверяющим и ключевым центром, пользователями сети ViPNet и центрами регистрации (см. [Взаимодействие с программой ViPNet Registration Point](#)).

ЦУС обменивается данными с программой ViPNet Удостоверяющий и ключевой центр через единую базу данных SQL. Таким образом, если программа ViPNet Удостоверяющий и ключевой центр установлена отдельно от программы ViPNet Центр управления сетью (а точнее, от его серверного приложения), необходимо обеспечить сетевое соединение между компьютерами, на которых установлены эти программы. Подробнее см. раздел [Установка и первичная инициализация программы ViPNet Удостоверяющий и ключевой центр](#).



Рисунок 6. Взаимодействие компонентов ПО ViPNet Administrator

Когда администратор ЦУСа вносит в структуру сети какие-либо изменения, формирует справочники или обрабатывает межсетевую информацию, в программе ViPNet Удостоверяющий и ключевой центр блокируются действия по созданию ключей, операции с мастер-ключами и сертификатами администраторов. И наоборот, если администратор Удостоверяющего и ключевого центра формирует ключи для объектов сети, производит смену мастер-ключей или сертификата администратора, в ЦУСе блокируются все операции по добавлению новых объектов в структуру сети и изменению свойств существующих объектов.

Если в ЦУСе создается новая структура сети или конвертируется старая структура, в программе ViPNet Удостоверяющий и ключевой центр блокируются все операции. При этом по завершении работы со структурой сети Удостоверяющий и ключевой центр требуется перезапустить и заново произвести первичную инициализацию, поскольку вместе со структурой сети удаляется текущая

ключевая структура. В Центре управления сетью также могут быть заблокированы все операции — при создании или восстановлении в программе ViPNet Удостоверяющий и ключевой центр резервной копии конфигурации.

Данные блокировки необходимы для того, чтобы не происходила рассинхронизация данных в используемой базе. Информация о блокировке операций отображается в соответствующих сообщениях и в строке состояния главного окна программы.

Взаимодействие с программой ViPNet Registration Point

Программа ViPNet Registration Point предназначена для выполнения функций центра регистрации пользователей. Администратор программы ViPNet Registration Point имеет возможность зарегистрировать нового пользователя и создать для пользователя запрос на получение сертификата электронной подписи или дистрибутива ключей ViPNet. Впоследствии администратор центра регистрации также может сформировать запрос на аннулирование, приостановление или возобновление действия сертификата.

Сформированные запросы из ViPNet Registration Point передаются на обработку в программу ViPNet Удостоверяющий и ключевой центр с помощью [транспортного модуля ViPNet MFTP](#). Необходимая информация из запросов автоматически записывается в базу данных, после чего эти запросы передаются в программу ViPNet Удостоверяющий и ключевой центр. Администратор УКЦ может удовлетворить либо отклонить полученные запросы.

В ЦУСе запросы автоматически регистрируются, на основе запросов на дистрибутивы ключей в базе данных регистрируются пользователи. После этого запросы перенаправляются в УКЦ. Администратор УКЦ удовлетворяет или отклоняет поступившие запросы.

Процесс взаимодействия УКЦ с программой ViPNet Registration Point представлен на схеме ниже на примере обработки запроса на дистрибутив ключей.

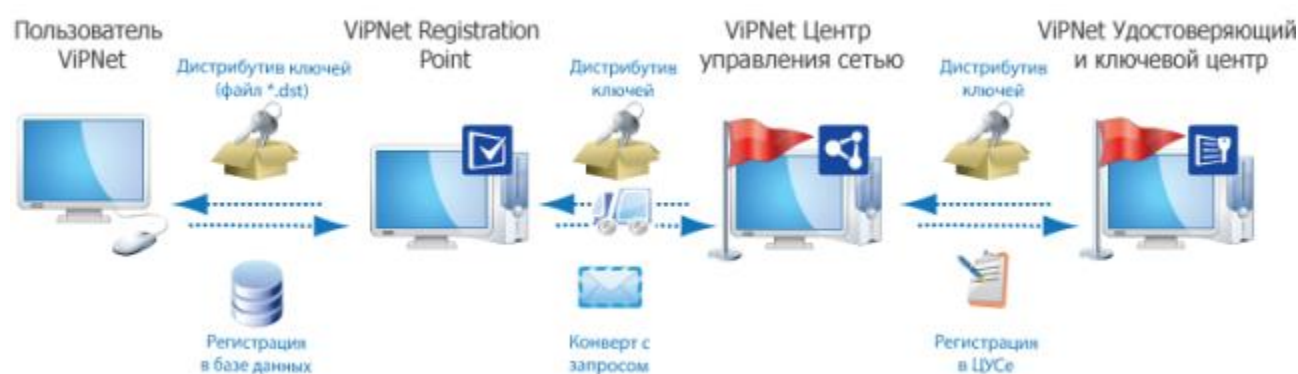


Рисунок 7. Взаимодействие с программой ViPNet Registration Point

Взаимодействие с программой ViPNet Publication Service

Программа [ViPNet Publication Service](#) предназначена для публикации сертификатов пользователей, администраторов УКЦ, кросс-сертификатов и списков аннулированных сертификатов (CRL), которые издаются в программе ViPNet Удостоверяющий и ключевой центр, в общедоступных хранилищах данных (AD, FTP-сервер) или в различных [точках распространения](#) с целью обеспечения доступа к ним пользователей инфраструктуры открытого ключа (PKI). Обычно это требуется в том случае, если сеть ViPNet используется для электронного документооборота.



Примечание. В точках распространения могут размещаться только CRL и сертификаты издателей.

Взаимодействие всех компонентов, участвующих в процессе публикации, представлено на схеме ниже.



Рисунок 8. Схема взаимодействия узлов, участвующих в документообороте

Также программа ViPNet Publication Service может производить автоматический опрос точек распространения сторонних удостоверяющих центров и скачивание сертификатов издателей и CRL из доверенных сетей, если требуется постоянная актуализация их сертификатов издателей и CRL на узлах вашей сети.

Подробную информацию о взаимодействии с сервисом публикации и настройке параметров публикации данных см. в разделе [Публикация сертификатов и списков аннулированных сертификатов](#).

Совместимость с программным обеспечением ViPNet

Если версии программы ViPNet Удостоверяющий и ключевой центр и ПО ViPNet на сетевых узлах, используемые в вашей сети, различаются, следует учитывать следующие особенности:

- Программы ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр разных версий несовместимы друг с другом.
- Программа ViPNet Удостоверяющий и ключевой центр версии 4.x может быть несовместима с программами ViPNet Registration Point и ViPNet Publication Service версий ниже 4.x.
- Первый дистрибутив ключей, созданный в УКЦ версии 4.2.x или выше, невозможно установить на сетевые узлы с ПО ViPNet Client или ViPNet CryptoService версий ниже 3.2.9. На сетевые узлы с ПО ViPNet Client или ViPNet CryptoService версий 3.2.9 и выше установить первый дистрибутив ключей, созданный в УКЦ версии 4.2.x или выше, можно только дважды щелкнув файл дистрибутива ключей.
- На сетевых узлах с ПО ViPNet Client для Windows версии 3.2.x не поддерживается аутентификация по персональному ключу, сохраненному на внешних устройствах семейства eToken Aladdin. Поэтому при задании для пользователей таких узлов способа аутентификации **Устройство (персональный ключ)** следует сохранять персональный ключ на устройствах другого типа либо следует задавать другой способ аутентификации.
- Если на сетевых узлах с ПО ViPNet Client для Windows версии 3.1.x или 3.2.x, а также на узлах с ПО ViPNet CryptoService версии 3.1.x или 3.2.x. установлены ключи, созданные в УКЦ версии 3.2.x, то на них будут корректно приняты обновления ключей, созданные в УКЦ версии 4.2.x или выше.
- Ключи, созданные в УКЦ версии 4.2.x или выше, можно установить на координаторах с версией ПО ViPNet Coordinator Linux 3.7.x и на программно-аппаратных комплексах ViPNet Coordinator HW версии 3.2 или выше.
- В случае компрометации ключей пользователя, а также при смене мастер-ключа персональных ключей невозможно обновить справочники и ключи путем удаленной отправки ключей из ЦУСа на сетевых узлах с ПО ViPNet Terminal (панель — ViPNet ThinClient), ПАК ViPNet Coordinator HW, ViPNet Client for Android и ViPNet Client for iOS в случаях, перечисленных в разделе [Смена мастер-ключей защиты и обмена](#). В этих случаях обновить ключи на сетевом узле можно только путем развертывания нового дистрибутива.

2

Начало работы с программой ViPNet Удостоверяющий и ключевой центр

Установка и первичная инициализация программы ViPNet Удостоверяющий и ключевой центр	31
Запуск и завершение работы программы	33
Интерфейс программы ViPNet Удостоверяющий и ключевой центр	36

Установка и первичная инициализация программы ViPNet Удостоверяющий и ключевой центр

Чтобы развернуть программное обеспечение ViPNet Удостоверяющий и ключевой центр, выполните следующие действия:

1 Перед установкой УКЦ:

- Убедитесь, что вы располагаете установочным файлом программы ViPNet Удостоверяющий и ключевой центр.
- Если вы планируете разместить ЦУС и УКЦ на одном компьютере, убедитесь в том, что на данном компьютере установлено серверное приложение ЦУСа.
- Если вы планируете разместить ЦУС и УКЦ на разных компьютерах, убедитесь в том, что компьютер, на котором вы планируете установить УКЦ, имеет сетевой доступ к базе данных SQL серверного приложения ЦУСа, находящейся на другом компьютере.
- Убедитесь, что пользователь, от имени которого вы установите, проведёте первичную инициализацию и будете работать с УКЦ, обладает правами администратора.

2 Установите программу ViPNet Удостоверяющий и ключевой центр.

Будет запущен мастер первичной инициализации программ, следуйте его указаниям. Подробнее см. в документе «ViPNet Administrator. Руководство по установке», в разделе «Первичная инициализация программы ViPNet Удостоверяющий и ключевой центр».

В результате будет создана учетная запись администратора УКЦ, созданы мастер-ключи (см. [Работа с мастер-ключами](#)). В случае если ваша лицензия разрешает использование функций удостоверяющего центра, также будет издан сертификат проверки электронной подписи администратора УКЦ (см. [Издание сертификата администратора](#)).

3 Если ваш УКЦ выступает в роли подчиненного удостоверяющего центра, получите в вышестоящем удостоверяющем центре сертификат издателя, которым вы сможете подписывать издаваемые сертификаты пользователей (см. [Установление доверительных отношений с вышестоящим или подчиненным удостоверяющим центром](#)).

Если необходимо установить с другим удостоверяющим центром доверительные отношения на основе распределенной модели, следуйте указаниям раздела [Установление доверительных отношений с равнозначным удостоверяющим центром](#).

Подробная информация об установке и первичной инициализации программы ViPNet Удостоверяющий и ключевой центр содержится в документе «ViPNet Administrator. Руководство по установке».

Запуск и завершение работы программы

Чтобы запустить программу ViPNet Удостоверяющий и ключевой центр:

- 1 На начальном экране откройте список приложений и выберите **ViPNet > Удостоверяющий и ключевой центр**.



Примечание. Во время установки положение программы в меню **Пуск** или в списке приложений могло быть изменено.

- 2 Чтобы начать работу с программой, в окне **Вход в Удостоверяющий и ключевой центр** выберите учетную запись администратора, под которой будет производиться вход в программу, и введите **пароль**.



Внимание! Если вы 3 раза ввели неправильный пароль, то дальнейший ввод пароля будет возможен по истечении 40 секунд.

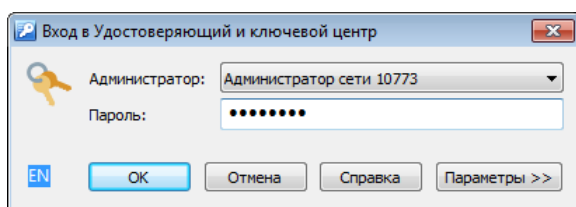


Рисунок 9. Окно входа в программу

- 3 Укажите место хранения **ключей администратора** в том случае, если оно было изменено либо если ключи находятся на внешнем устройстве хранения данных. Для этого в окне входа в программу нажмите кнопку **Параметры** и в скрытой ранее группе **Устройство хранения ключей** установите переключатель в положение:
 - **Папка**, если ключи администратора хранятся в папке на компьютере. После этого с помощью кнопки  укажите путь к нужной папке с ключами.
 - **Устройство**, если ключи администратора хранятся на внешнем устройстве (см. [Внешние устройства](#)). После этого подключите устройство хранения ключей, выберите его в соответствующем списке и введите ПИН-код (если требуется).



Примечание. Необходимость ввода ПИН-кода зависит от типа используемого внешнего устройства. Чтобы сохранить ПИН-код и в дальнейшем не вводить его при аутентификации, в окне входа в УКЦ установите соответствующий флажок.

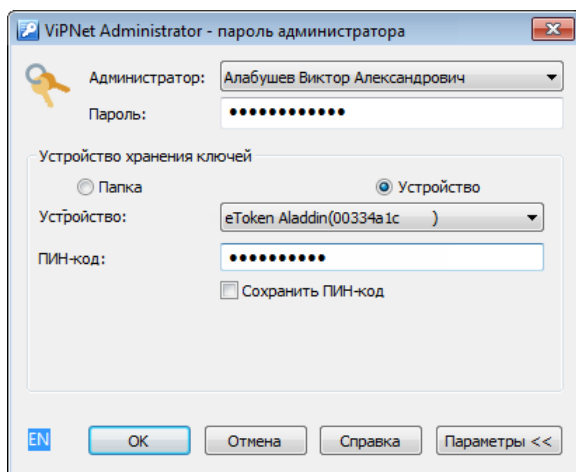


Рисунок 10. Окно входа в программу с указанием места хранения ключей

- 4 После ввода необходимых для аутентификации данных нажмите кнопку **ОК**.

Будет выполнена проверка соединения с SQL-сервером. Если проверка пройдет успешно, произойдет вход в программу под выбранной учетной записью администратора и появится главное окно УКЦ (см. [Интерфейс программы ViPNet Удостоверяющий и ключевой центр](#)). В противном случае появится окно подключения к SQL-серверу. Проверьте правильность параметров, заданных в данном окне, и при необходимости их измените. Подробнее см. раздел [Подключение к SQL-серверу при запуске программы](#).

После появления главного окна программы можно приступить к работе с УКЦ.



Примечание. Если в настройках автоматического режима (см. [Настройка автоматического режима](#)) выбраны операции **Создавать ключи узлов** и **Удовлетворять запросы на дистрибутивы ключей**, появится электронная рулетка. Следуйте указаниям в окне **Электронная рулетка**.

Чтобы свернуть окно программы на панель задач, нажмите кнопку **Свернуть**  в правом верхнем углу окна.

Чтобы завершить работу с программой выполните одно из действий:

- В окне программы в меню **УКЦ** выберите пункт **Выход**.
- Нажмите кнопку **Заккрыть**  в правом верхнем углу окна.

Подключение к SQL-серверу при запуске программы

При каждом запуске УКЦ после ввода пароля администратора производится проверка подключения к [SQL-серверу](#), на котором размещена база данных программы. Первоначально параметры подключения к серверу задаются в процессе первичной инициализации (см. документ

«ViPNet Administrator. Руководство по установке»), но при необходимости они могут быть изменены.

При успешной проверке осуществляется вход в программу, в случае возникновения ошибок в ходе проверки появляется окно подключения к SQL-серверу (см. рисунок ниже).

При возникновении ошибок требуется установить их причину (см. [Не удается войти в программу ViPNet Удостоверяющий и ключевой центр](#)), проверить и, если требуется, изменить параметры в появившемся окне **Подключение к SQL Server**. Чтобы изменить параметры подключения:

- 1 В окне **Подключение к SQL Server** в поле **Сервер** укажите SQL-сервер, на котором была развернута база данных.

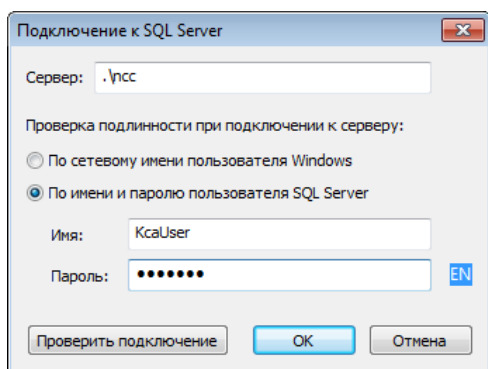


Рисунок 11. Подключение к SQL-серверу

- 2 Выберите тип аутентификации при подключении к SQL-серверу, установив переключатель в нужное положение.

При выборе типа **По имени и паролю пользователя SQL Server** укажите имя пользователя, под учетной записью которого необходимо подключиться к SQL-серверу, и пароль.

По умолчанию заданы имя пользователя `KcaUser` и пароль `Number1`.

- 3 Нажмите кнопку **Проверить подключение**. Если подключение к указанному SQL-серверу было проведено успешно, кнопка **OK** станет активной. В противном случае измените настройки подключения и нажмите кнопку **Проверить подключение** еще раз.
- 4 Нажмите кнопку **OK**.



Внимание! В случае возникновения проблем с подключением к SQL-серверу, не пытайтесь устранить их самостоятельно, обратитесь к администратору используемого SQL-сервера (подробнее см. документ «ViPNet Administrator. Руководство по установке», глава «Установка программного обеспечения ViPNet Administrator», раздел «Информация для администраторов SQL»).

Интерфейс программы ViPNet Удостоверяющий и ключевой центр

Внешний вид окна программы ViPNet Удостоверяющий и ключевой центр представлен на рисунке ниже:

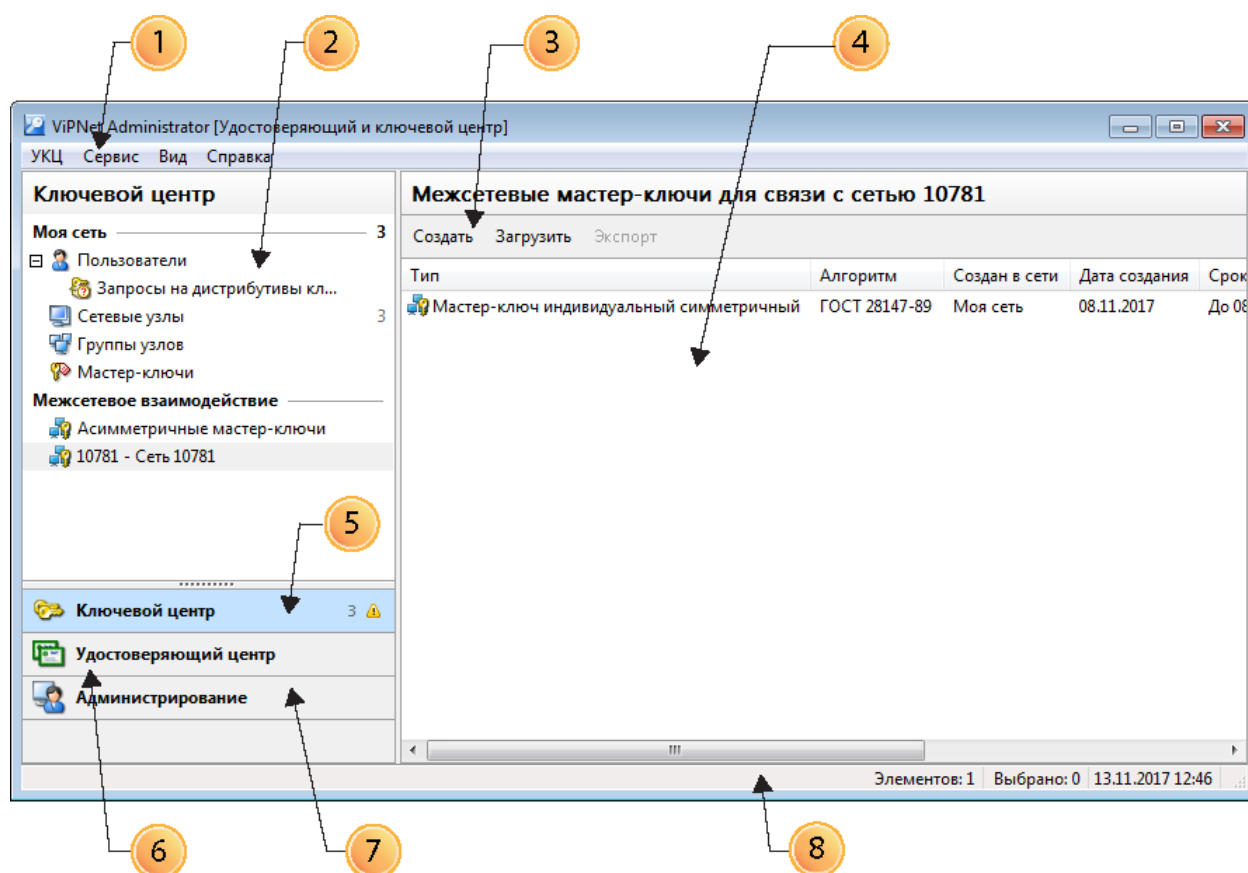


Рисунок 12. Интерфейс программы ViPNet Удостоверяющий и ключевой центр

Цифрами на рисунке обозначены:

- 1 Главное меню программы.
- 2 Панель навигации. Отображает элементы одного из трех выбранных представлений: **Ключевой центр** (5), **Удостоверяющий центр** (6) и **Администрирование** (7). Для перехода в нужное представление выберите его на панели навигации или щелкните в меню **Вид** соответствующий пункт.
- 3 Панель инструментов. Отображается при выборе определенных разделов на панели навигации.
- 4 Панель просмотра. Отображает раздел, выбранный на панели навигации (2).

- 5 Представление  **Ключевой центр**. При выборе представления **Ключевой центр** на панели навигации отображаются объекты вашей сети ViPNet и ключи, созданные для этих объектов, а также информация о межсетевых мастер-ключях, созданных для организации взаимодействия вашей сети с доверенными сетями ViPNet (см. [Представление «Ключевой центр»](#)).
- 6 Представление  **Удостоверяющий центр**. При выборе представления **Удостоверяющий центр** на панели навигации отображаются разделы для управления изданными сертификатами пользователей и различными запросами на сертификаты (см. [Представление «Удостоверяющий центр»](#)).
- 7 Представление  **Администрирование**. При выборе представления **Администрирование** на панели навигации отображаются разделы для управления учетными записями администраторов и получателями списков аннулированных сертификатов (CRL), а также для работы с сертификатами, кросс-сертификатами и CRL (см. [Представление «Администрирование»](#)).
- 8 Строка состояния. Информировать о количестве объектов выбранного раздела, которое содержится в базе данных программы и отображается в текущий момент. Чтобы показать или скрыть строку состояния, в меню **Вид** выберите пункт **Строка состояния**.
- 9 Строка поиска  (на рисунке не обозначено). Отображается в разделах, в которых на панели просмотра содержатся списки пользователей, сетевых узлов, сертификатов, запросов или иных объектов. Для поиска элементов в разделе укажите столбец поиска и сочетание букв для поиска. При поиске по дате укажите интервал времени.



Примечание. Следует учесть, что поиск может производиться только по информации в отображаемых столбцах раздела. То есть, например, для поиска сертификата по ИНН в списке сертификатов должен присутствовать столбец с ИНН для каждого сертификата. В разделе со списками сертификатов поиск сертификатов возможен по множеству столбцов. Все возможные столбцы вы можете просмотреть в окне **Выбор столбцов в таблице** (меню **Вид** > **Выбрать столбцы**).

Если от вас требуется выполнить в программе некоторые важные операции, например, создать ключи для пользователя, обновить CRL или обработать 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.

Вы можете выделить сразу все объекты в рамках одного раздела, для которых требуется выполнить одну и ту же операцию. Для этого перейдите в нужный раздел и в меню **Вид** выберите пункт **Выделить требующие внимания** или нажмите сочетание клавиш **Ctrl+W**.

Представление «Ключевой центр»

Чтобы получить сведения об объектах вашей сети ViPNet и ключах, созданных в процессе работы программы в роли ключевого центра, выберите представление **Ключевой центр**.

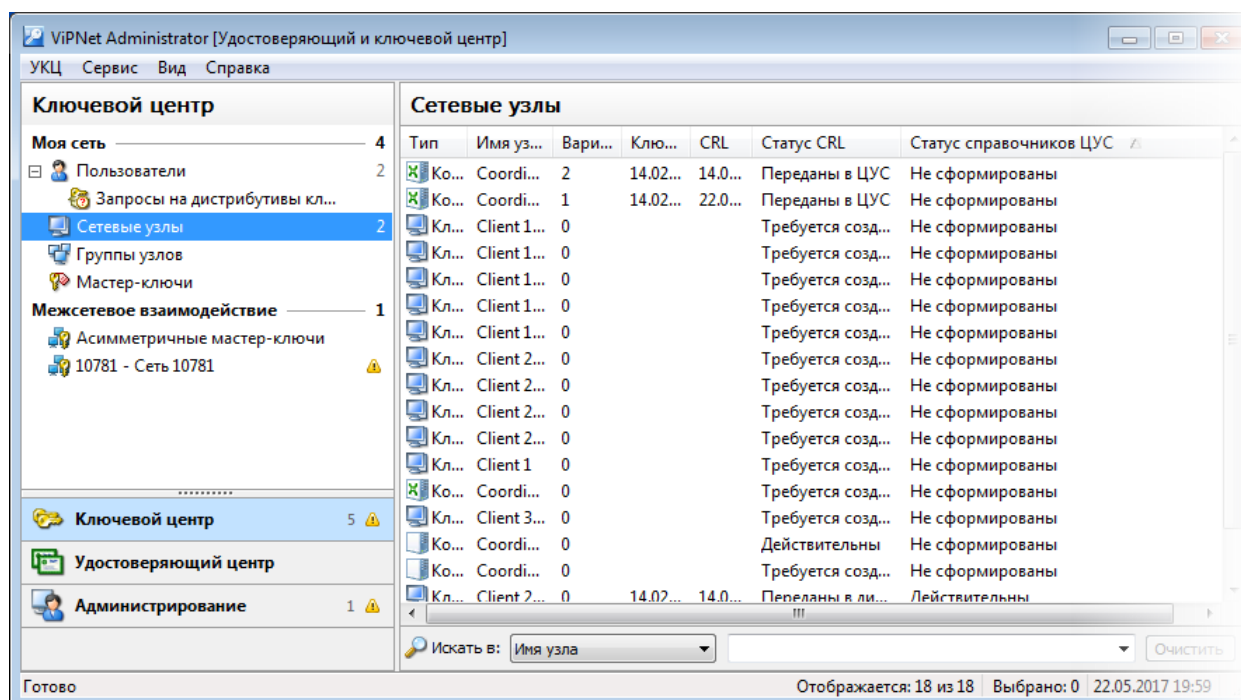


Рисунок 13. Информация об узлах своей сети ViPNet

На панели навигации будут отображены следующие разделы:

- **Моя сеть.** В этом разделе сведения об объектах вашей сети и их ключах распределены по соответствующим вложенным разделам следующим образом:
 - **Пользователи** — содержит список всех пользователей, зарегистрированных в вашей сети ViPNet. Вложенные разделы содержат информацию о резервных наборах персональных ключей, а также поступившие в УКЦ запросы на дистрибутивы ключей.
 - **Сетевые узлы** — содержит список всех сетевых узлов, имеющих в вашей сети ViPNet.
 - **Группы узлов** — содержит список групп узлов, организованных в вашей сети ViPNet.
 - **Мастер-ключи** — содержит мастер-ключи, используемые в вашей сети ViPNet: мастер-ключ персональных ключей, мастер-ключ ключей защиты и мастер-ключ ключей обмена.
- **Межсетевое взаимодействие.** Во вложенном разделе **Асимметричные мастер-ключи** приводятся все созданные в процессе работы УКЦ асимметричные межсетевые мастер-ключи. Если установлено межсетевое взаимодействие с доверенной сетью ViPNet, то во вложенном разделе с номером данной сети содержатся:
 - созданные или импортированные индивидуальные межсетевые мастер-ключи для связи вашей сети с доверенной сетью;
 - импортированные из доверенной сети открытые части асимметричных мастер-ключей.

Представление «Удостоверяющий центр»

Чтобы получить сведения о сертификатах и запросах на сертификаты, созданных или используемых в процессе работы программы в роли удостоверяющего центра, выберите представление **Удостоверяющий центр**.

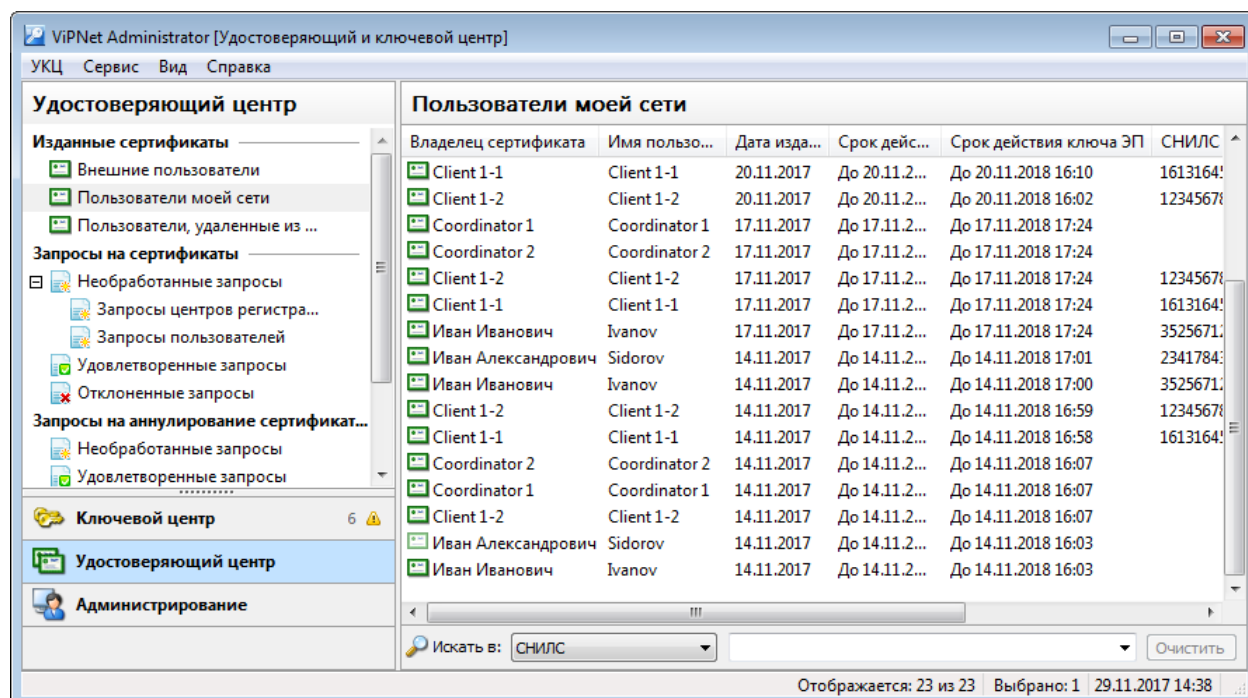


Рисунок 14. Информация об изданных сертификатах пользователей своей сети ViPNet

На панели навигации будут отображены следующие разделы:

- **Изданные сертификаты** — содержит информацию об изданных сертификатах подписи **внешних пользователей** и **пользователей сети ViPNet**, включая тех, которые были удалены из сети ViPNet.



Совет. По умолчанию в подразделах раздела **Изданные сертификаты** отображается не более 100 сертификатов пользователей. О том, как увеличить количество отображаемых сертификатов, см. в разделе [Настройка количества сертификатов, отображаемых в окне программы](#).

- **Запросы на сертификаты** — содержит информацию о запросах на издание сертификатов пользователей, поступивших из центров регистрации и от пользователей вашей сети ViPNet. Обработанные запросы содержатся во вложенных разделах **Удовлетворенные запросы** и **Отклоненные запросы** в соответствии с тем, как они были обработаны — удовлетворены или отклонены.
- **Запросы на аннулирование сертификатов** — содержит информацию о поступивших из центров регистрации запросов на аннулирование, приостановление и возобновление

действия сертификатов пользователей. Обработанные запросы содержатся во вложенных разделах **Удовлетворенные запросы** и **Отклоненные запросы** в соответствии с тем, как они были обработаны — удовлетворены или отклонены.

- **Запросы с ошибками** — содержит информацию о запросах, которые не могут быть обработаны по причине ошибок в них (например, если файл с запросом был поврежден).

Представление «Администрирование»

Для управления учетными записями администраторов и получателями списков аннулированных сертификатов (CRL), а также для работы с сертификатами, кросс-сертификатами и CRL выберите представление **Администрирование**.

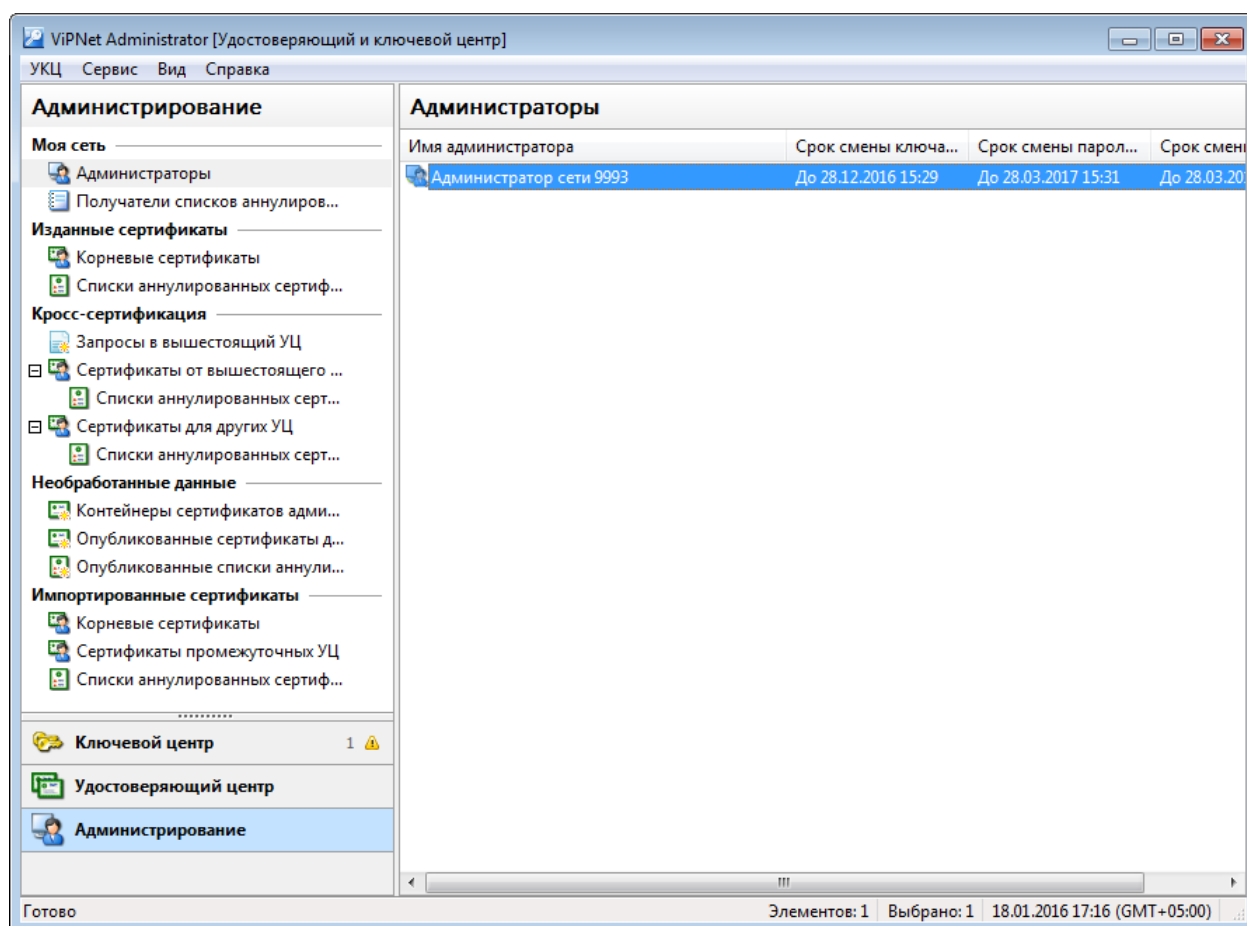


Рисунок 15. Управление учетными записями администраторов

На панели навигации будут отображены следующие разделы:

- **Моя сеть**. Этот раздел содержит два вложенных раздела:
 - **Администраторы** — в этом разделе вы можете просматривать сроки действия ключей электронной подписи администраторов, паролей администраторов, ключа защиты УКЦ, а также удалять учетные записи администраторов программы ViPNet Удостоверяющий и ключевой центр.

- **Получатели списков аннулированных сертификатов** — в этом разделе вы можете формировать список получателей CRL в вашей сети ViPNet.
- **Изданные сертификаты** — содержит информацию об изданных корневых сертификатах администраторов и CRL.
- **Кросс-сертификация** — содержит информацию о сертификатах администраторов, полученных из вышестоящих удостоверяющих центров, запросах на сертификаты к вышестоящему удостоверяющему центру и сертификатах, изданных в УКЦ по запросам из других удостоверяющих центров.
- **Необработанные данные** — содержит информацию о сертификатах администраторов и CRL доверенных сетей, которые не были обработаны (в том числе о контейнерах с сертификатами и CRL).
- **Импортированные сертификаты** — содержит информацию об импортированных сертификатах администраторов и CRL доверенных сетей.

3

Режимы работы в программе ViPNet Удостоверяющий и ключевой центр

Режимы работы УКЦ	43
Работа в автоматическом режиме	45
Настройка автоматического режима	48
Особенности работы в автоматическом режиме	50

Режимы работы УКЦ

Работа в программе ViPNet Удостоверяющий и ключевой центр возможна в двух режимах: ручном и автоматическом.

В ручном режиме администратором выполняются, как правило, такие операции, как издание сертификатов администраторов, работа с кросс-сертификатами и другие, а также операции по работе с дистрибутивами ключей, ключами пользователей, резервными наборами ключей и мастер-ключами.

Автоматический режим работы УКЦ удобно использовать в следующих случаях:

- Во время отсутствия администратора на рабочем месте (например, в ночное время, если программа запущена круглосуточно).
- Для того чтобы освободить администратора от выполнения некоторых операций (если администратор сети работает сразу в двух программах: в ЦУСе и в УКЦ, либо если в УКЦ поступает большое количество запросов на сертификаты, которые требуется обрабатывать одновременно).

В ручном режиме администратором программы также могут выполняться операции автоматического режима. В автоматическом режиме выполняются те операции, которые определены в настройках программы. В окне автоматического режима администратор может только следить за ходом выполнения операций, а также за уведомлениями об операциях, которые потребуется выполнить в ручном режиме работы.

В таблице ниже приведены списки операций, которые могут быть выполнены автоматически и которые могут быть выполнены только вручную.

Таблица 1. Операции, выполняемые в разных режимах работы

Операции, которые могут быть выполнены в автоматическом и ручном режимах	Операции, которые могут быть выполнены только в ручном режиме
• Создание ключей узлов. • Удовлетворение запросов на сертификаты, подписанных пользователями сети ViPNet. • Удовлетворение запросов на сертификаты, подписанных в центрах регистрации. • Удовлетворение запросов на аннулирование сертификатов, подписанных в центрах регистрации. • Удовлетворение запросов на дистрибутивы ключей, подписанные в центрах регистрации. • Загрузка списков аннулированных сертификатов из доверенных сетей ViPNet и их передача на узлы. • Импорт списков аннулированных сертификатов других удостоверяющих центров с помощью программы ViPNet Publication Service. • Обновление списков аннулированных сертификатов и их отправка в доверенные сети ViPNet. • Отправка обновления списка аннулированных сертификатов на все узлы сети ViPNet. • Передача на публикацию списков аннулированных сертификатов с помощью программы ViPNet Publication Service. • Создание резервных копий конфигурации сети ViPNet (см. Настройка параметров создания резервных копий).	• Создание дистрибутивов ключей, ключей пользователей, резервных наборов персональных ключей. • Создание и обновление мастер-ключей (в том числе межсетевых). • Издание сертификатов издателей и кросс-сертификатов. • Создание запросов на кросс-сертификаты. • Передача на публикацию сертификатов издателей и сертификатов пользователей. • Импорт сертификатов издателей, полученных с помощью сервиса публикации из других удостоверяющих центров.

Операции, которые должны выполняться в автоматическом режиме, определяются на усмотрение администратора. Так, например, если в ходе эксплуатации сети ViPNet не используется [инфраструктура PKI](#), но при этом довольно часто меняется структура сети (добавляются новые узлы, изменяются связи), то в автоматическом режиме целесообразно выполнять создание ключей узлов и их передачу пользователям. Остальные операции могут быть не выбраны для выполнения в автоматическом режиме.

Либо, наоборот, если пользователи сети ViPNet в своей работе используют электронную подпись, то постоянно требуется поддерживать списки аннулированных сертификатов (CRL) в актуальном состоянии. В этом случае УКЦ может переводиться в автоматический режим для обновления списков аннулированных сертификатов (см. [Обновление списков аннулированных сертификатов](#)).

Работа в автоматическом режиме

Переход в автоматический режим работы может производиться двумя способами:

- По команде администратора. В этом случае для перехода в автоматический режим в меню **УКЦ** выберите пункт **Перейти в автоматический режим**.

Если для автоматического режима работы выбраны операции **Создавать ключи узлов** и **Удовлетворять запросы на дистрибутивы ключей**, при переходе в автоматический режим работы появится электронная рулетка, если в текущем сеансе работы она не запускалась. Следуйте указаниям в окне **Электронная рулетка**.

- При неактивности администратора, то есть когда в программе не производятся никакие действия в течение заданного в настройках времени (см. [Настройка автоматического режима](#)). В этом случае за 30 секунд до перехода в автоматический режим появится окно с сообщением. Если вы против перехода в автоматический режим, в окне с сообщением нажмите кнопку **Отмена**.

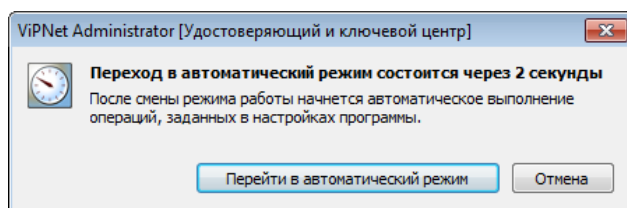


Рисунок 16. Сообщение о переходе в автоматический режим работы



Примечание. Если у вас открыты другие окна программы кроме главного (например, окно настроек), то переход в автоматический режим не будет выполнен даже по истечении заданного времени бездействия.

При переходе в автоматический режим работы появляется окно, в котором вы можете контролировать автоматическое выполнение операций (в окне отображается очередь операций, прогресс выполнения текущей операции и другое), а также следить за списком тех операций, которые требуется выполнить в ручном режиме.

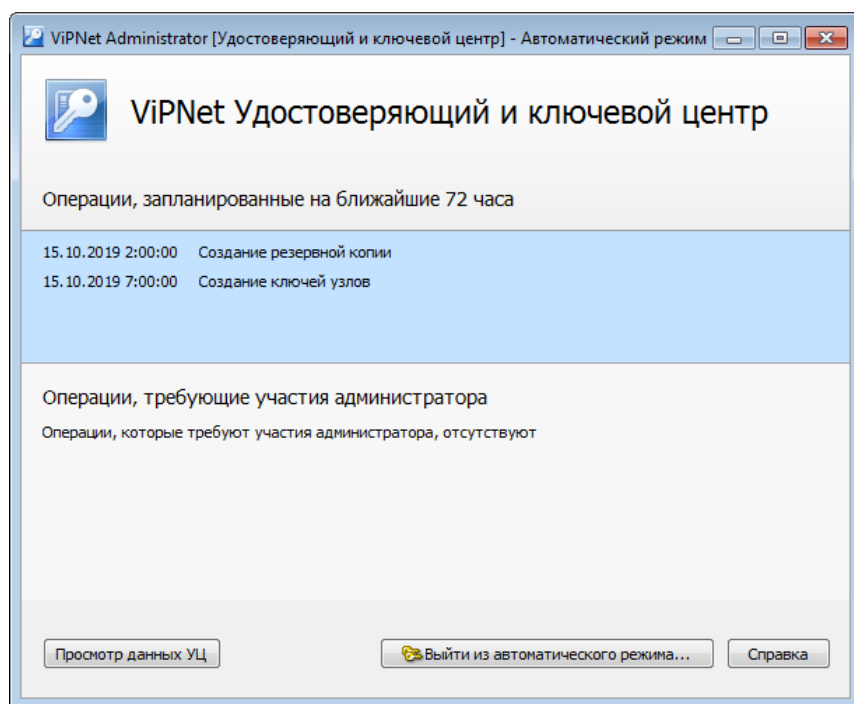


Рисунок 17. Работа программы в автоматическом режиме

При необходимости вы можете перейти из окна автоматического режима в окно просмотра данных удостоверяющего центра (изданных сертификатов и другой информации). Для этого нажмите кнопку **Просмотр данных УЦ**. Данные удостоверяющего центра в появившемся окне доступны только для чтения.



Примечание. Как правило, просмотр данных удостоверяющего центра может вам потребоваться в случае издания сертификатов по запросам в автоматическом режиме, когда нужно проанализировать количество изданных сертификатов или найти нужный сертификат, не переходя в ручной режим работы.

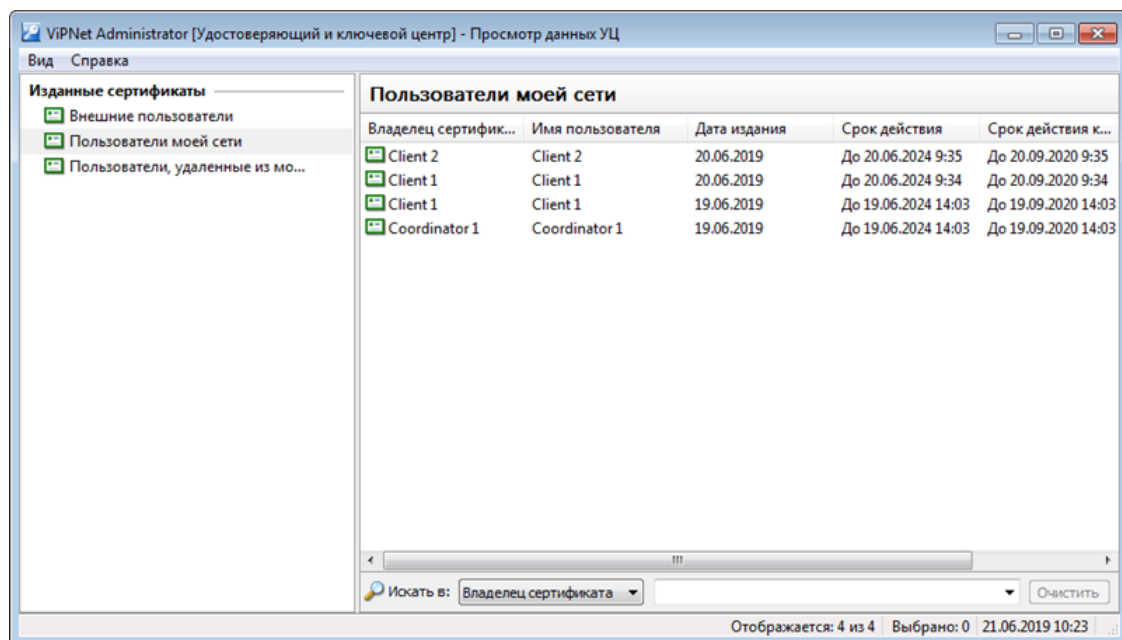


Рисунок 18. Просмотр изданных сертификатов при работе в автоматическом режиме

Чтобы перейти в ручной режим работы, в окне автоматического режима нажмите кнопку **Выйти из автоматического режима**, после чего в появившемся окне введите ваш пароль администратора. При подтверждении введенного пароля появится главное окно программы (см. [Интерфейс программы ViPNet Удостоверяющий и ключевой центр](#)).

Чтобы свернуть окно автоматического режима, выполните одно из действий:

- Нажмите кнопку **Заккрыть**  в правом верхнем углу окна.
- Нажмите сочетание клавиш **Alt+F4**.

Чтобы снова развернуть окно программы, щелкните значок  в области уведомлений на панели задач.

Настройка автоматического режима

Параметры работы УКЦ в автоматическом режиме выбираются в процессе первичной инициализации программы (подробно см. в документе «ViPNet Administrator. Руководство по установке», в главе «Начало работы»). Чтобы изменить эти параметры:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В окне **Настройка** перейдите в раздел **Автоматический режим**.

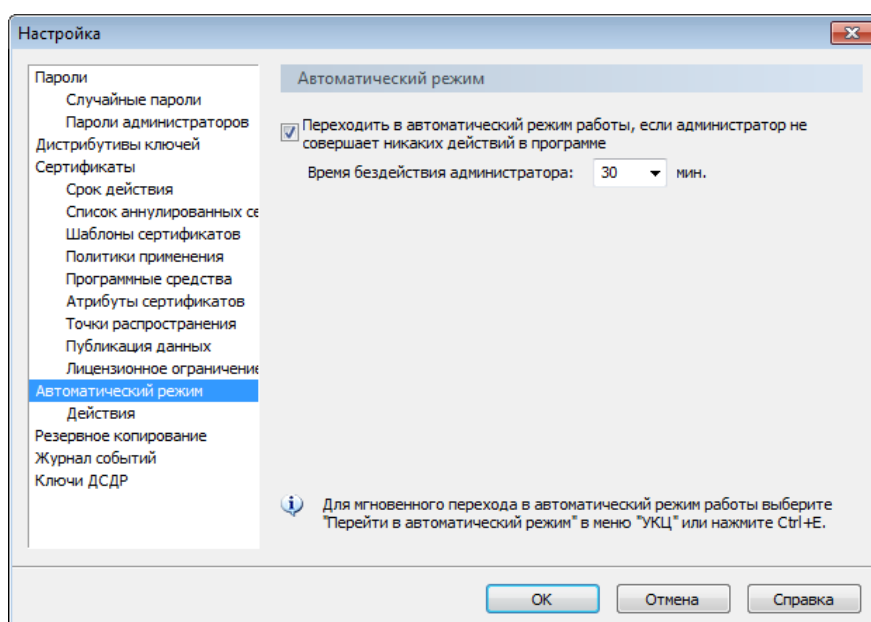


Рисунок 19. Настройка перехода ViPNet Certification Authority в автоматический режим работы

- 3 При необходимости перехода программы в автоматический режим работы, если администратор не совершает никаких действий, установите соответствующий флажок и укажите время неактивности администратора до перехода программы в автоматический режим работы в минутах.
- 4 Чтобы выбрать операции, которые должны выполняться в автоматическом режиме, в окне **Настройка** перейдите в раздел **Автоматический режим** > **Действия**. На панели просмотра отобразится список операций.

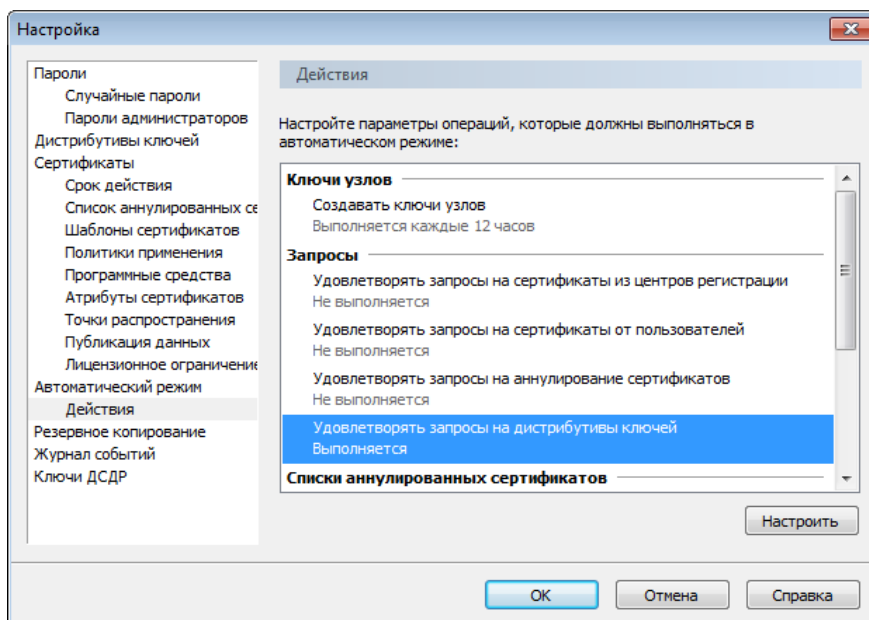


Рисунок 20. Выбор операций, которые должны выполняться в автоматическом режиме



Примечание. Если у вас отсутствует лицензия на работу УКЦ в роли удостоверяющего центра (см. [Общие сведения](#)), для выполнения в автоматическом режиме работы программы вы можете выбрать только операции создания ключей узлов и удовлетворения запросов на дистрибутивы ключей.

Чтобы операция выполнялась в автоматическом режиме работы УКЦ:

- 4.1 На панели просмотра выберите нужную операцию и нажмите кнопку **Настроить**.
- 4.2 В появившемся окне установите флажок и нажмите кнопку **ОК**.

При выборе некоторых операций укажите, когда или с какой периодичностью они должны выполняться. Подробную информацию о таких операциях см. в следующих разделах:

- [Настройка автоматического создания ключей узлов.](#)
- [Настройка автоматического обновления CRL.](#)
- [Настройкой автоматической передачи CRL.](#)

- 5 Для сохранения настроек нажмите кнопку **ОК**.



Примечание. Если для автоматического режима выбраны операции **Создавать ключи узлов** и **Удовлетворять запросы на дистрибутивы ключей** и установлен флажок **Переходить в автоматический режим работы, если администратор не совершает никаких действий в программе**, появится электронная рулетка (если в текущем сеансе работы она не запускалась). Следуйте указаниям в окне **Электронная рулетка**.

Особенности работы в автоматическом режиме

При работе в автоматическом режиме важно помнить о следующих особенностях:

- При переходе в автоматический режим составляется очередь операций, в соответствии с которой данные операции начинают выполняться. В очередь попадают операции, которые указаны в настройках УКЦ как автоматические (см. [Настройка автоматического режима](#)), а также автоматическое создание резервных копий конфигурации сети ViPNet (см. [Настройка параметров создания резервных копий](#)).
- Если операции создания ключей узлов или обновления списков аннулированных сертификатов (CRL) должны выполняться с определенной периодичностью, то при переходе в автоматический режим они попадут в очередь только в том случае, если истек заданный период времени с момента последнего автоматического создания ключей или обновления CRL.
- Ключи узлов при создании в автоматическом режиме сразу передаются в программу ViPNet Центр управления сетью. Поэтому для других операций с ключами узлов их требуется создавать вручную. Все возможные операции с ключами узлов описаны в разделе [Работа с ключами узлов](#).
- Если список аннулированных сертификатов обновляется в автоматическом режиме, то в случае наличия межсетевого взаимодействия с другими сетями ViPNet этот список сразу передается в доверенные сети вместе с корневым сертификатом администратора (сертификатом издателя).

4

Управление ключевой структурой ViPNet

Ключевая структура ViPNet	52
Работа с дистрибутивами ключей	55
Работа с ключами узлов	65
Работа с ключами пользователей	69
Работа с резервными наборами персональных ключей	77
Действия в случае компрометации ключей	80
Работа с мастер-ключами	88

Ключевая структура ViPNet

В технологии ViPNet для шифрования применяется комбинация криптографических алгоритмов с симметричными и асимметричными ключами.

Таблица 2. Применение криптографических алгоритмов в ПО ViPNet

Криптографические алгоритмы	
С симметричными ключами	С асимметричными ключами
• шифрование IP-трафика • шифрование сообщений программы ViPNet Деловая почта • шифрование прикладных и служебных конвертов	• создание и проверка электронной подписи • шифрование в сторонних приложениях с помощью криптопровайдера ViPNet CSP

Симметричные ключи в ПО ViPNet

Симметричные алгоритмы используются для шифрования информации и контроля ее целостности. Для каждой пары сетевых узлов ViPNet в программе ViPNet Удостоверяющий и ключевой центр создается симметричный ключ обмена, предназначенный для шифрования обмена данными между этими сетевыми узлами. Таким образом, формируется матрица симметричных ключей, содержащая данные обо всех созданных для сетевых узлов симметричных ключах обмена. Эта матрица зашифрована ключами защиты, которые в свою очередь зашифрованы персональным ключом пользователя, поэтому доступ к этой матрице имеет только пользователь на сетевом узле. Симметричные ключи обмена следует передавать по защищенным каналам (дистрибутивы для первой установки справочников и ключей передаются лично). Если злоумышленники завладеют симметричными ключами, вся система защиты сетевого узла будет скомпрометирована.

Симметричные ключи обмена используются для шифрования IP-трафика, почтовых сообщений, прикладных и транспортных конвертов.



Рисунок 21. Применение ключей обмена

Для защиты ключей обмена применяется три уровня шифрования:

- ключи обмена зашифрованы на ключах защиты;
- ключи защиты зашифрованы на персональных ключах;
- в свою очередь, персональные ключи зашифрованы на парольных ключах.

Сетевой узел

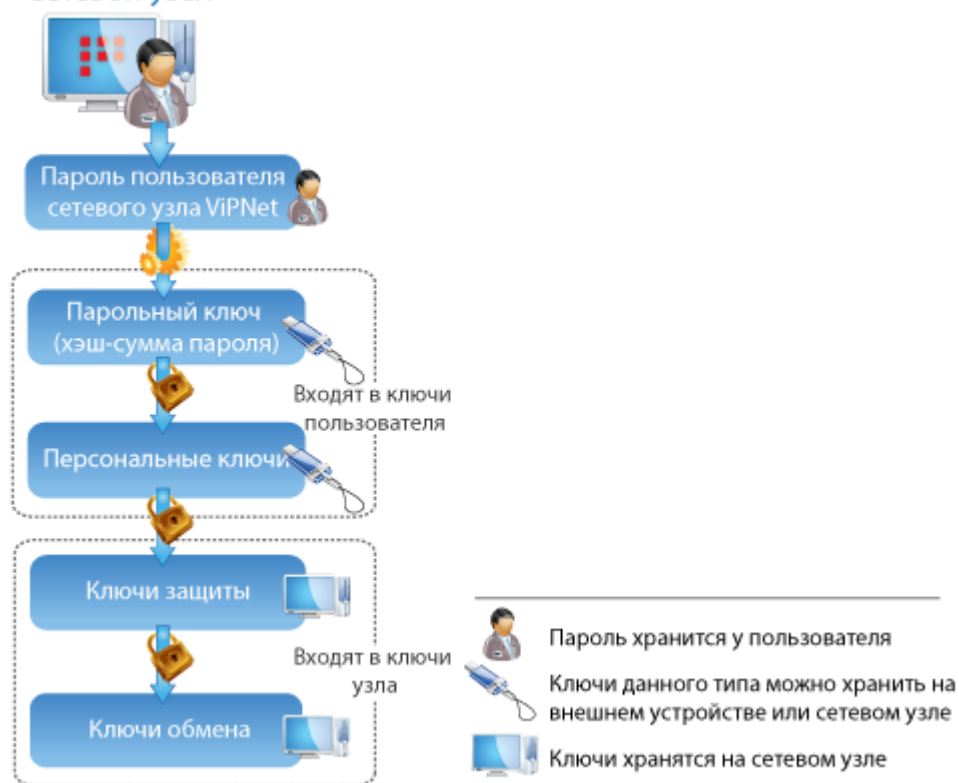


Рисунок 22. Иерархия защиты ключей обмена на сетевом узле

В ПО ViPNet для шифрования используется российский стандарт симметричного шифрования ГОСТ 28147-89 (длина ключа 256 бит).

Асимметричные ключи в ПО ViPNet

При использовании симметричного алгоритма зашифрование и расшифрование выполняются с помощью одного и того же ключа. При использовании асимметричного алгоритма ключ, с помощью которого шифруется сообщение, является открытым (известен всем отправителям), а ключ, с помощью которого это сообщение расшифровывается, является закрытым (известен только получателю зашифрованного сообщения).

Каждый пользователь имеет пару ключей шифрования — открытый ключ и закрытый ключ. Закрытый ключ необходимо держать в тайне, а открытый ключ можно свободно распространять. Между этими ключами существует математическая связь, однако на практике невозможно за конечное время получить закрытый ключ из открытого.

Асимметричные ключи используются в технологии ViPNet для издания сертификатов и создания электронных подписей (см. [Сочетание хэш-функции и асимметричного алгоритма электронной подписи](#)). Если на компьютере установлено ПО ViPNet, в состав которого входит криптопровайдер ViPNet CSP, асимметричные ключи можно использовать для шифрования (см. [Асимметричное шифрование](#)). Одна и та же пара асимметричных ключей может использоваться как для шифрования, так и для подписи. Однако, в отличие от шифрования, для подписи используется закрытый ключ (ключ электронной подписи), а для проверки подписи — сертификат ключа проверки электронной подписи. Сертификат содержит открытый ключ (ключ проверки электронной подписи), удостоверенный (в том числе подписанный) уполномоченным лицом (администратором УКЦ), информацию о владельце сертификата, сроке его действия и прочее.

Пару асимметричных ключей можно независимо создать на сетевом узле ViPNet.

Ключ электронной подписи хранится в зашифрованном виде в файле, который называется контейнером ключей. Его следует хранить в тайне от других пользователей: рекомендуется использовать съемные носители или [внешние устройства](#). Схема защиты ключа электронной подписи в зависимости от места его хранения изображена на следующем рисунке.



Рисунок 23. Схема защиты ключа электронной подписи

Если ключ электронной подписи хранится на внешнем устройстве, [ключом защиты](#) для него является парольный ключ. Если ключ электронной подписи хранится на жестком диске или в дистрибутиве ключей, ключом защиты для него является персональный ключ.

Ключи проверки электронной подписи в сетях ViPNet передаются в составе подписанного сообщения программы ViPNet Деловая почта. Также ключи проверки электронной подписи могут храниться в составе сертификатов в общем хранилище сертификатов, например в службе каталогов Active Directory.

Асимметричное шифрование подразумевает отправку зашифрованного сообщения владельцу выбранного при зашифровании сертификата. Зашифрование сообщений можно выполнять в таких приложениях, как Microsoft Outlook, Outlook Express и так далее. Для этого сертификат получателя должен содержать в соответствующем поле адрес электронной почты.

Следует понимать, что технология асимметричного шифрования основана на стандартном использовании интерфейса Microsoft CryptoAPI. Следовательно, при использовании данной технологии пользователи ViPNet могут быть не связаны между собой в смысле топологии сети ViPNet (их сети могут не являться доверенными). Для расшифрования сообщения получателю достаточно закрытого ключа, сертификата и установленного на компьютере программного обеспечения, в состав которого входит криптопровайдер ViPNet CSP.

Работа с дистрибутивами ключей

Дистрибутив ключей — файл *.dst, который содержит все необходимое для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.



Примечание. Если пользователь зарегистрирован в программе ViPNet Центр управления сетью более чем на одном сетевом узле, то количество создаваемых дистрибутивов ключей определяется количеством сетевых узлов, на которых он зарегистрирован.

Состав дистрибутива ключей представлен на схеме ниже.

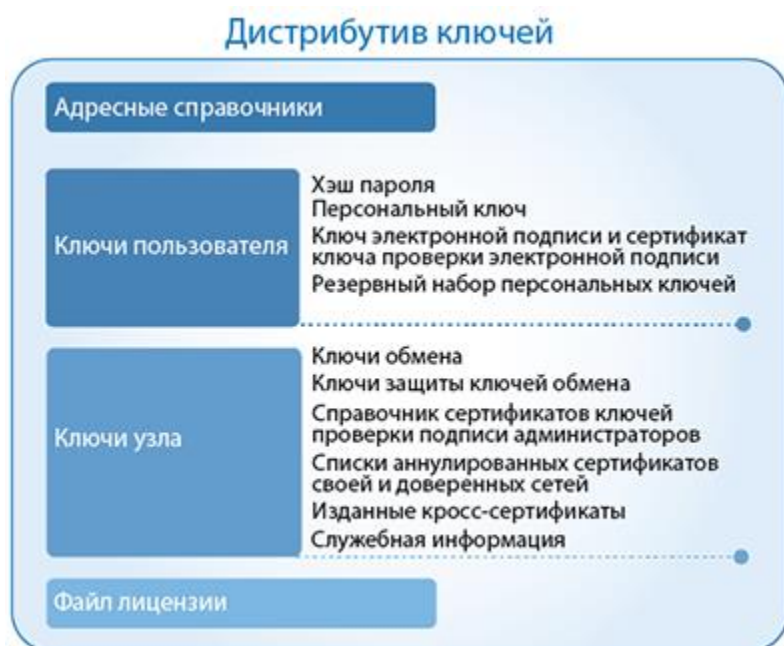


Рисунок 24. Состав дистрибутива ключей

Если версии ПО ViPNet Administrator и ПО ViPNet, установленные на сетевых узлах в вашей сети, различаются, следует учитывать особенности, описанные в разделе [Совместимость с программным обеспечением ViPNet](#).

Когда следует создавать дистрибутивы ключей?

Чаще всего дистрибутив ключей вам требуется создавать при добавлении пользователя в сеть ViPNet (для развертывания узла ViPNet, на котором он зарегистрирован). Но может возникнуть ситуация, при которой вам потребуется сформировать дистрибутив ключей для пользователя повторно, а именно:

- Проблемы при функционировании узла пользователя в сети ViPNet, например, если произошла поломка компьютера и информация, хранившаяся на нем, была повреждена, и восстановить ее невозможно (в том числе справочники и ключи).
- Текущее состояние узла пользователя не позволяет выполнять отправку и прием зашифрованных писем, шифрование трафика, при этом удаленное обновление справочников и ключей по каким-либо причинам не может быть произведено.
- Вариант ключей узла достиг своего максимального числа 255 и не может быть изменен (см. [Изменение вариантов персонального ключа пользователя и ключей узла](#)).
- Изменение варианта персонального ключа пользователя, номер которого равен единице (см. [Изменение вариантов персонального ключа пользователя и ключей узла](#)).
- Смена мастер-ключа персональных ключей, если вариант персонального ключа пользователя равен двум и более (см. [Смена мастер-ключа персональных ключей](#)).

Особенности создания дистрибутивов ключей

При создании дистрибутивов ключей важно помнить о следующих особенностях:

- Каждый дистрибутив ключей создается для работы пользователя на конкретном узле ViPNet, поэтому при создании дистрибутива ключей для конкретного пользователя выбирается пункт контекстного меню сетевого узла, на котором он зарегистрирован.
- Перед созданием дистрибутива ключей убедитесь, что для узла, на котором зарегистрирован пользователь, в программе ViPNet Центр управления сетью созданы актуальные справочники. О том, как создать справочники, см. документ «ViPNet Центр управления сетью. Руководство администратора», главу «Управление сетью ViPNet», раздел «Создание справочников».
- Если на сетевом узле зарегистрировано несколько пользователей, то вы можете выбрать пользователей узла, для которых будет сформирован дистрибутив.
- Если пользователь зарегистрирован на нескольких сетевых узлах, требуется формировать дистрибутив ключей для каждого из этих узлов.
- Если в процессе создания дистрибутива произошла ошибка (например, [межсетевой мастер-ключ](#) не был создан или введен в действие при установке взаимодействия с доверенной сетью ViPNet), то появится соответствующее сообщение с предложением пропустить или отменить создание дистрибутива ключей для данного пользователя. В этом случае вам следует выбрать одно из предложенных действий и установить причину ошибки. После устранения ошибки вы сможете возобновить процесс создания дистрибутива ключей.
- При создании самого первого дистрибутива ключей в программе задается пароль администратора группы узлов «Вся сеть» (см. [Создание и смена пароля администратора сетевого узла или группы узлов](#)). При отказе от задания пароля администратора создание дистрибутива ключей будет невозможно.
- При создании для пользователя первого дистрибутива ключей задается пароль данного пользователя. При отказе от задания пароля пользователя дальнейшее создание дистрибутива ключей будет невозможно.

- Если пользователь не имеет [максимальных полномочий](#) для работы в ПО ViPNet, установленном на сетевом узле, то перед формированием дистрибутива ключей для такого пользователя на данном узле рекомендуется задать пароль администратора его сетевого узла. Ограничения функциональных возможностей продуктов ViPNet, которые зависят от уровня полномочий пользователя, описаны в документации соответствующих продуктов.

При передаче повторного дистрибутива ключей следует настоятельно рекомендовать пользователю перед его установкой на узле расшифровать все зашифрованные письма в программе ViPNet Деловая почта. Это позволит предотвратить возможные проблемы с их прочтением после повторной инициализации дистрибутива ключей.

- Сформировать первый дистрибутив ключей для узла, созданного по запросу из центра регистрации, можно только удовлетворив соответствующий запрос (см. [Создание дистрибутивов ключей по запросам из центра регистрации](#)).
- При создании первого дистрибутива ключей для узла по запросу из центра регистрации (программы ViPNet Registration Point) необходимо учитывать следующее:
 - Если пароль пользователя задан при создании запроса на дистрибутив ключей в центре регистрации, то к нему применяются текущие настройки создаваемых паролей в программе ViPNet Registration Point (подробно см. в документе «ViPNet Registration Point. Руководство администратора», в главе «Работа с дистрибутивами ключей»).
 - Если пароль пользователя не был задан в программе ViPNet Registration Point, то при удовлетворении этого запроса в УКЦ всегда формируется случайный пароль пользователя в соответствии с текущими настройками создаваемых случайных паролей в программе ViPNet Удостоверяющий и ключевой центр.

Настройка параметров создания дистрибутивов ключей

В программе ViPNet Удостоверяющий и ключевой центр вы можете настроить следующие параметры создания дистрибутивов ключей: папка для сохранения дистрибутивов ключей, способ сохранения ключей электронной подписи и возможность выбора способа аутентификации пользователей в мастере выдачи дистрибутива ключей (см. [Создание дистрибутивов ключей](#)).

Чтобы настроить параметры создания дистрибутивов ключей:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Дистрибутивы ключей**.

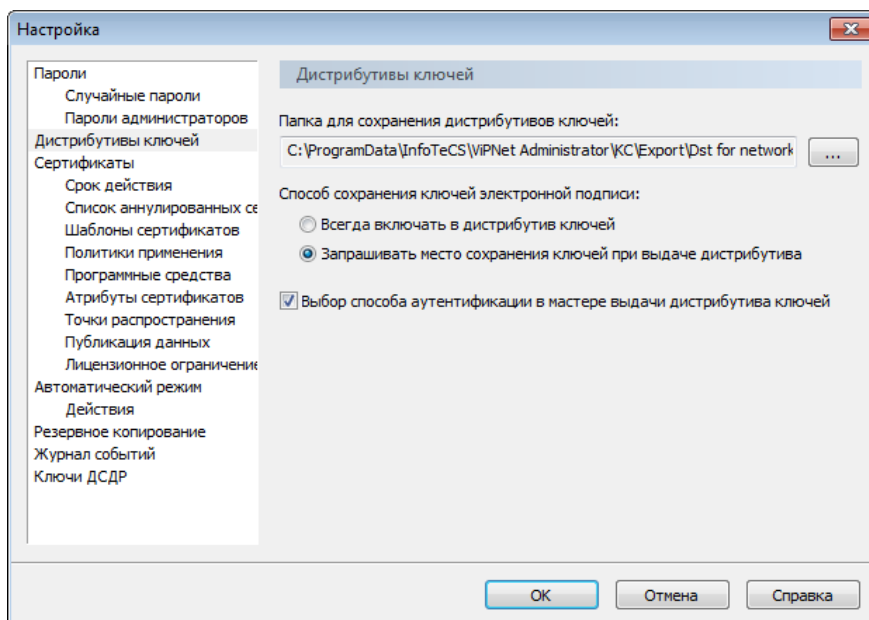


Рисунок 25. Настройка параметров выдачи дистрибутивов ключей

- 3 В поле **Папка для сохранения дистрибутивов ключей** с помощью кнопки  измените папку, в которой будут сохраняться дистрибутивы ключей. По умолчанию используется папка `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Export\Dst for network <номер сети>`.
- 4 Если вы хотите указывать место сохранения ключей электронной подписи пользователей при создании дистрибутивов ключей, установите переключатель **Способ сохранения ключей электронной подписи** в положение **Запрашивать место сохранения ключей при выдаче дистрибутива**. По умолчанию ключи электронной подписи сохраняются в дистрибутив ключей.
- 5 Если вы хотите указывать способ аутентификации пользователей в мастере создания дистрибутива ключей, установите соответствующий флажок.
- 6 Для сохранения настроек нажмите кнопку **ОК**.

Создание дистрибутивов ключей

При создании дистрибутивов ключей появление некоторых страниц и выполнение некоторых действий зависят от следующих настроек программы ViPNet Удостоверяющий и ключевой центр:

- Мастер подготовки к созданию ключей пользователя и мастер редактирования полей сертификатов появляются, если вы включили создание ключей электронной подписи и редактирование полей сертификатов при издании (см. [Настройка создания ключа электронной подписи и ключа проверки электронной подписи для пользователей сети ViPNet](#)).
- Страница выбора способа аутентификации пользователя в ПО ViPNet на узле появляется, если вы включили возможность выбора способа аутентификации пользователей при создании дистрибутивов ключей (см. [Настройка параметров создания дистрибутивов ключей](#)).

- Страница выбора места для сохранения ключей электронной подписи появляется, если вы не включили автоматическое сохранение данных ключей в дистрибутив (см. [Настройка параметров создания дистрибутивов ключей](#)).
- Страница задания пароля пользователя появляется, если вы создаете дистрибутив ключей пользователя в первый раз и в настройках по умолчанию выбрали тип пароля пользователя Собственный пароль (см. [Настройка типа создаваемых паролей](#)). Если в настройках программы по умолчанию вы выбрали тип Случайный пароль на основе парольной фразы, то пароль будет задан автоматически случайным образом.
- Сохранение паролей пользователей в файл или их печать, в зависимости от способа выдачи паролей, указанного в настройках в разделе Пароли (см. [Настройка способа выдачи паролей пользователей](#)).

В общем случае, чтобы создать дистрибутивы ключей для пользователей:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Сетевые узлы**.
- 2 В списке сетевых узлов на панели просмотра выберите узлы пользователей, для которых требуется создать дистрибутивы ключей.
- 3 Щелкните узлы правой кнопкой мыши и в контекстном меню выберите пункт **Выдать новый дистрибутив ключей**.

В результате будет запущен процесс создания дистрибутивов ключей для пользователей выбранных сетевых узлов.

- 4 Появится [электронная рулетка](#), если она еще не запускалась в рамках текущего сеанса работы программы. Следуйте указаниям в окне **Электронная рулетка**.

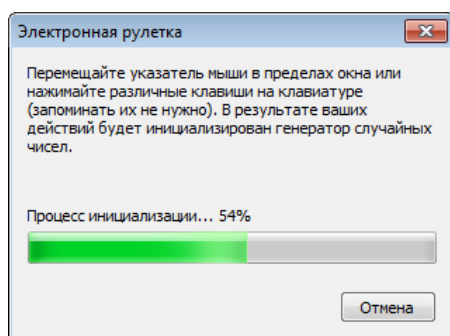


Рисунок 26. Запуск электронной рулетки

- 5 Если на сетевом узле зарегистрировано несколько пользователей, в мастере **Подготовка к выдаче новых дистрибутивов** на странице **Обнаружены узлы с несколькими зарегистрированными пользователями** выберите пользователей, для которых требуется создать дистрибутив ключей. По умолчанию установлен флажок напротив пользователей, дистрибутив которым еще не выдавался.

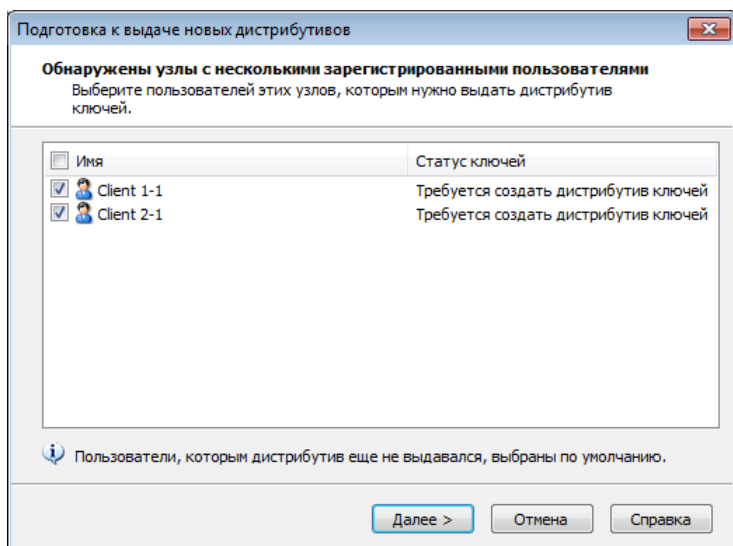


Рисунок 27. Выбор пользователей при выдаче дистрибутива ключей

- 6 На следующих страницах выберите шаблон сертификатов пользователей, задайте срок действия и настройте используемые расширения сертификатов, как описано в разделе [Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ](#). Если вы создаете дистрибутивы ключей нескольких пользователей, то заданные настройки будут использованы для издания сертификатов выбранных пользователей.
- 7 На странице **Способ аутентификации при разворачивании дистрибутива ключей** настройте способ аутентификации пользователя, как описано в разделе [Задание способа аутентификации пользователя](#).

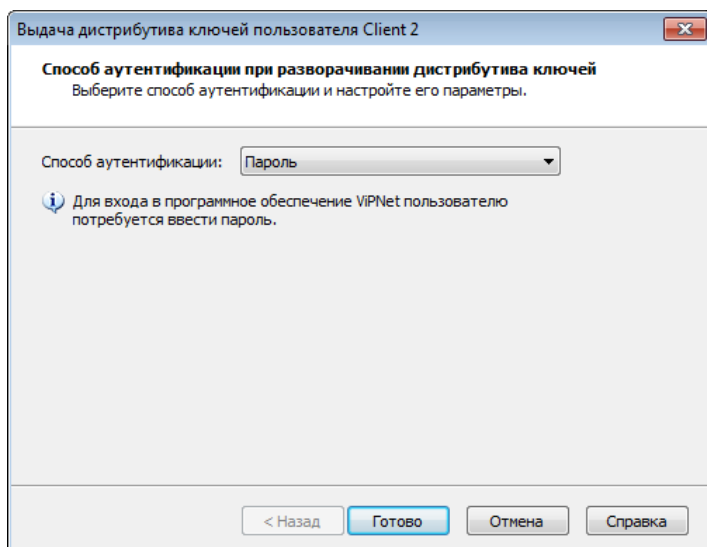


Рисунок 28. Выбор способа аутентификации пользователя при создании дистрибутива ключей

- 8 На странице **Способ сохранения ключей электронной подписи** установите переключатель в положение **Включить в дистрибутив ключей** или **Сохранить на устройстве**. В последнем случае на следующей странице мастера выберите внешнее устройство, на котором будут сохранены ключи электронной подписи пользователя.

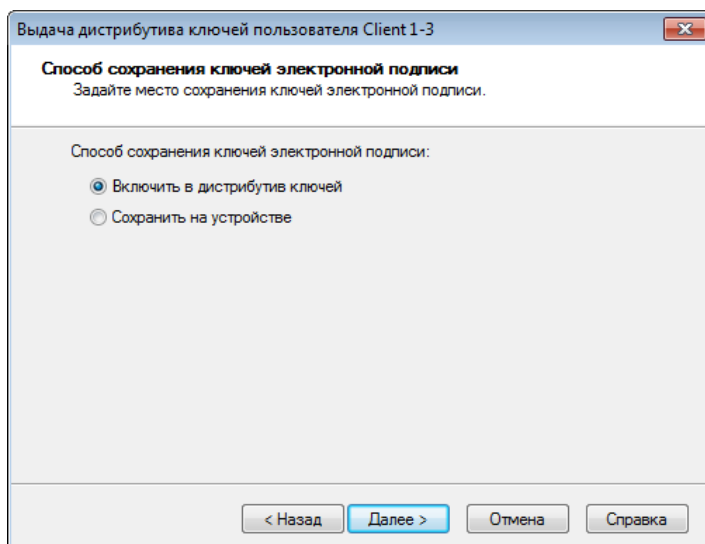


Рисунок 29. Выбор места для сохранения ключей электронной подписи пользователей

- 9 На странице **Пароль пользователя** задайте пароль пользователя.



Совет. Рекомендуется задавать сложные пароли, в состав которых входят буквы в разных регистрах, цифры и специальные символы.

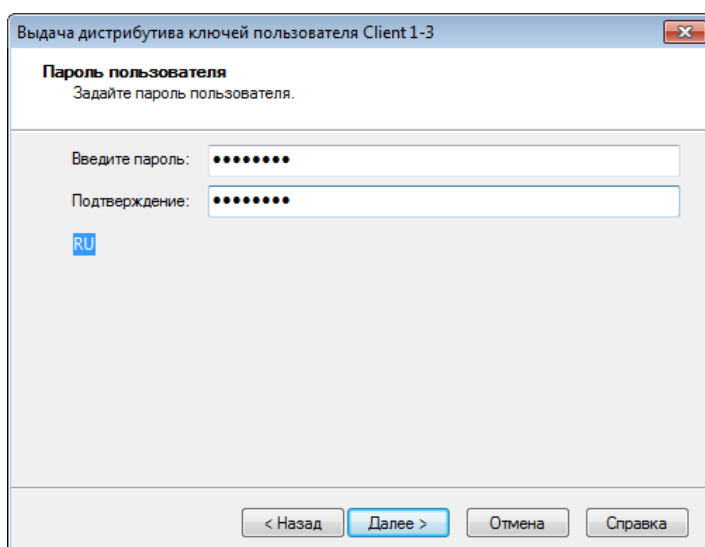


Рисунок 30. Задание пароля пользователя

- 10 В следующем окне при необходимости отредактируйте поля сертификата пользователя, как описано в разделе [Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ](#).
- 11 Нажмите кнопку **Готово**.

Дистрибутив ключей будет создан и сохранен в файле *.dst в заданной папке (см. [Настройка параметров создания дистрибутивов ключей](#)), при этом папка будет открыта в Проводнике Windows. Пароли пользователей будут сохранены в файл или переданы на печать в

зависимости от настроек программы. Пароли пользователей доступны для просмотра в окне свойств пользователей (см. [Просмотр свойств пользователя](#)).

Если при формировании дистрибутива ключей для пользователя были созданы ключи подписи, то в разделе **Моя сеть > Пользователи** в столбце **Ключи электронной подписи** напротив данного пользователя появится дата создания ключей. При необходимости вы можете сохранить ключи электронной подписи в отдельном файле (см. [Создание и сохранение ключей электронной подписи пользователя в файл](#)).

Изданный сертификат пользователя появится в представлении **Удостоверяющий центр** в разделе **Изданные сертификаты > Пользователи моей сети**. При необходимости вы можете просмотреть сертификат (см. [Просмотр сертификатов](#)).

Создание дистрибутивов ключей по запросам из центра регистрации

Запросы на дистрибутивы ключей, созданные в центре регистрации (с помощью программы ViPNet Registration Point), поступают в программу ViPNet Центр управления сетью. В ЦУСе на основе данных, указанных в запросах, автоматически создаются новые пользователи и сетевые узлы с заданными свойствами либо изменяются свойства существующих пользователей и узлов. Затем запросы поступают на обработку в УКЦ.

В УКЦ запросы на дистрибутивы ключей могут обрабатываться автоматически в том случае, если выполнены необходимые настройки УКЦ и программа работает в автоматическом режиме (см. [Настройка автоматического режима](#)). В противном случае требуется обработать запросы вручную. Обработка вручную также требуется для тех запросов, которые по каким-либо причинам были отклонены в автоматическом режиме. Например, будут отклонены запросы, подписанные недействительным сертификатом администратора центра регистрации. При обработке вручную вы можете удовлетворить или отклонить запросы.

Чтобы обработать запросы на дистрибутивы ключей вручную:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Пользователи > Запросы на дистрибутивы ключей**.
- 2 На панели просмотра выберите один или несколько запросов и на панели инструментов нажмите кнопку **Удовлетворить** или кнопку **Отклонить**. Перед обработкой вы можете просмотреть параметры запроса, для этого дважды щелкните запрос.
- 3 Если вы отклонили запросы, они останутся в списке, и при необходимости вы можете удалить их.
- 4 При удовлетворении запросов начнется процесс создания дистрибутивов ключей. Если в настройках программы в разделе **Сертификаты** установлен флажок **Редактировать поля сертификатов при издании**, будет запущен мастер **Подготовка к выдаче новых дистрибутивов**, затем мастер **Редактирование полей сертификата**, следуйте их указаниям (см. [Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ](#)).

Изданный сертификат появится в представлении **Удостоверяющий центр** в разделе **Изданные сертификаты** > **Пользователи моей сети**. Созданный дистрибутив ключей через ЦУС будет автоматически передан в программу ViPNet Registration Point с помощью транспортного модуля ViPNet MFTP.

Создание дистрибутива ключей для ПАК ViPNet Coordinator KB

Перед созданием дистрибутива ключей для ПАК ViPNet Coordinator KB:

- Получите [ключевой блокнот ДСДР](#) и зарегистрируйте в УКЦ (см. [Учет ключей ДСДР](#)).
- Убедитесь, что в настройках УКЦ задан выбор способа аутентификации пользователя при создании дистрибутива ключей (см. [Настройка параметров создания дистрибутивов ключей](#)).
- Подготовьте внешнее устройство аутентификации (см. [Внешние устройства](#)) и отформатируйте его.

Чтобы создать дистрибутивы ключей для ПАК ViPNet Coordinator KB:

- 1 В УКЦ выберите **Сервис** > **Настройка** > **Дистрибутивы ключей** и установите флажок **Выбор способа аутентификации в мастере выдачи дистрибутива ключей**.
- 2 В контекстном меню узла выберите пункт **Выдать новый дистрибутив ключей**. Откроется мастер создания дистрибутива ключей (см. [Создание дистрибутивов ключей](#)).
- 3 На странице **Способ аутентификации при разворачивании дистрибутива ключей**:
 - 3.1 В списке **Способ аутентификации** выберите один из следующих пунктов:
 - **Устройство (персональный ключ)** — для ПАК ViPNet Coordinator KB версии 2.7 и выше.

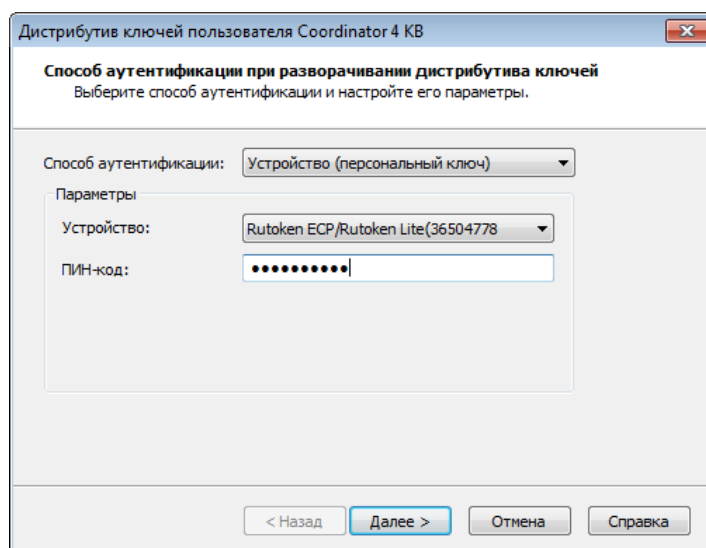


Рисунок 31. Создание ключей для ПАК ViPNet Coordinator KB версии 2.7 и выше

- **Устройство (парольный ключ)** — для ПАК ViPNet Coordinator KB версии 2.5 и ниже.

Этот способ аутентификации отображается в интерфейсе только при создании дистрибутивов для узлов с ролями «Coordinator KB100» и «Coordinator KB1000». Пользователя, использующего этот способ аутентификации, не следует регистрировать на других узлах сети. В противном случае могут возникнуть ошибки в работе узлов, на которых будет зарегистрирован этот пользователь.

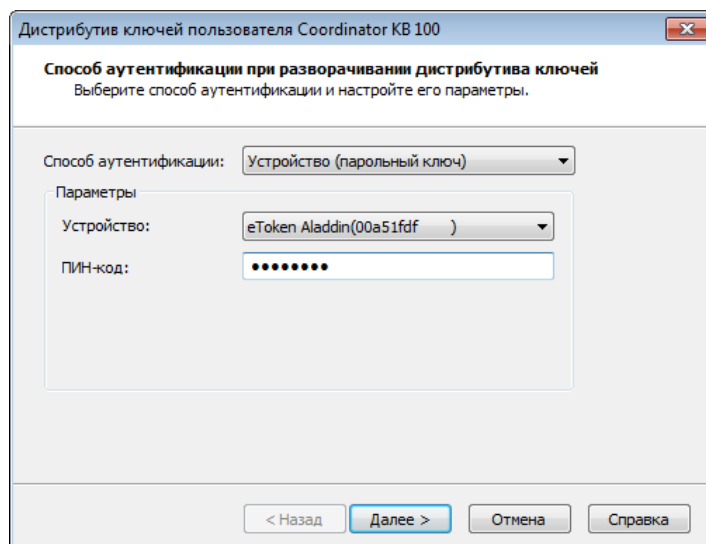


Рисунок 32. Создание ключей для ПАК ViPNet Coordinator KB версии 2.5 и ниже

- 3.2 Подключите к компьютеру устройство аутентификации пользователя.
- 3.3 В списке **Устройство** укажите подключенное внешнее устройство и в соответствующем поле введите ПИН-код устройства.
- 4 Если внешнее устройство уже содержит ключи, будет предложено их перезаписать.
- 5 Передайте созданный файл дистрибутива ключей (*.dst) и устройство пользователю.

Работа с ключами узлов

Ключи узла ViPNet — набор файлов, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого узла сети ViPNet. Основное содержание ключей узла — ключи для шифрования передаваемого трафика и информации ViPNet-приложений (ViPNet SDK, ViPNet Деловая почта), которой обмениваются сетевые узлы, и другие служебные файлы. Полный состав ключей узла приведен в описании дистрибутива ключей.

Когда следует создавать ключи узлов?

Новые ключи для узла вам требуется создавать в следующих случаях:

- Добавление или удаление связи с другим сетевым узлом вашей сети ViPNet или доверенной сети.
- Смена мастер-ключа обмена или мастер-ключа защиты (см. [Работа с мастер-ключами](#)).
- Смена межсетевого мастер-ключа, в случае, если текущий сетевой узел имеет связь с узлами доверенной сети (см. [Смена межсетевого мастер-ключа](#)).
- Скомпрометированы ключи пользователя текущего сетевого узла (см. [Действия в случае компрометации ключей пользователя](#)).
- Скомпрометированы ключи пользователя сетевого узла, с которым установлена связь.
- Изменен вариант ключей узла (см. [Изменение вариантов персонального ключа пользователя и ключей узла](#)).
- Смена пароля администратора сетевого узла или группы узлов (см. [Создание и смена пароля администратора сетевого узла или группы узлов](#)). В этих случаях требуется сформировать ключи узла либо ключи всех узлов, входящих в данную группу, соответственно.
- Смена способа аутентификации пользователя (см. [Задание способа аутентификации пользователя](#)).
- Регистрация ключей ДСДР (см. [Учет ключей ДСДР](#)).

Особенности создания ключей узлов

При создании ключей узлов важно помнить о следующих особенностях:

- Ключи узлов могут создаваться в автоматическом режиме (см. [Режимы работы УКЦ](#)) или вручную (по команде администратора). В автоматическом режиме создание ключей может производиться с определенной периодичностью либо сразу после обновления справочников для данных узлов в программе ViPNet Центр управления сетью. Чтобы ключи узлов создавались в автоматическом режиме работы УКЦ, требуется выполнить соответствующие настройки (см. [Настройка автоматического создания ключей узлов](#)).

При создании ключей узла в автоматическом режиме они сразу передаются в программу ViPNet Центр управления сетью. В случае создания ключей узлов вручную они могут быть либо переданы в ЦУС (см. [Создание и передача ключей узлов в ЦУС](#)), либо сохранены в файл (см. [Создание и сохранение ключей узлов в файл](#)).

- Если в процессе создания ключей узла произошла ошибка (например, [межсетевой мастер-ключ](#) не был создан или введен в действие при установке взаимодействия с доверенной сетью ViPNet), то появится соответствующее сообщение с предложением пропустить или отменить создание ключей для данного узла. В этом случае вам следует выбрать одно из предложенных действий и установить причину ошибки. После устранения ошибки вы сможете возобновить процесс создания ключей.

Настройка автоматического создания ключей узлов

Ключи узлов могут создаваться в автоматическом режиме работы программы (см. [Работа в автоматическом режиме](#)) по следующему расписанию:

- Раз в несколько часов.
- Каждый день в конкретное время.
- Сразу после того, как в программе ViPNet Центр управления сетью будут изменены справочники для данных узлов.

Поэтому, если вы выбрали операцию создания ключей узлов для выполнения в автоматическом режиме работы программы (см. [Настройка автоматического режима](#)), в окне **Параметры действия в автоматическом режиме** укажите расписание создания ключей узлов, установив переключатель в нужное положение.

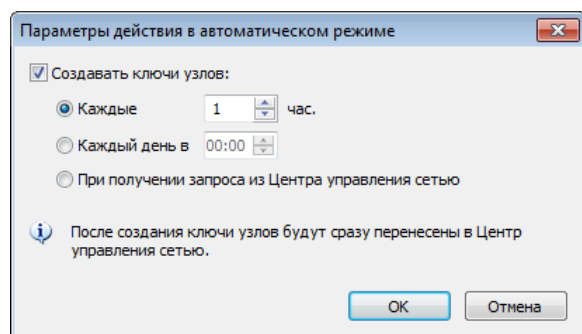


Рисунок 33. Настройка автоматического создания ключей узлов

При создании ключей узла в автоматическом режиме, они сразу передаются в ЦУС. В данном случае сохранение ключей узла в файл невозможно. Для сохранения ключей в файл создайте их вручную (см. [Создание и сохранение ключей узлов в файл](#)).

Создание и передача ключей узлов в ЦУС

Создание ключей узлов и их передача в программу ViPNet Центр управления сетью производятся для того, чтобы впоследствии новые ключи были централизованно отправлены из нее на узлы сети. Если ключи узла создаются в автоматическом режиме (см. [Режимы работы УКЦ](#)), то они сразу передаются в ЦУС.

Чтобы вручную создать и передать ключи узла в ЦУС:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Сетевые узлы**.
- 2 В списке на панели просмотра выберите нужный узел. При необходимости выберите несколько узлов.
- 3 Щелкните узлы правой кнопкой мыши и в контекстном меню выберите пункт **Создать и передать ключи в ЦУС**.

Создание и сохранение ключей узлов в файл

Вы можете создать новые ключи узла и сохранить их в файл. Данный файл может быть передан пользователю для обновления ключей узла на сетевом узле вручную. Это необходимо в случае, когда ключи, высылаемые из программы ViPNet Центр управления сетью, не могут быть приняты автоматически. Например, передача ключей через координатор становится невозможна, если в процессе смены мастер-ключа новые ключи еще не введены в действие на узле, но уже введены в действие на координаторе, за которым стоит этот узел.

Чтобы создать и сохранить ключи узла в файл:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Сетевые узлы**.
- 2 В списке на панели просмотра выберите нужный узел. При необходимости выберите несколько узлов.
- 3 Щелкните узлы правой кнопкой мыши и в контекстном меню выберите пункт **Создать и сохранить ключи в файл**.
- 4 В появившемся окне выберите папку на жестком или съемном диске.

В результате ключи выбранного узла будут созданы и сохранены в файл `apn_XXXX.ke` (где XXXX — шестнадцатеричный идентификатор узла в сети) в указанную папку.

Передайте файл с ключами узла пользователю. Пользователю необходимо выполнить следующие действия:

- 1 Поместить этот файл по следующему пути:
 - При использовании программы ViPNet Client for Windows версии ниже 4.5.1 — в папку установки программы в подпапку `\CCC\key\`.

- При использовании программы ViPNet Client for Windows версии 4.5.1 и выше — в транспортный каталог `C:\ProgramData\InfoTeCS\ViPNet Client\<идентификатор узла>`. Например, `C:\ProgramData\InfoTeCS\ViPNet Client\10E10C20`.

2. Перезапустить программу ViPNet Client.

Работа с ключами пользователей

Ключи пользователя ViPNet — набор файлов, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сети ViPNet. Основное содержание ключей пользователя — информация, идентифицирующая пользователя и позволяющая ему работать с программным обеспечением ViPNet. В ключах пользователя также могут присутствовать ключи электронной подписи (в [контейнере ключей](#)). Полный состав ключей пользователя приведен в описании дистрибутива ключей (см. [Работа с дистрибутивами ключей](#)).

О том, в каких случаях пользователю сети ViPNet выдаются ключи подписи, см. раздел [Настройка создания ключа электронной подписи и ключа проверки электронной подписи для пользователей сети ViPNet](#).

Когда следует создавать ключи пользователей?

Ключи пользователя вам требуется создавать в таких случаях, как:

- Скомпрометированы ключи пользователя (см. [Действия в случае компрометации ключей пользователя](#)).
- Изменен вариант персонального ключа пользователя (см. [Изменение вариантов персонального ключа пользователя и ключей узла](#)).
- Смена мастера персональных ключей (см. [Работа с мастер-ключами](#)).
- Выдача ключа электронной подписи и ключа проверки электронной подписи пользователю (см. [Настройка создания ключа электронной подписи и ключа проверки электронной подписи для пользователей сети ViPNet](#)).
- Издание нового сертификата пользователя при истечении срока действия имеющегося у него [ключа электронной подписи](#) и соответствующего [сертификата ключа проверки электронной подписи](#).



Примечание. При одновременном истечении срока действия ключа электронной подписи и сертификата пользователь может получить новый ключ электронной подписи и сертификат только в составе своих новых ключей. В этом случае обновление сертификата (и, соответственно, ключа электронной подписи) по запросу невозможно.

Особенности создания ключей пользователей

При создании ключей пользователя важно помнить о следующих особенностях:

- После создания ключи пользователя могут быть автоматически переданы в ЦУС (см. [Создание и передача ключей пользователей в ЦУС](#)) либо сохранены в файл (см. [Создание и сохранение ключей пользователей в файл](#)).
- Если в процессе создания ключей пользователя произошла ошибка (например, истек срок действия ключа электронной подписи администратора, который производит формирование ключей пользователя), то появится соответствующее сообщение с предложением пропустить или отменить создание ключей для данного пользователя. В этом случае вам следует выбрать одно из предложенных действий и установить причину ошибки. После устранения ошибки вы сможете возобновить процесс создания ключей.

Настройка создания ключа электронной подписи и ключа проверки электронной подписи для пользователей сети ViPNet

Для пользователей сети ViPNet могут создаваться ключ электронной подписи и ключ проверки электронной подписи и издаваться сертификаты ключей проверки электронной подписи (см. [Издание сертификатов](#)). При наличии этих ключей у пользователя в программах ViPNet, установленных на его сетевом узле, становятся доступными опции, связанные с использованием сертификатов. Например, в программе ViPNet Client в окне настроек параметров безопасности появляется вкладка **Электронная подпись**.

Ключ электронной подписи и ключ проверки электронной подписи создаются для пользователя при формировании его ключей или дистрибутива ключей, если есть соответствующее разрешение. При наличии разрешения на создание ключа электронной подписи и ключа проверки электронной подписи в представлении **Ключевой центр** в разделе **Моя сеть > Пользователи** в столбце **Создание ключей электронной подписи** напротив данного пользователя отображается значение **Будут создаваться**. В противном случае эти ключи для пользователя не создаются.

Если пользователю не нужны ключ электронной подписи и ключ проверки электронной подписи (например, он является администратором координатора), то создание этих ключей для него можно запретить.



Внимание! Если для пользователя вначале создать ключи электронной подписи и издать действительный сертификат, а потом запретить создание ключей и выслать ключи на его узел (см. [Создание и передача ключей узлов в ЦУС](#)), то он не сможет использовать текущие ключи и сертификат в приложениях ViPNet (например, в ПО ViPNet Client пропадет вкладка **Электронная подпись**). При чем если пользователь зарегистрирован на нескольких узлах, то данное ограничение будет распространяться только на его [основной узел](#). На остальных узлах он сможет пользоваться ключами и сертификатом в ПО ViPNet.

Чтобы настроить создание ключа электронной подписи и ключа проверки электронной подписи для конкретного пользователя:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Пользователи**.
- 2 В списке пользователей на панели просмотра выберите нужного пользователя. При необходимости можно выбрать несколько пользователей.
- 3 Выполните одно из следующих действий:
 - В контекстном меню пользователя выберите пункт **Ключи пользователя** и установите или снимите отметку напротив пункта **Создавать ключи электронной подписи**.
 - Дважды щелкните учетную запись пользователя и в окне свойств пользователя на вкладке **Сертификаты** установите или снимите флажок **Создавать ключи электронной подписи**.

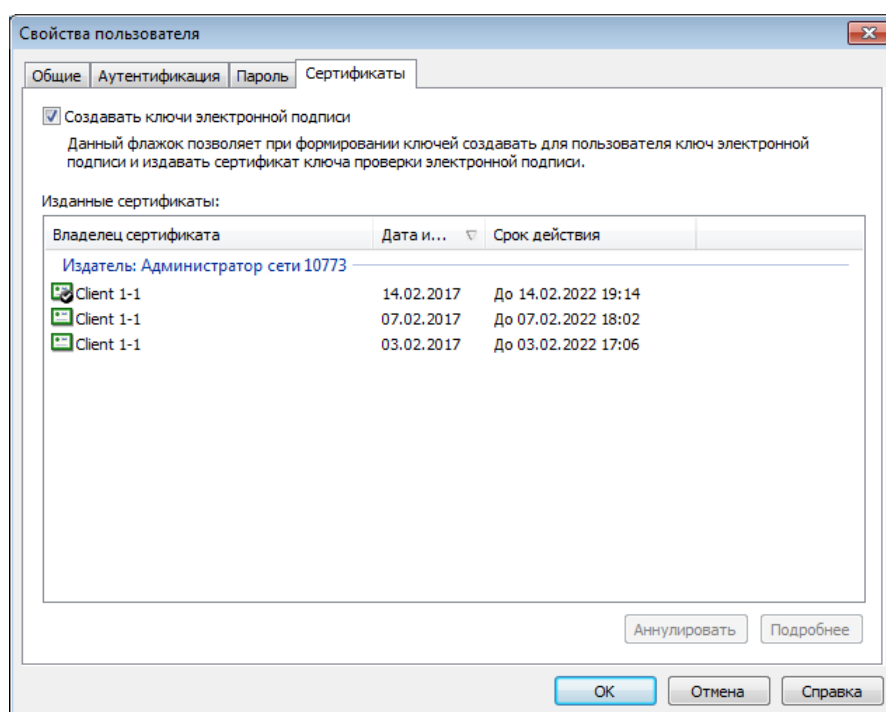


Рисунок 34. Назначение пользователю права электронной подписи

После настройки создания ключа электронной подписи и ключа проверки электронной подписи сформируйте и отправьте на узел пользователя новые ключи пользователя, ключи узла и файл со всеми CRL. Ключ электронной подписи и ключ проверки электронной подписи при необходимости могут быть переданы пользователю не в составе его ключей, а в отдельном файле (см. [Создание и сохранение ключей электронной подписи пользователя в файл](#)). Если настройка создания таких ключей была отключена, то на узел пользователя нужно отправить ключи узла и комплект CRL (см. [Распространение списков аннулированных сертификатов](#)).



Совет. Если до отключения настройки у пользователя имелся сертификат, и необходимо гарантировать, что пользователь не сможет им воспользоваться, отзовите сертификат данного пользователя (см. [Аннулирование, приостановление действия, возобновление действия сертификатов](#)).

Чтобы не настраивать создание ключа электронной подписи и ключа проверки электронной подписи для каждого нового пользователя в отдельности, в настройках программы в разделе

Сертификаты установите или снимите флажок **Создавать ключи электронной подписи**. В этом случае для всех новых пользователей сети ViPNet, которые были зарегистрированы в программе ViPNet Центр управления сетью, будет разрешено или запрещено создание ключей.

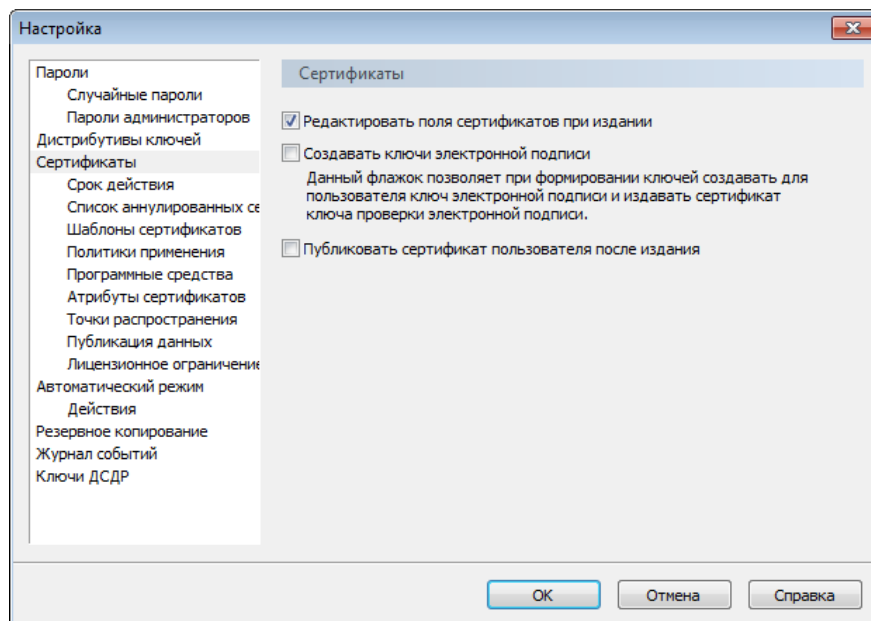


Рисунок 35. Настройка создания ключей подписи для новых пользователей

Создание и передача ключей пользователей в ЦУС

Чтобы создать ключи пользователей без резервного набора персональных ключей и передать их в ЦУС для последующей централизованной отправки пользователям на сетевые узлы:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Пользователи**.
- 2 В списке пользователей на панели просмотра выберите пользователей, для которых требуется создать и передать в ЦУС новые ключи.
- 3 В контекстном меню пользователей выберите пункт **Ключи пользователя > Создать и передать ключи в ЦУС**.

В результате будет запущен процесс создания ключей пользователей.

- 4 Появится электронная рулетка, если она еще не запускалась в рамках текущего сеанса работы программы. Поводите указателем в пределах окна **Электронная рулетка**.
- 5 Если для пользователя назначено создание ключа электронной подписи и ключа проверки электронной подписи (см. [Настройка создания ключа электронной подписи и ключа проверки электронной подписи для пользователей сети ViPNet](#)), то будет создан контейнер с ключом электронной подписи и издан сертификат ключа проверки электронной подписи. Если создание ключей назначено, но фактически пользователю не нужны ключ электронной

подписи, ключ проверки электронной подписи и сертификат, то вы можете отменить издание сертификата, нажав в мастере **Подготовка к изданию сертификатов** или **Редактирование полей сертификата** кнопку **Отмена** (см. раздел [Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ](#)). Контейнер с ключом электронной подписи в этом случае также не будет создан.

Примечание. Мастер подготовки к изданию сертификата и мастер редактирования полей сертификата запускаются, только если в настройках программы в разделе Сертификаты установлен флажок **Редактировать поля сертификатов при издании**.



Если в процессе создания ключей указанные мастера не запустятся, отменить создание ключа электронной подписи и издание сертификата будет невозможно. Сертификат в этом случае будет издан автоматически в соответствии с параметрами шаблона, выбранного по умолчанию. Подробнее см. раздел Создание и редактирование шаблонов сертификатов (см. [Создание и изменение шаблонов сертификатов](#)).

По завершении создания ключи пользователей будут переданы в ЦУС. При этом в разделе **Моя сеть > Пользователи** в столбце **Ключи** напротив данных пользователей появится дата создания и передачи ключей в ЦУС.

Если при формировании ключей пользователя были созданы ключи электронной подписи, то в столбце **Ключи электронной подписи** напротив данного пользователя также появится дата создания ключей. Изданный сертификат пользователя появится в представлении **Удостоверяющий центр** в разделе **Изданные сертификаты > Пользователи моей сети**. Вы можете просмотреть сертификат (см. [Просмотр сертификатов](#)).



Примечание. Резервные наборы персональных ключей и ключи электронной подписи могут быть созданы и сохранены в файлы отдельно. Подробнее см. в разделах [Работа с резервными наборами персональных ключей](#) и [Создание и сохранение ключей электронной подписи пользователя в файл](#).

Пароли пользователей, для которых формировались ключи, вы можете посмотреть, сохранить в текстовый файл и сменить в свойствах пользователей на вкладке **Пароль** (см. [Просмотр свойств пользователя](#)).

Создание и сохранение ключей пользователей в файл

Вы можете создать ключи пользователя и сохранить их в файл. Это может потребоваться для передачи ключей непосредственно пользователю в целях их обновления на сетевом узле вручную, в том случае, если ключи, высылаемые из программы ViPNet Центр управления сетью, не могут быть приняты автоматически. Ситуация, при которой ключи пользователя на узле не могут быть обновлены автоматически, может возникнуть, если пользователь зарегистрирован на нескольких сетевых узлах с ПО ViPNet Client или ViPNet Coordinator. В этом случае ключи пользователя будут

отправлены только на [основной узел пользователя](#). На остальных узлах, на которых зарегистрирован этот пользователь, ключи необходимо обновить вручную.

Чтобы создать и сохранить ключи пользователя в файл:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Пользователи**.
- 2 В списке пользователей на панели просмотра выберите пользователей, для которых требуется создать и сохранить новые ключи в файл.
- 3 В контекстном меню пользователей выберите пункт **Ключи пользователя > Создать и сохранить ключи в файл**.
- 4 В появившемся окне выберите папку на жестком или съемном диске.

Далее будет запущен процесс создания ключей пользователей (см. [Создание и передача ключей пользователей в ЦУС](#)). По завершении создания ключи выбранных пользователей будут сохранены в файл `abn_АААА.ke` (где АААА — шестнадцатеричный идентификатор пользователя в сети) в указанную папку.

Передайте файл с ключами пользователю. Если в составе ключей пользователя есть ключи электронной подписи, то они также будут содержаться в файле `abn_АААА.ke`.

Передайте файл с ключами узла пользователю. Пользователю необходимо выполнить следующие действия:

- 1 Поместить этот файл по следующему пути:
 - При использовании программы ViPNet Client for Windows версии ниже 4.5.1 — в папку установки программы в подпапку `\CCC\key\`.
 - При использовании программы ViPNet Client for Windows версии 4.5.1 и выше — в транспортный каталог `C:\ProgramData\Infotecs\<папка с идентификатором узла>\`.

Таблица 3. Расположение ключей пользователя

Программа	Папка по умолчанию
ViPNet Client for Windows версии ниже 4.5.1 ViPNet Coordinator for Windows версии ниже 4.5.1	• <code>C:\Program Files\InfoTeCS\<Название программы>\CCC\key\</code> — в 32-битных версиях Windows; • <code>C:\Program Files (x86)\InfoTeCS\<Название программы>\CCC\key\</code> — в 64-битных версиях.
ViPNet Client for Windows версии 4.5.1 и выше ViPNet Coordinator for Windows версии 4.5.1 и выше	<code>C:\ProgramData\Infotecs\<папка с идентификатором узла>\</code>

- 2 Перезапустить программу ViPNet Client.



Примечание. Ключи электронной подписи могут быть созданы и сохранены в файл отдельно. Подробнее см. в разделах [Создание и сохранение ключей электронной подписи пользователя в файл](#).

Пароли пользователей, для которых формировались ключи, вы можете посмотреть, сохранить в текстовый файл и сменить в свойствах пользователей на вкладке **Пароль** (см. [Просмотр свойств пользователя](#)).

Создание и сохранение ключей электронной подписи пользователя в файл

Ключи электронной подписи могут быть созданы в процессе формирования дистрибутива ключей или ключей пользователя (см. [Настройка создания ключа электронной подписи и ключа проверки электронной подписи для пользователей сети ViPNet](#)). Если ключи электронной подписи не создавались в составе дистрибутива или ключей пользователя, при необходимости вы можете создать и сохранить их в отдельном файле. Такая потребность может возникнуть, например, если у пользователя нет в наличии внешнего устройства, но при этом ему необходимо получить контейнер с ключами электронной подписи в виде отдельного файла на съемном диске, а не в составе ключей пользователя 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 Webservice.

При сохранении ключи электронной подписи будут зашифрованы на пароле, заданном для пользователя в УКЦ (см. [Просмотр свойств пользователя](#)).



Примечание. В процессе переноса дистрибутива ключей в папку ключи электронной подписи могут быть сохранены отдельно от него, но только на внешнем устройстве.

Чтобы создать и сохранить ключи электронной подписи пользователя в файл:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Пользователи**.
- 2 В списке на панели просмотра выберите нужного пользователя. При необходимости выберите нескольких пользователей.
- 3 В контекстном меню для данного пользователя выберите пункт **Ключи пользователя > Создать ключи электронной подписи и сохранить в файл**.
- 4 В появившемся окне выберите папку на жестком или съемном диске.

В результате будет создан контейнер ключей электронной подписи для выбранного пользователя, который будет сохранен в указанную папку в файл `abn_AAAA.key`, где `<AAAA>` — шестнадцатеричный идентификатор пользователя в сети. Передайте контейнер ключей в этом файле пользователю. При последующем создании дистрибутива или ключей пользователя в их составе не будет ключей электронной подписи.

Полученный контейнер ключей пользователь сможет установить в криптопровайдере ViPNet CSP или другом программном обеспечении ViPNet, которое поддерживает работу с ключами электронной подписи (например, в ПО ViPNet Client). После этого он сможет использовать ключи электронной подписи по назначению.

Работа с резервными наборами персональных ключей

Резервный набор персональных ключей (РНПК) — набор из нескольких персональных ключей, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сети ViPNet на основе одного и того же [мастер-ключа](#).

Основное назначение резервного набора персональных ключей заключается в том, что, будучи заранее созданным и переданным пользователю, он позволяет при компрометации пользователя или смене в сети мастера персональных ключей дистанционно обновить [ключи пользователя](#) и [ключи узла](#) без необходимости высылать пользователю новый персональный ключ по скомпрометированному каналу.

Каждый резервный набор состоит из 20 персональных ключей, при этом 1 ключ в наборе всегда остается неиспользованным. Если в наборе были использованы все ключи из допустимых (то есть 19 ключей), то автоматически создается новый набор. При этом последний оставшийся ключ старого набора используется для шифрования нового резервного набора и переходит в его состав.

Когда следует создавать резервные наборы персональных ключей?

Создание резервного набора персональных ключей пользователя производится программой автоматически в следующих случаях:

- формирование дистрибутива ключей пользователя;
- создание ключей пользователя после смены мастер-ключа персональных ключей (при этом РНПК содержится только в первых ключах пользователя);
- создание ключей в случае компрометации пользователя или изменения варианта его персонального ключа, если в текущем резервном наборе пользователя были использованы все допустимые персональные ключи.



Примечание. В последних двух случаях создается новый резервный набор, который зашифровывается на персональном ключе пользователя из старого набора.

Резервный набор ключей вы также можете создать вручную. Это может потребоваться для обновления ключей на узлах, если по каким-то причинам у пользователя нет резервного набора на узле, перед проведением следующих операций:

- смены мастер-ключа персональных ключей в сети;
- компрометации ключей пользователя;

- изменением варианта персонального ключа;
- изменением варианта ключей узла, если отмечен флажок **Применить новый вариант ключей для всех пользователей выбранных сетевых узлов**.

В процессе данных операций меняется персональный ключ пользователя — берется новый ключ из [резервного набора персональных ключей \(РНПК\) пользователя](#). Как правило, на сетевые узлы файл с РНПК попадает в составе дистрибутива ключей. Но может возникнуть ситуация, когда его может не быть на узле. Например, если вы для восстановления работоспособности узла или обновления справочников и ключей повторно развернули дистрибутив ключей, в котором не было РНПК. В этом случае создайте РНПК для пользователя и передайте РНПК на сетевой узел доверенным способом. После создания резервный набор автоматически сохраняется по указанному вами пути в файл `AAAA.pk`, где `<AAAA>` — шестнадцатеричный идентификатор пользователя в сети. При сохранении он зашифровывается на пароле пользователя.

Стоит учесть, что содержание резервных наборов, созданных вручную, не изменяется, остается таким же, как и в предыдущих наборах, созданных программой автоматически.

Создание и сохранение резервных наборов персональных ключей в файл

Чтобы создать резервные наборы персональных ключей для пользователей:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Пользователи**.
- 2 В списке пользователей на панели просмотра выберите пользователей, для которых требуется создать резервные наборы ключей.
- 3 В контекстном меню пользователей выберите пункт **Ключи пользователя > Создать и сохранить РНПК в файл**.
- 4 В появившемся окне укажите папку на жестком или съемном диске для сохранения файлов РНПК.

В результате резервные наборы персональных ключей будут сохранены в указанную папку в файлы `*.pk` и зашифрованы на паролях пользователей. В представлении **Ключевой центр** в разделе **Моя сеть > Пользователи** в столбце **Резервные наборы персональных ключей** напротив пользователей, для которых создавались резервные наборы, появится дата создания наборов.

Передайте файлы с резервными наборами пользователям, предварительно ознакомившись с правилами передачи (см. [Правила передачи резервных наборов персональных ключей](#)). При передаче файлов сообщите пользователям пароли, на которых зашифрованы резервные наборы. При первом обращении к файлам с резервными наборами пользователям потребуется указать эти пароли.

Правила передачи резервных наборов персональных ключей

При передаче резервного набора персональных ключей непосредственно пользователю (не в составе дистрибутива ключей или ключей пользователя) соблюдайте следующие правила:

- Переносите файлы с резервными наборами ключей *.pk на отдельные устройства хранения данных.
- Устройства с резервными наборами передавайте пользователям лично в руки либо другим доверенным способом.
- Рекомендуйте пользователям хранить резервные наборы персональных ключей в безопасном месте, отдельно от других ключей (например, в сейфе), поскольку после получения они будут нести личную ответственность за хранение своих резервных наборов ключей в секрете от посторонних лиц.

Действия в случае компрометации ключей

Под компрометацией ключей понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, неотрекаемость). События, при которых ключи могут считаться скомпрометированными, определяются регламентом политики безопасности вашей организации. Как правило, ключи пользователя считаются скомпрометированными в следующих случаях:

- посторонним лицам мог стать доступен файл дистрибутива ключей пользователя;
- посторонним лицам могло стать доступно съемное устройство с ключами пользователя;
- посторонние лица могли получить неконтролируемый физический доступ к ключам пользователя, хранящимся на компьютере;
- уволился пользователь, имевший доступ к паролям и ключам;
- съемное устройство с ключами вышло из строя, и не опровергнут тот факт, что это произошло в результате несанкционированных действий злоумышленника.

Если один из перечисленных фактов имел место, администратору УКЦ незамедлительно следует:

- провести служебное расследование;
- уведомить скомпрометированного пользователя и администратора программы ViPNet Центр управления сетью о факте и обстоятельствах компрометации и выполнить действия, описанные в разделе [Действия в случае компрометации ключей пользователя](#);
- приостановить работу скомпрометированного узла до получения новых ключей.

В случае если есть подозрение, что посторонним лицам может быть известен пароль доступа к ключам, которые используются в приложении ViPNet, но доступ к компьютеру этих посторонних лиц был и остается невозможен, следует сменить пароль и продолжить работу.

Если нет фактов, говорящих о компрометации ключей пользователя, но есть подозрение, что злоумышленник получил доступ к ключам (например, пользователь отошел от компьютера, не заблокировав его), то достаточно изменить вариант персонального ключа пользователя и вариант ключей узла (см. [Изменение вариантов персонального ключа пользователя и ключей узла](#)).

Действия в случае компрометации ключей пользователя

В случае компрометации ключей какого-либо пользователя выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в представлении **Ключевой центр** в разделе **Пользователи** выберите одного или нескольких пользователей и в контекстном меню выберите пункт **Безопасность и плановые работы > Считать ключи скомпрометированными**.
- 2 В появившемся окне подтвердите, что нужно считать ключи пользователя скомпрометированными. Если вместе с ключами пользователя были скомпрометированы его ключи электронной подписи, установите флажок **Аннулировать сертификаты выбранных пользователей**.

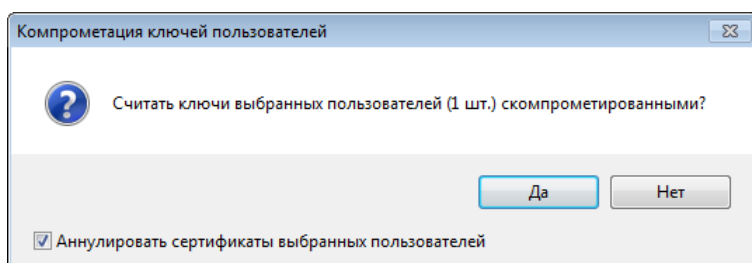


Рисунок 36. Окно с запросом подтверждения, что ключи пользователя считаются скомпрометированными

После этого ключи пользователя будут считаться скомпрометированными, его значок изменится на . Также будут изменены (увеличены на единицу) [вариант персонального ключа пользователя](#) и вариант ключей всех узлов, на которых зарегистрирован пользователь.



Внимание! Если при компрометации вариант персонального ключа пользователя равен единице, создайте для сетевого узла новый дистрибутив ключей (см. [Создание дистрибутивов ключей](#)).

- 3 Создайте и передайте в ЦУС новые ключи для пользователя, только после этого создайте и передайте в ЦУС ключи для узлов, на которых он зарегистрирован. Затем создайте и передайте в ЦУС ключи для всех узлов, связанных с узлами, на которых зарегистрирован скомпрометированный пользователь.



Примечание. Если у скомпрометированного пользователя есть в наличии ключи электронной подписи и сертификат, которые хранятся на его узле, то создайте для него новые ключи и сертификат. Это связано с тем, что на узле ключи электронной подписи защищены персональным ключом пользователя. Поэтому после смены персонального ключа пользователь не сможет получить доступ к своим текущим ключам электронной подписи и сертификату.

Если узел скомпрометированного пользователя (скомпрометированный узел) является координатором с установленным программным обеспечением ViPNet Coordinator Linux или программно-аппаратным комплексом ViPNet Coordinator HW версии ниже 4.2, то для этого узла может потребоваться создать новый дистрибутив ключей (см. [Совместимость с программным обеспечением ViPNet](#)).



Внимание! Если в текущем резервном наборе персональных ключей пользователя использованы все допустимые ключи, для такого пользователя в процессе создания ключей сформируется новый резервный набор ключей (см. [Когда следует создавать резервные наборы персональных ключей?](#)).

Новые ключи из ЦУСа должны быть отправлены сначала на узел или узлы, на которых зарегистрирован пользователь, ключи которого считаются скомпрометированными, а затем на все остальные узлы.

Если скомпрометированы ключи пользователя, зарегистрированного на координаторе, то созданные ключи передайте на узлы не через ЦУС по сети, а другим доверенным способом с указанием даты и времени их обновления. Обновление ключей должно осуществляться с отложенной датой применения либо в следующем порядке:

- Обновляются ключи на клиентах, у которых данный координатор является транспортным сервером.
 - Обновляются ключи на скомпрометированном координаторе, других координаторах сети ViPNet и оставшихся клиентах. Если скомпрометирован координатор ViPNet Coordinator Linux или ViPNet Coordinator HW, для которого потребовалось создать новый дистрибутив ключей, то сначала на этом координаторе устанавливается дистрибутив ключей, затем обновляются ключи на других координаторах и оставшихся клиентах.
 - Обновляются ключи на узле администратора сети.
- 4 При наличии связи с доверенными сетями выполните [экспорт межсетевой информации](#). После получения экспорта межсетевой информации администратор доверенной сети должен создать новые ключи для узлов, имеющих связь с узлом вашей сети, на котором зарегистрирован пользователь со скомпрометированными ключами.



Внимание! Если скомпрометированы ключи пользователя, зарегистрированного на координаторе, который является шлюзовым при организации межсетевого взаимодействия, то экспорт служебных данных в доверенные сети требуется выполнить до отправки на данный координатор новых ключей. В противном случае экспорт не сможет быть отправлен по сети, и его потребуется передавать вручную администраторам доверенных сетей.

Изменение вариантов персонального ключа пользователя и ключей узла

Если нет фактов, говорящих о компрометации ключей пользователя, но есть подозрение, что злоумышленник получил доступ к ключам (например, пользователь отошел от компьютера, не заблокировав его), измените [вариант персонального ключа пользователя и вариант ключей узла](#).

Также изменение варианта персонального ключа пользователя и варианта ключей узла могут производиться планово в соответствии с регламентом политики безопасности вашей организации (обычно раз в год), но не одновременно со сменой мастер-ключей.

Автоматически происходит изменение варианта персонального ключа пользователя и варианта ключей узла в следующих случаях:

- При изменении варианта персонального ключа пользователя автоматически изменяется вариант ключей всех узлов, на которых он зарегистрирован. При изменении варианта ключей узла вы можете при необходимости изменить варианты персональных ключей всех пользователей, зарегистрированных на этом узле.
- При компрометации ключей пользователя.
- При создании нового пользователя или сетевого узла, после того как был достигнут максимальный номер идентификатора объекта сети ViPNet и началось повторное использование идентификаторов.

Максимальным значением варианта ключей узла является число 255, при достижении которого для изменения варианта персонального ключа пользователя необходимо провести смену мастер-ключа персональных ключей (см. [Смена мастер-ключа персональных ключей](#)).

При достижении числа 255 значение варианта ключей узла после смены мастер-ключей считается исчерпанным (не обнуляется).

Изменить вариант персонального ключа можно только один раз. В этом случае вариант персонального ключа изменится с нуля до единицы. Если вам нужно изменить вариант персонального ключа, равный единице, создайте для сетевого узла новый дистрибутив ключей (см. [Создание дистрибутивов ключей](#)).

Чтобы изменить вариант персонального ключа пользователя и вариант ключей его узла:

- 1 В ЦУСе убедитесь, что на сетевых узлах приняты обновления ключей (отсутствуют неприменившиеся обновления ключей).
- 2 В УКЦ в представлении **Ключевой центр** выполните одно из действий:
 - В разделе **Пользователи** выберите пользователя (или нескольких пользователей) и в контекстном меню выберите пункт **Безопасность и плановые работы > Применить новый вариант персонального ключа**. При этом будут автоматически изменены варианты ключей узлов, на которых зарегистрированы выбранные пользователи.
 - Если вы хотите изменить вариант их персональных ключей для всех пользователей, зарегистрированных на определенном узле, в разделе **Сетевые узлы** выберите сетевой узел (или несколько сетевых узлов) и в контекстном меню выберите пункт **Безопасность и плановые работы > Применить новый вариант ключей**.
- 3 Подтвердите изменение варианта персонального ключа или варианта ключей узла.

Если вы изменяете вариант ключей узла и хотите также изменить вариант персонального ключа для всех пользователей, зарегистрированных на этом узле, установите флажок **Применить новый вариант ключей для всех пользователей выбранных сетевых узлов**.

Если вариант ключей узла достиг числа 255, вы не можете изменить это значение. В этом случае при компрометации ключей узла создайте новый узел в ЦУС и выдайте новый дистрибутив ключей.

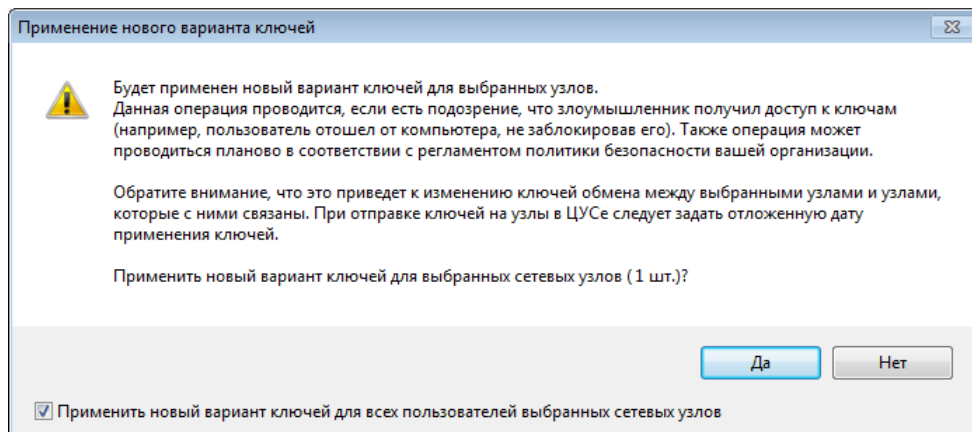


Рисунок 37. Изменение варианта ключей узла и варианта персонального ключа всех пользователей узла

- 4 Вариант персонального ключа пользователя из резервного набора и вариант ключей узла или нескольких узлов, на которых зарегистрирован пользователь, будет изменен (увеличен на единицу). Теперь создайте и передайте в ЦУС новые ключи пользователя и ключи узла. Ключи пользователя будут созданы на основе нового персонального ключа из резервного набора.

Если на узле отсутствует РНПК, создайте РНПК для пользователя и передайте на сетевой узел доверенным способом (см. [Работа с резервными наборами персональных ключей](#)).

- 5 В ЦУСе отправьте ключи на узлы с отложенной датой применения.



Примечание. Если у пользователя есть в наличии ключи электронной подписи и сертификат, которые хранятся на его узле, то создайте для него новые ключи и сертификат. Это связано с тем, что на узле ключи электронной подписи защищены персональным ключом пользователя. Поэтому после смены варианта персонального ключа он не сможет получить доступ к своим текущим ключам электронной подписи и сертификату.



Внимание! Если в текущем резервном наборе персональных ключей пользователя использованы все допустимые ключи, для такого пользователя в процессе создания ключей сформируется новый резервный набор ключей (см. [Когда следует создавать резервные наборы персональных ключей?](#)).

Действия при утрате резервного набора персональных ключей пользователя

Резервный набор персональных ключей пользователя считается скомпрометированным в случае потери устройства с резервным набором персональных ключей либо дистрибутива ключей, содержащего резервный набор.

Когда произошла компрометация резервного набора персональных ключей, выполнять обычную последовательность действий, как в случае компрометации пользователя, нельзя (см. [Действия в случае компрометации ключей пользователя](#)), поскольку злоумышленник может принять новые ключи пользователя и от его имени действовать в сети ViPNet. Поэтому в данном случае вы можете выбрать один из следующих вариантов:

- Удалить скомпрометированного пользователя и узел из структуры сети ViPNet и создать нового пользователя. В данном случае:
 - После регистрации нового пользователя в ЦУСе создайте для него дистрибутив ключей (см. [Создание дистрибутивов ключей](#)).
 - Для узлов, связанных с узлом скомпрометированного пользователя, создайте ключи узлов (см. [Создание и передача ключей узлов в ЦУС](#)).
- Сменить мастер-ключ персональных ключей (см. [Работа с мастер-ключами](#)) и создать новые ключи для скомпрометированного и связанных с ним пользователей и узлов, и передать их в ЦУС.



Примечание. Вариант формирования нового мастер-ключа является более трудоемким, по сравнению с вариантом удаления скомпрометированного и создания нового пользователя.

Действия в случае компрометации ключа электронной подписи пользователя

Ключ электронной подписи пользователя считается скомпрометированным в следующих случаях:

- при утрате устройства с [контейнером ключей](#);
- при утрате дистрибутива ключей, содержащего контейнер ключей;
- при увольнении сотрудника.

В случае компрометации ключа электронной подписи:

- 1 Аннулируйте сертификат ключа проверки электронной подписи, соответствующего скомпрометированному ключу электронной подписи (см. раздел [Аннулирование, приостановление действия, возобновление действия сертификатов](#)).

При этом будет автоматически обновлен список аннулированных сертификатов (CRL).



Примечание. Если были скомпрометированы все ключи пользователя, то в процессе смены ключей вы можете автоматически аннулировать все его сертификаты (см. [Действия в случае компрометации ключей пользователя](#)).

- 2 Передайте обновленный CRL на узлы своей сети (см. [Распространение списков аннулированных сертификатов](#)) и в доверенные сети (см. [Экспорт межсетевой информации](#)).
- 3 Если необходимо, издайте для владельца скомпрометированного ключа новый сертификат (см. раздел [Издание сертификатов](#)).

Действия в случае компрометации ключей администратора УКЦ

Ключи администратора программы ViPNet Удостоверяющий и ключевой центр считаются скомпрометированными в следующих случаях:

- при утрате пароля или [ключей администратора](#);
- при увольнении администратора;
- если посторонние лица получили доступ к компьютеру с УКЦ.



Примечание. Последовательность действий в случае компрометации ключей администратора УКЦ зависит от регламента политики безопасности, принятой в вашей организации.

Если посторонним лицам стал известен ваш пароль, но они не имеют доступа к вашему компьютеру, в этом случае смените пароль администратора и продолжайте свою работу.

Если посторонним лицам стали доступны ваши ключи, то в этом случае для обеспечения безопасности:

- 1 Выполните смену мастер-ключей своей сети (см. [Работа с мастер-ключами](#)).
- 2 Выполните смену межсетевых мастер-ключей (см. [Создание межсетевых мастер-ключей](#)), предварительно согласовав ее с администраторами доверенных сетей.
- 3 Для всех пользователей своей сети сформируйте и передайте новые дистрибутивы ключей. Настоятельно рекомендуем пользователям перед установкой дистрибутивов ключей расшифровать все зашифрованные письма в программе ViPNet Деловая почта. Это позволит предотвратить потерю писем после установки новых дистрибутивов ключей.



Примечание. Если не было установлено факта компрометации резервных наборов персональных ключей пользователей при увольнении администратора сети ViPNet, то политика безопасности организации может разрешать не формировать новые дистрибутивы ключей пользователей, поскольку в данном случае защищенный канал ViPNet не считается скомпрометированным. Тогда вместо дистрибутивов ключей сформируйте новые ключи пользователей и ключи узлов и отправьте их на узлы своей сети.

- 4 Проконтролируйте процесс развертывания новых дистрибутивов на узлах своей сети.

Работа с мастер-ключами

При формировании персональных ключей пользователей, ключей обмена и ключей защиты, входящих в состав ключей узлов, используются соответствующие [мастер-ключи](#):

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

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

Смена мастер-ключей защиты и обмена

Смена мастер-ключей защиты и обмена влечет за собой смену всех ключей в сети ViPNet. Она может быть как плановой, так и внеплановой. Плановая смена мастер-ключей проводится с периодичностью один раз в 15 месяцев (1 год и 3 месяца). Внеплановая смена мастер-ключей производится при компрометации ключей (см. [Действия в случае компрометации ключей](#)).

- Чтобы после смены мастер-ключей все узлы, даже самые удаленные, получили обновления ключей одновременно, выберите в зависимости от размера сети промежуток времени 5-10 дней при отложенной отправке обновлений.
- Проинформируйте всех пользователей и администраторов сети ViPNet о планируемом обновлении ключей и сроках его проведения.
- Рекомендуйте пользователям расшифровать все сообщения программы ViPNet Деловая почта, включая архивные сообщения. После того как на узлах будут установлены ключи, созданные на основе новых мастер-ключей, зашифрованные на старых ключах сообщения невозможно будет прочитать.

После смены мастер-ключей и обновления ключей на узлах пользователи могут зашифровать письма. См. «ViPNet Деловая почта. Руководство пользователя», раздел «Шифрование и расшифрование писем».

- Рекомендуйте пользователям ViPNet SafeDisk-V создать резервную копию ключей контейнера данных. В случае неудачной смены мастер-ключей и установки нового дистрибутива ключей на узле будет возможно восстановить доступ к защищенной информации, находящейся в файле контейнера ViPNet SafeDisk-V, с помощью резервной копии ключей контейнера.

Для смены мастер-ключей:

- 1 В окне программы на панели навигации перейдите в представление **Ключевой центр** и выберите раздел **Моя сеть > Мастер-ключи**.
- 2 Поочередно вызовите контекстное меню мастер-ключа ключей защиты и обмена и выберите пункт **Сменить**.



Примечание. Если произошла компрометация пользователя сети вследствие утраты доверия к его резервному набору персональных ключей (см. [Действия при утрате резервного набора персональных ключей пользователя](#)), то необходимо сменить мастер-ключ персональных ключей. Остальные мастер-ключи в данном случае менять необязательно.

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

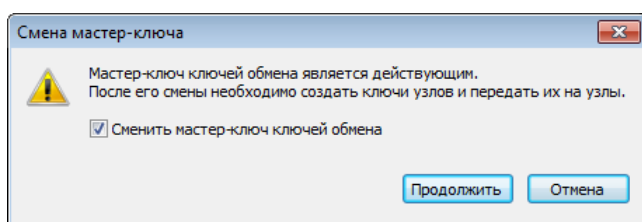


Рисунок 38. Предупреждение при смене мастер-ключа

- 4 В окне ввода пароля введите пароль для учетной записи администратора УКЦ.
В результате будет произведена смена мастер-ключей.

После смены мастер-ключей выполните следующие действия:

- 1 Создайте и передайте в ЦУС ключи для всех узлов (см. [Создание и передача ключей пользователей в ЦУС](#)). Из ЦУСа ключи должны быть отправлены на узлы с отложенной датой применения (см. документ «ViPNet Центр управления сетью. Руководство администратора», главу «Управление сетью ViPNet», раздел «Отправка обновлений на сетевые узлы»).
- При этом обновить ключи путем удаленной отправки ключей из ЦУСа невозможно на сетевых узлах:
- ViPNet Terminal — если используется внешнее устройство для аутентификации пользователя на сетевом узле.
 - ViPNet Coordinator HW — если пароль пользователя был изменен локально и отличается от пароля, заданного в УКЦ.
 - ViPNet Client 4U — если для пользователей задан [минимальный уровень полномочий](#).
 - В этих случаях создайте новые дистрибутивы ключей (см. [Создание дистрибутивов ключей](#)) и передайте их доверенным способом пользователям узлов или администраторам координаторов.
- 2 Совместно с администратором ЦУСа проконтролируйте процесс принятия новых ключей на узлах.

Смена мастер-ключа персональных ключей

Смена мастер-ключей персональных ключей влечет за собой смену всех ключей в сети ViPNet. Она может быть как плановой, так и внеплановой. Плановая смена мастер-ключей персональных ключей проводится с периодичностью один раз в 15 месяцев. Внеплановая смена мастер-ключей персональных ключей производится при компрометации ключей (см. [Действия в случае компрометации ключей](#)).



Внимание! Если при смене мастер-ключа вариант персонального ключа пользователя равен двум и более, создайте для сетевого узла новый дистрибутив ключей (см. [Создание дистрибутивов ключей](#)). Иначе ключи не обновятся по сети через ЦУС, и узел будет недоступен.

Перед сменой мастер-ключей:

- Чтобы после смены мастер-ключей все узлы, даже самые удаленные, получили обновления ключей одновременно, выберите в зависимости от размера сети промежуток времени 5-10 дней при отложенной отправке обновлений.
- Проинформируйте всех пользователей и администраторов сети ViPNet о планируемом обновлении ключей и сроках его проведения.
- Рекомендуйте пользователям расшифровать все сообщения программы ViPNet Деловая почта, включая архивные сообщения. После того как на узлах будут установлены ключи, созданные на основе новых мастер-ключей, зашифрованные на старых ключах сообщения невозможно будет прочитать.

После смены мастер-ключей и обновления ключей на узлах пользователи могут зашифровать письма. См. «ViPNet Деловая почта. Руководство пользователя», раздел «Шифрование и расшифрование писем».

- Рекомендуйте пользователям ViPNet SafeDisk-V создать резервную копию ключей контейнера данных. В случае неудачной смены мастер-ключей и установки нового дистрибутива ключей на узле будет возможно восстановить доступ к защищенной информации, находящейся в файле контейнера ViPNet SafeDisk-V, с помощью резервной копии ключей контейнера.

Для смены мастер-ключа персональных ключей:

- 1 В окне программы на панели навигации перейдите в представление **Ключевой центр** и выберите раздел **Моя сеть > Мастер-ключи**.
- 2 Щелкните мастер-ключ персональных ключей правой кнопкой мыши и в контекстном меню выберите пункт **Сменить**.



Примечание. Если произошла компрометация пользователя сети вследствие утраты доверия к его резервному набору персональных ключей (см. [Действия при утрате резервного набора персональных ключей пользователя](#)), то необходимо сменить мастер-ключ персональных ключей. Остальные мастер-ключи в данном случае менять необязательно.

- 3 В появившемся окне с сообщением о смене мастер-ключа установите флажок **Сменить мастер-ключ персональных ключей** и нажмите кнопку **Продолжить**.

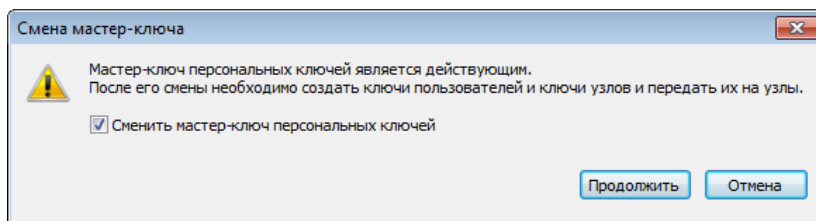


Рисунок 39. Предупреждение при смене мастер-ключа персональных ключей

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

После смены мастер-ключа персональных ключей выполните обновление ключей одним из способов:

- Создайте и передайте новые ключи по сети через ЦУС согласно документу «ViPNet Administrator. Руководство по смене мастер-ключей в сети ViPNet», раздел «Обновление ключей узлов», если этот способ не противоречит правилам безопасности вашей организации.
- Если по правилам безопасности вам требуется передавать новые ключи доверенным способом, создайте и передайте новые ключи в порядке, указанном ниже.

Чтобы обновить ключи доверенным способом:

- 1 Создайте новые ключи для всех пользователей и сохраните их на диск.
- 2 Создайте ключи для всех узлов и сохраните их на диск.
- 3 Создайте новые дистрибутивы ключей для сетевых узлов:
 - ViPNet Terminal — если используется внешнее устройство для аутентификации пользователя на сетевом узле;
 - ViPNet Coordinator HW;
 - ViPNet Client for Android или ViPNet Client for iOS.
- 4 Передайте новые ключи или дистрибутивы ключей пользователям сетевых узлов доверенным способом.
 - 4.1 На сетевых узлах с ViPNet Client for Windows необходимо поместить файлы с ключами пользователя `abn_XXXX.ke` и с ключами узла `apn_XXXX.ke` (где XXXX — шестнадцатеричный идентификатор узла в сети) по следующему пути:
 - при использовании программы ViPNet Client for Windows версии ниже 4.5.1 — в папку установки программы в подпапку `\CCC\key\`;
 - при использовании программы ViPNet Client for Windows версии 4.5.1 и выше — в транспортный каталог `C:\ProgramData\Infotecs\<папка с идентификатором узла>\`.
 - 4.2 Затем пользователю необходимо перезапустить программу ViPNet Client.



Примечание. Убедитесь, что ключи пользователей, созданные после смены мастер-ключа персональных ключей, установлены на сетевых узлах. До этих пор не рекомендуется повторно создавать ключи пользователей и передавать их на узлы, так как это приведет к ошибке обновления ключей на узле.

5

Просмотр и изменение свойств объектов сети ViPNet

Задание способа аутентификации пользователя	94
Просмотр свойств пользователя	98
Просмотр свойств сетевого узла	100
Просмотр свойств группы узлов	101

Задание способа аутентификации пользователя

При добавлении пользователя в сеть ViPNet в программе ViPNet Удостоверяющий и ключевой центр требуется задать способ его аутентификации на узле. Способ аутентификации можно указать при создании дистрибутива ключей (см. [Создание дистрибутивов ключей](#)), если это было задано в настройках программы (см. [Настройка параметров создания дистрибутивов ключей](#)), или в свойствах пользователя. По умолчанию для пользователей задан способ аутентификации по паролю. Впоследствии заданный способ аутентификации может быть изменен вами либо пользователем в ПО ViPNet, установленном на сетевом узле, при наличии соответствующих полномочий.

В программе предусмотрены следующие способы аутентификации:

- **Пароль.** Для входа в программу пользователю требуется вводить пароль. Каждый раз после ввода пароля вычисляется парольный ключ, который используется для доступа к персональному ключу пользователя.

При первом входе в ПО ViPNet пользователю потребуется вводить тот [пароль](#), который вы задали для него в УКЦ. Данный пароль совпадает с паролем к дистрибутиву ключей. Впоследствии пользователь может сменить пароль.

- **Устройство (персональный ключ).** Для входа в программу пользователю требуется подключить внешнее устройство, на котором сохранен персональный ключ пользователя, и ввести ПИН-код. При настройке данного способа аутентификации администратор УКЦ должен располагать внешним устройством пользователя, на котором сохранен персональный ключ пользователя или его ключи электронной подписи. Способ аутентификации по персональному ключу имеет следующие ограничения:
 - Одно внешнее устройство невозможно использовать для аутентификации нескольких пользователей ViPNet.
 - Одно внешнее устройство невозможно использовать для аутентификации одного пользователя на нескольких узлах ViPNet.
 - Если используется этот способ аутентификации, тогда ключи электронной подписи пользователя, созданные в УКЦ, настоятельно рекомендуется хранить на одном устройстве с персональным ключом.

- **Устройство (сертификат).** Для входа в программу пользователю требуется подключить внешнее устройство, на котором сохранен сертификат, и ввести ПИН-код.

Для аутентификации по сертификату пользователь может использовать сертификат, изданный в стороннем удостоверяющем центре по различным алгоритмам. Контейнер ключей при этом должен быть сохранен на внешнем устройстве, которое поддерживает стандарт PKCS#11, в том числе операции подписи и шифрования. Кроме этого, если требуется выполнять аутентификацию по сертификату, изданному в соответствии с алгоритмом ГОСТ, следует использовать устройство с аппаратной поддержкой криптографического алгоритма ГОСТ.

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

Для аутентификации может использоваться сертификат, изданный своим или сторонним удостоверяющим центром, при этом должны выполняться следующие условия:

- Сертификат должен быть действительным.
- В системное хранилище Windows на компьютере администратора УКЦ должны быть установлены сертификат издателя и актуальный список аннулированных сертификатов (CRL).
- Для сертификата в расширении «Использование ключа» должен быть указан параметр «Шифрование ключей», в расширении «Расширенное использование ключа» — параметр «Проверка подлинности клиента».

Чтобы задать или изменить способ аутентификации пользователя:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Пользователи**.
- 2 В списке на панели просмотра выберите пользователя, для которого требуется задать способ аутентификации, и дважды щелкните его учетную запись.
- 3 В окне свойств пользователя перейдите на вкладку **Аутентификация**.

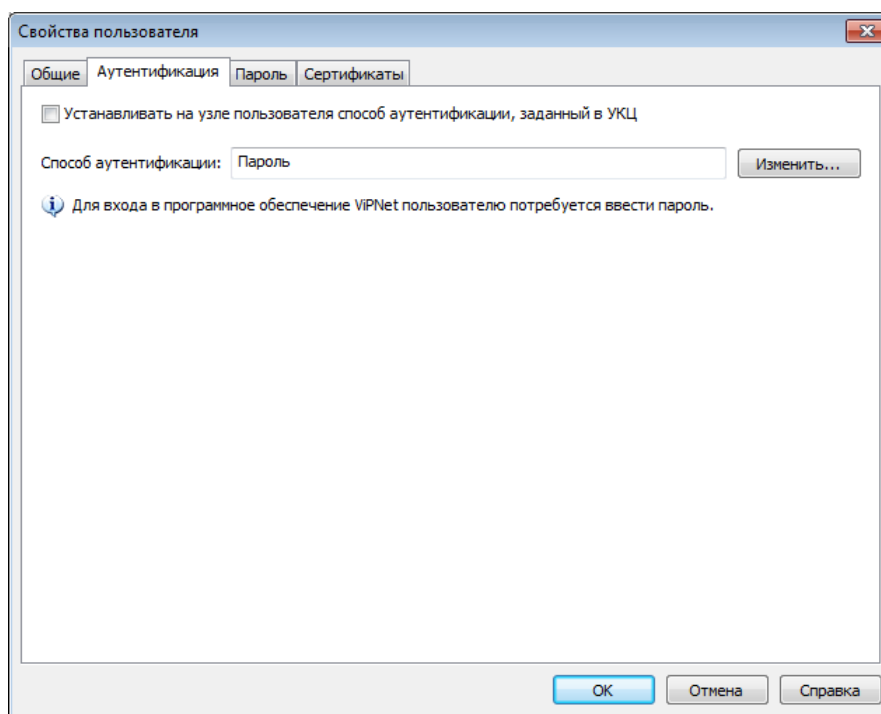


Рисунок 40. Задание способа аутентификации пользователя

- 4 Нажмите кнопку **Изменить** и в появившемся окне в списке **Способ аутентификации** выберите нужный способ.
- 5 При выборе одного из способов аутентификации с помощью устройства выполните следующие действия:
 - 5.1 Подключите внешнее устройство (см. [Внешние устройства](#)), на которое будет записан парольный или персональный ключ пользователя либо на котором в контейнере ключей хранится сертификат для аутентификации пользователя на узле. В последнем случае внешнее устройство хранения данных должно поддерживать стандарт PKCS#11, в том числе операции подписи и шифрования.
 - 5.2 В окне **Настройка способа аутентификации** в соответствующем списке выберите способ аутентификации:
 - **Устройство (сертификат)** — чтобы задать способ аутентификации с помощью сертификата пользователя, хранящегося на устройстве. В списке сертификатов, обнаруженных на устройстве, выберите нужный сертификат.
 - **Устройство (персональный ключ)** — чтобы задать способ аутентификации с помощью персонального ключа пользователя.
 - 5.3 В соответствующем списке выберите устройство.
 - 5.4 Введите ПИН-код, если требуется (необходимость ввода ПИН-кода зависит от типа используемого внешнего устройства). Нажмите кнопку **ОК**.

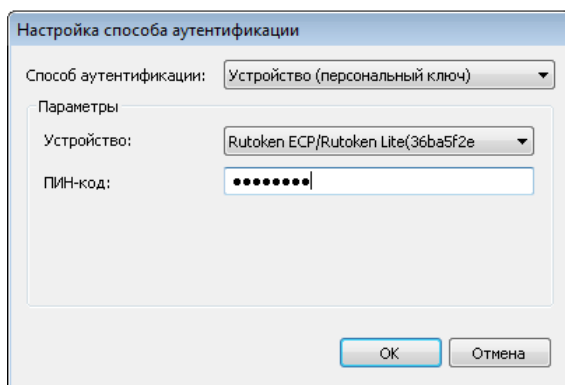


Рисунок 41. Настройка аутентификации с помощью устройства

- 6 При выборе способа аутентификации **Сертификат** выполните следующие действия:
 - 6.1 Нажмите кнопку **Выбрать сертификат** и укажите сертификат, который будет использоваться пользователем при аутентификации.
 - 6.2 Нажмите кнопку **ОК**.

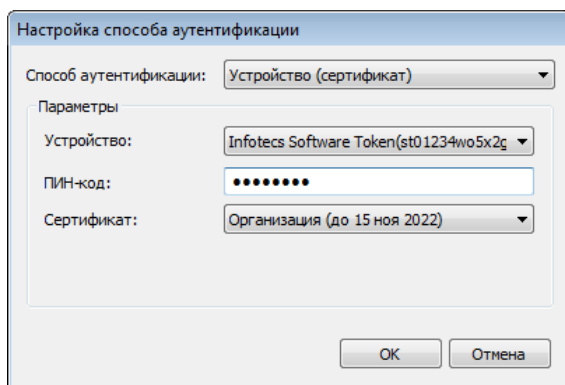


Рисунок 42. Настройка аутентификации по сертификату

- 7 Если вы изменили способ аутентификации пользователя и хотите, чтобы заданный способ вступил в действие при обработке ключей узла пользователя, на вкладке **Аутентификация** установите соответствующий флажок сверху окна. Тогда в случае отличия способа аутентификации пользователя на узле от заданного в УКЦ, он будет изменен при входе в программу.



Внимание! При изменении способа аутентификации сообщите об этом пользователю. Кроме этого, предоставьте пользователю все необходимые данные для успешной аутентификации (парольную информацию, устройство или сертификат).

Впоследствии не снимайте этот флажок, если при обработке ключей узла пользователя требуется контролировать соответствие между способом аутентификации, который используется на узле, и способом, заданным в УКЦ.



Совет. Чтобы пользователи узла не могли изменять способ аутентификации, можно воспользоваться понижением их полномочий в программе ViPNet Центр управления сетью. См. документ «ViPNet Центр управления сетью. Руководство администратора», раздел «Изменение уровня полномочий пользователя». В таком случае также не следует сообщать пользователям пароль администратора сетевого узла (см. [Сохранение паролей администраторов сетевых узлов](#)).

- 8 По завершении действий нажмите кнопку **OK**.

Просмотр свойств пользователя

Чтобы просмотреть сведения о пользователях вашей сети:

- 1 В окне программы перейдите в представление **Ключевой центр** и выберите раздел **Моя сеть > Пользователи**.
- 2 В списке на панели просмотра дважды щелкните учетную запись пользователя, сведения о котором вы хотите просмотреть.
- 3 В окне просмотра свойств пользователя ознакомьтесь с информацией на следующих вкладках:
 - **Общие** — содержит имя и идентификатор пользователя (идентификатор автоматически формируется в программе ViPNet Центр управления сетью), текущий **вариант персонального ключа пользователя**, а также список сетевых узлов, на которых данный пользователь зарегистрирован.

Вы можете распечатать персональную информацию о пользователе — содержимое данной вкладки — с помощью кнопки **Печать**, а также сохранить эту информацию в файле на компьютере или внешнем устройстве с помощью кнопки **Сохранить в файле**.

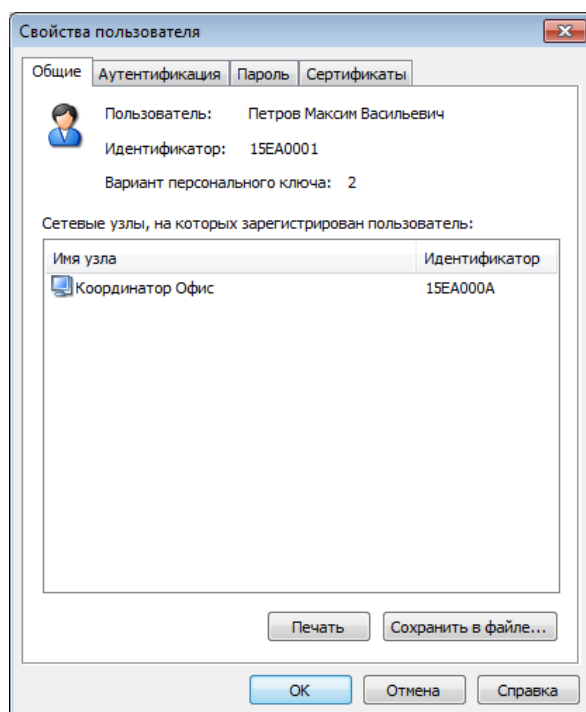


Рисунок 43. Просмотр общей информации о пользователе сети ViPNet

- **Аутентификация** — содержит информацию о заданном способе аутентификации пользователя (см. **Задание способа аутентификации пользователя**). Вы можете изменить способ аутентификации пользователя с помощью кнопки **Изменить**.
- **Пароль** — содержит информацию о заданном пароле пользователя. При необходимости вы можете с помощью соответствующих кнопок сменить пароль (см. **Смена паролей пользователей ViPNet**) или выдать его пользователю (см. **Выдача паролей пользователей**).

в файле или распечатанным на ПИН-конверте (зависит от способа передачи, указанного в настройках программы в разделе **Пароли**).

- **Сертификаты.** На данной вкладке имеется флажок, с помощью которого вы можете выполнить настройку создания ключей подписи и издания сертификатов для пользователя (см. [Настройка создания ключа электронной подписи и ключа проверки электронной подписи для пользователей сети ViPNet](#)), а также список изданных сертификатов пользователя. В списке сертификатов указан сертификат издателя (под заголовком **Издатель:**), дата издания сертификата и его срок действия, а также значком  отмечен сертификат, изданный последним. При необходимости вы можете аннулировать выбранный сертификат пользователя, нажав соответствующую кнопку. Подробнее см. в разделе [По инициативе администратора УКЦ](#).

Просмотр свойств сетевого узла

Чтобы посмотреть сведения об узлах вашей сети:

- 1 В окне программы на панели навигации в представлении **Ключевой центр** выберите раздел **Моя сеть > Сетевые узлы**.
- 2 В списке на панели просмотра дважды щелкните сетевой узел, сведения о котором вы хотите просмотреть.
- 3 В окне просмотра свойств сетевого узла ознакомьтесь с информацией на следующих вкладках:
 - **Общие** — содержит имя и идентификатор сетевого узла (идентификатор автоматически формируется в программе ViPNet Центр управления сетью), используемый в настоящий момент вариант **ключей узла**, а также список пользователей, зарегистрированных на данном узле.

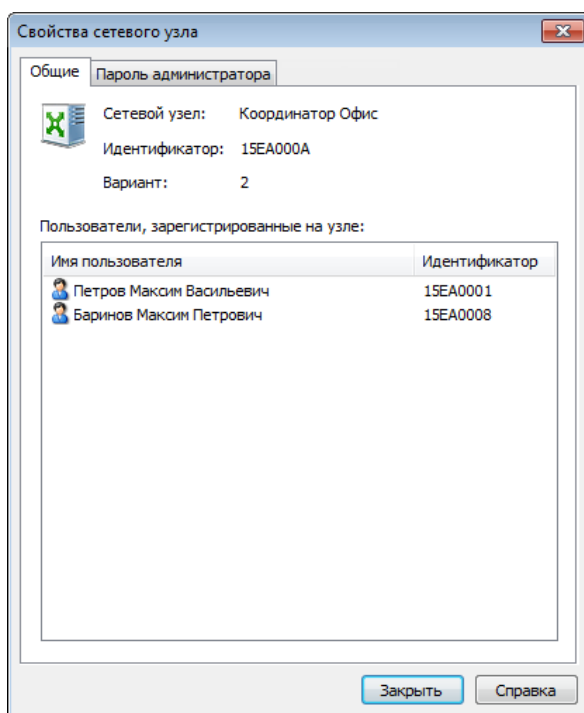


Рисунок 44. Просмотр общей информации об узле

- **Пароль администратора** — содержит сведения о пароле администратора сетевого узла ViPNet.

Если пароль не был создан, вы можете создать его с помощью кнопки **Создать пароль**. Если пароль уже создан, при необходимости вы можете его сменить (см. [Создание и смена пароля администратора сетевого узла или группы узлов](#)) или сохранить в файле (см. [Сохранение паролей администраторов сетевых узлов](#)).



Примечание. При необходимости пароль администратора сетевого узла ViPNet можно удалить (см. [Сброс пароля администратора сетевого узла](#)).

Просмотр свойств группы узлов

Чтобы просмотреть сведения о [группах узлов, сформированных в вашей сети](#):

- 1 В окне программы на панели навигации в представлении **Ключевой центр** выберите раздел **Моя сеть > Группы узлов**.
- 2 В списке на панели просмотра дважды щелкните группу, сведения о которой вы хотите просмотреть.
- 3 В окне просмотра свойств группы узлов ознакомьтесь с информацией на следующих вкладках:
 - **Общие** – содержит имя и идентификатор группы узлов (идентификатор автоматически формируется в программе ViPNet Центр управления сетью), а также список зарегистрированных в данной группе узлов.

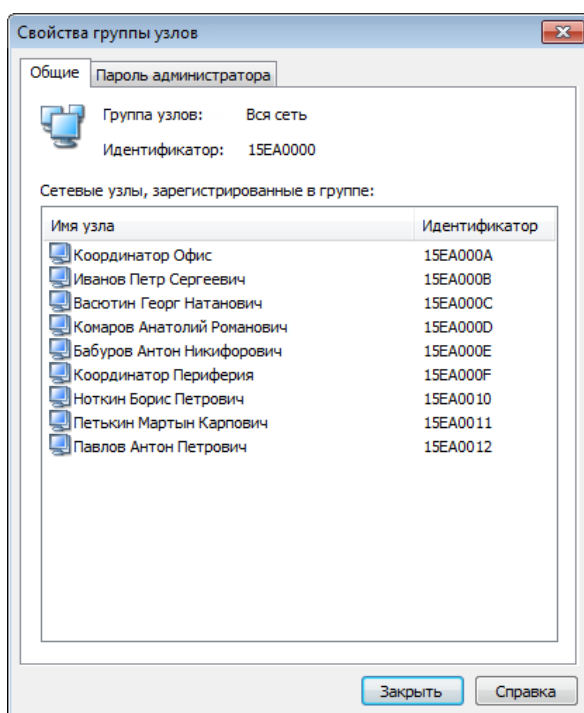


Рисунок 45. Общие свойства группы узлов

- **Пароль администратора** — содержит сведения о пароле администратора группы узлов. Если пароль не был создан, вы можете создать его с помощью кнопки **Создать пароль**. Если пароль уже создан, при необходимости вы можете его сменить (см. [Создание и смена пароля администратора сетевого узла или группы узлов](#)) или сохранить в файле (см. [Сохранение паролей администраторов сетевых узлов](#)).

6

Управление паролями пользователей и администраторов сетевых узлов ViPNet

Смена паролей пользователей ViPNet	103
Выдача паролей пользователей	105
Создание и смена пароля администратора сетевого узла или группы узлов	110
Сброс пароля администратора сетевого узла	113
Сохранение паролей администраторов сетевых узлов	115
Настройка оповещений об истечении срока действия паролей администраторов сетевых узлов и групп узлов	116
Настройка типа создаваемых паролей	118

Смена паролей пользователей ViPNet

В целях безопасности в сети ViPNet рекомендуется осуществлять периодическую смену паролей пользователей. Смена пароля осуществляется самим пользователем средствами имеющегося на его сетевом узле программного обеспечения ViPNet.

Администратор программы ViPNet Удостоверяющий и ключевой центр может средствами программы рекомендовать пользователю осуществить смену пароля. В этом случае после отправки новых ключей пользователю на его сетевом узле отобразится предупреждение о необходимости сменить пароль.

Чтобы рекомендовать пользователю осуществить смену пароля:

- 1 В окне программы на панели навигации в представлении **Ключевой центр** выберите раздел **Моя сеть > Пользователи**.
- 2 В списке пользователей на панели просмотра выберите пользователя, для которого требуется сменить пароль. Если требуется сменить пароль одновременно для нескольких пользователей, то выберите нескольких пользователей.
- 3 Выполните одно из следующих действий:
 - В контекстном меню пользователя (пользователей) выберите пункт **Пароль > Сменить**.
 - Дважды щелкните учетную запись пользователя и в окне свойств пользователя на вкладке **Пароль** нажмите кнопку **Сменить пароль**.
- 4 В появившемся окне подтвердите смену пароля пользователя (пользователей), нажав кнопку **Да**.
- 5 В зависимости от типа пароля, выбранного в качестве используемого по умолчанию при задании новых паролей в настройках программы (см. [Настройка типа создаваемых паролей](#)), выполните одно из действий:
 - Если в настройках выбран тип **Собственный пароль**, в появившемся окне **Пароль пользователя** задайте пароль и нажмите кнопку **ОК**.
 - Если в настройках выбран тип **Случайный пароль на основе парольной фразы**, будет запущено автоматическое создание пароля. Появится электронная рулетка, если она еще не запускалась в рамках текущего сеанса работы программы. Поводите указателем в пределах окна **Электронная рулетка**. Дождитесь завершения создания пароля.
- 6 В УКЦ для пользователей, пароли которых были изменены, создайте новые ключи (см. [Создание и передача ключей пользователей в ЦУС](#)).
- 7 После создания передайте новые ключи в ЦУС для отправки пользователям.

После того как новые ключи пользователя (пользователей) будут получены и приняты на сетевом узле, в течение часа появится информационное сообщение о том, что в соответствии с политиками

безопасности сети ViPNet пароль недействителен, и его необходимо сменить. Пользователь сможет сменить пароль непосредственно из окна информационного сообщения. Новый пароль будет сформирован в соответствии с параметрами, заданными в настройках параметров безопасности программного обеспечения ViPNet на сетевом узле.

Внимание! Несмотря на то, что был создан новый пароль, который отображается в окне просмотра свойств данного пользователя (см. [Просмотр свойств пользователя](#)), пользователь будет продолжать входить в программу по своему старому паролю либо по новому паролю, который пользователь задаст сам в соответствии с рекомендацией сменить пароль.

Новый пароль, отображаемый в окне просмотра свойств пользователя, будет использован для аутентификации в программе только в случае повторного создания дистрибутивов (см. [Создание дистрибутивов ключей](#)) для данного пользователя.



После смены пароля пользователя программное обеспечение ViPNet, установленное на его сетевом узле, обратится к файлу резервного набора персональных ключей (файл *.pk) (см. [Создание и сохранение резервных наборов персональных ключей в файл](#)) для его перешифровки на новом пароле. Если в этот момент файл не будет найден, перешифрование не будет произведено и файл станет недоступным для использования.

В результате, если в будущем произойдет компрометация ключей пользователя, будет невозможно выслать пользователю новые ключи дистанционно, и придётся формировать для него новый дистрибутив ключей.

Выдача паролей пользователей

При создании дистрибутива ключей (см. [Создание дистрибутивов ключей](#)) задается пароль пользователя ViPNet. Пароль должен быть выдан пользователю вместе с дистрибутивом ключей после его создания или при необходимости в других случаях.

Вы можете выдать пароль пользователю в электронном виде – в файле, либо в распечатанном виде – на специальном ПИН-конверте. Способ выдачи пароля пользователю задается в настройках программы.

ПИН-конверты представляют собой бумажные конверты с несколькими слоями и запечатанной секретной частью, в которой содержится конфиденциальная информация (пароль пользователя). Выдача пароля в ПИН-конверте позволяет исключить доступ к паролю посторонних лиц, поэтому данный способ выдачи является рекомендуемым. При выдаче паролей в файлах по требованиям безопасности вы должны обеспечить их защиту самостоятельно с помощью организационных мер.

По завершении формирования дистрибутива ключей пароль пользователя автоматически сохраняется в файл или отправляется на печать, в зависимости от того, какой способ выдачи пароля указан в настройках. Если вам требуется выдать пароль одному или нескольким пользователям ViPNet повторно, выполните следующие действия:

- 1 Убедитесь, что в настройках программы указан нужный вам способ выдачи пароля пользователю (см. [Настройка способа выдачи паролей пользователей](#)).
- 2 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Пользователи**.
- 3 В списке на панели просмотра выберите одну или несколько учетных записей пользователей, которым требуется выдать пароли, щелкните их правой кнопкой мыши и в контекстном меню выберите пункт **Пароль > Выдать**.
- 4 В окне подтверждения операции нажмите кнопку **Продолжить**.

В зависимости от того, какой способ выдачи задан в настройках, пароли пользователей будут сохранены в файлах *.xps в указанной папке либо отправлены на печать с использованием указанного принтера.

Для просмотра файлов с паролями пользователей используется программа Средство просмотра XPS. Если просмотр файлов с паролями недоступен, ознакомьтесь с разделом [Не удается посмотреть пароль, сохраненный в файле](#).



Примечание. Вы также можете выдать пароль из окна свойств пользователя на вкладке **Пароль**.

Настройка способа выдачи паролей пользователей

Для задания способа выдачи паролей пользователям ViPNet:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Пароли** и укажите один из способов выдачи пароля:
 - Для выдачи паролей в файлах установите переключатель в положение **Сохранять пароль в файл XPS в папку** и укажите папку, в которой будут сохраняться файлы с паролями.
 - Для выдачи паролей в распечатанном виде установите переключатель в положение **Печатать пароль на принтере** и в списке принтеров выберите принтер, который будет использоваться для печати.

После этого распечатайте тестовую страницу с помощью кнопки **Тестовая печать**. Если при тестовой печати данные были расположены на ПИН-конверте неверно, выполните калибровку принтера как описано в разделе [Настройка печати паролей пользователей](#).

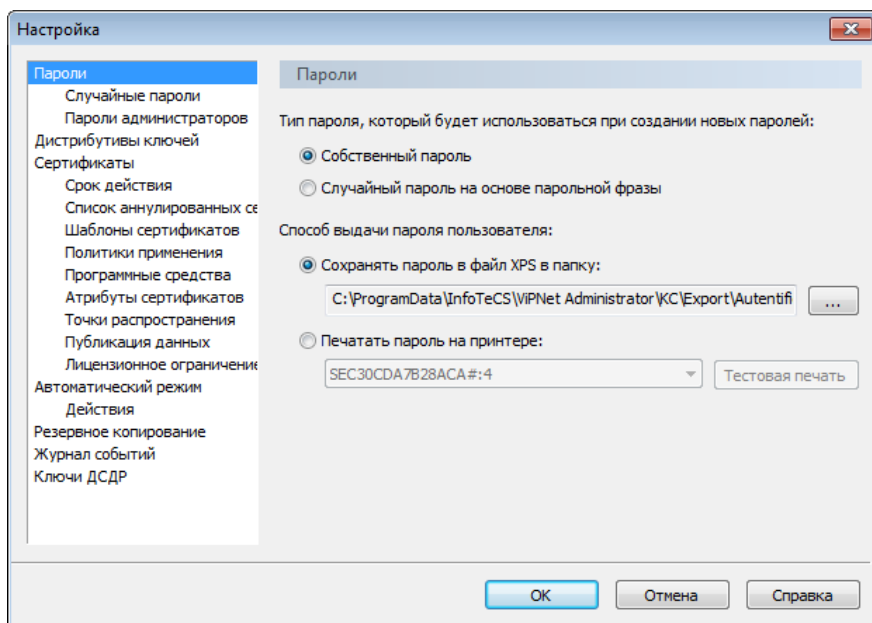


Рисунок 46. Настройка способа выдачи паролей пользователей

- 3 Для сохранения настроек нажмите кнопку **ОК**.

Настройка печати паролей пользователей

Вы можете распечатывать пароли пользователей, созданные в программе ViPNet Удостоверяющий и ключевой центр, на специальных ПИН-конвертах. Для печати паролей пользователей могут

использоваться разные типы ПИН-конвертов. По умолчанию в программе ViPNet Удостоверяющий и ключевой центр настроена печать паролей на стандартных четырехслойных ПИН-конвертах с расширенным полем для секретной информации.



Совет. Для печати паролей на ПИН-конвертах рекомендуется использовать специализированные принтеры для печати ПИН-конвертов или аналогичные матричные принтеры модели OKI ML5100FB.

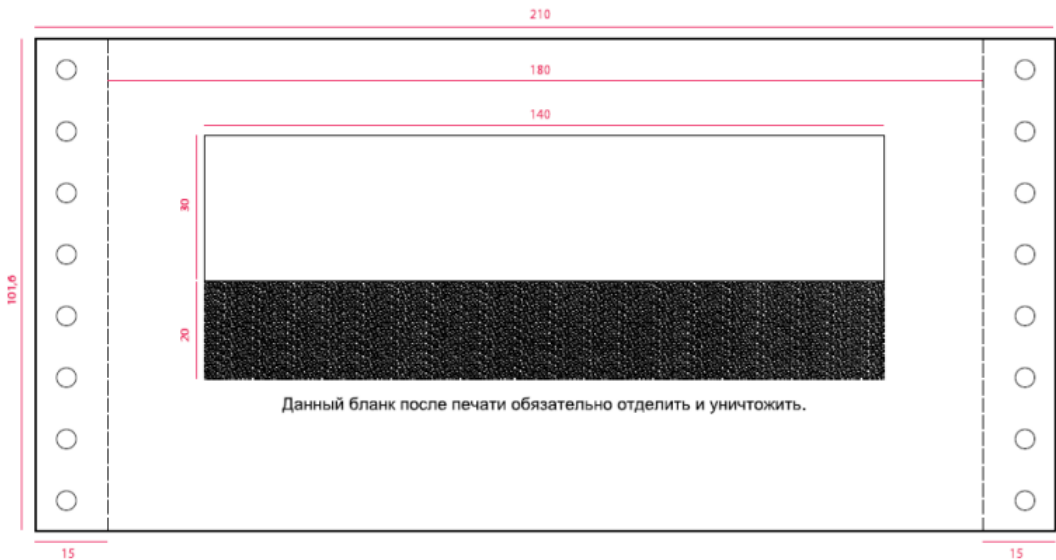


Рисунок 47. Внешний вид стандартного ПИН-конверта, размеры указаны в миллиметрах

Если вы будете использовать ПИН-конверты другого типа, выполните калибровку принтера, иначе данные могут располагаться на ПИН-конверте неверно. Для калибровки выполните следующие действия:

- 1 Откройте файл C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\ini\envelope.ini.
- 2 Отрегулируйте значения следующих параметров ПИН-конвертов:

Название параметра	Описание	Единица измерения	Значение по умолчанию	Примечание
EnvelopeHeight	Высота конверта	мм	102	Минимальное значение — 80 Максимальное значение — 250
EnvelopeWidth	Ширина конверта	мм	210	Минимальное значение — 110 Максимальное значение — 355
HeightAdjustment	Корректировка расположения информации по высоте	мм	4	Минимальное значение — -40 Максимальное значение — 40

Название параметра	Описание	Единица измерения	Значение по умолчанию	Примечание
PINAreaHeight	Высота закрытой области печати	мм	20	Минимальное значение — 10 Максимальное значение равно высоте конверта
PINAreaWidth	Ширина закрытой области печати	мм	140	Минимальное значение — 20 Максимальное значение равно ширине конверта
PINAreaLeftCornerX	Координаты левого нижнего угла закрытой области печати по оси X (горизонтальной оси)	мм	35	Минимальное значение — 0 Максимальное значение равно ширине конверта
PINAreaLeftCornerY	Координаты левого нижнего угла закрытой области печати по оси Y (по вертикальной оси)	мм	32	Минимальное значение — 0 Максимальное значение равно высоте конверта
PINAreaFontSize	Размер шрифта закрытой области печати	пт	13	Минимальное значение — 5 Максимальное значение — 16
PINAreaPhraseFontSize	Размер шрифта парольной фразы, если таковая есть, в закрытой области ПИН-конверта	пт	13	Минимальное значение — 5 Максимальное значение — 16
TextFieldHeight	Высота открытой области печати	мм	30	Минимальное значение — 10 Максимальное значение равно высоте конверта
TextFieldWidth	Ширина открытой области печати	мм	140	Минимальное значение — 50 Максимальное значение равно ширине конверта
TextFieldLeftCornerX	Координаты левого нижнего угла открытой области печати по оси X (по горизонтальной оси)	мм	35	Минимальное значение — 0 Максимальное значение равно ширине конверта

Название параметра	Описание	Единица измерения	Значение по умолчанию	Примечание
TextFieldLeftCornerY	Координаты левого нижнего угла открытой области печати по оси Y (по вертикальной оси)	мм	52	Минимальное значение — 0 Максимальное значение равно высоте конверта
TextFieldFontSize	Размер шрифта открытой области печати	пт	13	Минимальное значение — 5 Максимальное значение — 16
TextDescriptionFieldFontSize	Размер шрифта подсказки, кем был выдан ПИН-конверт, в открытой области ПИН-конверта	пт	10	Минимальное значение — 5 Максимальное значение — 16



Примечание. Значения параметров не должны выходить за указанные пределы. Если для какого-либо параметра будет установлено значение больше максимального или меньше минимального, то значение будет автоматически изменено на максимальное или минимальное соответственно.

- 3 Сохраните изменения и закройте файл.
- 4 Для проверки измененных значений параметров ПИН-конвертов выполните тестовую печать. Для этого в настройках программы в разделе **Пароли** нажмите кнопку **Тестовая печать**.



Примечание. В процессе работы с принтером при переключении режима подачи бумаги с ленточной на одиночную (или наоборот) необходимо проводить повторную калибровку принтера, иначе данные на ПИН-конвертах будут расположены неверно.

Создание и смена пароля администратора сетевого узла или группы узлов

Пользователи сети ViPNet могут выполнять расширенные настройки программного обеспечения ViPNet, установленного на их сетевых узлах. Для входа в режим расширенных настроек требуется ввести [пароль администратора сетевого узла ViPNet](#). При работе в данном режиме все ограничения, накладываемые уровнем полномочий пользователя, снимаются.



Внимание! Без ввода пароля администратора получить доступ к дополнительным настройкам ПО ViPNet на сетевом узле невозможно.

Пароль администратора каждого сетевого узла задается в программе ViPNet Удостоверяющий и ключевой центр. При этом он может быть задан одним из двух способов:

- Индивидуально для отдельного сетевого узла.
- Для узлов, входящих в [группу узлов](#), заданную в программе ViPNet Центр управления сетью. В этом случае для всех узлов группы создается одинаковый пароль администратора. Если узел входит в несколько групп узлов, для каждой группы можно создать отдельный пароль администратора.

На сетевом узле в качестве пароля администратора можно использовать как пароль, заданный индивидуально для данного узла, так и пароли, заданные для групп узлов, в которые входит данный узел. Вы можете разграничить доступ лиц, осуществляющих настройки ПО ViPNet на сетевых узлах, сообщая им только пароли, которые соответствуют уровню их полномочий и позволяют им управлять дополнительными настройками ПО ViPNet только на тех узлах, для которых это требуется.



Примечание. При создании сети ViPNet в ЦУСе автоматически создается группа «Вся сеть», в которую входят все узлы данной сети ViPNet. При первом запуске УКЦ в обязательном порядке задается пароль администратора сетевых узлов группы «Вся сеть».

Для создания или смены пароля администратора сетевого узла:

- 1 Выполните одно из действий:
 - Чтобы создать или изменить пароль администратора для отдельного сетевого узла, в представлении **Ключевой центр** выберите раздел **Моя сеть > Сетевые узлы** и в списке на панели просмотра дважды щелкните нужный сетевой узел. Откроется окно **Свойства сетевого узла** (см. [Просмотр свойств сетевого узла](#)).

- Чтобы создать или изменить пароль для узлов, входящих в группу узлов, в представлении **Ключевой центр** выберите раздел **Моя сеть > Группы узлов** и в списке на панели просмотра дважды щелкните нужную группу. Откроется окно **Свойства группы узлов** (см. [Просмотр свойств группы узлов](#)).
- 2 В зависимости от того, создается ли пароль заново, на вкладке **Пароль администратора** выполните одно из действий:
- Если пароль создается впервые, нажмите кнопку **Создать пароль**.
 - Если пароль уже был создан ранее, он будет отображаться на вкладке. Для смены пароля нажмите кнопку **Сменить пароль**.
- 3 В окне **Пароль администратора** задайте тип нового пароля:
- **Собственный** — пароль, задаваемый вами вручную. Пароль данного типа должен включать в себя не менее 8 символов.
 - **На основе парольной фразы** — [пароль, формируемый автоматически на основе парольных фраз](#) согласно параметрам, заданным в настройках программы (см. [Настройка параметров случайных паролей](#)).

После этого в зависимости от выбранного типа пароля, выполните соответствующие действия:

- Если вы выбрали тип пароля **Собственный**, задайте и подтвердите пароль.
- Если вы выбрали тип пароля **На основе парольной фразы**, появится электронная рулетка, если она еще не запускалась в рамках текущего сеанса работы программы. Поводите указателем в пределах окна **Электронная рулетка**.

Если вы выбрали тип пароля **На основе парольной фразы**, то появится автоматически сформированный пароль с парольной фразой, помогающей запомнить пароль.

При необходимости измените параметры или длину случайного пароля на основе парольной фразы с помощью кнопки **Свойства**, после чего создайте другой пароль, нажав кнопку **Другой**.



Совет. Рекомендуется задавать сложные пароли, в состав которых входят буквы в разных регистрах, цифры и специальные символы.

Рисунок 48. Изменение пароля администратора сетевого узла

- 4 В группе **Срок действия** задайте срок действия создаваемого пароля.
- 5 Нажмите кнопку **ОК**.

В результате пароль администратора сетевого узла или группы узлов будет изменен (либо задан впервые).

- 6 Сформируйте ключи узлов (см. [Создание и передача ключей узлов в ЦУС](#)) и отправьте их на сетевые узлы, для которых был создан пароль администратора.



Внимание! После получения новых ключей на сетевом узле старый пароль администратора данного сетевого узла станет недействительным.

Сброс пароля администратора сетевого узла

Если в сети ViPNet вы перешли на использование программного обеспечения ViPNet Administrator 4.x, выполнив конвертацию базы данных программ ViPNet Центр управления сетью 3.2.x и ViPNet Удостоверяющий и ключевой центр 3.2.x, то в УКЦ могут появиться искаженные или недействительные пароли администраторов сетевых узлов. По этой причине создание ключей для этих узлов будет невозможно, и при каждой проверке текущих данных (в том числе при запуске программы) будут появляться соответствующие сообщения об ошибках (см. [Проверка текущих данных](#)).

Чтобы вы смогли создать ключи для данных узлов, следует сменить или удалить пароли. Сменить пароль администратора можно для конкретного узла или группы узлов, заданной в программе ViPNet Центр управления сетью. См. раздел [Создание и смена пароля администратора сетевого узла или группы узлов](#). Если вы не хотите формировать новые пароли администраторов сетевых узлов, то рекомендуется удалить их текущие пароли. Удалить пароли администраторов вы можете одновременно для нескольких выборочных узлов.



Внимание! Стоит учесть, что без пароля администратора на сетевом узле невозможно выполнить расширенные настройки ПО ViPNet.

Для удаления (сброса) пароля администратора сетевого узла:

- 1 В окне программы на панели навигации в представлении **Ключевой центр** выберите раздел **Моя сеть > Сетевые узлы**.
- 2 В списке сетевых узлов выберите узел, пароль администратора которого нужно сбросить. При необходимости выберите несколько сетевых узлов.
- 3 Щелкните узел правой кнопкой мыши и в контекстном меню выберите пункт **Пароль администратора > Сбросить**.
- 4 В появившемся окне подтвердите сброс пароля администратора выбранного сетевого узла. Если вы выбрали несколько сетевых узлов и не уверены, что все из них имеют искаженные или недействительные пароли администраторов, то в данном окне установите флажок **Применить только к недействительным паролям**. В результате будут сброшены только недействительные и искаженные пароли, действующие пароли администраторов будут сохранены.

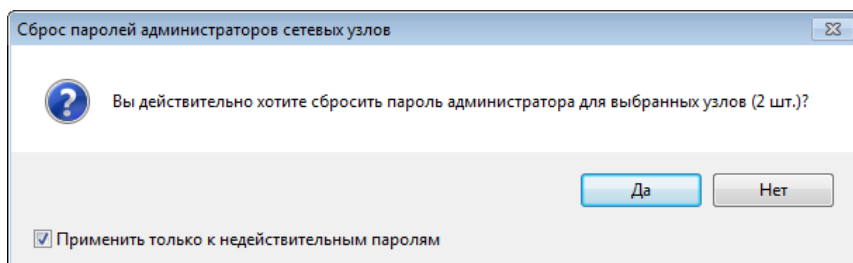


Рисунок 49. Подтверждение сброса паролей администраторов сетевых узлов

- 5 Если вы хотите, чтобы пароль администратора был удален на сетевом узле, сформируйте и отправьте новые ключи для данного узла (см. [Создание и передача ключей узлов в ЦУС](#)).

Сохранение паролей администраторов сетевых узлов

При необходимости (например, если нужно выполнить дополнительные настройки ПО ViPNet на сетевых узлах) вы можете сохранить пароли администраторов сетевых узлов или групп узлов в файл.



Внимание! Файлы с сохраненными паролями необходимо хранить в безопасном месте (например, на съемном носителе в сейфе) в секрете от посторонних лиц.

Чтобы сохранить пароли администраторов сетевых узлов или администраторов групп узлов в файл:

- 1 В зависимости от того, какие пароли вам требуется сохранить, в окне программы в меню **Сервис** выберите пункт **Сохранить пароли в файле** и далее соответствующую команду:
 - **Пароли администраторов сетевых узлов** для сохранения паролей сетевых узлов;
 - **Пароли администраторов групп узлов** для сохранения паролей администраторов групп узлов.
- 2 В появившемся окне укажите место, в котором следует сохранить файл с паролями.
- 3 Нажмите кнопку **Сохранить**.

Сохраненный файл будет содержать все пароли соответствующего типа для вашей сети.

Настройка оповещений об истечении срока действия паролей администраторов сетевых узлов и групп узлов

Пароли администраторов сетевых узлов и групп узлов, которые задаются в программе ViPNet Удостоверяющий и ключевой центр, имеют ограниченный срок действия. Для оповещения об истечении срока действия таких паролей:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Пароли** > **Пароли администраторов**.

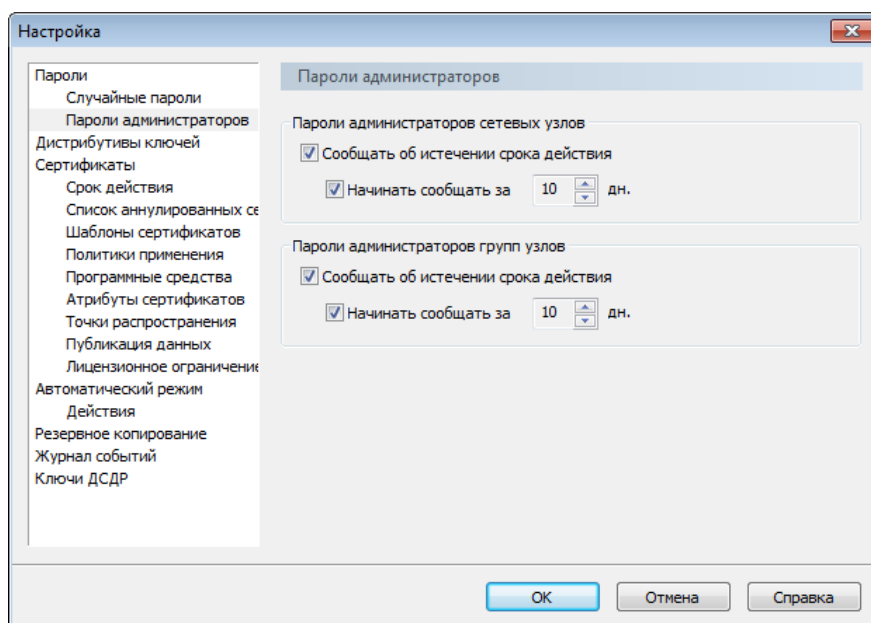


Рисунок 50. Настройка оповещений об истечении срока действия паролей администраторов

- 3 В разделе **Пароли администраторов**:
 - Для предварительного оповещения об истечении срока действия паролей администраторов сетевых узлов в группе **Пароли администраторов сетевых узлов** установите флажки **Сообщать об истечении срока действия** и **Начинать сообщать за** и в поле справа введите количество дней до истечения срока действия, когда следует производить оповещение.

Если будет установлен только флажок **Сообщать об истечении срока действия**, то оповещение будет производиться уже после истечения срока действия пароля.

- Для предварительного оповещения об истечении срока действия паролей администраторов групп узлов аналогичным образом укажите необходимые параметры в группе **Пароли администраторов групп узлов**.



Примечание. По умолчанию в настройках включена опция оповещения об истечении срока действия паролей администраторов групп узлов (за 10 дней до его истечения).

4 Для сохранения настроек нажмите кнопку **ОК**.

Настройка типа создаваемых паролей

При выполнении некоторых операций в программе ViPNet Удостоверяющий и ключевой центр (например, при формировании ключей пользователей или дистрибутивов ключей) создание паролей производится на основе типа, выбранного в настройках программы. Чтобы в ходе данных операций по умолчанию создавались пароли нужного типа, предварительно выполните следующие действия:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Пароли**.

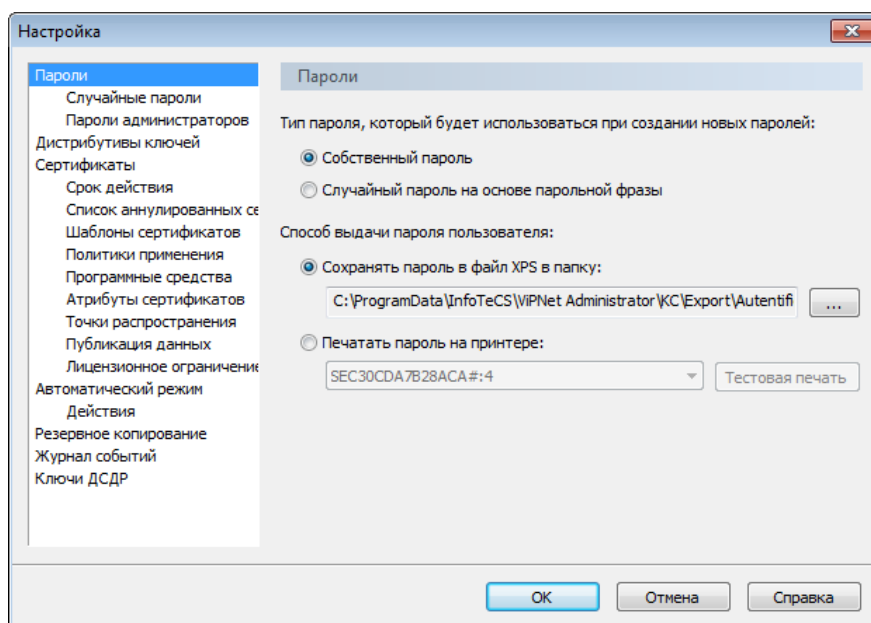


Рисунок 51. Выбор типа создаваемых паролей

- 3 В разделе **Пароли** выберите тип пароля, который будет использоваться по умолчанию при создании новых паролей:
 - **Собственный пароль** — для создания паролей, определяемых администратором УКЦ. Длина таких паролей должна быть не менее 8 символов.
 - **Случайный пароль на основе парольной фразы** — для создания [паролей, формируемых автоматически на основе парольных фраз](#) по заданным параметрам.



Примечание. При выборе типа **Случайный пароль на основе парольной фразы** дополнительно настройте параметры случайных паролей (см. [Настройка параметров случайных паролей](#)).

- 4 Нажмите кнопку **ОК**.

В результате создание паролей будет производиться в соответствии с выбранным типом.

Настройка параметров случайных паролей

Если в процессе работы в программе ViPNet Удостоверяющий и ключевой центр будут создаваться случайные цифровые пароли или [пароли на основе парольных фраз](#), предварительно настройте параметры их создания.



Примечание. Параметры случайных паролей первоначально могут быть заданы в процессе выполнения первичной инициализации (см. документ «ViPNet Administrator. Руководство по установке», главу «Начало работы», раздел «Первый запуск программы ViPNet Удостоверяющий и ключевой центр»).

Чтобы настроить параметры создания случайных паролей:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Пароли > Случайные пароли**.

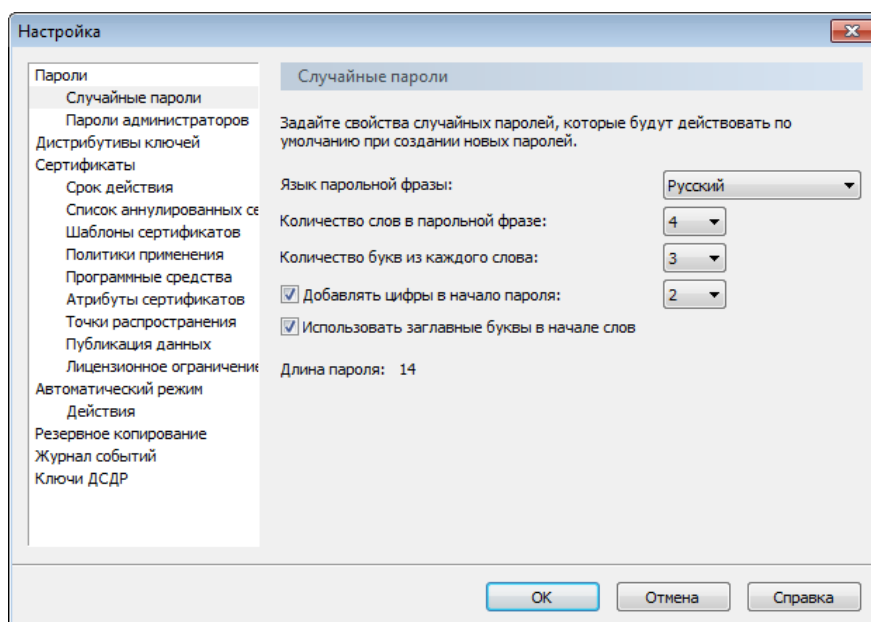


Рисунок 52. Настройка параметров случайных паролей

- 3 При настройке параметров случайных паролей на основе парольных фраз в группе **Пароль на основе парольной фразы** выполните следующие действия:
 - В списке **Язык** выберите язык парольной фразы (русский, английский, немецкий, испанский, французский или португальский).
 - В списке **Количество слов в парольной фразе** выберите число слов (3, 4 или 5), из которых будет состоять парольная фраза. Чем больше число слов, тем длиннее и, соответственно, надежнее будет пароль.

- В списке **Количество букв из каждого слова** выберите число начальных букв каждого слова (3 или 4), которые войдут в пароль.
- При необходимости установите флажок **Добавлять цифры в начало пароля** и в списке рядом выберите количество цифр (2, 3 или 4), которые будут добавлены в начало пароля.
- Чтобы первые буквы слов парольной фразы были заглавными, установите соответствующий флажок.

В строке **Длина пароля** отобразится количество символов в пароле, который будет сформирован с учетом указанных параметров.

4 Для сохранения параметров нажмите кнопку **ОК**.

В результате создание случайных паролей будет производиться в соответствии с указанными параметрами.

7

Организация межсетевого взаимодействия

Порядок организации межсетевого взаимодействия	122
Типы межсетевых мастер-ключей	124
Создание межсетевых мастер-ключей	126
Экспорт межсетевого мастер-ключа	128
Импорт межсетевого мастер-ключа	130
Ввод в действие и прекращение использования межсетевого мастер-ключа	132
Импорт контейнеров сертификатов администраторов доверенных сетей ViPNet	133
Смена межсетевого мастер-ключа	136
Удаление межсетевого мастер-ключа	138
Экспорт межсетевой информации	139

Порядок организации межсетевого взаимодействия

При организации взаимодействия с доверенной сетью ViPNet требуется обмениваться межсетевой информацией и [межсетевым мастер-ключом](#). Формирование межсетевой информации производится в программе ViPNet Центр управления сетью. Подробнее об этом см. документ «ViPNet Центр управления сетью. Руководство администратора», главу «Межсетевое взаимодействие». Создание и ввод в действие межсетевого мастер-ключа выполняется в программе ViPNet Удостоверяющий и ключевой центр.



Внимание! Если при установлении межсетевого взаимодействия вы обменяетесь с доверенной сетью только межсетевой информацией, без создания межсетевого мастер-ключа, то в обеих сетях невозможно будет сформировать ключи узлов и дистрибутивы ключей из-за отсутствия ключа, необходимого для формирования ключей обмена между узлами вашей и доверенной сети.

Для организации межсетевого взаимодействия в УКЦ выполните действия из приведенного ниже списка.

Таблица 4. Порядок действий в УКЦ для организации межсетевого взаимодействия

Действие	Ссылка
☐ Совместно с администратором доверенной сети выберите тип ключа (и параметры ключа, если он будет асимметричного типа) и согласуйте дату его создания и ввода в действие. Определите, кто будет инициировать межсетевое взаимодействие.	Типы межсетевых мастер-ключей
☐ Создайте межсетевой мастер-ключ выбранного типа.	Создание межсетевых мастер-ключей
☐ Если вы являетесь инициатором взаимодействия, экспортируйте созданный мастер-ключ или открытую часть асимметричного мастер-ключа и защищенным способом передайте в составе межсетевой информации администратору сети, с которой устанавливается связь. Администратор сети, с которой устанавливается связь, должен импортировать полученный мастер-ключ или открытую часть асимметричного мастер ключа.	Экспорт межсетевого мастер-ключа

☐ Если инициатором взаимодействия является администратор другой сети, импортируйте полученный мастер-ключ или открытую часть асимметричного мастер-ключа. Администратор сети, с которой устанавливается связь, должен предварительно экспортировать созданный им мастер-ключ или открытую часть асимметричного мастер ключа.	Импорт межсетевого мастер-ключа
☐ Введите межсетевого мастер-ключ в действие. Администратор сети, с которой устанавливается связь, также должен ввести в действие данный мастер-ключ.	Ввод в действие и прекращение использования межсетевого мастер-ключа
☐ Сформируйте новые ключи для узлов своей сети, имеющих связь с доверенной сетью, и передайте их в программу ViPNet Центр управления сетью для дальнейшей отправки на узлы. Администратор доверенной сети также должен создать новые ключи для своих узлов.	Создание и передача ключей узлов в ЦУС
☐ Совместно с администратором ЦУСа проконтролируйте процесс принятия новых ключей на узлах.	
☐ Импортируйте сертификаты и списки аннулированных сертификатов администраторов доверенных сетей, которые поступили в составе межсетевого информации из доверенной сети при ее экспорте в ЦУСе.	Импорт контейнеров сертификатов администраторов доверенных сетей ViPNet

Типы межсетевых мастер-ключей

В программе ViPNet Удостоверяющий и ключевой центр вы можете создать межсетевые мастер-ключи двух типов:

- Симметричный межсетевой мастер-ключ.

Если взаимодействие с доверенной сетью устанавливается на основе симметричных ключей шифрования, то межсетевой мастер-ключ создается только в одной сети (администратором, который выступает в роли инициатора) для организации связи с определенной доверенной сетью. Выбор инициатора межсетевого взаимодействия осуществляется по взаимной договоренности. После создания ключ зашифровывается на пароле и передается администратору доверенной сети лично либо защищенным способом. На основе созданного межсетевого мастер-ключа впоследствии формируются ключи обмена между узлами вашей и доверенной сети.

Основным преимуществом межсетевого мастер-ключа такого типа является то, что взаимодействие, установленное на его основе, считается наиболее защищенным (при условии, что канал, по которому передавался мастер-ключ в доверенную сеть, является надежным). В некоторых случаях процесс организации взаимодействия с доверенными сетями с помощью таких ключей может быть достаточно трудоемким (особенно если требуется установить связь сразу с большим количеством сетей), поскольку на основе одного симметричного мастер-ключа можно установить связь только между двумя сетями ViPNet.



Примечание. Если хотя бы для одной из сетей ViPNet, между которыми устанавливается межсетевое взаимодействие, лицензией запрещено использование функций удостоверяющего центра, межсетевое взаимодействие может быть организовано только с использованием симметричных межсетевых мастер-ключей.

- Асимметричный межсетевой мастер-ключ.

Если взаимодействие устанавливается с помощью асимметричных ключей, то межсетевой мастер-ключ создается администратором каждой сети. Такой мастер-ключ состоит из закрытой части (ключа электронной подписи) и открытой части (сертификата ключа проверки электронной подписи) и может быть использован для организации связи с несколькими сетями ViPNet. После формирования мастер-ключей администраторы сетей, между которыми устанавливается взаимодействие, обмениваются между собой только их открытыми частями (сертификатами). На основе закрытой части своего ключа и полученной открытой части ключа из доверенной сети в каждой сети формируется согласованный ключ, который потом используется для создания ключей обмена между узлами данных сетей.

Взаимодействие, основанное на асимметричных ключах, считается безопасным, поскольку закрытая часть каждого мастер-ключа остается известной только тому администратору, который создавал этот мастер-ключ. При этом установить его в какой-то степени проще, поскольку открытые части данных ключей можно передавать по незащищенному каналу.



Примечание. Если межсетевое взаимодействие было установлено с помощью асимметричных ключей, созданных в УКЦ версии 3.2.x, то оно сохранится после обновления в одной из сетей ПО ViPNet Administrator до версии 4.2.x и выше.

Создание межсетевых мастер-ключей

Чтобы создать межсетевой мастер-ключ выбранного типа:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и выполните следующие действия:
 - Для создания асимметричного мастер-ключа перейдите в раздел **Межсетевое взаимодействие** > **Асимметричные мастер-ключи** и на панели инструментов нажмите кнопку **Создать**.
 - Для создания симметричного мастер-ключа перейдите в раздел с номером доверенной сети, для связи с которой он будет использоваться, и на панели инструментов нажмите кнопку **Создать**.



Примечание. Разделы с номером доверенной сети появляются после того, как в программе ViPNet Центр управления сетью была сформирована или обработана межсетевая информация для организации взаимодействия с данными сетями.

- 2 При создании асимметричного мастер-ключа появится окно, в котором укажите алгоритм для формирования согласованного ключа.

Таблица 5. Характеристики алгоритмов

Алгоритм формирования ключа	Описание	Длина открытого ключа
ГОСТ Р 34.10-2012/512 (длина закрытого ключа 256 бит)	OID «1.2.643.7.1.1.1.1»	512 бит
ГОСТ Р 34.10-2012/1024 (длина закрытого ключа 512 бит)	OID «1.2.643.7.1.1.1.2»	1024 бит
ГОСТ Р 34.10-2001 EDH	См. RFC 4357 OID «1.2.643.2.2.19» OID «1.2.643.2.2.98»	512 бит



Примечание. Параметры, которые вы укажете при создании вашего асимметричного ключа, должны совпадать с параметрами алгоритма, указанными при создании асимметричного мастер-ключа в доверенной сети. Взаимодействие между сетями с использованием согласованных ключей, сформированных по алгоритмам с разными параметрами, невозможно.

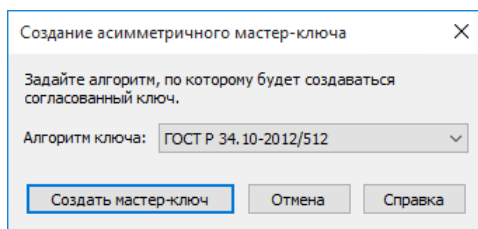


Рисунок 53. Задание алгоритма формирования согласованного ключа

После задания алгоритма в окне **Создание асимметричного мастер-ключа** нажмите кнопку **Создать мастер-ключ**.

- 3 Независимо от типа создаваемого мастер-ключа появится окно с сообщением о необходимости согласования мастер-ключа с администратором доверенной сети. Нажмите в данном окне кнопку **Да**.

В результате межсетевой мастер-ключ будет создан и отобразится в соответствующем разделе.

Экспорт межсетевого мастер-ключа

После создания или смены межсетевого мастер-ключа экспортируйте его для передачи в доверенные сети.



Примечание. У асимметричного мастер-ключа экспортируется только открытая часть (сертификат).

Экспорт межсетевого мастер-ключа осуществляется путем его сохранения в файл. Чтобы сохранить межсетевой мастер-ключ в файл:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите:
 - в раздел **Асимметричные мастер-ключи** для экспорта межсетевого асимметричного мастер-ключа;
 - в раздел с номером доверенной сети для экспорта межсетевого симметричного мастер-ключа.
- 2 В списке на панели просмотра выберите нужный межсетевой мастер-ключ.
- 3 Щелкните по ключу правой кнопкой мыши и в контекстном меню выберите пункт **Экспорт**.
- 4 При экспорте симметричного межсетевого мастер-ключа появится окно ввода пароля. Укажите в нем пароль и его подтверждение и нажмите кнопку **ОК**. На указанном пароле будет зашифрован экспортируемый ключ.



Совет. Запомните пароль. Его необходимо будет сообщить администратору доверенной сети при передаче экспортируемого мастер-ключа.

При экспорте асимметричного мастер-ключа ввод пароля не требуется, поскольку данный мастер-ключ не зашифровывается на пароле. Асимметричный мастер-ключ (его открытая часть), в свою очередь, подписывается сертификатом администратора, который его экспортирует.

- 5 В появившемся окне укажите папку, в которую будет сохранен межсетевой мастер-ключ, затем нажмите кнопку **ОК**.

Межсетевой мастер-ключ будет экспортирован в выбранную папку в виде файла:

- симметричный межсетевой мастер-ключ — `net <номер вашей сети>.key`;
- асимметричный межсетевой мастер-ключ (его открытая часть) — `net <номер вашей сети>.cer`.

Файл с экспортированным мастер-ключом передайте администратору доверенной сети в составе межсетевой информации по защищенному каналу связи. При передаче мастер-ключа симметричного типа также предоставьте пароль, на котором данный ключ зашифрован. При передаче мастер-ключа асимметричного типа убедитесь, что в составе межсетевой информации присутствует сертификат администратора, которым был подписан данный мастер-ключ, и соответствующий сертификату список аннулированных сертификатов (CRL).

Примечание. Без сертификата администратора открытая часть асимметричного мастер-ключа (сертификат) не может быть импортирована в доверенной сети.



Открытую часть асимметричного ключа можно передать в доверенную сеть и по незащищенному каналу связи, но при условии, что администратор этой сети в процессе импорта свяжется с вами для проверки сертификата и сравнит значения атрибутов полученного сертификата с отправленным.

После экспорта вы можете ввести мастер-ключ в действие (см. [Ввод в действие и прекращение использования межсетевого мастер-ключа](#)).

Импорт межсетевого мастер-ключа

При установке межсетевого взаимодействия, в случае, когда межсетевой мастер-ключ создан в доверенной сети, необходимо импортировать этот ключ в УКЦ. Межсетевой мастер-ключ передается доверенным способом.

В случае использования симметричной схемы установления межсетевого взаимодействия это будет симметричный мастер-ключ (файл `net <номер вашей сети>.key`), в случае асимметричной — открытая часть (сертификат) асимметричного мастер-ключа (файл `net <номер вашей сети>.cer`).

Внимание! Мастер-ключ симметричного типа перед передачей зашифровывается на пароле, поэтому при импорте такого мастер-ключа убедитесь, что вы располагаете этим паролем.

Перед импортом асимметричного межсетевого мастер-ключа убедитесь, что выполнены следующие условия:



- В программе ViPNet Центр управления сетью установлено межсетевое взаимодействие с доверенной сетью (см. документ «ViPNet Центр управления сетью. Руководство администратора»).
- Полученные контейнеры сертификатов администраторов доверенных сетей обработаны. После данной обработки (см. [Импорт контейнеров сертификатов администраторов доверенных сетей ViPNet](#)) в представлении **Администрирование** в разделе **Импортированные сертификаты > Корневые сертификаты** и **Импортированные сертификаты > Списки аннулированных сертификатов** отображаются соответствующие сертификаты и CRL, принятые из доверенной сети.

Без сертификата администратора импорт асимметричного мастер-ключа будет невозможен.

Чтобы импортировать межсетевой мастер-ключ:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел с номером доверенной сети, из которой поступил данный мастер-ключ.
- 2 На панели инструментов нажмите кнопку **Загрузить**.
- 3 При импорте симметричного межсетевого мастер-ключа появится окно ввода пароля. Введите пароль, на котором был зашифрован данный ключ. При правильном вводе пароля мастер-ключ будет импортирован.

При импорте асимметричного мастер-ключа будет произведен поиск сертификата администратора доверенной сети, которым был подписан данный ключ. Мастер-ключ будет импортирован только в том случае, если будет найден сертификат администратора.

Импортированный мастер-ключ будет сразу введен в действие и добавлен в список межсетевых мастер-ключей выбранного раздела.

Ввод в действие и прекращение использования межсетевого мастер-ключа

Межсетевой мастер-ключ используется для формирования ключей обмена между узлами вашей и доверенной сети, в случае если он является действующим.

Если межсетевой мастер-ключ импортируется из другой сети (см. [Импорт межсетевого мастер-ключа](#)), он вводится в действие автоматически. Если вы экспортировали межсетевой мастер-ключ в другую сеть (см. [Экспорт межсетевого мастер-ключа](#)), введите его в действие в своем Удостоверяющем и ключевом центре вручную, чтобы начать использовать.

Чтобы ввести в действие мастер-ключ:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите:
 - в раздел **Асимметричные мастер-ключи** для ввода в действие межсетевого мастер-ключа асимметричного типа;
 - в раздел с номером доверенной сети для ввода в действие межсетевого мастер-ключа симметричного типа.
- 2 В списке на панели просмотра выберите межсетевой мастер-ключ, который требуется ввести в действие, и щелкните по нему правой кнопкой мыши.
- 3 В контекстном меню ключа выберите команду **Текущий**.
- 4 В появившемся окне с сообщением нажмите кнопку **Да**.

В результате выбранный межсетевой мастер-ключ будет введен в действие (его статус изменится на **Текущий**).



Внимание! Если для связи с определенной сетью в УКЦ имеется несколько симметричных или асимметричных межсетевых мастер-ключей, действующим может быть только один из них.

Если при вводе в действие межсетевого мастер-ключа имеются другие мастер-ключи, с которыми его нельзя использовать одновременно, эти мастер-ключи перестают быть действующими (их статус меняется на **Экспортирован**).

Действие межсетевого мастер-ключа можно прекратить, например, если был выявлен факт его компрометации. Для этого в контекстном меню действующего мастер-ключа снимите отметку **Текущий**, после чего в появившемся окне с вопросом о прекращении использования мастер-ключа нажмите кнопку **Да**.

Импорт контейнеров сертификатов администраторов доверенных сетей ViPNet

Если ваша сеть взаимодействует с доверенными сетями ViPNet, требуется обеспечить доверие к сертификатам пользователей этих сетей со стороны пользователей вашей сети. Для проверки сертификатов пользователей доверенных сетей требуются сертификаты издателей (администраторов доверенных сетей) и соответствующие списки аннулированных сертификатов (CRL).



Примечание. Если вы устанавливаете межсетевое взаимодействие с использованием асимметричного межсетевого мастер-ключа, то сертификаты администраторов доверенных сетей необходимы также для импорта открытой части асимметричного ключа, полученного из доверенной сети. См. раздел [Импорт межсетевого мастер-ключа](#).

Импорт сертификатов и CRL администраторов доверенных сетей осуществляется в Удостоверяющем и ключевом центре. Затем импортированные сертификаты и CRL через программу ViPNet Центр управления сетью рассылаются на узлы сети в составе комплектов CRL или новых ключей узлов. При импорте сертификаты заверяются сертификатом текущего администратора УКЦ.

Сертификаты и CRL администраторов из доверенных сетей поступают в программу в специальных [контейнерах сертификатов администраторов](#) (файлах *.p7s), обычно в составе межсетевой информации. В некоторых случаях контейнеры сертификатов могут быть переданы не в составе межсетевой информации (в виде отдельных файлов) и без использования средств ViPNet. При этом дополнительно для каждого сертификата из контейнера должна быть передана его бумажная копия.

При импорте сертификатов и CRL администраторов доверенной сети необходимо учитывать следующие особенности:

- Если сертификаты и CRL администраторов поступили из доверенной сети в составе межсетевой информации, полученные контейнеры сертификатов администраторов будут отображены в представлении **Администрирование** в разделе **Необработанные данные > Контейнеры сертификатов администраторов сетей ViPNet**. Если сертификаты и CRL, поступившие в контейнере, ранее не импортировались в УКЦ, импортируйте их вручную.
- При повторном поступлении сертификатов и CRL они могут быть импортированы из контейнера и переданы на узлы через ЦУС в автоматическом режиме. Для этого должны быть выполнены соответствующие настройки программы.
- Если вы устанавливаете межсетевое взаимодействие с доверенными сетями ViPNet, УКЦ которых являются подчиненными, необходимо также импортировать сертификаты издателей и

соответствующие CRL вышестоящих удостоверяющих центров. Вы можете сделать это вручную, если данные сертификаты и CRL переданы вам в виде файлов, либо установив межсетевое взаимодействие с вышестоящими удостоверяющими центрами.

- Если на момент импорта CRL еще не наступило время издания, указанное в импортируемом файле CRL (например, в результате неточной настройки даты и времени на компьютере с УКЦ вашей или доверенной сети), такой CRL не может быть импортирован. Необходимо дождаться, пока на компьютере, на котором вы выполняете импорт CRL, наступит указанное время издания.
- Если в доверенных сетях используется программное обеспечение ViPNet Administrator версии 3.1 и ниже, то сертификаты администраторов в составе межсетевой информации будут присутствовать не в контейнерах, а в файлах *.tr1. Это связано с тем, что программа УКЦ, входящая в состав ранних версий ПО ViPNet Administrator, не поддерживает работу с файлами формата PKCS #7.

Если сертификаты и CRL администраторов доверенной сети были переданы вам в виде файлов, по отдельности выполните:

- [Импорт сертификатов администраторов, полученных из вышестоящего удостоверяющего центра.](#)
- [Импорт списков аннулированных сертификатов, полученных из вышестоящего удостоверяющего центра.](#)

Чтобы вручную импортировать поступившие сертификаты и CRL администраторов доверенной сети из контейнера:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр перейдите в представление **Администрирование** и на панели навигации выберите раздел **Необработанные данные > Контейнеры сертификатов администраторов сетей ViPNet**.
- 2 На панели просмотра выберите контейнеры, сертификаты и CRL из которых требуется импортировать, и на панели инструментов нажмите кнопку **Обработать**.

В появившемся окне будет представлен список администраторов, сертификаты и CRL которых содержатся в выбранных контейнерах.

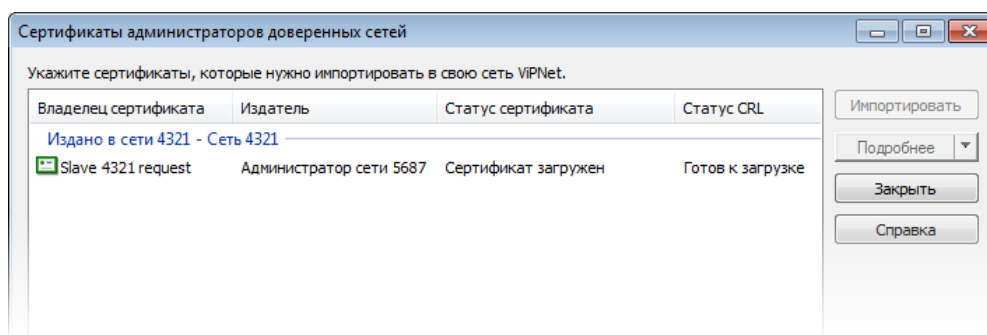


Рисунок 54. Список администраторов, сертификаты которых содержатся в контейнере

- 3 Прежде чем импортировать сертификаты и CRL, вы можете проверить их содержимое. Для этого:
 - Выберите в списке имя администратора доверенной сети.

- Нажмите кнопку **Подробнее** и в меню выберите один из пунктов: **Сертификат администратора** или **Список аннулированных сертификатов**.

Откроется окно просмотра сертификата (см. [Просмотр сертификатов](#)) или CRL.



Примечание. Сертификаты, которые еще не были импортированы, не являются действительными. В связи с этим при просмотре и проверке этих сертификатов на вкладке **Путь сертификации** отображается информация о том, что нет доверия к корневому сертификату центра сертификации. Данное сообщение не является препятствием для импорта сертификата. При отсутствии других ошибок и совпадении содержимого полей сертификата с содержимым в бумажной копии, сертификат может быть импортирован. После импорта он станет действительным.

- 4 Чтобы импортировать сертификаты и CRL определенного администратора, выберите его в списке и нажмите кнопку **Импортировать**.

Для просмотра импортированных сертификатов и CRL в представлении **Администрирование** в разделе **Импортированные сертификаты** выберите соответствующий подраздел.

- 5 После импорта сертификатов администраторов доверенных сетей передайте на узлы, имеющие связь с узлами данных доверенных сетей комплекты CRL (см. [Передача CRL на узлы вручную](#)).

Смена межсетевого мастер-ключа

Как и обычные мастер-ключи, которые используются в вашей сети, межсетевые мастер-ключи, с помощью которых установлена связь между вашей и доверенными сетями, также должны меняться (обновляться). Смена межсетевого мастер-ключа — это создание нового мастер-ключа такого же типа и использование его вместо старого. В связи с этим, при смене межсетевого мастер-ключа изменяются все ключи обмена между узлами, созданные на его основе.

Смена межсетевых мастер-ключей также может быть как плановой, так и внеплановой. Плановая смена производится, как правило, не реже одного раза в год. Внеплановая смена производится при компрометации межсетевых мастер-ключей.

При каждом запуске программы ViPNet Удостоверяющий и ключевой центр, а также по команде **Проверка текущих данных** выполняется проверка сроков действия используемых межсетевых мастер-ключей. Если во время проверки будут обнаружены межсетевые мастер-ключи, созданные более 1 года назад, появится сообщение об истечении их срока действия (см. [Проверка текущих данных](#)). В этом случае выполните смену указанных межсетевых мастер-ключей, как описано ниже в этом разделе. При этом до смены межсетевых мастер-ключей межсетевое взаимодействие продолжит функционировать с использованием текущих ключей.

Перед сменой межсетевых мастер-ключей вам следует договориться с администраторами доверенных сетей о времени ее проведения и последующей отправке новых ключей на узлы сетей.



Внимание! После смены межсетевого мастер-ключа связь между узлами сетей, в которых используется данный мастер-ключ, будет возможна только после обновления ключей на всех соответствующих узлах данных сетей.

Сценарий смены межсетевых мастер-ключей определяется их типом. Смену симметричных межсетевых мастер-ключей производит один из администраторов, выступающий инициатором. Смена асимметричных мастер-ключей шифрования осуществляется администратором каждой сети, участвующей во взаимодействии.

Для смены межсетевого мастер-ключа:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите:
 - в раздел **Асимметричные мастер-ключи**, если вам требуется обновить асимметричный межсетевого мастер-ключ;
 - в раздел с номером доверенной сети, если вы собираетесь обновить симметричный межсетевого мастер-ключ.
- 2 В списке на панели просмотра выберите нужный межсетевого мастер-ключ, щелкните по нему правой кнопкой мыши и в контекстном меню выберите пункт **Создать**.
- 3 В появившемся окне с сообщением о необходимости согласования нового мастер-ключа с администратором доверенной сети нажмите кнопку **Да**.

В результате в списке появится новый межсетевой мастер-ключ.

После смены межсетевого мастер-ключа выполните действия, которые требуется выполнять после создания нового межсетевого мастер-ключа. Подробнее см. раздел [Порядок организации межсетевого взаимодействия](#).

Удаление межсетевого мастер-ключа

Межсетевые мастер-ключи, которые прекратили свое действие (например, вследствие смены (см. [Смена межсетевого мастер-ключа](#))), следует удалять. В первую очередь это необходимо для того, чтобы избежать их случайного ввода в действие (см. [Ввод в действие и прекращение использования межсетевого мастер-ключа](#)).

Чтобы удалить ненужный межсетевого мастер-ключ:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите:
 - в раздел **Асимметричные мастер-ключи** для удаления асимметричного межсетевого мастер-ключа;
 - в раздел с номером доверенной сети для удаления симметричного межсетевого мастер-ключа.
 - 2 В списке на панели просмотра выберите межсетевого мастер-ключ, который следует удалить, и щелкните по нему правой кнопкой мыши.
 - 3 В контекстном меню выберите пункт **Удалить**.
 - 4 В появившемся окне подтвердите удаление мастер-ключа, нажав кнопку **Да**.
- В результате ненужный межсетевого мастер-ключ будет удален.

Экспорт межсетевой информации

Для организации межсетевого взаимодействия с доверенными сетями требуется набор служебных данных. Часть этих данных содержится в программе ViPNet Удостоверяющий и ключевой центр и при установке межсетевого взаимодействия должна быть экспортирована и отправлена в соответствующие доверенные сети с помощью программы ViPNet Центр управления сетью.

Из УКЦ экспортируются следующие служебные данные:

- список сертификатов администраторов;
- списки аннулированных сертификатов (CRL) пользователей своей сети ViPNet.

Экспорт списков сертификатов администраторов производится автоматически каждый раз при их изменении (например, при издании нового сертификата администратора (см. [Издание сертификата администратора](#))). Экспорт CRL выполняется сразу после их обновления только в случае обновления списков аннулированных сертификатов в автоматическом режиме (см. [Настройка автоматического обновления CRL](#)).

При необходимости экспорт всех указанных данных может быть выполнен вручную (см. [Экспорт межсетевой информации вручную](#)).



Внимание! Если ваш УКЦ является подчиненным, для организации межсетевого взаимодействия с доверенными сетями ViPNet вам необходимо вручную экспортировать сертификаты и CRL вышестоящих удостоверяющих центров и передать их администратору доверенной сети.

Экспорт межсетевой информации вручную

Если в доверенную сеть ViPNet по каким-то причинам требуется передать обновленную межсетевую информацию со списками сертификатов и CRL, в УКЦ выполните ее экспорт вручную. Для этого в окне программы в меню **Сервис** выберите пункт **Экспорт межсетевой информации**. По завершении экспорта появится соответствующее сообщение. Межсетевая информация будет автоматически передана в базу данных программы ViPNet Центр управления сетью, после чего сможет быть отправлена ЦУСом в доверенную сеть.

8

Управление сертификатами

Издание сертификатов	141
Настройка параметров издания сертификатов	156
Издание квалифицированных сертификатов	171
Аннулирование, приостановление действия, возобновление действия сертификатов	179
Просмотр запросов и сертификатов	183
Просмотр истории сертификатов	188
Экспорт сертификатов	189
Проверка сертификатов	192
Печать сертификатов	193
Настройка количества сертификатов, отображаемых в окне программы	194

Издание сертификатов

В программе ViPNet Удостоверяющий и ключевой центр вы можете издавать сертификаты пользователей, если это разрешено вашей лицензией (см. [Лицензионные ограничения](#)).

Сертификаты пользователей могут издаваться:

- по вашей собственной инициативе (при создании для пользователей своей сети ViPNet ключей или дистрибутивов ключей) (см. [Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ](#));
- по запросам, сформированным пользователями сети ViPNet (см. [Издание сертификатов по запросам от пользователей своей сети ViPNet](#));
- по запросам, поступающим из центров регистрации (см. [Издание сертификатов по запросам, поступившим из центра регистрации](#));
- по запросам от внешних пользователей (см. [Издание сертификатов по запросам от внешних пользователей](#)).

Издание сертификатов невозможно в следующих случаях:

- Вы издали максимальное количество сертификатов, разрешенное вашей лицензией. Обратитесь за расширением лицензии к представителю компании ИнфоТеКС.
- Истек срок действия вашего текущего сертификата. Издайте новый сертификат (см. [Издание сертификата администратора](#)) либо получите новый сертификат по запросу в вышестоящем удостоверяющем центре, если ваш удостоверяющий центр (функции которого выполняет УКЦ) является подчиненным (см. [Создание запроса на сертификат к вышестоящему удостоверяющему центру](#)).
- Истек срок действия списка аннулированных сертификатов (CRL), соответствующего вашему текущему сертификату. Обновите данный CRL (см. [Обновление CRL вручную](#)).

Перед изданием сертификатов выполните следующие дополнительные настройки, если такие требуются:

- Чтобы при издании сертификатов появлялись мастер подготовки к изданию сертификата и мастер редактирования полей сертификата, с помощью которых вы сможете изменять параметры издаваемых сертификатов, в окне программы в меню **Сервис** выберите пункт **Настройка** и в разделе **Сертификаты** установите флажок **Редактировать поля сертификатов при издании**.
- Если при издании сертификатов будут использоваться шаблоны сертификатов, в настройках программы в разделе **Сертификаты > Шаблоны сертификатов** убедитесь, что присутствуют необходимые шаблоны, или создайте недостающие. Информацию по созданию и редактированию шаблонов сертификатов см. в разделе **Создание и редактирование шаблонов сертификатов** (см. [Создание и изменение шаблонов сертификатов](#)).
- Чтобы сертификаты пользователей издавались в формате **квалифицированных**, перед их изданием в настройках программы в разделе **Сертификаты > Программные средства** укажите ряд дополнительных параметров. Кроме этого, убедитесь, что ваш текущий сертификат

администратора имеет формат квалифицированного. Информацию по настройке см. в разделе [Издание квалифицированных сертификатов](#).

- Чтобы атрибуты в сертификатах специальным образом размещались в полях «Владелец» и «Дополнительное имя владельца», то перед изданием сертификатов в настройках программы в разделе **Сертификаты > Атрибуты сертификатов** укажите, какие атрибуты в какие поля должны быть помещены. Информацию по настройке см. в разделе [Настройка распределения атрибутов сертификатов](#).

Особенности издания сертификатов

При издании сертификатов следует учитывать следующие особенности:

- При издании сертификатов в процессе создания ключей пользователей (см. [Создание и передача ключей пользователей в ЦУС](#)), ключей электронной подписи (см. [Создание и сохранение ключей электронной подписи пользователя в файл](#)) или дистрибутивов ключей (см. [Создание дистрибутивов ключей](#)) создается пара ключей: **ключ электронной подписи** и **ключ проверки электронной подписи**; ключ электронной подписи помещается в специальный контейнер. После издания сертификат с ключом проверки электронной подписи помещается также в этот контейнер и в составе ключей передается пользователю.
- При издании сертификатов по запросам ключ электронной подписи не создается, поскольку он был создан пользователем в процессе формирования запроса; издается только сертификат, который после этого отправляется пользователю вместе с ключом проверки электронной подписи. Сертификаты пользователей хранятся в базе данных ПО ViPNet Administrator.
- Издание сертификатов в процессе создания ключей пользователей (см. [Создание и передача ключей пользователей в ЦУС](#)), ключей электронной подписи (см. [Создание и сохранение ключей электронной подписи пользователя в файл](#)) или дистрибутивов ключей (см. [Создание дистрибутивов ключей](#)) производится только в том случае, если для пользователей разрешено создание ключей электронной подписи (см. [Настройка создания ключа электронной подписи и ключа проверки электронной подписи для пользователей сети ViPNet](#)). При издании сертификатов используются параметры шаблона сертификата, установленного по умолчанию, или другого указанного вами шаблона.
- Если пользователь зарегистрирован на нескольких сетевых узлах и дистрибутивы ключей (см. [Создание дистрибутивов ключей](#)) создаются для каждого узла по отдельности, количество изданных сертификатов пользователя будет совпадать с числом созданных дистрибутивов. Если дистрибутивы ключей создаются сразу для всей группы узлов, на которых зарегистрирован пользователь, то будет издан один сертификат для всех дистрибутивов этого пользователя.
- Издание сертификатов по запросам от пользователей сети и из центров регистрации может производиться в автоматическом режиме (см. [Работа в автоматическом режиме](#)) или вручную. Издание сертификатов по запросам от внешних пользователей выполняется только вручную. При издании сертификатов по запросам могут использоваться как параметры из шаблона сертификата, так и параметры из самого запроса.

- При издании сертификаты пользователей заверяются вашим текущим сертификатом. Поэтому они не могут быть изданы на срок, превышающий срок действия сертификата издателя.
- Если сертификат пользователя издается по запросу (в качестве источника параметров выбран именно запрос на сертификат) и в запросе присутствует политика применения, которая не зарегистрирована в УКЦ (см. [Настройка списка политик применения сертификата](#)), данная политика не будет добавлена в изданный сертификат.
- В сертификате пользователя не будет указан срок действия ключа электронной подписи (не будет расширения «Срок действия закрытого ключа» (PrivateKeyUsagePeriod)) в следующих случаях:
 - Сертификат издается на срок равный или менее 15 месяцев и для хранения ключа электронной подписи используется файл на компьютере либо внешнее устройство без аппаратной поддержки российских криптографических алгоритмов.
 - Сертификат издается на срок равный или менее 36 месяцев и для хранения ключа электронной подписи используется устройство с аппаратной поддержкой российских криптографических алгоритмов.

Срок действия ключа в данных случаях будет равен сроку действия сертификата.

Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ

В программе ViPNet Удостоверяющий и ключевой центр вы можете издавать сертификаты ключа проверки электронной подписи для пользователей сети ViPNet, если для них разрешено создание ключа электронной подписи и ключа проверки электронной подписи (см. [Настройка создания ключа электронной подписи и ключа проверки электронной подписи для пользователей сети ViPNet](#)). В данном случае сертификаты можно издать при создании ключей пользователей либо дистрибутивов ключей.

Если в настройках программы в разделе **Сертификаты** установлен флажок **Редактировать поля сертификатов при издании**, то вы сможете изменить параметры издаваемого сертификата в появившемся мастере подготовки к изданию сертификата и мастере редактирования полей сертификата. Если указанный флажок не установлен, то все параметры сертификата будут полностью заимствованы из шаблона, выбранного по умолчанию. Поэтому во втором случае убедитесь, что по умолчанию выбран нужный шаблон.



Примечание. Из шаблона сертификата полностью заимствуются такие параметры, как криптопровайдер и параметры алгоритма подписи. Поэтому независимо от того, производится ли редактирование полей сертификата, данные параметры невозможно изменить при издании сертификата (они не отображаются в мастере подготовки к изданию сертификата). В связи с этим перед изданием сертификата убедитесь, что в шаблоне, который будет использоваться, правильно указаны эти параметры (см. раздел Создание и редактирование шаблонов сертификатов (см. [Создание и изменение шаблонов сертификатов](#))).

Чтобы издать сертификат ключа проверки электронной подписи для пользователя:

- 1 В процессе создания ключей пользователя, ключей электронной подписи либо дистрибутивов ключей при соответствующих настройках программы будет запущен мастер подготовки к созданию ключей либо мастер подготовки к выдаче новых дистрибутивов, следуйте его указаниям.
- 2 На странице **Выбор шаблона сертификата** выберите шаблон, из которого будут заимствованы параметры издаваемого сертификата. Затем нажмите кнопку **Далее**.

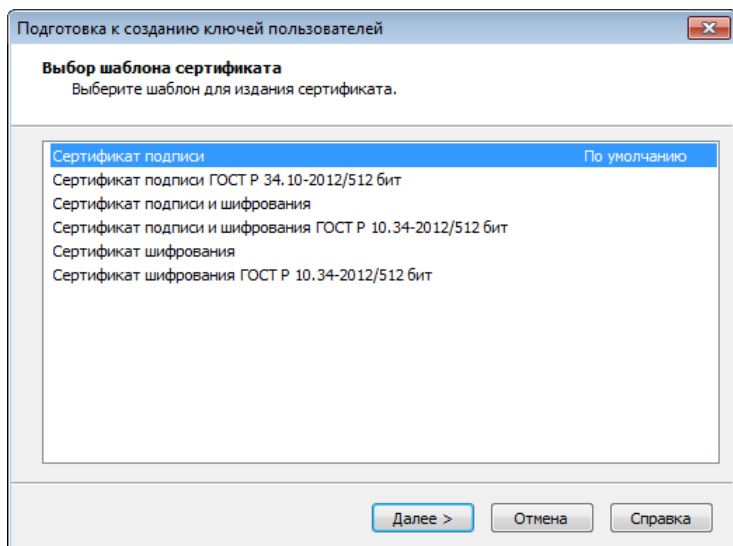


Рисунок 55. Выбор шаблона сертификата

- 3 На странице **Срок действия сертификата** при необходимости измените срок действия издаваемого сертификата любым удобным способом, после чего нажмите кнопку **Далее**.

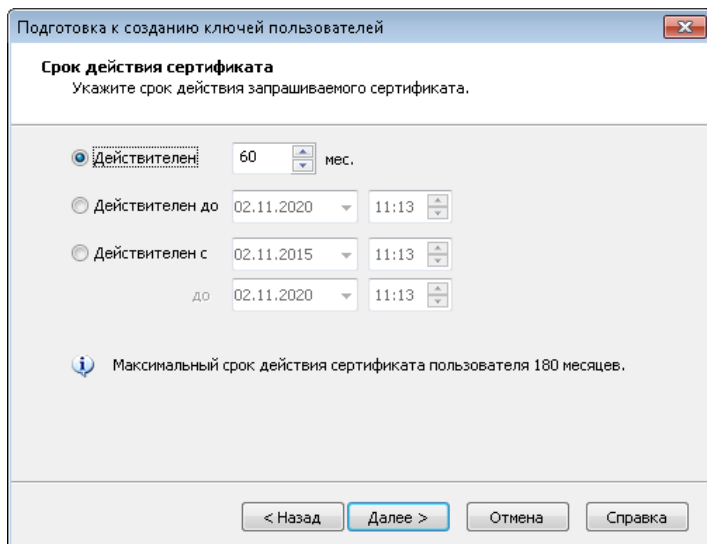


Рисунок 56. Указание срока действия сертификата



Примечание. Заданный срок действия сертификата определит срок действия ключа электронной подписи. Если срок действия сертификата не более 12 месяцев (1 года), то такой же срок действия будет у ключа электронной подписи. Если срок действия сертификата больше 12 месяцев (1 года), то срок действия ключа электронной подписи не будет превышать 15 месяцев (1 год и 3 месяца). Максимальный срок действия сертификата пользователя составляет 180 месяцев (15 лет).

- 4 На странице **Назначения сертификата** при необходимости измените расширения издаваемого сертификата или добавьте новые. Расширения сертификата позволяют регулировать возможности использования сертификата для выполнения определенных действий и работы с различными сервисами, например, **OCSP-сервером**, **TSP-сервером**, EFS (шифрованная файловая система) и другими.

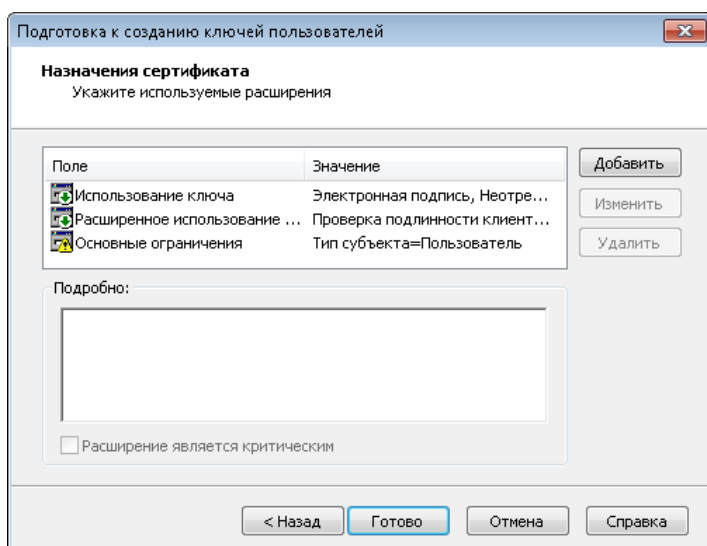


Рисунок 57. Формирование назначений сертификата

Для добавления расширения нажмите кнопку **Добавить** и в окне **Допустимые расширения** выберите одно из расширений:

- **Использование ключа.** В появившемся окне настройте параметры использования ключа и нажмите кнопку **ОК**.

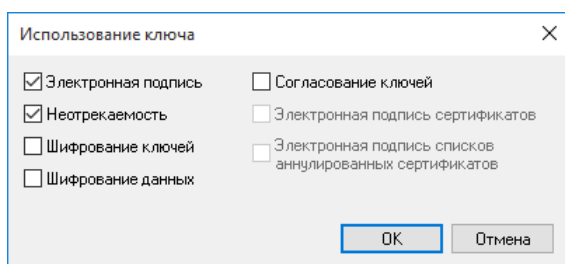


Рисунок 58. Настройка параметров использования ключа

- **Расширенное использование ключа.** В появившемся окне с помощью кнопок **Добавить** и **Удалить** сформируйте список назначений ключа и нажмите кнопку **ОК**.

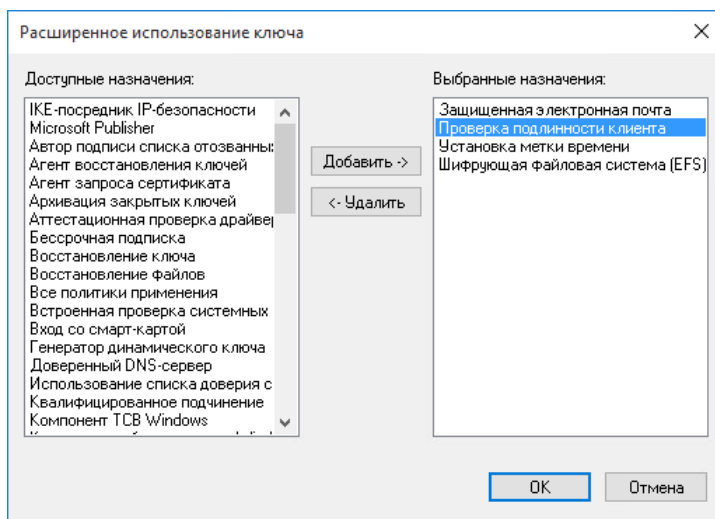


Рисунок 59. Выбор назначений расширенного использования ключа

- **Политики сертификата.** В появившемся окне с помощью кнопок **Добавить** и **Удалить** выберите политики применения сертификата, которые должны быть включены в сертификат, и нажмите кнопку **ОК**. При необходимости предварительно выполните настройку списка политик применения сертификата (см. [Настройка списка политик применения сертификата](#)).

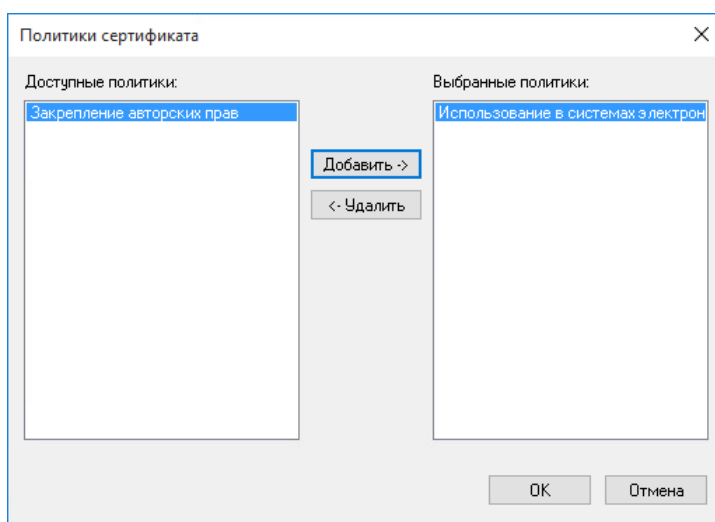


Рисунок 60. Добавление политики применения сертификата

- **Дополнительное имя субъекта.** Для указания дополнительного имени пользователя (например, DNS-имени компьютера или имени пользователя сервиса) нажмите кнопку **Добавить**, в появившемся окне задайте тип имени и его значение, затем нажмите кнопку **ОК**.

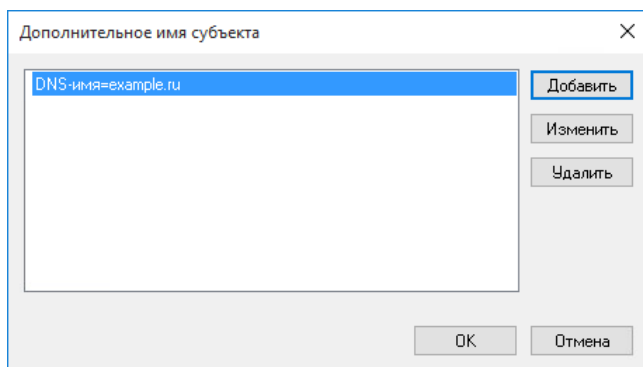


Рисунок 61. Задание альтернативного имени владельца сертификата ключа проверки электронной подписи

Для изменения параметров используемого расширения воспользуйтесь кнопкой **Изменить**, для удаления ненужного расширения — кнопкой **Удалить**.



Примечание. Расширение **Основные ограничения** нельзя изменить или удалить. С его помощью определяется, что сертификат издается для пользователя.

Если при издании сертификата вы добавили расширение **Использование ключа** или выбрали шаблон, содержащий это расширение, то данное расширение нельзя будет удалить. С его помощью определяется, в каких целях может быть использован сертификат.

При необходимости для выбранного расширения установите флажок **Расширение является критическим**. В этом случае расширение будет отмечено как критическое. Это означает, что если прикладное ПО не сможет обработать такое расширение, то сертификат будет признан недействительным.

- 5 Нажмите кнопку **Готово**. Появится **электронная рулетка**, если она еще не запускалась в рамках текущего сеанса работы программы. Следуйте указаниям в окне **Электронная рулетка**.

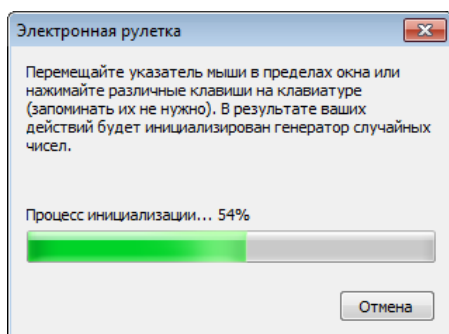


Рисунок 62. Запуск электронной рулетки



Внимание! При издании нескольких сертификатов заданные на предыдущих страницах настройки будут применены ко всем издаваемым сертификатам.

- 6 После запуска мастера **Редактирование полей сертификата** на первых трех страницах **Сведения о владельце сертификата** укажите основные данные о владельце сертификата и нажмите кнопку **Далее**.



Примечание. Если для пользователя ранее уже издавался в УКЦ сертификат, то на страницах со сведениями о владельце сертификата будут указаны данные о нем. Эти данные берутся автоматически из последнего сертификата, изданного для пользователя. При необходимости, вы можете их изменить.

Просмотреть список всех сертификатов, изданных для пользователя, и узнать, какой из них — последний, вы можете в окне просмотра свойств пользователя (см. [Просмотр свойств пользователя](#)).

Редактирование полей сертификата

Сведения о владельце сертификата
Заполните сведения о владельце запрашиваемого сертификата.

Имя: Иван

Фамилия: Иванов

Приобретенное имя: Иванович

ИНН: 77211226003

СНИЛС: 12345978900

Электронная почта: ivan.ivanov@company.ru

< Назад Далее > Отмена Справка

Рисунок 63. Заполнение основных сведений о владельце сертификата ключа проверки электронной подписи

- 7 На четвертой странице **Сведения о владельце сертификата** с помощью кнопки **Изменить** отредактируйте дополнительные данные о владельце и нажмите кнопку **Далее**.

Редактирование полей сертификата

Сведения о владельце сертификата
Заполните сведения о владельце запрашиваемого сертификата.

Атрибуты	Значения
Серийный номер	
Псевдоним	
Неструктурированное имя	
Инициалы	
Компонента доменного имени	
Неструктурированный адрес	
Телефон	
Департамент	
ОГРНИП	
Описание	

Изменить

< Назад Далее > Отмена Справка

Рисунок 64. Заполнение дополнительных сведений о владельце сертификата ключа проверки электронной подписи

- 8 На странице **Состав сертификата** убедитесь в правильности параметров издаваемого сертификата, заданных на предыдущих страницах мастера, и нажмите кнопку **Готово**. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.



Внимание! При нажатии на кнопку **Отмена** на этой странице или на предыдущих страницах мастер прекратит свою работу, сертификат не будет издан, и дистрибутивы ключей не будут созданы.

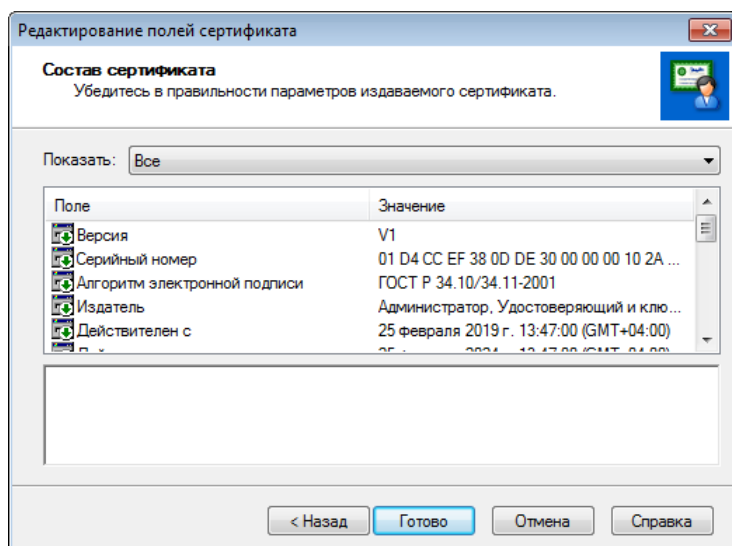


Рисунок 65. Просмотр параметров издаваемого сертификата

В результате по завершении создания ключей будет создан контейнер с ключом электронной подписи и издан сертификат ключа проверки электронной подписи пользователя. Пользователь получит изданный сертификат после того, как ключи будут переданы в программу ViPNet Центр управления сетью и отправлены на узел пользователя.

Изданный сертификат появится в представлении **Удостоверяющий центр** в разделе **Изданные сертификаты > Пользователи моей сети**. При необходимости вы можете его там найти и просмотреть (см. [Просмотр сертификатов](#)).

Издание сертификатов по запросам от пользователей своей сети ViPNet

Если срок действия ключа электронной подписи и соответствующего сертификата ключа проверки электронной подписи заканчивается, либо пользователь по каким-либо причинам желает получить новый сертификат (например, сертификат с новым назначением или расширениями), он может создать [запрос на новый сертификат](#) в ПО ViPNet, установленном на своем сетевом узле, и передать его в программу ViPNet Удостоверяющий и ключевой центр через Центр управления сетью. Запрос будет содержаться в файле *.sok.

При поступлении запросы на сертификаты от пользователей помещаются в раздел **Запросы на сертификаты > Необработанные запросы > Запросы пользователей** представления **Удостоверяющий центр**. Все поступившие запросы требуется обработать: удовлетворить либо отклонить. Запросы на сертификаты могут обрабатываться в автоматическом режиме (см. [Работа в автоматическом режиме](#)) или вручную. При автоматической обработке запросы всегда удовлетворяются. Отклонить запрос можно только при обработке вручную.

Для обработки запросов на сертификаты от пользователей в автоматическом режиме должны быть выполнены соответствующие настройки (см. [Настройка автоматического режима](#)). Чтобы обработать запросы на сертификаты вручную:

- 1 В окне программы на панели навигации выберите представление **Удостоверяющий центр** и перейдите в раздел **Запросы на сертификаты > Необработанные запросы > Запросы пользователей**.
- 2 На панели просмотра выберите один или несколько запросов и на панели инструментов нажмите кнопку **Удовлетворить** или кнопку **Отклонить**. При необходимости просмотрите параметры запроса (см. [Просмотр запроса на сертификат](#)).
- 3 При удовлетворении запроса начнется процесс издания сертификата. Если в настройках программы в разделе **Сертификаты** установлен флажок **Редактировать поля сертификатов при издании**, будет запущен мастер редактирования полей сертификата. Вы можете изменить параметры издаваемого сертификата, следуя указаниям мастера:
 - 3.1 На страницах **Сведения о владельце сертификата** выберите тип владельца сертификата и укажите необходимые данные о владельце сертификата.

Рисунок 66. Выбор типа владельца сертификата при удовлетворении запроса на сертификат

- 3.2 На странице **Источник параметров сертификата** укажите источник, из которого будут заимствованы параметры издаваемого сертификата: запрос на сертификат либо шаблон сертификата. Во втором случае в списке также выберите нужный шаблон. Чтобы отказаться от просмотра параметров издаваемого сертификата снимите флажок **Показывать параметры сертификата**.

- 3.3 Если на странице **Источник параметров сертификата** был установлен флажок **Показывать параметры сертификата**, на остальных страницах мастера при необходимости измените параметры сертификата, установленные по умолчанию в соответствии с выбранным источником.
- 3.4 На странице **Состав сертификата** убедитесь в правильности параметров издаваемого сертификата, заданных на предыдущих страницах мастера, и нажмите кнопку **Готово**.



Примечание. При удовлетворении запроса с недействительной подписью появится сообщение с предложением отклонить запрос. Издать сертификат по такому запросу нельзя.

- 4 При отклонении запроса в появившемся окне с сообщением подтвердите операцию.

В результате удовлетворения запроса будет издан сертификат, после чего отправлен на сетевой узел пользователя. Изданный сертификат появится в разделе **Изданные сертификаты** > **Пользователи моей сети**, запрос будет перемещен в раздел **Запросы на сертификаты** > **Удовлетворенные запросы**.

В результате отклонения запроса на сетевой узел пользователя будет отправлен файл запроса в неизменном виде. Подобный ответ будет интерпретирован как отказ в издании сертификата. Запрос будет перемещен в раздел **Запросы на сертификаты** > **Отклоненные запросы**.

Издание сертификатов по запросам, поступившим из центра регистрации

Выдача сертификатов подписи пользователям своей сети ViPNet или зарегистрированным внешним пользователям может производиться по специальным запросам через центры регистрации. В данном случае в программе ViPNet Registration Point для пользователя формируется запрос на сертификат, который заверяется сертификатом администратора центра регистрации, после чего передается в программу ViPNet Удостоверяющий и ключевой центр через Центр управления сетью (см. раздел [Взаимодействие с программой ViPNet Registration Point](#)).

При поступлении запроса на сертификаты из центра регистрации помещаются в раздел **Запросы на сертификаты** > **Необработанные запросы** > **Запросы центров регистрации представления Удостоверяющий центр**. Все поступившие запросы требуется обработать: удовлетворить либо отклонить. Запросы на сертификаты могут обрабатываться в автоматическом режиме (см. [Работа в автоматическом режиме](#)) или вручную. При автоматической обработке запросы всегда удовлетворяются. Отклонить запрос можно только при обработке вручную.



Совет. Если требуется, чтобы сертификаты, изданные по запросам из центров регистрации, содержали информацию об этих центрах — имя и серийный номер сертификата администратора центра регистрации — перед обработкой запросов выполните соответствующую настройку (см. [Настройка добавления информации о центрах регистрации в сертификаты пользователей](#)).

Для обработки запросов на сертификаты из центра регистрации в автоматическом режиме должны быть выполнены соответствующие настройки (см. [Настройка автоматического режима](#)). Чтобы обработать запросы на сертификаты вручную:

- 1 В окне программы на панели навигации выберите представление **Удостоверяющий центр** и перейдите в раздел **Запросы на сертификаты > Необработанные запросы > Запросы центров регистрации**.
- 2 На панели просмотра выберите один или несколько запросов и на панели инструментов нажмите кнопку **Удовлетворить** или кнопку **Отклонить**. При необходимости просмотрите параметры запроса (см. [Просмотр запроса на сертификат](#)).
- 3 При удовлетворении запроса начнется процесс издания сертификата. Если в настройках программы в разделе **Сертификаты** установлен флажок **Редактировать поля сертификатов при издании**, будет запущен мастер редактирования полей сертификата. Вы можете изменить параметры издаваемого сертификата, следуя указаниям мастера:
 - 3.1 На страницах **Сведения о владельце сертификата** выберите тип владельца сертификата и укажите необходимые данные о владельце сертификата.

Рисунок 67. Выбор типа владельца сертификата при удовлетворении запроса на сертификат

- 3.2 На странице **Источник параметров сертификата** укажите источник, из которого будут заимствованы параметры издаваемого сертификата: запрос на сертификат либо шаблон сертификата. Во втором случае в списке также выберите нужный шаблон. Чтобы отказаться от просмотра параметров издаваемого сертификата снимите флажок **Показывать параметры сертификата**.

- 3.3 Если на странице **Источник параметров сертификата** был установлен флажок **Показывать параметры сертификата**, на остальных страницах мастера при необходимости измените параметры сертификата, установленные по умолчанию в соответствии с выбранным источником.
- 3.4 На странице **Состав сертификата** убедитесь в правильности параметров издаваемого сертификата, заданных на предыдущих страницах мастера, и нажмите кнопку **Готово**.



Примечание. При удовлетворении запроса с недействительной подписью появится сообщение с предложением отклонить запрос. Издать сертификат по такому запросу нельзя.

- 4 При отклонении запроса в появившемся окне с сообщением подтвердите операцию.

В результате удовлетворения запроса будет издан сертификат, после чего отправлен в центр регистрации. Изданный сертификат для пользователя своей сети ViPNet появится в разделе **Изданные сертификаты > Пользователи моей сети**. Изданный сертификат для внешнего пользователя появится в разделе **Изданные сертификаты > Внешние пользователи**. Запрос будет перемещен в раздел **Запросы на сертификаты > Удовлетворенные запросы**.

В результате отклонения запроса в центр регистрации будет отправлен файл с запросом в неизменном виде. Подобный ответ будет интерпретирован как отказ в издании сертификата. Запрос будет перемещен в раздел **Запросы на сертификаты > Отклоненные запросы**.

Издание сертификатов по запросам от внешних пользователей

Запросы на издание сертификатов могут поступать напрямую от внешних пользователей. Такие запросы передаются в виде файлов в одном из следующих форматов:

- PKCS #10 (файл *.p10) — широко распространенный формат запросов на сертификат, поддерживаемый большинством удостоверяющих центров. Подробнее см. [RFC 2986](#).
- СМС (файл *.смс) — менее распространенный формат запросов на сертификат. Подробнее см. [RFC 5272](#).

Запросы на издание сертификатов от внешних пользователей вы можете обработать только вручную. Для этого выполните следующие действия:

- 1 В окне программы на панели навигации выберите представление **Удостоверяющий центр** и перейдите в раздел **Изданные сертификаты > Внешние пользователи**.
- 2 На панели просмотра нажмите кнопку **Загрузить и обработать запрос**.
- 3 В появившемся окне выберите файл *.p10 или *.смс, в котором содержится запрос.



Примечание. При необходимости можно выбрать сразу несколько файлов с запросами.

Запросы, размер которых превышает 10 Кбайт, загрузить нельзя.

- В окне **Издание сертификатов пользователей** в списке ознакомьтесь с параметрами запроса: для кого запрошен сертификат и какой статус у запроса в текущий момент. При необходимости просмотрите параметры запроса с помощью кнопки **Свойства** (см. [Просмотр запроса на сертификат](#)).

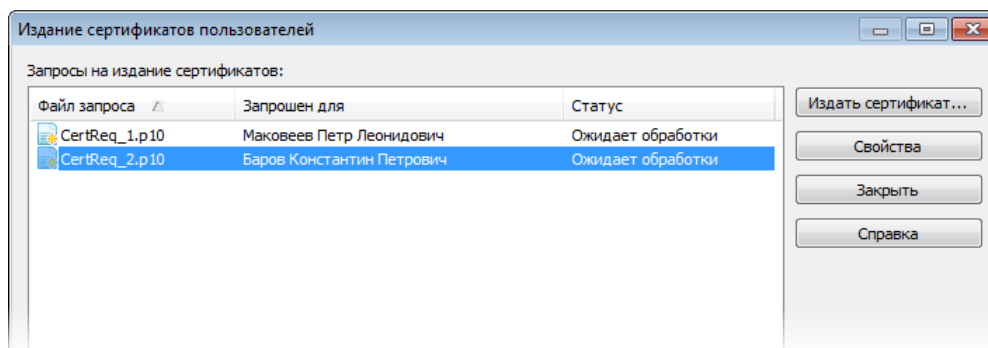


Рисунок 68. Выбор запроса для издания сертификата

- Выберите запрос в списке, после чего нажмите кнопку **Издать сертификат**. Если в настройках программы в разделе **Сертификаты** установлен флажок **Редактировать поля сертификатов при издании**, будет запущен мастер редактирования полей сертификата. Вы можете изменить параметры издаваемого сертификата, следуя указаниям мастера.
- На страницах **Сведения о владельце сертификата** выберите тип владельца сертификата и укажите необходимые данные о владельце сертификата.
- На странице **Источник параметров сертификата** укажите источник, из которого будут заимствованы параметры издаваемого сертификата: запрос на сертификат либо шаблон сертификата. Во втором случае в списке также выберите нужный шаблон. Чтобы отказаться от просмотра параметров издаваемого сертификата снимите флажок **Показывать параметры сертификата**.

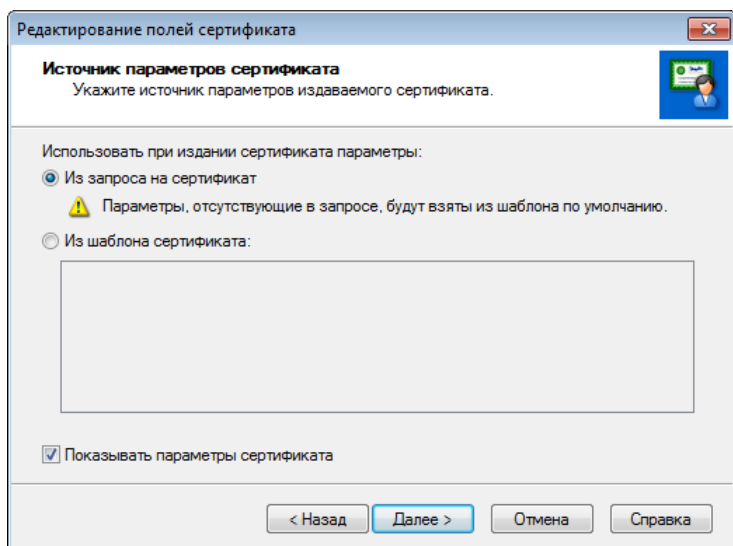


Рисунок 69. Выбор источника параметров издаваемого сертификата

- 8 Если на странице **Источник параметров сертификата** был установлен флажок **Показывать параметры сертификата**, на остальных страницах мастера при необходимости измените параметры сертификата, установленные по умолчанию в соответствии с выбранным источником.
- 9 На странице **Состав сертификата** убедитесь в правильности параметров издаваемого сертификата, заданных на предыдущих страницах мастера, после чего нажмите кнопку **Готово**.
- 10 В окне сообщения об успешном издании сертификата нажмите кнопку **ОК**.

В результате будет издан сертификат, который появится в представлении **Удостоверяющий центр** в разделе **Изданные сертификаты > Внешние пользователи**. Выполните экспорт сертификата (см. [Экспорт сертификатов](#)) для его последующей передачи пользователю.

Настройка параметров издания сертификатов

Создание и изменение шаблонов сертификатов

В программе ViPNet Удостоверяющий и ключевой центр при издании сертификатов ключа проверки электронной подписи используются [шаблоны сертификатов](#) в следующих случаях:

- всегда при издании сертификатов по инициативе администратора УКЦ;
- при издании сертификатов по запросам, если в качестве источника параметров сертификата выбран шаблон.

В зависимости от настроек программы во время издания сертификата его параметры могут либо заимствоваться из шаблона полностью без возможности изменения, либо дополняться и изменяться (за исключением криптопровайдера и параметров алгоритма подписи, которые всегда берутся из шаблона).



Примечание. Параметры всех шаблонов сертификатов хранятся в файле `cert_tem.ini` в папке `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\ini`. При обновлении программного обеспечения существующие шаблоны не изменяются и не удаляются.

В конфигурацию программы входит несколько стандартных шаблонов сертификатов подписи и шифрования с разными алгоритмами подписи:

- «Сертификат подписи» — пользователь может использовать ключ для электронной подписи и не может отказаться от совершенного действия.
- «Сертификат подписи и шифрования» — пользователь может использовать ключ для электронной подписи, шифрования ключей и данных, согласования ключей и не может отказаться от совершенного действия.
- «Сертификат шифрования» — пользователь может использовать ключ для шифрования ключей и данных, а также согласования ключей.



Примечание. По требованиям ФСБ России после 31 декабря 2019 года использование алгоритма ГОСТ Р 34.10-2001 для формирования электронной подписи недопустимо. Поэтому в качестве шаблона сертификата вы можете назначить только шаблон с алгоритмом ГОСТ Р 34.10-2012.

При необходимости администратор УКЦ может с помощью мастера создать другие шаблоны сертификатов или отредактировать существующие.

Для создания нового шаблона сертификата:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Сертификаты > Шаблоны сертификатов**.

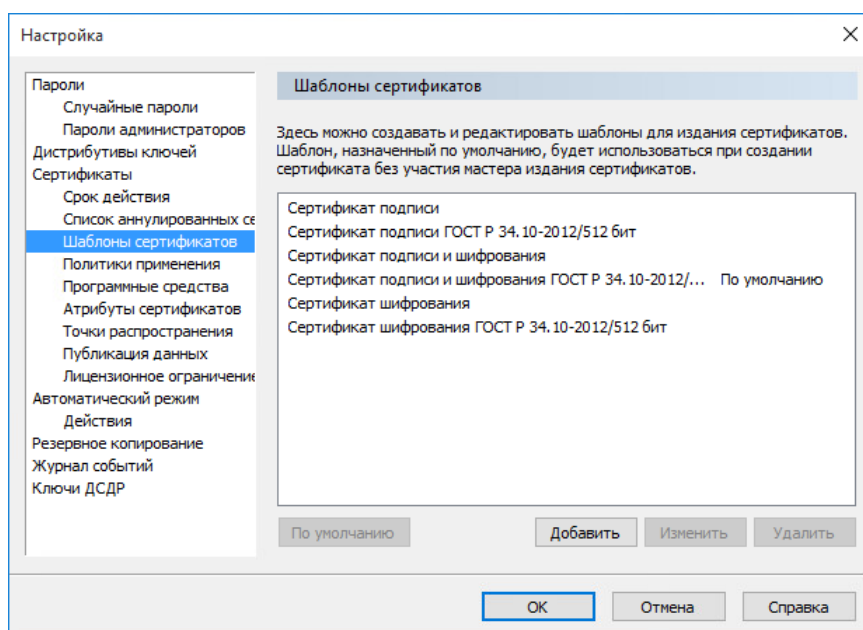


Рисунок 70. Управление шаблонами сертификатов

- 3 В разделе **Шаблоны сертификатов** нажмите кнопку **Добавить** и следуйте указаниям мастера создания шаблона сертификата.
- 4 На первой странице мастера введите имя шаблона и нажмите кнопку **Далее**. Имя шаблона должно быть уникальным.
- 5 На странице **Алгоритм и параметры ключа** выберите криптопровайдер в соответствии с приведенной ниже таблицей либо другой криптопровайдер, установленный на компьютере. Выбранный криптопровайдер определит алгоритм электронной подписи, по которому будут создаваться ключ электронной подписи и ключ проверки электронной подписи.

Кроме этого, укажите параметры алгоритма электронной подписи. В соответствии с заданными параметрами будет автоматически определена длина ключа проверки электронной подписи.



Примечание. Сертификаты пользователей, изданные по алгоритмам ГОСТ Р 34.10-2012, не могут использоваться в ПО ViPNet версии 3.2 и ниже.

Таблица 6. Характеристика криптопровайдеров и алгоритмов электронной подписи

Криптопровайдер и соответствующий ему алгоритм электронной подписи	Параметры алгоритма подписи	Длина ключа проверки электронной подписи и алгоритм хэширования
Infotecs GOST 2012/512	ГОСТ Р 34.10 - 2001. Параметры	512 бит
Cryptographic Service Provider	по умолчанию (рекомендуется)	ГОСТ Р 34.11-2012/256
ГОСТ Р 34.10-2012/512	OID «1.2.643.2.2. 35.1»	
Новый стандарт электронной	ГОСТ Р 34.10 - 2001 Параметры	

Криптопровайдер и соответствующий ему алгоритм электронной подписи	Параметры алгоритма подписи	Длина ключа проверки электронной подписи и алгоритм хэширования
подписи от 2012 года с длиной ключа электронной подписи 256 бит OID «1.2.643.7.1.1.1.1»	подписи В OID «1.2.643.2.2. 35.2» ГОСТ Р 34.10 - 2001. Параметры подписи С OID «1.2.643.2.2. 35.3»	
Infotecs GOST 2012/1024 Cryptographic Service Provider ГОСТ Р 34.10-2012/1024 Новый стандарт электронной подписи от 2012 года с длиной ключа электронной подписи 512 бит OID «1.2.643.7.1.1.1.2»	ГОСТ Р 34.10 - 2012/1024. Набор параметров А ГОСТ Р 34.10 - 2012/1024. Набор параметров В	1024 бит ГОСТ Р 34.11-2012/512



Совет. Рекомендуется использовать параметры алгоритма, предлагаемые по умолчанию. Данные параметры характеризуются наибольшей скоростью вычисления и проверки электронной подписи.

После этого нажмите кнопку **Далее**.

Шаблон сертификата

Алгоритм и параметры ключа
Укажите алгоритм и параметры ключа

Криптопровайдер: Infotecs GOST 2012/512 Cryptographic Service Provide

Алгоритм электронной подписи: ГОСТ Р 34.10-2012/512

Параметры алгоритма ЭП: ГОСТ Р 34.10 Параметры по умолчанию

Длина ключа проверки ЭП (бит): 512

< Назад **Далее >** Готово Отмена Справка

Рисунок 71. Настройка параметров ключа электронной подписи

- На следующей странице задайте срок действия сертификата, после чего нажмите кнопку **Далее**.

Рисунок 72. Указание срока действия сертификата



Примечание. Заданный срок действия сертификата определяет срок действия ключа электронной подписи. Если срок действия сертификата не более 12 месяцев (1 года), то такой же срок действия будет у ключа электронной подписи. Если срок действия сертификата больше 12 месяцев (1 года), то срок действия ключа электронной подписи не будет превышать 15 месяцев (1 год и 3 месяца). Максимальный срок действия сертификата пользователя составляет 180 месяцев (15 лет).

- 7 На странице **Расширения сертификата** укажите необходимые расширения, которые будут добавлены в новый шаблон. Расширения сертификата позволяют регулировать возможности использования сертификата для выполнения определенных действий и работы с различными сервисами, например, **OCSP-сервером**, **TSP-сервером**, EFS (шифрованная файловая система) и другими.

По умолчанию в шаблон добавлено расширение **Основные ограничения**, с помощью которого определяется, что сертификат издается для пользователя. Удалить это расширение или изменить его нельзя.

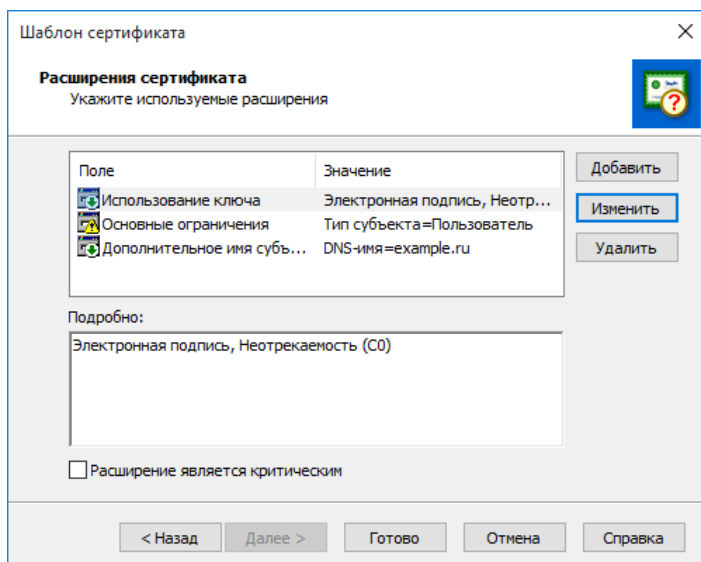


Рисунок 73. Формирование расширений сертификата

Для добавления расширения нажмите кнопку **Добавить** и в окне **Допустимые расширения** выберите одно из расширений:

- **Тип идентификации.** В появившемся окне укажите тип идентификации владельца сертификата.

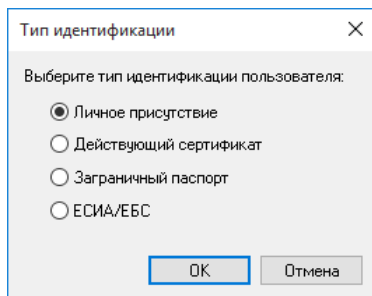


Рисунок 74. Выбор типа идентификации владельца сертификата

- **Использование ключа.** В появившемся окне укажите назначение ключа и сертификата, установив соответствующие флажки, и нажмите кнопку **ОК**.

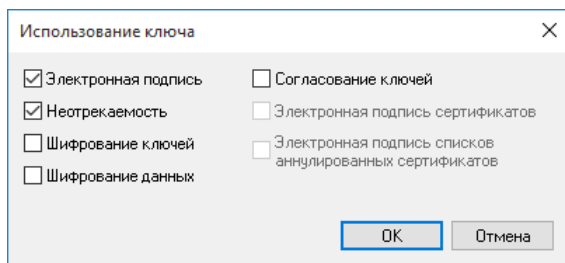


Рисунок 75. Настройка параметров использования ключа

- **Улучшенный ключ.** В окне **Расширенное использование ключа** с помощью кнопок **Добавить** и **Удалить** сформируйте список расширенного использования ключа и нажмите кнопку **ОК**.

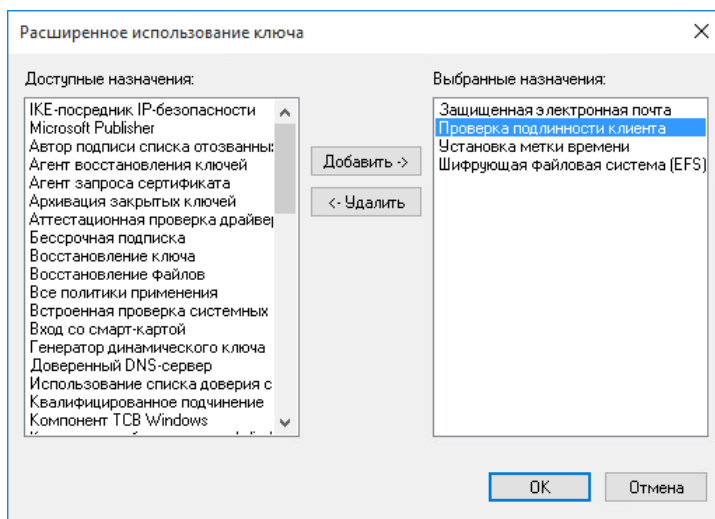


Рисунок 76. Выбор назначений расширенного использования ключа

- **Политики сертификата.** В появившемся окне с помощью кнопок **Добавить** и **Удалить** выберите политики применения сертификата и нажмите кнопку **ОК**. При необходимости предварительно выполните настройку списка политик применения сертификата (см. [Настройка списка политик применения сертификата](#)).

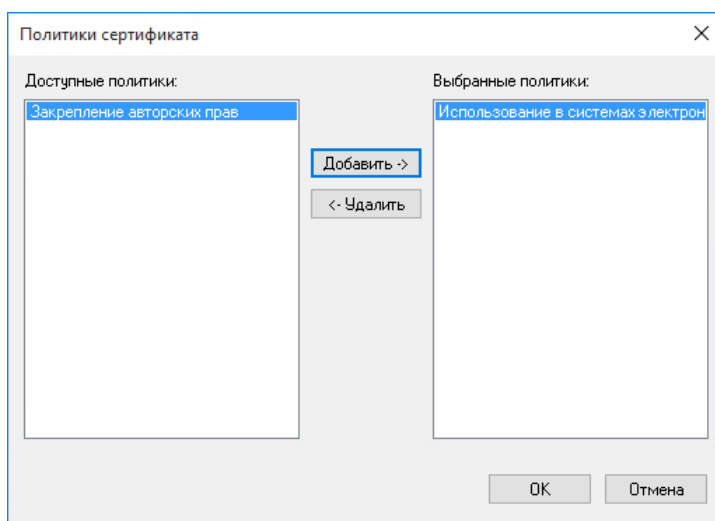


Рисунок 77. Добавление политики применения сертификата



Примечание. В настройках программы в списке используемых политик применения присутствуют политики, описывающие класс защиты средств удостоверяющего центра. В создаваемые шаблоны их добавить нельзя. В издаваемые сертификаты пользователей эти политики добавляются всегда по умолчанию при соответствующих настройках программы (см. [Настройка параметров издания квалифицированных сертификатов](#)).

- **Дополнительное имя субъекта.** Для указания дополнительного имени пользователя сертификата (например, DNS-имени компьютера или имени пользователя сервиса) нажмите кнопку **Добавить**, в появившемся окне задайте тип имени и его значение, затем нажмите кнопку **ОК**.

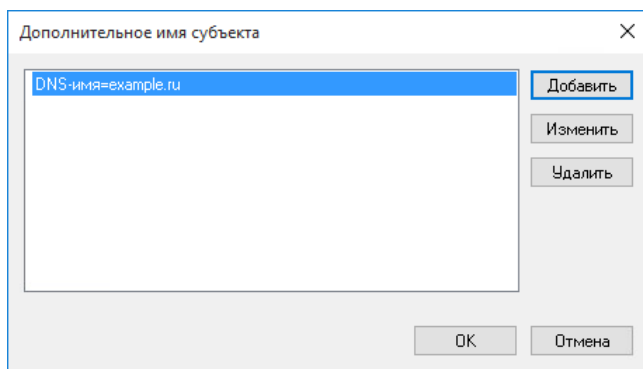


Рисунок 78. Задание альтернативного имени владельца сертификата ключа проверки электронной подписи

Для изменения параметров используемого расширения воспользуйтесь кнопкой **Изменить**, для удаления ненужного расширения — кнопкой **Удалить**.

При необходимости для выбранного расширения установите флажок **Расширение является критическим**. В этом случае расширение будет отмечено как критическое. Это означает, что если прикладное ПО не сможет обработать такое расширение, то сертификат будет признан недействительным.

- 8 Нажмите кнопку **Готово**. При необходимости изменения параметров шаблона вернитесь на нужную страницу с помощью кнопки **Назад**.
- 9 В результате в списке шаблонов сертификатов появится новый шаблон. Для сохранения созданного шаблона нажмите кнопку **ОК**.

Чтобы изменить параметры шаблона сертификата, выберите его в списке и нажмите кнопку **Изменить**, затем на страницах мастера внесите необходимые коррективы (см. выше) и нажмите кнопку **ОК**.

Чтобы удалить ненужный шаблон, выберите его в списке и нажмите кнопку **Удалить**.



Примечание. При взаимодействии с центрами регистрации (узлами с программным обеспечением [ViPNet Registration Point](#)) после добавления, изменения или удаления шаблонов сертификатов сформируйте и отправьте на них ключи узлов (см. [Создание и передача ключей узлов в ЦУС](#)). Данная операция требуется для того, чтобы в центры регистрации поступила актуальная информация о шаблонах сертификатов, сформированных в УКЦ.

Чтобы назначить шаблон используемым по умолчанию, выберите его в списке и нажмите кнопку **По умолчанию**. В соответствии с параметрами данного шаблона будет производиться издание сертификатов ключа проверки электронной подписи при автоматическом создании ключей и дистрибутивов.

Настройка списка политик применения сертификата

Область использования сертификата ключа проверки электронной подписи можно определить путем добавления в него специального расширения — [политики применения](#). То есть, если сертификат следует использовать для каких-то определенных целей, например, только на торговой площадке или только для подписи отчетной документации, то при его издании можно добавить соответствующую политику, которая будет определять сферу его действия (подробнее см. [RFC 5280](#)).

С политикой применения изданного сертификата ключа проверки электронной подписи можно ознакомиться, нажав кнопку **Заявление издателя** в окне просмотра сертификата.

Примечание. Политика применения может быть представлена в виде текста или ссылки на веб-страницу.



В конфигурации программы имеются политики применения, описывающие классы защищенности средств электронной подписи, но они скрыты от администратора и в настройках программы не отображаются. Данные политики в обязательном порядке добавляются в издаваемые квалифицированные сертификаты при соответствующих настройках программы (см. [Издание квалифицированных сертификатов](#)).

Политики применения также можно добавлять в шаблоны сертификатов. Подробнее см. раздел [Создание и редактирование шаблонов сертификатов](#) (см. [Создание и изменение шаблонов сертификатов](#)).

Прежде чем добавить политику применения в издаваемый сертификат или шаблон сертификата, ее предварительно требуется создать. Чтобы создать политику применения:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Сертификаты > Политики применения**.

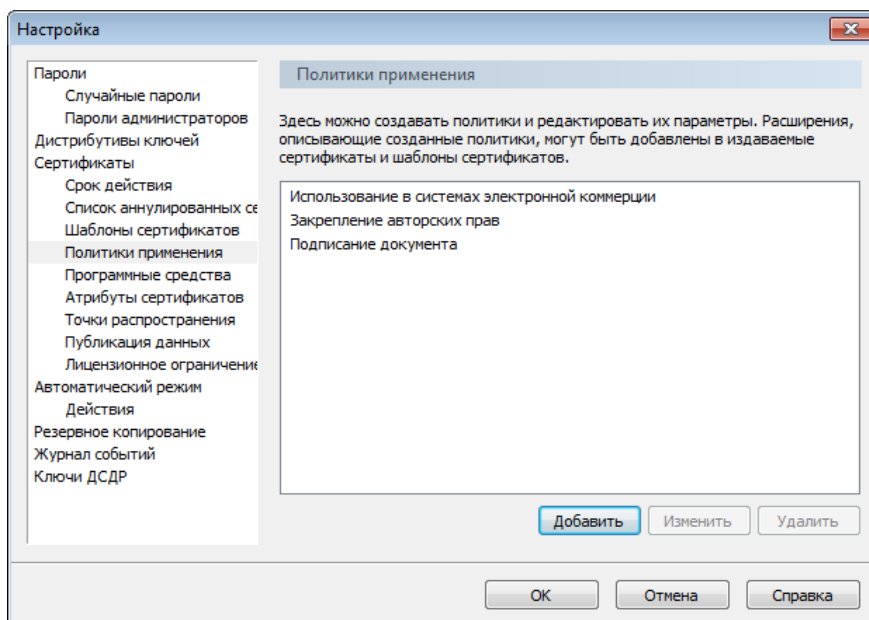


Рисунок 79. Управление политиками применения сертификатов

3 В разделе **Политики применения** нажмите кнопку **Добавить**.

4 В окне **Политика применения сертификата**:

- В поле **Наименование** введите название политики.
- В поле **Идентификатор** введите идентификатор политики — **OID**. Идентификатор должен состоять из набора десятичных чисел, разделенных точками. Длина идентификатора должна быть не более 64 символов.



Внимание! Идентификатор политики применения должен начинаться с корневого идентификатора организации, зарегистрированного в мировом пространстве идентификаторов объектов. Российский сегмент этого пространства имеет корневой идентификатор 1.2.643.

Поля **Наименование** и **Идентификатор** обязательно должны быть заполнены. Кроме того, идентификатор должен иметь уникальное значение в пределах данного удостоверяющего центра.

- В поле **Адрес описания** введите URL-адрес документа, содержащего описание политики (в виде HTTP, FTP, файла или адреса LDAP).
- В поле **Краткое описание** введите краткое описание политики сертификации.

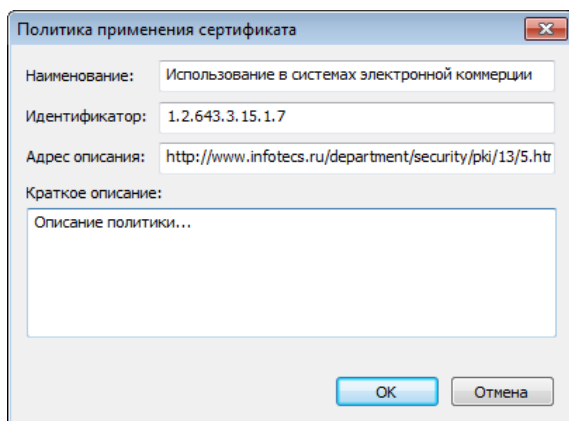


Рисунок 80. Добавление политики применения

5 По окончании ввода данных нажмите кнопку **ОК**. Созданная политика появится в списке в разделе **Политики применения**.

6 Для сохранения новой политики применения нажмите кнопку **ОК**.

Чтобы редактировать политику, выберите ее в списке и нажмите кнопку **Изменить**, затем в окне **Политика применения сертификата** внесите необходимые коррективы (см. выше) и нажмите кнопку **ОК**.

Чтобы удалить политику, выберите ее в списке и нажмите кнопку **Удалить**.



Примечание. При взаимодействии с центрами регистрации (узлами с программным обеспечением [ViPNet Registration Point](#)) после добавления, изменения или удаления политик применения сертификатов сформируйте и отправьте на них ключи узлов (см. [Создание и передача ключей узлов в ЦУС](#)). Данная операция требуется для того, чтобы в центры регистрации поступила актуальная информация о политиках применения, заданных в УКЦ.

Настройка добавления информации о центрах регистрации в сертификаты пользователей

В сертификаты пользователей, издаваемые по запросам из центров регистрации (см. [Издание сертификатов по запросам, поступившим из центра регистрации](#)), может добавляться информация об этих центрах — имя и серийный номер сертификата администратора центра регистрации.



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

Чтобы информация о центрах регистрации добавлялась в издаваемые сертификаты пользователей:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Сертификаты > Атрибуты сертификатов**.

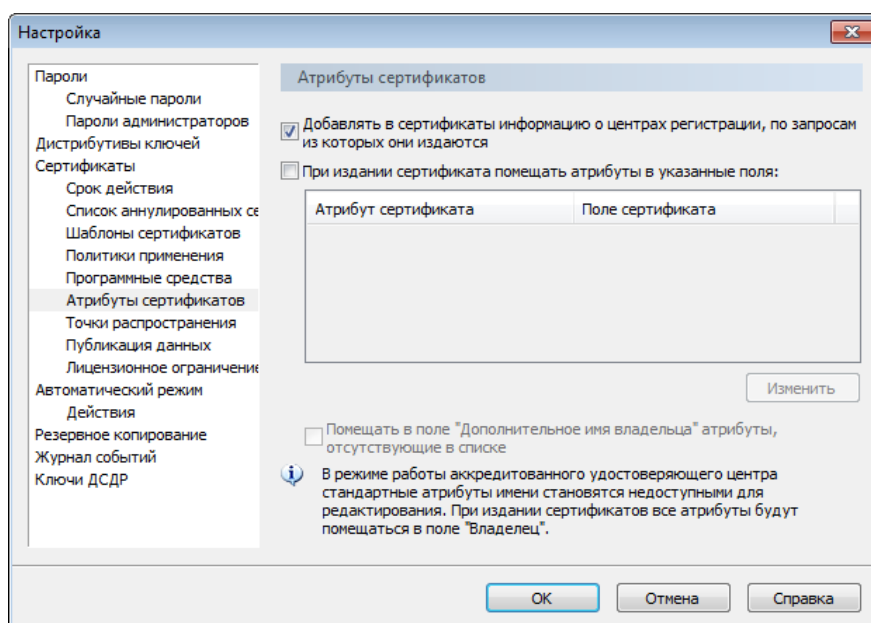


Рисунок 81. Настройка добавления информации о центрах регистрации в издаваемые сертификаты

- 3 Установите флажок **Добавлять в сертификаты информацию о центрах регистрации, по запросам из которых они издаются**.
- 4 Чтобы сохранить настройки, нажмите кнопку **ОК**.

В результате информация о центрах регистрации будет добавляться в сертификаты, издаваемые по их запросам.

Настройка распределения атрибутов сертификатов

Для передачи идентификационных данных о владельце сертификата используются атрибуты имени. Например, такие как «ИНН», «СНИЛС», «E-mail». В сертификатах атрибуты имени могут размещаться в полях типа «Владелец» или «Дополнительное имя владельца». Если вы хотите, чтобы

в соответствии с рекомендациями приказа ФСБ от 27.12.2011 № 795 в сертификатах часть атрибутов имени находилась в поле «Владелец», а часть — в поле «Дополнительное имя владельца», то вы можете указать, в какое поле должны помещаться те или иные атрибуты при издании сертификатов.



Внимание! Заданное распределение атрибутов будет распространяться только на сертификаты пользователей.

В квалифицированных сертификатах все атрибуты автоматически помещаются в поле «Владелец». Если в запросе на сертификат для каких-то атрибутов было указано поле «Дополнительное имя владельца», то в режиме работы аккредитованного удостоверяющего центра оно будет автоматически изменено на поле «Владелец». Возможность изменения полей в настройках УКЦ для стандартных атрибутов станет недоступна.

Чтобы указать, в каких полях должны располагаться атрибуты в издаваемых сертификатах, выполните следующие действия:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Сертификаты > Атрибуты сертификатов**.

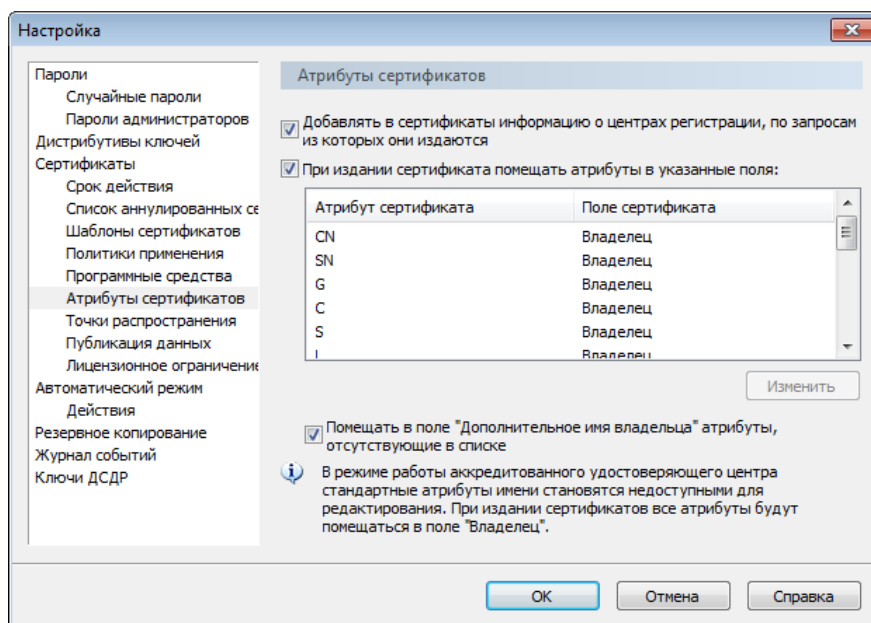


Рисунок 82. Распределение атрибутов сертификатов

- 3 В разделе **Атрибуты сертификатов** установите флажок **При издании сертификата помещать атрибуты в указанные поля** и для нужных атрибутов в списке с помощью кнопки **Изменить** укажите поле, в которое они должны помещаться при издании сертификатов.



Примечание. В списке представлены наиболее распространенные атрибуты сертификатов.

- 4 Если вы издаете сертификаты с атрибутами, которые не указаны в списке и которые по требованиям не должны попадать в поле «Владелец», установите флажок **Помещать в поле «Дополнительное имя владельца» атрибуты, отсутствующие в списке**. При издании сертификатов такие атрибуты будут помещаться в поле «Дополнительное имя владельца».
- 5 Для сохранения настроек нажмите кнопку **ОК**.

Настройка оповещения об истечении срока действия сертификатов пользователей

Ключи подписи и сертификаты пользователей имеют ограниченный срок действия. В программе ViPNet Удостоверяющий и ключевой центр предусмотрена возможность оповещения об истечении срока действия изданных сертификатов пользователей своей сети. В зависимости от настроек программы оповещение может производиться как перед истечением срока действия, так и после него.

Чтобы настроить параметры оповещения об истечении срока действия сертификатов пользователей:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Сертификаты > Срок действия**.

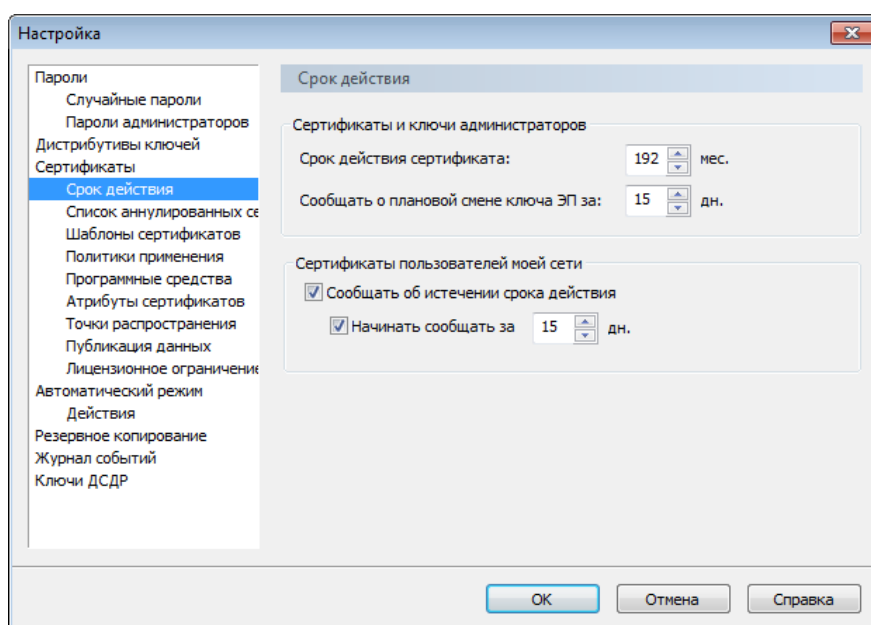


Рисунок 83. Настройка оповещения об окончании сроков действия изданных сертификатов пользователей своей сети

- 3 В разделе **Срок действия** в группе **Сертификаты пользователей моей сети** установите флажки **Сообщать об истечении срока действия** и **Начинать сообщать за** для предварительного оповещения об окончании срока действия изданных сертификатов пользователей своей сети.

В поле справа от флажка **Начинать сообщать за** введите количество дней до истечения срока действия (не более 30), когда следует производить оповещение.

Если будет установлен только флажок **Сообщать об истечении срока действия**, то оповещение будет производиться уже после окончания срока действия изданных сертификатов пользователей своей сети.

4 Для сохранения указанных настроек нажмите кнопку **ОК**.

Настройка обработки поля ИНН

Начиная с версии 4.6.9, дополнительный атрибут имени — ИНН зависит от типа владельца сертификата запроса и задается в разных полях:

- в новом поле **ИНН ЮЛ** (расширение INNLE) — для юридических лиц. Состоит из 10 цифр.
- в старом поле **ИНН** (расширение INN) — для физических лиц и индивидуальных предпринимателей. Состоит из 12 цифр (два нуля и 10 цифр). В УКЦ версии 4.6.7 и ниже ИНН для юридических лиц также указывался в этом формате и в начало номера ИНН добавлялись два нуля.

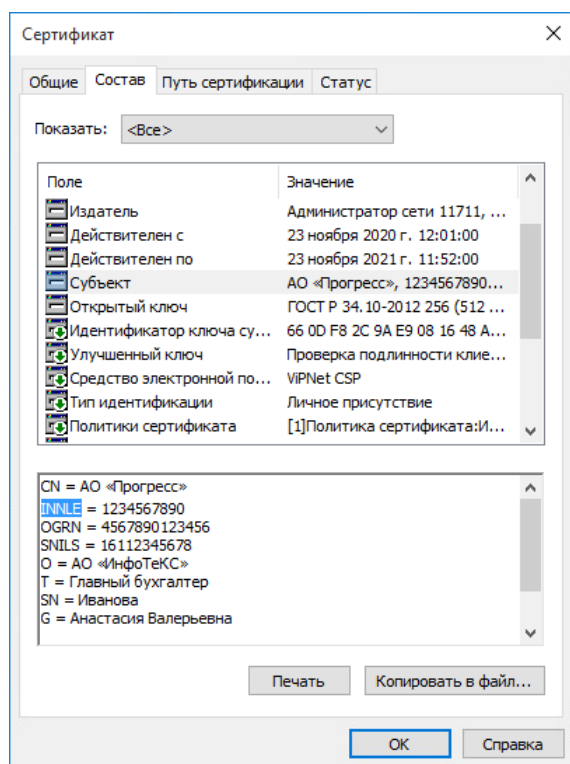


Рисунок 84. Пример сертификата с атрибутом имени ИНН ЮЛ (в новом формате)

Для совместимости полей ИНН для юридических лиц в старом и новом формате предназначены два режима обработки этого поля:

- **1** (по умолчанию) — если запрос на сертификат содержит ИНН из 12 цифр в старом формате или из 10 цифр в новом формате, то сертификат выдается с ИНН из 10 цифр в новом формате с расширением 1.2.643.100.4 (INNLE);
- **0** — если запрос на сертификат содержит ИНН из 12 цифр в старом формате или из 10 цифр в новом формате, то сертификат выдается с ИНН из 12 цифр в старом формате с расширением INN.

Чтобы для юридических лиц использовать ИНН старого формата:

- 1 Завершите работу с УКЦ.
- 2 Откройте файл `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\ini\KC.ini`.
- 3 В секции `[Certification]` для параметра `Mode use subject name OID` укажите значение **0**.
- 4 Запустите УКЦ.

Издание квалифицированных сертификатов

Требования к изданию квалифицированных сертификатов

Если удостоверяющий центр, функции которого осуществляет программа ViPNet Удостоверяющий и ключевой центр, выступает в качестве [аккредитованного](#), то все издаваемые сертификаты пользователей и сертификаты администраторов, которыми они заверяются, должны быть в формате, соответствующем требованиям приказа ФСБ от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи». Кроме того, чтобы издавать квалифицированные сертификаты, в качестве текущего сертификата администратора УКЦ (см. [Выбор текущего сертификата администратора](#)) должен быть выбран квалифицированный сертификат, полученный от удостоверяющего центра Минкомсвязи России (см. [Установление доверительных отношений с удостоверяющим центром Минкомсвязи России](#)).



Примечание. Издаваемые сертификаты в этом случае будут являться квалифицированными.

Для соответствия требованиям приказа № 795 в издаваемых сертификатах (в том числе, и в сертификатах администраторов) в обязательном порядке должны присутствовать:

- Дополнительные атрибуты имени владельца сертификата.

Наборы атрибутов, которые должны содержаться в квалифицированных сертификатах, выдаваемых разным видам субъектов, приведены в разделе ниже (см. [Дополнительные атрибуты имени в квалифицированных сертификатах разных видов субъектов](#)).

- Расширения, содержащие:
 - Наименование средств удостоверяющего центра.
 - Наименование средства электронной подписи, используемого в удостоверяющем центре.
 - Номера сертификатов соответствия средств удостоверяющего центра и средств электронной подписи удостоверяющего центра требованиям контролирующих органов (требованиям, установленным в соответствии с Федеральным законом 06.04.2011 № 63-ФЗ «Об электронной подписи» ([текст закона](#))).
 - Политики сертификата, в соответствии с которыми должен использоваться квалифицированный сертификат и которые описывают класс защищенности средств электронной подписи. Указываются в расширении «Политики сертификата» путем включения идентификаторов, описанных в таблице ниже:

Таблица 7. Идентификаторы политик классов защищенности

Класс защищенности	Идентификатор политики (OID)
Класс средств КС1	1.2.643.100.113.1
Класс средств КС2	1.2.643.100.113.1
	1.2.643.100.113.2
Класс средств КС3	1.2.643.100.113.1
	1.2.643.100.113.2
	1.2.643.100.113.3
Класс средств КВ1	1.2.643.100.113.1
	1.2.643.100.113.2
	1.2.643.100.113.3
	1.2.643.100.113.4
Класс средств КВ2	1.2.643.100.113.1
	1.2.643.100.113.2
	1.2.643.100.113.3
	1.2.643.100.113.4
	1.2.643.100.113.5
Класс средств КА1	1.2.643.100.113.1
	1.2.643.100.113.2
	1.2.643.100.113.3
	1.2.643.100.113.4
	1.2.643.100.113.5
	1.2.643.100.113.6



Совет. Для средств электронной подписи, класс которых отличается от класса средств удостоверяющего центра, где они используются, следует указывать идентификаторы класса средств удостоверяющего центра.

При необходимости дополнительно можно указать информацию о средстве электронной подписи владельцев сертификатов (в сертификатах пользователей).

- Тип идентификации владельца сертификата:
 - Личное присутствие.
 - Действующий сертификат.
 - Заграничный паспорт.
 - ЕСИА/ЕБС (Единая система идентификации и аутентификации/Единая биометрическая система).

Дополнительные атрибуты имени владельца сертификата требуется добавлять вручную в каждый издаваемый сертификат, поэтому в процессе издания параметры сертификатов должны отображаться для редактирования. В большей степени это относится к сертификатам пользователей, поскольку их можно издавать без мастера редактирования полей сертификатов. Подробнее см. раздел [Издание сертификатов](#).

Остальные расширения из перечисленных в издаваемые сертификаты добавляются автоматически, в том случае, если в УКЦ заданы дополнительные настройки. Данные настройки вы можете задать либо при первичной инициализации (см. [Установка и первичная инициализация программы ViPNet Удостоверяющий и ключевой центр](#)), либо непосредственно при работе с программой (см. [Настройка параметров издания квалифицированных сертификатов](#)). Разница состоит в следующем:

- В первом случае изданный в процессе инициализации сертификат администратора УКЦ, а также сертификаты пользователей, изданные сразу после развертывания УКЦ, будут в формате квалифицированных (поскольку в них будут все необходимые расширения).
- Во втором случае имеющийся сертификат администратора и сертификаты пользователей придется переиздавать, чтобы они получили формат квалифицированных сертификатов.

Дополнительные атрибуты имени в квалифицированных сертификатах разных видов субъектов

Набор дополнительных атрибутов имени, которые должны присутствовать в квалифицированном сертификате, зависит от того, для какого субъекта издается данный сертификат. Наборы дополнительных атрибутов имени в сертификатах разных видов субъектов с указанием соответствующих расширений приведены в таблице ниже.

Таблица 8. Списки атрибутов имени в квалифицированных сертификатах разных видов субъектов

Атрибут имени владельца сертификата	Расширение сертификата
Сертификат для физического лица:	
Фамилия, имя, отчество владельца сертификата	Common Name
ИНН (индивидуальный номер налогоплательщика) владельца сертификата	INN
СНИЛС (страховой номер индивидуального лицевого счета) владельца сертификата	SNILS
Страна (RU)	Country
Фамилия владельца сертификата	Surname
Имя и отчество владельца сертификата	Given Name

Атрибут имени владельца сертификата	Расширение сертификата
Сертификат для субъекта, являющегося физическим лицом и представляющего юридическое лицо:	
Наименование организации, которую представляет владелец сертификата	Common Name
СНИЛС владельца сертификата (представителя организации)	SNILS
Фамилия владельца сертификата	Surname
Имя и отчество владельца сертификата	Given Name
Наименование организации, которую представляет владелец сертификата	Organization
Наименование подразделения организации, сотрудником которого является владелец сертификата	Organization Unit
Должность владельца сертификата	Title
ИНН (индивидуальный номер налогоплательщика) организации — юридического лица	INN
ОГРН (основной государственный регистрационный номер) организации — юридического лица	OGRN
Страна (RU)	Country
Субъект Российской Федерации, в котором зарегистрирована организация	State
Сертификат для юридического лица:	
Наименование организации (юридического лица), которая является владельцем сертификата	Common Name
Наименование организации	Organization
ИНН организации (12 символов)	INN
Примечание. ИНН в сертификате из 12 символов. В сертификатах юридических лиц перед основным номером автоматически добавляется два нуля.	
ИНН ЮЛ (10 символов)	INNLE
ОГРН организации	OGRN
Страна (RU)	Country
Субъект Российской Федерации, в котором зарегистрирована организация	State
Сертификат для индивидуального предпринимателя:	
Фамилия, имя, отчество владельца сертификата	Common Name
Наименование предприятия индивидуального предпринимателя, которого представляет владелец сертификата	Organization
Фамилия владельца сертификата	Surname

Атрибут имени владельца сертификата	Расширение сертификата
Имя и отчество владельца сертификата	Given Name
ИНН индивидуального предпринимателя	INN
ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя)	OGRNIP
Страна (RU)	Country
Субъект Российской Федерации, в котором зарегистрирован индивидуальный предприниматель	State

Настройка параметров издания квалифицированных сертификатов

Расширения, содержащие сведения о средствах удостоверяющего центра, средстве его электронной подписи, их сертификатах соответствия, а также политиках применения, описывающих класс данных средств, по умолчанию добавляются в издаваемые сертификаты, если в программе ViPNet Удостоверяющий и ключевой центр заданы дополнительные настройки. Поэтому если данные настройки не были заданы в процессе первичной инициализации, то прежде чем начать издание сертификатов в формате квалифицированных, выполните следующие действия:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Сертификаты > Программные средства**.

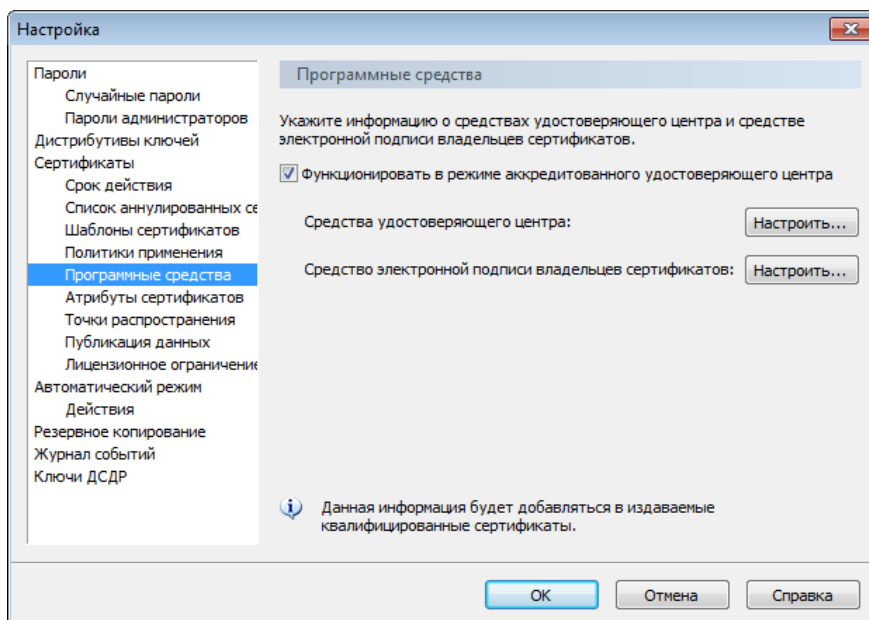


Рисунок 85. Настройка параметров работы УКЦ в режиме аккредитованного удостоверяющего центра

- 3 В разделе **Программные средства** установите флажок **Функционировать в режиме аккредитованного удостоверяющего центра**. Если флажок не будет установлен, дальнейшие настройки будут невозможны.
- 4 Укажите сведения о средствах вашего удостоверяющего центра. Для этого нажмите кнопку **Настроить** напротив названия **Средства удостоверяющего центра**, после чего в появившемся окне укажите следующую информацию:
 - На вкладке **Программные средства** в соответствующих полях введите:
 - полное наименование криптографического средства, которое используется для создания электронной подписи издателя (администратора УКЦ);
 - полное наименование программного средства, которое используется для реализации функций удостоверяющего центра.

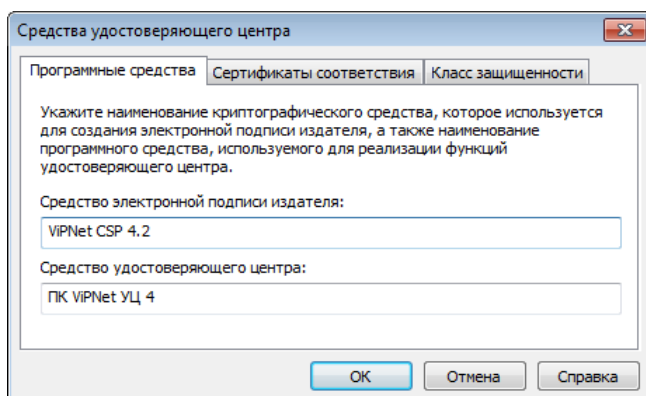


Рисунок 86. Указание сведений о средствах удостоверяющего центра

- На вкладке **Сертификаты соответствия** в нужных полях введите номера сертификатов соответствия средства электронной подписи и средства удостоверяющего центра требованиям Федерального закона № 63.



Примечание. Копии сертификатов соответствия предоставляются вашим поставщиком программного обеспечения.

Рисунок 87. Указание сертификатов соответствия средств удостоверяющего центра требованиям Федерального закона

- На вкладке **Класс защищенности** выберите класс защищенности, которому соответствуют указанные программные средства. Согласно выбранному классу в издаваемые сертификаты будут добавляться расширения с нужными политиками применения.

Рисунок 88. Указание класса защищенности средств удостоверяющего центра

Нажмите кнопку **ОК**.

- 5 Если вы хотите, чтобы в издаваемые сертификаты добавлялась информация о криптографическом средстве, которое используется для создания электронной подписи их владельцев, то нажмите кнопку **Настроить** напротив названия **Средство электронной подписи владельцев сертификатов**, после чего в появившемся окне укажите наименование данного средства и нажмите кнопку **ОК**.

Стоит учесть, что данная информация будет добавляться только в сертификаты, издаваемые для пользователей по запросам, в которых не содержится информация о средстве электронной

подписи владельца. Если информация о средстве электронной подписи владельца содержится в запросе, то именно она помещается в издаваемый сертификат.

В сертификаты администраторов и сертификаты пользователей, издаваемые по инициативе администратора УКЦ, в качестве наименования средства создания электронной подписи владельца всегда добавляется наименование средства создания электронной подписи издателя. Для вашего сведения оно отображается в не редактируемом поле.

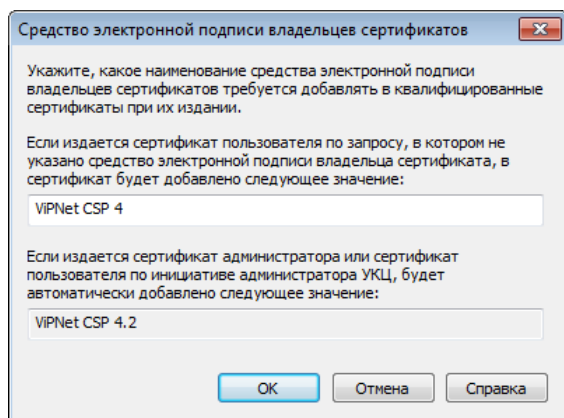


Рисунок 89. Указание сведений о средстве создания электронной подписи владельца сертификата ключа проверки электронной подписи

- 6 Для сохранения настроек нажмите кнопку **OK**.

В результате во все издаваемые сертификаты будут добавляться расширения, содержащие указанные выше сведения.

Аннулирование, приостановление действия, возобновление действия сертификатов

В некоторых случаях может возникнуть необходимость аннулирования или приостановления действия сертификата пользователя, например:

- Компрометация ключей пользователя (см. [Действия в случае компрометации ключа электронной подписи пользователя](#)).
- Смена места работы владельца сертификата.
- Издание нового сертификата с другими параметрами вместо действующего сертификата.

Аннулирование, приостановление действия и возобновление действия сертификата пользователя может происходить:

- По запросу из центра регистрации.
- По инициативе администратора УКЦ.

Возобновить действие сертификата можно только, если ранее его действие было приостановлено.

Иногда также может возникнуть необходимость аннулирования кросс-сертификатов, изданных при установлении доверительных отношений (см. [Установление доверительных отношений с другими удостоверяющими центрами](#)).

Вы можете аннулировать, приостанавливать действие или возобновлять действие приостановленных сертификатов пользователей сети ViPNet, пользователей, удаленных из сети ViPNet, или внешних пользователей, а также аннулировать изданные кросс-сертификаты администраторов других удостоверяющих центров, в случае, если вы являетесь их издателем. Если вы не являетесь издателем сертификата, то при попытке аннулирования появится сообщение о невозможности выполнения операции.

Аннулированный или приостановленный в действии сертификат попадает в ваш список аннулированных сертификатов (CRL), который находится в разделе **Изданные сертификаты > Списки аннулированных сертификатов** представления **Администрирование**. При возобновлении действия приостановленного сертификата он удаляется из списка аннулированных сертификатов. В связи с этим после каждой операции аннулирования, приостановления или возобновления действия сертификата вам требуется рассылать обновленный CRL на узлы вашей сети. Подробнее о способах передачи CRL см. в разделе [Работа со списками аннулированных сертификатов](#).

По запросу из центра регистрации

Администратор центра регистрации может инициировать аннулирование, приостановление действия или возобновление действия сертификатов, выдача которых производилась через центр регистрации. Для этого он формирует соответствующие запросы в программе ViPNet Registration Point и передает их в ViPNet Удостоверяющий и ключевой центр (см. раздел [Взаимодействие с программой ViPNet Registration Point](#)).

Запросы на аннулирование, приостановление и возобновление действия сертификатов пользователей при поступлении в УКЦ помещаются в раздел **Запросы на аннулирование сертификатов > Необработанные запросы** представления **Удостоверяющий центр**. Все поступившие запросы требуется обработать: удовлетворить либо отклонить. Запросы могут обрабатываться в автоматическом режиме (см. [Работа в автоматическом режиме](#)) или вручную. При автоматической обработке запросы могут быть только удовлетворены. Отклонить запрос можно только при обработке вручную.

Для обработки запросов в автоматическом режиме должны быть выполнены соответствующие настройки (см. [Настройка автоматического режима](#)). Чтобы обработать запросы вручную:

- 1 В окне программы на панели навигации выберите представление **Удостоверяющий центр** и перейдите в раздел **Запросы на аннулирование сертификатов > Необработанные запросы**.
- 2 На панели просмотра выберите один или несколько запросов и на панели инструментов нажмите кнопку **Удовлетворить** или кнопку **Отклонить**.
- 3 В появившемся окне с сообщением подтвердите операцию, которая будет выполнена.

В результате удовлетворения запроса статус сертификата будет изменен, запрос будет перемещен в раздел **Запросы на аннулирование сертификатов > Удовлетворенные запросы**. При аннулировании либо приостановлении действия сертификата попадет в ваш список аннулированных сертификатов (CRL), который вы можете найти в разделе **Изданные сертификаты > Списки аннулированных сертификатов** представления **Администрирование**. Для аннулированного сертификата будет указана причина аннулирования, содержащаяся в запросе. Измененный CRL передайте на узлы вашей сети (см. [Распространение списков аннулированных сертификатов](#)).

В результате отказа в обработке запроса администратору центра регистрации будет отправлен файл запроса в неизменном виде. Такой запрос будет перемещен в раздел **Запросы на аннулирование сертификатов > Отклоненные запросы**.

По инициативе администратора УКЦ

Чтобы аннулировать, приостановить действие или возобновить действие приостановленного сертификата:

- 1 В окне программы на панели навигации выберите:
 - Представление **Удостоверяющий центр** и перейдите в раздел:

- **Изданные сертификаты > Пользователи моей сети** для работы с сертификатами пользователей сети ViPNet.
 - **Изданные сертификаты > Пользователи, удаленные из моей сети** для работы с сертификатами пользователей, которые были удалены из сети ViPNet.
 - **Изданные сертификаты > Внешние пользователи** для работы с сертификатами внешних пользователей.
- Представление **Администрирование** и перейдите в раздел **Кросс-сертификация > Сертификаты для других УЦ** для работы с изданными кросс-сертификатами администраторов других удостоверяющих центров.
- 2 На панели просмотра щелкните правой кнопкой мыши по нужному сертификату и в контекстном меню выберите:
- пункт **Аннулировать** для аннулирования сертификата пользователя или кросс-сертификата.
 - пункт **Приостановить** для приостановления действия сертификата пользователя.
 - пункт **Возобновить** для возобновления действия ранее приостановленного сертификата пользователя.
- В **режиме работы аккредитованного УЦ** вы можете только аннулировать квалифицированные сертификаты.
- 3 В случае аннулирования сертификата в появившемся окне **Аннулирование сертификата** выполните следующие действия:

3.1 В списке укажите одну из причин аннулирования:

- **Прекращение действия** — если сертификат пользователя не предполагает дальнейшего использования.
- **Компрометация ключа** — если произошла компрометация ключей пользователя (например, вследствие утери им контейнера ключей).
- **Изменение принадлежности** — при изменении удостоверяющего центра.
- **Сертификат заменен** — если данные, указанные в сертификате пользователя, стали неактуальными.

3.2 Нажмите кнопку **Аннулировать**.

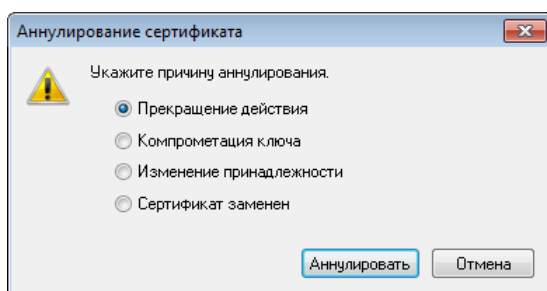


Рисунок 90. Аннулирование сертификата

- 4 После аннулирования или приостановления действия сертификата в колонке **Статус** для данного сертификата появится соответствующее значение. В окне **Сертификат** на вкладке **Общие** (см. [Просмотр сертификатов](#)) также появится соответствующая информация.

Чтобы аннулировать сертификаты, изданные для конкретного пользователя:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр**.
- 2 Перейдите в раздел **Моя сеть > Пользователи**.
- 3 На панели просмотра дважды щелкните кнопкой мыши нужного пользователя.
- 4 В появившемся окне **Свойства пользователя** перейдите на вкладку **Сертификаты**.
- 5 В списке **Изданные сертификаты** выберите сертификат и нажмите кнопку **Аннулировать**.

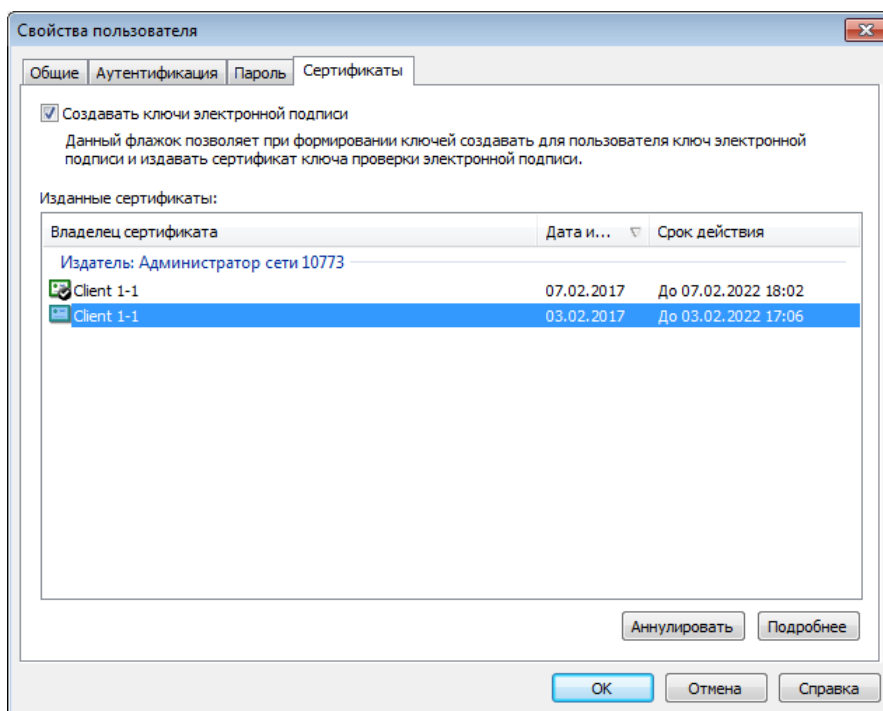


Рисунок 91. Аннулирование сертификата пользователя в окне **Свойства пользователя**

- 6 В появившемся окне **Аннулирование сертификата** выберите причину аннулирования и нажмите кнопку **Аннулировать**.

Просмотр запросов и сертификатов

Просмотр запроса на сертификат

Прежде чем обработать запрос на издание сертификата, вы можете просмотреть его параметры.

При необходимости также можно просмотреть параметры уже обработанных запросов.



Примечание. Просмотреть параметры запросов, поступающих от пользователей сети ViPNet или из центров регистрации, можно в том случае, если они не были обработаны в автоматическом режиме (см. [Работа в автоматическом режиме](#)).

Чтобы посмотреть подробную информацию о [запросе на сертификат](#) от пользователя сети ViPNet или из центра регистрации:

- 1 В окне программы на панели навигации перейдите в представление **Удостоверяющий центр** и выберите раздел, соответствующий состоянию запроса (необработанный, удовлетворенный или отклоненный).
- 2 Дважды щелкните нужный запрос либо в контекстном меню запроса выберите пункт **Открыть запрос**.

Посмотреть подробную информацию о запросе на сертификат от внешнего пользователя можно при его обработке в окне **Издание сертификатов пользователей** с помощью кнопки **Свойства**.

В зависимости от того, в каком приложении ViPNet был сформирован запрос на сертификат, внешний вид окна просмотра параметров запроса будет выглядеть по-разному. В окне просмотра параметров запроса от пользователя сети ViPNet или из центра регистрации содержится ряд вкладок, на которых отображается следующая информация:

- **Общие** — основная информация о запросе: номер запроса; имя администратора, подписавшего запрос; имя владельца ключа проверки электронной подписи; желательный срок действия сертификата; статус запроса и электронной подписи.
- **Владелец ключа** — сведения о пользователе ViPNet, для которого создан запрос на сертификат.
- **Срок действия** — срок действия сертификата, заявленный в запросе.
- **Ключ проверки электронной подписи** — параметры ключа проверки электронной подписи.
- **Состав** — список расширений, определяющих назначение сертификата.
- **Информация о запросе** — дополнительные сведения о владельце ключа проверки электронной подписи.

- **Статус** — текущий статус запроса и история запроса (дата и время создания, отправки, доставки и других статусов запроса).
- **Электронная подпись** — информация об электронной подписи, заверившей запрос, и контрольной сумме запроса. На вкладке также с помощью кнопки **Просмотр сертификата** можно просмотреть сведения о сертификате, которым был подписан запрос.

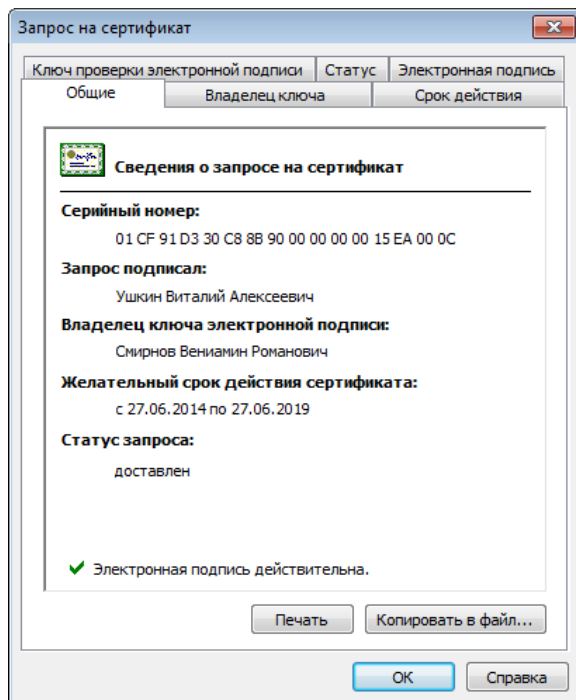


Рисунок 92. Просмотр общей информации о запросе

В окне просмотра параметров запроса на сертификат от внешнего пользователя вся информация о содержимом запроса представлена рядом расширений на вкладке **Состав запроса**. К данной информации относится:

- сведения о пользователе, для которого создан запрос на сертификат;
- параметры ключа проверки электронной подписи — алгоритм, который использовался при создании этого ключа;
- список назначений и политик применения, которые должны быть включены в сертификат.

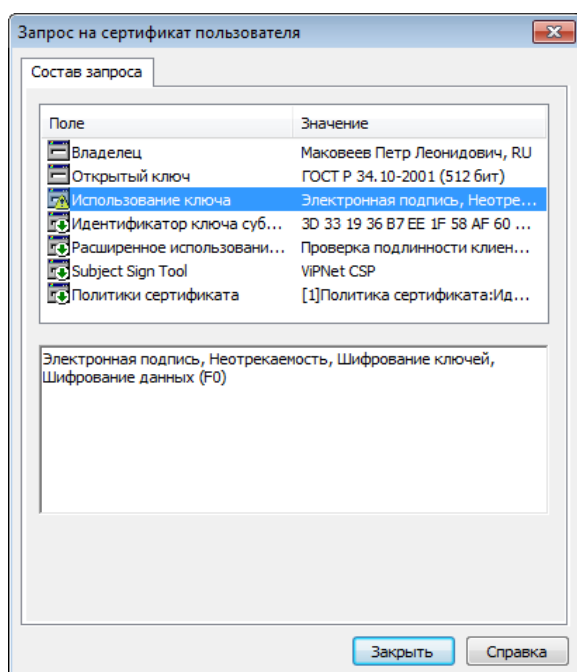


Рисунок 93. Просмотр информации о запросе на сертификат от внешнего пользователя

Просмотр сертификатов

Все сертификаты, изданные в программе ViPNet Удостоверяющий и ключевой центр, — сертификаты пользователей, администраторов, кросс-сертификаты, а также сертификаты, импортированные из сторонних удостоверяющих центров или доверенных сетей, вы можете просмотреть (в том числе аннулированные и приостановленные в действии).

Просмотр сертификата может понадобиться для получения информации о его назначении, издателе, составе полей, причине недействительности сертификата и так далее.

Чтобы просмотреть сведения, содержащиеся в сертификате:

- 1 Перейдите в представление **Удостоверяющий центр** для просмотра сертификата пользователя или в представление **Администрирование** для просмотра сертификата другого типа.
- 2 Выберите раздел, соответствующий типу сертификата.
- 3 Дважды щелкните нужный сертификат или в контекстном меню выберите пункт **Открыть**.



Примечание. Сертификаты пользователей сети ViPNet также можно просмотреть на вкладке **Сертификаты** в окне **Свойства пользователя**, сертификаты администраторов УКЦ — на вкладке **Сертификаты** в окне **Свойства администратора**.

В появившемся окне **Сертификат** сведения представлены на нескольких вкладках.

На вкладке **Общие** содержится основная информация о выбранном сертификате:

- назначение сертификата или (для недействительных сертификатов) причина недействительности сертификата;
- имя владельца ключа проверки электронной подписи, которому выдан сертификат;
- имя издателя сертификата;
- срок действия сертификата;
- срок действия ключа электронной подписи, соответствующего данному сертификату (только для сертификатов пользователей);
- информация о политиках применения сертификата, отображаемая при нажатии кнопки **Заявление издателя**.

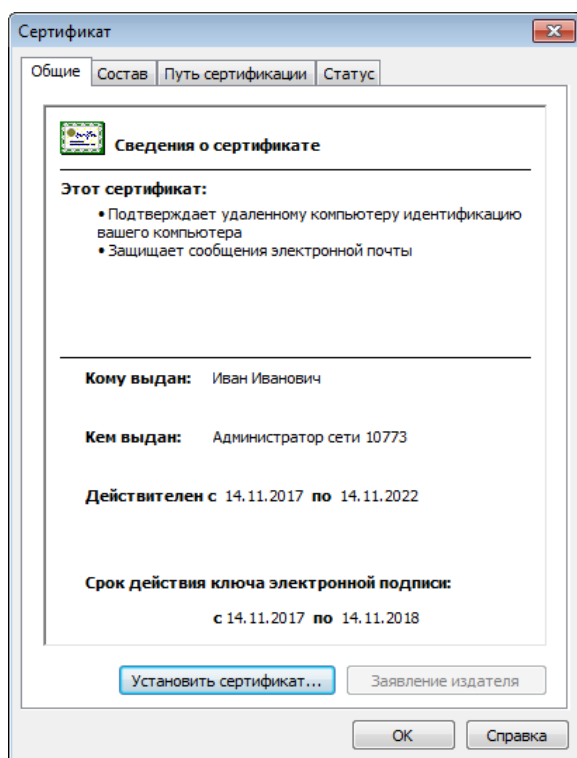


Рисунок 94. Просмотр сведений о сертификате

Вкладка **Состав** включает в себя список всех полей сертификата. Чтобы просмотреть содержимое интересующего поля, выберите его в списке. Для удобства вы можете ограничить количество просматриваемых полей, выбрав нужную группу полей в выпадающем списке **Показать**:

- **Только поля V1** — все поля, кроме расширений;
- **Только расширения** — дополнительные поля сертификата, соответствующего стандарту X.509 версии 3;



Примечание. Расширение **Срок действия ключа электронной подписи** отображается в том случае, если срок действия сертификата превышает 12 месяцев (1 год). Срок действия ключа электронной подписи в этом случае не может превышать 15 месяцев (1 год и 3 месяца).

- **Только критические расширения** — только те расширения, которые признаны издателем критическими;
- **Только свойства** — параметры, которые не являются полями сертификата, но присваиваются сертификату при хранении его в системном хранилище компьютера.

Кроме этого вы можете экспортировать сертификат в файл различных форматов с помощью кнопки **Копировать в файл** (см. раздел [Экспорт сертификатов](#)) или отправить его на принтер, нажав кнопку **Печать**. Сертификат будет распечатан (см. [Печать сертификатов](#)).

На вкладке **Путь сертификации** отображаются сертификаты, образующие иерархию издателей выбранного сертификата, — цепочка сертификации, а также информация об их статусе. При необходимости вы можете просмотреть более подробную информацию о каждом сертификате издателя из цепочки с помощью кнопки **Просмотр сертификата**.

На вкладке **Статус** содержатся сведения о текущем статусе сертификата, а также список операций, которые производились с сертификатом с момента его издания. Данная вкладка присутствует только в окне просмотра сертификатов пользователей, поскольку учет производимых операций ведется только для этих сертификатов.

Просмотр истории сертификатов

Операции, которые производятся с сертификатами пользователей в программе с момента их издания, фиксируются в истории сертификатов. Историю каждого изданного сертификата пользователя при необходимости впоследствии вы можете просмотреть.

Чтобы просмотреть историю сертификата внешнего пользователя или пользователя сети ViPNet:

- 1 В окне программы на панели навигации перейдите в представление **Удостоверяющий центр** и в разделе **Изданные сертификаты** выберите нужный подраздел.
- 2 На панели просмотра дважды щелкните сертификат или в контекстном меню сертификата выберите пункт **Открыть**.
- 3 В окне просмотра сертификата перейдите на вкладку **Статус** и ознакомьтесь с операциями, которые производились с сертификатом, а также датами их проведения.

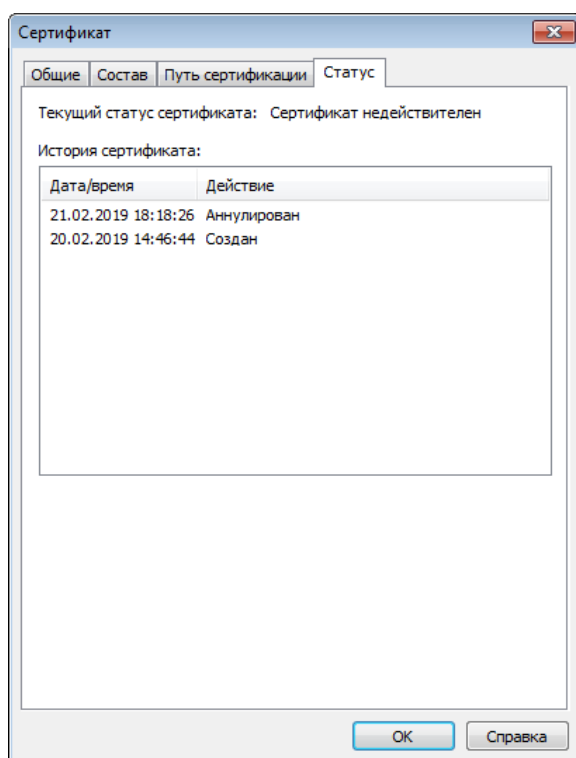


Рисунок 95. Просмотр истории сертификата

Экспорт сертификатов

Изданные сертификаты пользователей ViPNet, кросс-сертификаты, а также сертификаты администраторов вы можете экспортировать в различные форматы. Экспорт сертификатов может потребоваться в разных случаях, например, при архивировании сертификатов либо при выдаче сертификатов непосредственно внешним пользователям (без участия центра регистрации).



Примечание. Подробнее об экспорте кросс-сертификатов см. раздел [Экспорт кросс-сертификата](#).

Чтобы экспортировать сертификат:

- 1 В окне программы на панели навигации перейдите в представление **Удостоверяющий центр** для экспорта сертификата пользователя или в представление **Администрирование** для экспорта сертификата другого типа.
- 2 Выберите раздел, соответствующий типу сертификата.
- 3 На панели просмотра выберите в списке нужный сертификат.
- 4 Выполните одно из действий:
 - Щелкните сертификат правой кнопкой мыши и в контекстном меню выберите пункт **Экспорт**.
 - Дважды щелкните сертификат и в окне **Сертификат** на вкладке **Состав** нажмите кнопку **Копировать в файл**.

Будет запущен мастер экспорта сертификатов.

- 5 На начальной странице мастера экспорта сертификатов нажмите кнопку **Далее**.



Совет. Если при последующих запусках мастера желательно пропускать первую страницу, установите на ней флажок **Не отображать в дальнейшем эту страницу**.

- 6 На странице **Формат экспортируемого файла** выберите один из предлагаемых форматов (см. [Форматы экспорта сертификатов](#)), после чего нажмите кнопку **Далее**.

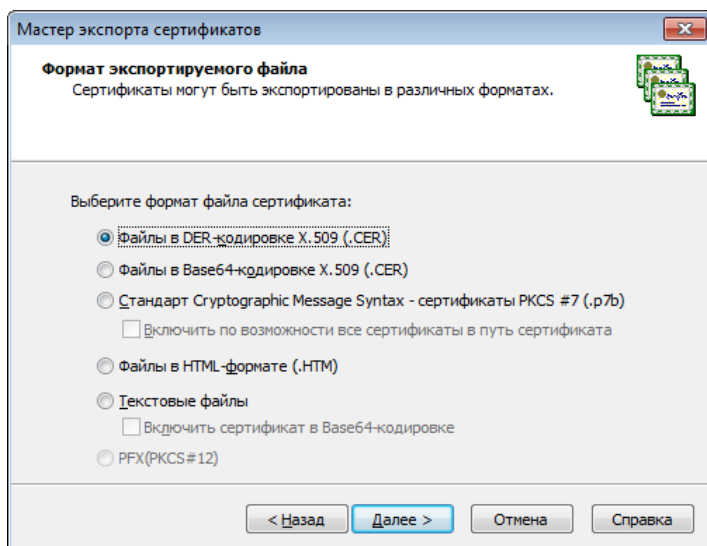


Рисунок 96. Выбор формата файла

- 7 На странице **Имя файла экспорта** укажите полный путь к создаваемому файлу, после чего нажмите кнопку **Далее**.
 - 8 На странице **Завершение работы мастера экспорта сертификатов** убедитесь в правильности параметров экспорта, заданных на предыдущих страницах мастера, после чего нажмите кнопку **Готово**.
 - 9 В окне с сообщением об успешном экспорте нажмите кнопку **ОК**.
- В результате экспорта сертификат будет сохранен в файле заданного формата по указанному пути.

Форматы экспорта сертификатов

При выборе формата экспорта сертификата следует руководствоваться перечисленными положениями.

- При экспорте сертификатов для импорта на компьютер с ОС Windows предпочтительный формат экспорта — PKCS #7, поскольку этот формат обеспечивает сохранение цепочки центров сертификации (пути сертификации). Некоторые приложения требуют при импорте сертификата из файла представления в виде DER или Base64. Поэтому формат экспорта необходимо выбирать в соответствии с требованиями приложения или системы, в которую этот сертификат предполагается импортировать.
- Для просмотра сертификата и вывода его на печать используются текстовый и HTML-форматы.

Ниже приведена подробная информация о каждом из форматов экспорта сертификатов, поддерживаемых ПО ViPNet.

- **Стандарт Cryptographic Message Syntax (PKCS #7)**

Формат PKCS #7 позволяет передавать сертификат и все сертификаты в цепочке сертификации с одного компьютера на другой или с компьютера на внешнее устройство. Файлы PKCS #7

обычно имеют расширение `.p7b` и совместимы со стандартом ITU-T X.509. Формат PKCS#7 разрешает такие атрибуты, как удостоверяющие подписи, связанные с обычными подписями. Для таких атрибутов, как метка времени, можно выполнить проверку подлинности вместе с содержимым сообщения. Дополнительные сведения о формате PKCS#7 см. на веб-сайте RSA Laboratories.

- **Файлы в DER-кодировке X.509**

DER (Distinguished Encoding Rules) для ASN.1, как определено в рекомендации ITU-T Recommendation X.509, — более ограниченный стандарт кодирования, чем альтернативный BER (Basic Encoding Rules) для ASN.1, определенный в рекомендации ITU-T Recommendation X.209, на котором основан DER. И BER, и DER обеспечивают независимый от платформы метод кодирования объектов, таких как сертификаты и сообщения, для передачи между устройствами и приложениями.

При кодировании сертификата большинство приложений используют стандарт DER, так как сертификат (сведения о запросе на сертификат) должен быть закодирован с помощью DER и подписан. Файлы сертификатов DER имеют расширение `.cer`.

Дополнительные сведения см. в документе «ITU-T Recommendation X.509, Information Technology — Open Systems Interconnection — The Directory: Authentication Framework» на веб-узле [International Telecommunication Union \(ITU\)](http://www.itu.int).

- **Файлы в Base64-кодировке X.509**

Этот метод кодирования создан для работы с протоколом S/MIME, который популярен при передаче бинарных файлов через Интернет. Base64 кодирует файлы в текстовый формат ASCII, что обеспечивает целостность информации при ее передаче по сети. Протокол S/MIME обеспечивает работу некоторых криптографических служб безопасности для приложений электронной почты, включая механизм неотрекаемости (с помощью электронных подписей), секретность и безопасность данных (с помощью кодирования, процесса проверки подлинности и целостности сообщений). Файлы сертификатов Base64 имеют расширение `.cer`.

MIME (Multipurpose Internet Mail Extensions, спецификация RFC 1341 и последующие) определяет механизмы кодирования произвольных двоичных данных для передачи по электронной почте.

Дополнительные сведения см. в документе «RFC 2633 S/MIME Version 3 Message Specification, 1999» на веб-узле [Internet Engineering Task Force \(IETF\)](http://www.ietf.org).

- **Файлы в HTML-формате**

Файлы для просмотра и печати в любом веб-браузере, а также в офисных и других программах, поддерживающих язык разметки гипертекста HTML.

- **Текстовые файлы**

Файлы в кодировке ANSI для просмотра в любом текстовом редакторе и вывода на печать.

- **Файлы в формате PFX (PKCS #12)**

Формат PFX (PKCS#12) поддерживает безопасное хранение сертификата и закрытого ключа, соответствующего сертификату пользователя, может содержать все сертификаты в цепочке доверия от сертификата пользователя до корневого сертификата удостоверяющего центра и CRL.

Проверка сертификатов

В процессе электронного взаимодействия у пользователей могут возникать вопросы, можно ли доверять тем или иным сертификатам (как правило, изданным в сторонних удостоверяющих центрах). В этом случае они вправе обратиться в свой удостоверяющий центр для проверки таких сертификатов.

В программе ViPNet Удостоверяющий и ключевой центр может быть выполнена процедура проверки сертификата ключа проверки электронной подписи по запросу пользователя. Для проведения процедуры проверки сертификата пользователь должен обратиться с заявлением в письменном либо электронном виде. Заявление в электронном виде должно быть подписано действующим сертификатом пользователя. Вместе с заявлением должен быть предоставлен файл сертификата подписи *.cer, который требуется проверить.

Чтобы проверить полученный сертификат пользователя:

- 1 В окне программы в меню **Сервис** выберите пункт **Открыть сертификат из файла**.
- 2 В появившемся окне выберите файл сертификата, который был вам предоставлен пользователем, и нажмите кнопку **Открыть**.
- 3 В появившемся окне **Сертификат** ознакомьтесь с информацией, которая содержится в проверяемом сертификате. Если на вкладке **Общие** указано, что срок действия сертификата или ключа электронной подписи истек, то сертификат является недействительным и ему не следует доверять. Если указано, что недостаточно информации для проверки сертификата, то в этом случае ему также не следует доверять. Если никакой из перечисленной информации в сертификате не содержится и на вкладке **Путь сертификации** окна **Сертификат** указано, что сертификат действителен, то сертификату можно доверять.
- 4 Сообщите пользователю о результатах проверки сертификата.

Печать сертификатов

Сертификаты, используемые либо изданные в программе ViPNet Удостоверяющий и ключевой центр, вы можете распечатать. Для вывода на печать любого сертификата в окне просмотра данного сертификата на вкладке **Состав** нажмите кнопку **Печать** (см. [Просмотр сертификатов](#)). Если вам требуется распечатать сразу несколько сертификатов пользователей, то укажите нужные сертификаты и в их контекстном меню выберите пункт **Печать**.

В результате сертификаты будут отправлены на принтер, используемый по умолчанию на вашем компьютере. Они будут распечатаны в соответствии с форматом, заданным в специальных шаблонах. Подробнее о том, как задать формат в шаблонах, см. документ «Печать сертификатов. Приложение к документации ViPNet» из комплекта поставки (см. [Комплект поставки](#)).

Настройка количества сертификатов, отображаемых в окне программы

По умолчанию в программе в списках сертификатов пользователей в подразделах раздела **Изданные сертификаты** отображается не более 100 сертификатов.

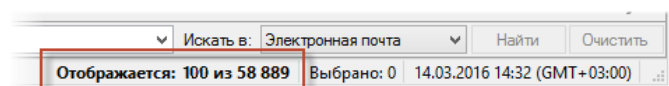


Рисунок 97: Количество сертификатов, отображаемых в программе по умолчанию

Чтобы в списках сертификатов этих разделов отображалось большее количество сертификатов:

- 1 В файле `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\ini\KC.ini` добавьте параметр `Certificates cache capacity` в секцию `[Certification]`.
- 2 В качестве значения параметра `Certificates cache capacity` укажите количество сертификатов, которое должно отображаться. Возможные значения параметра `Certificates cache capacity`: от 100 до 10000. Если будет задано значение меньше или больше возможного, то по умолчанию будет использоваться значение 100.

Например:

```
[Certification]
```

```
Certificates cache capacity=200
```



Примечание. Стоит учитывать, что при увеличении количества сертификатов будет снижаться скорость отображения списка сертификатов в программе.

9

Работа со списками аннулированных сертификатов

Общие сведения о списках аннулированных сертификатов	196
Обновление списков аннулированных сертификатов	197
Распространение списков аннулированных сертификатов	200
Просмотр списков аннулированных сертификатов	206
Экспорт списков аннулированных сертификатов в файл	208
Управление временем обновления и публикации CRL	210

Общие сведения о списках аннулированных сертификатов

В [списках аннулированных сертификатов](#) содержится информация о том, какие сертификаты пользователей были аннулированы либо действие которых было приостановлено. Эта информация используется для проверки действительности сертификата.



Примечание. В CRL содержится информация только о сертификатах, срок действия которых не истек. Подробнее см. [RFC 5280, раздел 5](#).

Списки аннулированных сертификатов создаются в процессе издания корневых сертификатов (см. [Издание сертификата администратора](#)) либо в процессе импорта сертификатов администраторов, изданных вышестоящим удостоверяющим центром при установлении доверительных отношений (см. [Импорт сертификата, выданного вышестоящим удостоверяющим центром](#)). Они отображаются в разделах представления **Администрирование**: в первом случае — в разделе **Изданные сертификаты > Списки аннулированных сертификатов**, во втором — в разделе **Кросс-сертификация > Списки аннулированных сертификатов**.

Списки аннулированных сертификатов, импортированные из доверенных сетей ViPNet или других удостоверяющих центров, содержатся в разделе **Импортированные сертификаты > Списки аннулированных сертификатов** представления **Администрирование**.

Обновление списков аннулированных сертификатов

Списки аннулированных сертификатов (CRL) имеют ограниченный срок действия и должны регулярно обновляться. При наличии CRL с истекшим сроком действия будет запрещено [издание сертификатов](#).

Обновление CRL может производиться несколькими способами:

- В автоматическом режиме по расписанию (см. [Настройка автоматического обновления CRL](#)). В данном случае обновляются сразу все CRL, которые соответствуют действительному ключу электронной подписи администратора, при работе программы в автоматическом режиме.
- Вручную по команде администратора (см. [Обновление CRL вручную](#)). В ручном режиме могут быть обновлены все CRL либо только выбранные CRL.

Кроме того, автоматическое обновление CRL выполняется при аннулировании или приостановлении действия сертификатов пользователей (см. [Аннулирование, приостановление действия, возобновление действия сертификатов](#)).

CRL после обновления действуют в течение срока, который задан в настройках программы. Поэтому перед обновлением CRL любым из указанных способов убедитесь, что в настройках задан нужный срок (см. [Настройка срока действия CRL](#)).

CRL, срок действия которых истек, автоматически удаляются во время проверки текущих данных (см. [Проверка текущих данных](#)) и перед созданием резервной копии по расписанию (см. [Настройка параметров создания резервных копий](#)). Также CRL удаляются при их обновлении, если срок действия ключа электронной подписи истек.

Настройка автоматического обновления CRL

Списки аннулированных сертификатов (CRL) могут обновляться в автоматическом режиме работы программы (см. [Работа в автоматическом режиме](#)) со следующей периодичностью:

- Раз в несколько минут, часов, дней или месяцев.
- Каждый день в конкретное время.

Поэтому, если вы выбрали операцию обновления CRL для выполнения в автоматическом режиме работы программы (см. [Настройка автоматического режима](#)), в окне **Параметры действия в автоматическом режиме** укажите периодичность обновления CRL, установив переключатель в нужное положение.

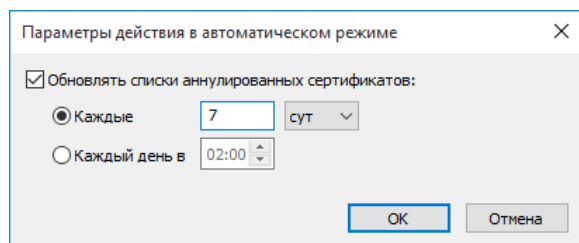


Рисунок 98. Настройка автоматического обновления CRL

В случае наличия межсетевого взаимодействия с другими сетями ViPNet при обновлении CRL в автоматическом режиме список аннулированных сертификатов сразу передается в доверенные сети вместе с корневым сертификатом администратора (сертификатом издателя).

При наличии доверительных отношений со сторонними удостоверяющими центрами обновите CRL вручную (см. [Обновление CRL вручную](#)), выполните экспорт обновленного CRL в файл (см. [Экспорт одного CRL в файл](#)), после чего передайте файл с CRL в данные удостоверяющие центры.

Обновление CRL вручную

Обновление списков аннулированных сертификатов (CRL) в программе ViPNet Удостоверяющий и ключевой центр вы можете производить вручную. Как правило, это может потребоваться при необходимости срочного обновления CRL, чтобы не переходить в автоматический режим работы и не ожидать обновления CRL по расписанию (см. [Настройка автоматического обновления CRL](#)).

Чтобы обновить CRL:

- 1 В окне программы на панели навигации перейдите в представление **Администрирование**.
- 2 Выберите раздел **Изданные сертификаты > Списки аннулированных сертификатов** (или **Кросс-сертификация > Сертификаты от вышестоящего УЦ > Списки аннулированных сертификатов**).

- 3 На панели просмотра выберите CRL и нажмите кнопку **Обновить**.

В результате выбранный CRL будет обновлен и будет действовать в течение срока, указанного в настройках программы (см. [Настройка срока действия CRL](#)).

- 4 Распространите обновленный CRL любым возможным способом (см. [Распространение списков аннулированных сертификатов](#)).

- 5 При наличии межсетевого взаимодействия с другими сетями ViPNet выполните экспорт служебных данных (см. [Экспорт межсетевой информации](#)) для передачи обновленного CRL в доверенные сети.

- 6 При наличии доверительных отношений со сторонними удостоверяющими центрами выполните экспорт обновленного CRL в файл (см. [Экспорт одного CRL в файл](#)), после чего передайте файл с CRL в данные удостоверяющие центры.

Настройка срока действия CRL

Списки аннулированных сертификатов (CRL) после обновления действуют в течение срока, указанного в настройках программы. Поэтому для обновления CRL в настройках задайте нужный срок в соответствии с регламентом работы вашей организации. Кроме этого, в настройках УКЦ вы также можете изменить количество дней или часов, за которое должно производиться оповещение об истечении срока действия CRL.

Чтобы настроить данные параметры:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В окне **Настройка** на панели навигации выберите раздел **Сертификаты** > **Список аннулированных сертификатов**.

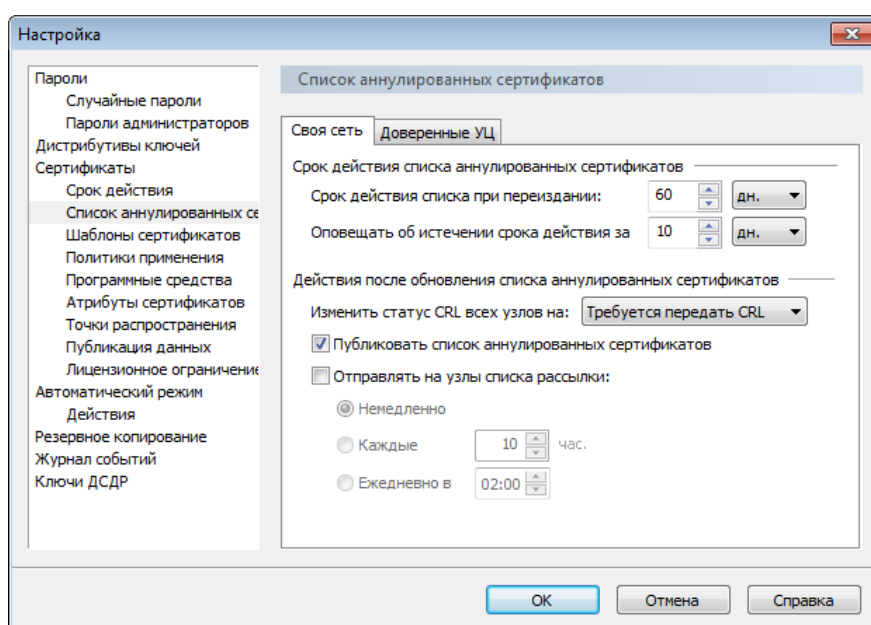


Рисунок 99. Настройка срока действия списков аннулированных сертификатов

- 3 На вкладке **Своя сеть** в группе **Срок действия списка аннулированных сертификатов**:
 - Задайте срок действия CRL. Для этого в списке рядом с полем **Срок действия списка при переиздании** выберите единицу измерения (дни или часы), затем в самом поле введите срок, в течение которого CRL будет действителен после своего обновления. По умолчанию установлено 60 дней.
 - Задайте время оповещения об истечении срока действия CRL. Для этого в списке рядом с полем **Сообщать об истечении срока действия за** выберите единицу измерения (дни или часы), затем в самом поле укажите количество дней или часов, за которое должно выдаваться предупреждение об истечении срока действия CRL с рекомендацией его обновить. По умолчанию установлено 10 дней.
- 4 Для сохранения указанных настроек нажмите кнопку **ОК**.

Распространение списков аннулированных сертификатов

На узлах пользователей сети ViPNet, которые работают с электронной подписью, должны присутствовать актуальные списки аннулированных сертификатов (CRL). Поэтому в перечисленных ниже случаях CRL следует своевременно передавать на все узлы сети:

- Обновление CRL вашей сети, если истек срок его действия либо был приостановлен или аннулирован сертификат пользователя в сети (см. [Обновление списков аннулированных сертификатов](#)).
- Издание нового корневого сертификата администратора (сертификата издателя) (см. [Издание сертификата администратора](#)).



Примечание. После издания корневого сертификата на сетевые узлы автоматически передается комплект CRL, в составе которого присутствует новый сертификат издателя и CRL для него.

- Получение сертификата администратора (сертификата издателя) в вышестоящем удостоверяющем центре (см. [Импорт сертификата, выданного вышестоящим удостоверяющим центром](#)), издание кросс-сертификата (см. [Издание кросс-сертификата по запросу](#)).
- Получение сертификатов администраторов либо CRL из доверенной сети ViPNet или сторонних удостоверяющих центров.

Распространять CRL вы можете несколькими способами:

- Через список рассылки (см. [Передача CRL через список рассылки](#)). Этим способом распространяется обновленный CRL, соответствующий текущему сертификату издателя. Распространяется данный CRL только на узлы, заданные в списке рассылки. Может передаваться автоматически.
- В автоматическом режиме УКЦ (см. [Настройка автоматической передачи CRL](#)). Этим способом распространяются все CRL, которые присутствуют в программе, включая CRL из доверенных сетей ViPNet или других удостоверяющих центров.
- Вручную по команде администратора (см. [Передача CRL на узлы вручную](#)). Этим способом распространяются все CRL, которые присутствуют в программе, включая CRL из доверенных сетей ViPNet или других удостоверяющих центров.
- Путем публикации в хранилищах данных (см. [Публикация сертификатов и списков аннулированных сертификатов](#)). Данный способ, как правило, используется, когда в сети организации развернута PKI-инфраструктура и передача данных по сети (в том числе CRL) не производится.

Передача CRL через список рассылки

Если в вашей сети есть узлы, на которых требуется гарантированное оперативное получение CRL (например, на узлах центров регистрации), организуйте распространение CRL через список рассылки. Для этого выполните следующие действия:

- 1 Сформируйте список рассылки CRL (список получателей CRL).
- 2 Настройте параметры передачи CRL на узлы списка рассылки.



Внимание! Через список рассылки может распространяться только текущий CRL после обновления (см. [Обновление списков аннулированных сертификатов](#)).

Чтобы сформировать список получателей CRL:

- 1 В окне программы в представлении **Администрирование** выберите раздел **Моя сеть > Получатели списков аннулированных сертификатов**.
- 2 Для добавления узла в перечень получателей CRL:
 - 2.1 Щелкните панель просмотра правой кнопкой мыши и в контекстном меню выберите **Добавить сетевой узел**.
 - 2.2 В окне **Добавление получателей списков аннулированных сертификатов** выберите один или несколько сетевых узлов. При необходимости воспользуйтесь строкой быстрого поиска.
 - 2.3 Нажмите кнопку **ОК**.
- 3 Для удаления узла из перечня получателей CRL в контекстном меню данного узла выберите пункт **Удалить**.



Совет. Добавляйте в список получателей только те сетевые узлы, на которых действительно требуется оперативное обновление CRL, чтобы не перегружать сеть постоянной рассылкой CRL.

Вы также можете добавить сетевые узлы в список получателей CRL следующим способом:

- 1 В окне программы в представлении **Ключевой центр** выберите раздел **Сетевые узлы**.
- 2 На панели просмотра выберите один или несколько сетевых узлов и в контекстном меню выберите пункт **Получать текущий CRL**. В результате напротив этого пункта появится флажок, а выбранные узлы будут добавлены в список получателей CRL.
- 3 Таким же способом вы можете удалить сетевые узлы из списка получателей CRL. Отсутствие флажка напротив пункта **Получать текущий CRL** означает отсутствие сетевого узла в списке получателей CRL.

Чтобы настроить параметры передачи CRL на узлы списка рассылки:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.

- 2 В появившемся окне на панели навигации выберите раздел **Сертификаты > Список аннулированных сертификатов**.
- 3 На вкладке **Своя сеть** установите флажок **Отправлять на узлы списка рассылки** и укажите условие отправки CRL, установив переключатель в одно из трех положений:
 - Для отправки изменений CRL сразу после их возникновения выберите **Немедленно**.
 - Для регулярной проверки наличия изменений в CRL выберите **Каждые** и в поле справа введите соответствующий временной интервал (в часах, в диапазоне от 1 до 999). При обнаружении изменений соответствующая информация будет отправлена получателям CRL.
 - Для ежедневной однократной проверки изменений в CRL выберите **Ежедневно в** и в поле справа введите желаемое время проверки. При обнаружении изменений соответствующая информация будет отправлена получателям CRL.
- 4 Для сохранения настроек нажмите кнопку **ОК**.

Настройка автоматической передачи CRL

После обновления CRL всем узлам присваивается статус CRL. Вы можете настроить значение статуса CRL, которое присваивается узлам. В зависимости от присвоенного узлам статуса будет происходить отправка CRL в автоматическом режиме УКЦ. Вы можете выбрать один из следующих статусов CRL для узлов:

- **Требуется передать CRL.** На узлы с таким статусом передается CRL в автоматическом режиме УКЦ по расписанию.
- **Неактуальные.** На узлы с таким статусом передается CRL только вручную, передача в автоматическом режиме УКЦ недоступна.

Периодичность отправки обновления CRL определяется настройками автоматического режима УКЦ. Вы можете автоматически передавать CRL на все узлы вашей сети ViPNet со следующей периодичностью:

- Каждые несколько часов.
- Каждый день в конкретное время.
- Сразу после изменения статуса CRL на **Требуется передать CRL**.

Чтобы в автоматическом режиме УКЦ передавать CRL по расписанию на все сетевые узлы вашей сети ViPNet:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В окне **Настройка** на панели навигации выберите раздел **Сертификаты > Список аннулированных сертификатов**.
- 3 На вкладке **Своя сеть** в группе **Действия после обновления списка аннулированных сертификатов** в списке **Изменить статус CRL всех узлов** на выберите **Требуется передать CRL**.

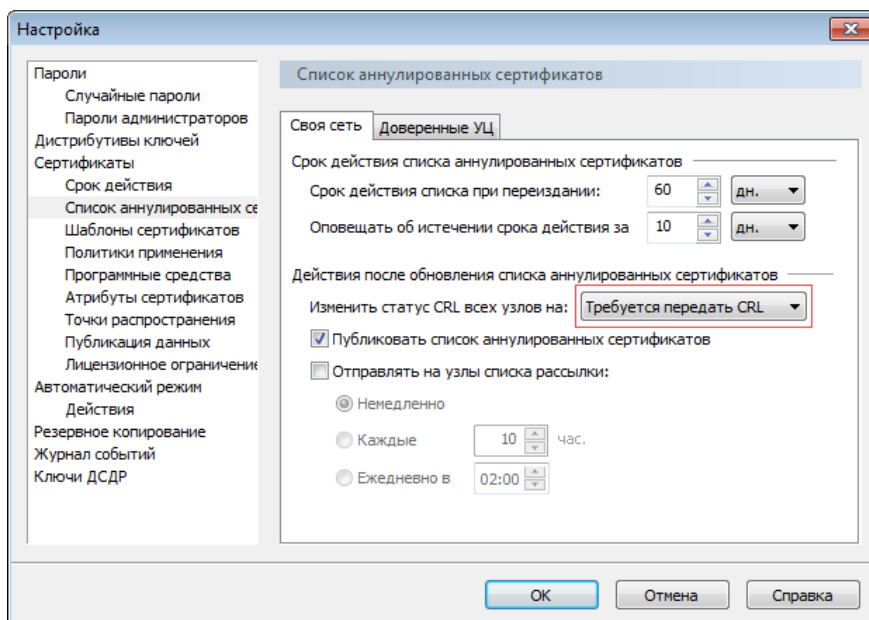


Рисунок 100. Настройка передачи обновления CRL в ЦУС для всех сетевых узлов

- 4 Чтобы после обновления CRL доверенной сети ViPNet автоматически передавать CRL на все узлы, связанные с доверенной сетью, на вкладке **Доверенные УЦ** в группе **Действия после обновления списка аннулированных сертификатов доверенной сети ViPNet** в соответствующем списке выберите **Требуется передать CRL**. При обновлении CRL доверенной сети статус CRL для сетевых узлов вашей сети, связанных с доверенной сетью, будет изменен на выбранный.
- 5 Чтобы после обновления CRL другого УЦ, с которым установлены доверительные отношения, автоматически передавать CRL на все узлы вашей сети, на вкладке **Доверенные УЦ** в группе **Действия после обновления списка аннулированных сертификатов стороннего УЦ** в соответствующем списке выберите **Требуется передать CRL**.

При обновлении CRL стороннего УЦ статус CRL для всех сетевых узлов вашей сети будет изменен на выбранный.

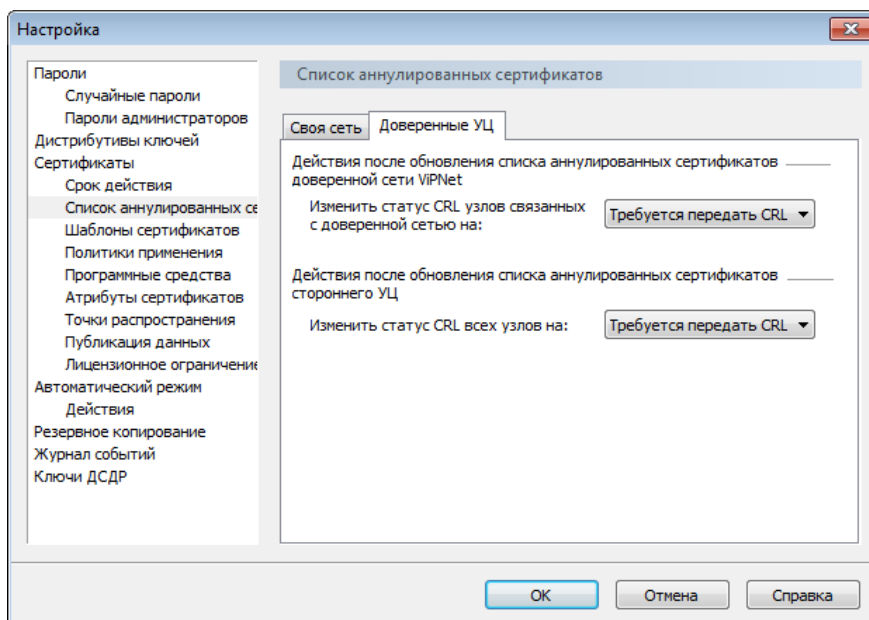


Рисунок 101. Передача CRL доверенных УЦ

- 6 В настройках автоматического режима УКЦ выберите операцию передачи всех CRL в ЦУС (см. [Настройка автоматического режима](#)).
- 7 В открывшемся окне **Параметры действия в автоматическом режиме** укажите периодичность обновления CRL, установив переключатель в нужное положение.

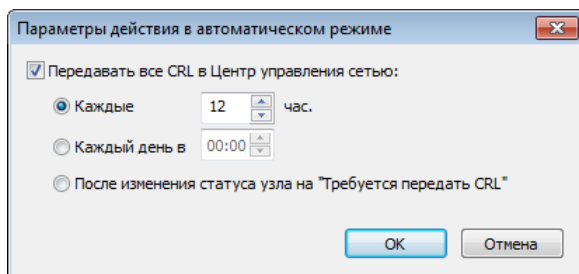


Рисунок 102. Настройка автоматической отправки CRL на все узлы

Если потребуется отключить передачу обновления CRL для всех узлов вашей сети в автоматическом режиме программы, в соответствующем списке выберите статус CRL **Неактуальные**. После обновления CRL статус CRL для узлов изменится на **Неактуальные**. В автоматическом режиме УКЦ CRL не будет отправлен. В этом случае обновленный CRL может быть отправлен только вручную (см. [Передача CRL на узлы вручную](#)).

Передача CRL на узлы вручную

Вы можете передать на узел сразу все списки аннулированных сертификатов (CRL), которые присутствуют в программе, в том числе CRL из доверенных сетей ViPNet или других удостоверяющих центров. Для этого выполните следующие действия:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Сетевые узлы**.
- 2 В списке на панели просмотра выберите нужный узел. При необходимости выберите несколько узлов.
- 3 В контекстном меню узла выберите **Передать все CRL в ЦУС**.

В результате CRL будут отправлены на узел через программу ViPNet Центр управления сетью.



Примечание. Вместе с CRL на узел также будет отправлен справочник сертификатов администраторов.

Просмотр списков аннулированных сертификатов

В программе ViPNet Удостоверяющий и ключевой центр вы можете просмотреть списки аннулированных сертификатов (CRL) вашей сети, а также импортированные CRL доверенных сетей ViPNet или других удостоверяющих центров.

Чтобы просмотреть CRL:

- 1 В окне программы на панели навигации перейдите в представление **Администрирование**.
- 2 Выберите раздел **Изданные сертификаты (Кросс-сертификация) > Списки аннулированных сертификатов** для просмотра CRL вашей сети или раздел **Импортированные сертификаты > Списки аннулированных сертификатов** для просмотра CRL доверенных сетей и сторонних УЦ.
- 3 На панели просмотра дважды щелкните CRL, который вы хотите просмотреть.
- 4 В окне **Список аннулированных сертификатов** ознакомьтесь с информацией на следующих вкладках:
 - **Общие** — содержит ряд полей, описывающих свойства списка аннулированных сертификатов: издатель списка (администратор УКЦ, для сертификата которого был издан список), дата ввода в действие и дата следующего обновления, алгоритм шифрования и другие.
 - **Список аннулированных сертификатов** — содержит серийные номера сертификатов, входящих в данный список, и дату окончания действия каждого из сертификатов. Вы можете просмотреть любой сертификат из списка с помощью кнопки **Просмотр сертификата** (см. [Просмотр сертификатов](#)).

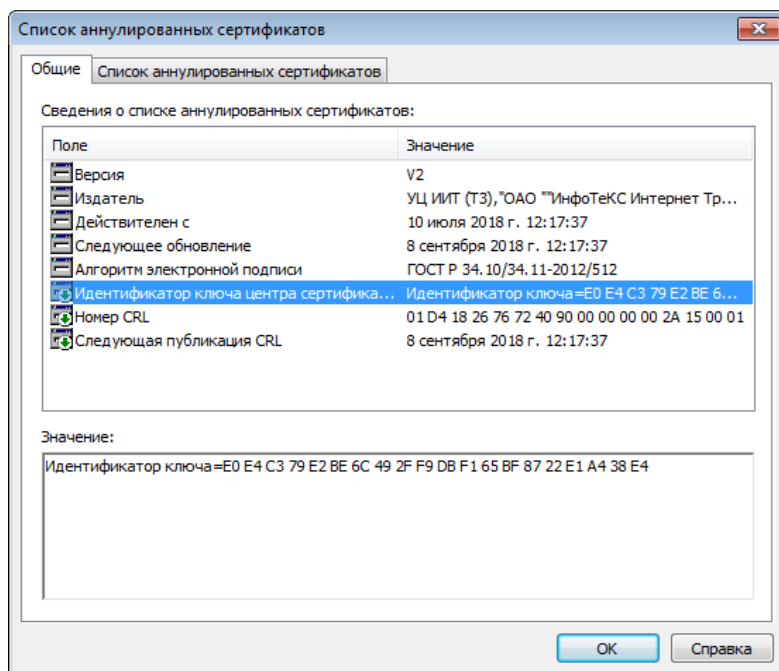


Рисунок 103. Просмотр общей информации о списке аннулированных сертификатов

Экспорт списков аннулированных сертификатов в файл

Вы можете экспортировать содержимое списков аннулированных сертификатов (CRL) в файлы. При этом несколько CRL могут экспортироваться несколькими способами:

- по отдельности в разные файлы (см. [Экспорт одного CRL в файл](#));
- сразу все в один файл (см. [Экспорт всех CRL в файл](#)).

Экспорт одного CRL в файл

Вы можете экспортировать отдельные списки аннулированных сертификатов (CRL), за исключением импортированных CRL доверенных сетей ViPNet или других удостоверяющих центров, в файлы *.crl.

Файлы с отдельными CRL, как правило, требуются в следующих случаях:

- Для передачи CRL в доверенные удостоверяющий центры.
- Для публикации CRL в сетевых хранилищах или точках распространения, например, без использования сервиса публикации.
- Для передачи CRL внешнему пользователю вместе с изданным сертификатом пользователя и сертификатом администратора.

Чтобы экспортировать конкретный CRL в файл:

- 1 В окне программы на панели навигации перейдите в представление **Администрирование**.
- 2 Выберите раздел **Изданные сертификаты** (или **Кросс-сертификация**) > **Списки аннулированных сертификатов**.
- 3 На панели просмотра щелкните нужный CRL правой кнопкой мыши и в контекстном меню выберите пункт **Экспорт в файл**.
- 4 В появившемся окне укажите путь сохранения файла с CRL.

В результате выбранный CRL будет сохранен в файле *.crl по указанному пути.

Экспорт всех CRL в файл

Вы можете экспортировать в файл сразу все списки отозванных сертификатов (CRL), которые присутствуют в программе, в том числе CRL из доверенных сетей ViPNet или других удостоверяющих центров. Это может потребоваться в том случае, если вам нужно отправить весь

комплект CRL на узел, но по сети он не может быть доставлен, например, из-за отсутствия связи с этим узлом. В таком случае вы можете передать CRL на узел в файле *.ke.

Экспортировать таким образом CRL можно только для конкретного узла. Поэтому для экспорта в данном случае выполните следующие действия:

- 1 В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Сетевые узлы**.
- 2 В списке на панели просмотра выберите нужный узел. При необходимости выберите несколько узлов.
- 3 В контекстном меню узла выберите **Сохранить все CRL в файл**.
- 4 В появившемся окне выберите папку на жестком или съемном диске.

В результате CRL для выбранного узла будут сохранены в файл `apn_XXXX.ke` (где XXXX — шестнадцатеричный идентификатор узла в сети) в указанную папку. Передайте файл с CRL пользователю узла, ему необходимо поместить этот файл в папку установки программы ViPNet Client в подпапку `\ccc\key\` и затем перезапустить программу ViPNet Монитор.



Примечание. Вместе с полным комплектом CRL в файле `apn_XXXX.ke` также будет присутствовать справочник сертификатов администраторов.

Управление временем обновления и публикации CRL

Время на компьютерах УКЦ и пользователей, которые получают CRL, может различаться. Чтобы при распространении CRL покрыть издержки рассинхронизации времени, вы можете управлять следующими параметрами:

- `Effective date indentation` — временем обновления CRL (полем «Действителен с»).

Задаёт время вступления в действие нового CRL, которое может быть до 10 минут раньше системного времени.

- `Publication date indent` — временем публикации следующего CRL (полем «Следующая публикация»).

Указывает время до истечения срока действия текущего CRL, за которое будет публиковаться новый CRL (до 24 часов). Позволяет начать заранее опрашивать точку распространения CRL, чтобы получить новый CRL.

Для этого:

- 1 Завершите работу с УКЦ.
- 2 Откройте файл `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\ini\KC.ini`.
- 3 В секции `[CRL]` укажите значения в секундах:
 - o `Effective date indentation`. Принимает значения от 0 до 600 секунд (10 минут).
 - o `Publication date indent`. Принимает значения от 0 до 86400 секунд (24 часа).

Например,

```
[CRL]
```

```
Effective date indentation=600
```

Если будет задано значение больше возможного, то будет использоваться значение по умолчанию 0.

- 4 Запустите УКЦ.

10

Публикация сертификатов и списков аннулированных сертификатов

Взаимодействие с сервисом публикации	212
Настройка параметров публикации данных	215

Взаимодействие с сервисом публикации

Поскольку компьютер с УКЦ исходя из требований безопасности не имеет выхода во внешние сети и доступа к общедоступным хранилищам, для размещения в них сертификатов и списков аннулированных сертификатов (CRL) используется сервис публикации — программа [ViPNet Publication Service](#).

Взаимодействие УКЦ с сервисом публикации осуществляется следующим образом:

- Программа ViPNet Удостоверяющий и ключевой центр помещает данные для публикации в заданную папку обмена (см. [Настройка папок обмена с программой ViPNet Publication Service](#)), откуда эти данные поступают в программу ViPNet Publication Service. Передача данных для публикации из УКЦ может производиться автоматически (см. [Режимы работы УКЦ](#)) и вручную. Автоматически могут передаваться на публикацию только CRL. Для этого должны быть выполнены соответствующие настройки (см. [Настройка автоматического режима](#)). Остальные данные (сертификаты пользователей и администраторов, кросс-сертификаты) на публикацию требуется передавать вручную.
- После этого сервис публикации размещает эти данные в соответствии со своими настройками в заданных хранилищах или точках распространения. Точки распространения, в которых будет размещать данные сервис публикации, могут быть также заданы в УКЦ для того, чтобы информация об этих точках автоматически добавлялась в издаваемые сертификаты пользователей. Подробнее см. раздел [Настройка списка точек распространения](#).

По завершении каждой публикации сервис формирует и отправляет в УКЦ отчет о результатах публикации в виде специального файла:

- Полностью успешная публикация означает, что данные опубликованы на всех выбранных в программе ViPNet Publication Service серверах доступа.
- Частично успешная публикация означает, что данные опубликованы не на всех выбранных серверах, но хотя бы на одном из них.
- Неудачная публикация означает, что данные не удалось опубликовать.

Файлы, которые не удалось опубликовать, вместе с отчетом помещаются в папку, заданную в УКЦ для приема неопубликованных данных.

- Если в сервисе публикации указаны точки распространения внешних удостоверяющих центров или доверенных сетей, то он производит их опрос с заданной периодичностью и скачивает из них новые сертификаты издателей и CRL.
- Данные, полученные из точек распространения, сервис публикации передает в УКЦ через папку, заданную для приема входящих файлов.
- УКЦ принимает полученные данные и импортирует их. Импорт CRL может производиться как автоматически, так и вручную, импорт сертификатов издателей — только вручную (см. [Импорт данных, опубликованных сторонними удостоверяющими центрами](#)). Для автоматического

импорта CRL должны быть выполнены соответствующие настройки (см. [Настройка автоматического режима](#)).

Затем импортированные данные могут быть отправлены через ЦУС на сетевые узлы в составе комплектов CRL или ключей узлов.

Подробнее о работе сервиса публикации см. документ «ViPNet Publication Service. Руководство администратора».

О том, как организовать взаимодействие между УКЦ и сервисом публикации, см. в разделе ниже.

Организация взаимодействия с сервисом публикации

Для того чтобы программа ViPNet Publication Service смогла опубликовать данные, произведите следующие настройки:

- 1 Задайте папки для обмена данными с программой ViPNet Publication Service (см. [Настройка папок обмена с программой ViPNet Publication Service](#)).
- 2 Если программы ViPNet Удостоверяющий и ключевой центр и ViPNet Publication Service установлены на разных компьютерах, то на компьютере с УКЦ средствами операционной системы откройте сетевой доступ к заданным папкам обмена для компьютера, на котором установлена программа ViPNet Publication Service.
- 3 Если вы хотите, чтобы списки аннулированных сертификатов (CRL) передавались на публикацию в автоматическом режиме, выполните дополнительные настройки УКЦ (см. [Настройка автоматического режима](#)).
- 4 Если сертификаты издателей и CRL будут публиковаться в точках распространения и вы хотите, чтобы в сертификаты пользователей добавлялась информация об этих точках, в настройках программы создайте эти точки распространения (см. [Настройка списка точек распространения](#)).

Передача данных для публикации вручную

Списки аннулированных сертификатов (CRL) для публикации могут передаваться в программу ViPNet Publication Service автоматически и вручную. Автоматическая передача CRL производится в том случае, если выполнены соответствующие настройки и программа работает в автоматическом режиме (см. [Настройка автоматического режима](#)). Сертификаты пользователей, сертификаты издателей (администраторов УКЦ), кросс-сертификаты для публикации требуется передавать вручную.

Чтобы вручную передать данные для публикации:

- 1 В окне программы выберите объекты, которые требуется передать для публикации.

- 2 В контекстном меню объектов выберите пункт **Опубликовать**.

В результате файлы с выбранными объектами будут помещены в папку, которая используется для обмена данными с программой ViPNet Publication Service.

Импорт данных, опубликованных сторонними удостоверяющими центрами

Сертификаты издателей и CRL, опубликованные сторонними удостоверяющими центрами и полученные сервисом публикации из точек распространения, передаются в УКЦ через папку обмена (см. [Настройка папок обмена с программой ViPNet Publication Service](#)). В УКЦ эти данные могут быть импортированы для дальнейшей рассылки на узлы своей сети. Сертификаты издателей могут быть импортированы только вручную, CRL — как вручную, так и автоматически (см. [Настройка автоматического режима](#)).



Примечание. Опубликованный CRL можно импортировать только после того, как будет импортирован сертификат его издателя. При этом сертификаты издателей можно импортировать только по одному.

Чтобы импортировать опубликованные данные вручную:

- 1 В окне программы на панели навигации выберите представление **Администрирование** и перейдите в раздел **Необработанные данные > Опубликованные сертификаты других УЦ**.
- 2 На панели просмотра выберите сертификат, который требуется импортировать, и на панели инструментов нажмите кнопку **Загрузить**. Импортированный сертификат будет перемещен в раздел **Импортированные сертификаты** в подраздел, соответствующий его типу.



Внимание! Прежде чем импортировать сертификат, рекомендуется проверить его параметры. Для просмотра параметров дважды щелкните сертификат (см. [Просмотр сертификатов](#)).

Таким же образом импортируйте все необходимые сертификаты издателей.

- 3 Перейдите в раздел **Необработанные данные > Опубликованные списки аннулированных сертификатов других УЦ** и аналогичным образом импортируйте необходимые CRL.

В результате выбранные CRL будут импортированы в УКЦ и перемещены в раздел **Импортированные сертификаты > Списки аннулированных сертификатов**.

Настройка параметров публикации данных

Сертификаты пользователей, сертификаты администраторов и списки аннулированных сертификатов (CRL), изданные в программе ViPNet Удостоверяющий и ключевой центр, могут быть опубликованы в общедоступных хранилищах или точках распространения с помощью программы ViPNet Publication Service (см. [Взаимодействие с сервисом публикации](#)). Ниже описана настройка параметров публикации данных в программе ViPNet Удостоверяющий и ключевой центр. Описание настройки программы ViPNet Publication Service приведено в документе «ViPNet Publication Service. Руководство администратора».

Настройка папок обмена с программой ViPNet Publication Service

Обмен данными между программами ViPNet Удостоверяющий и ключевой центр и ViPNet Publication Service осуществляется через папки, местоположение которых вы можете настраивать.

Для настройки папок обмена с программой ViPNet Publication Service:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Публикация данных**.

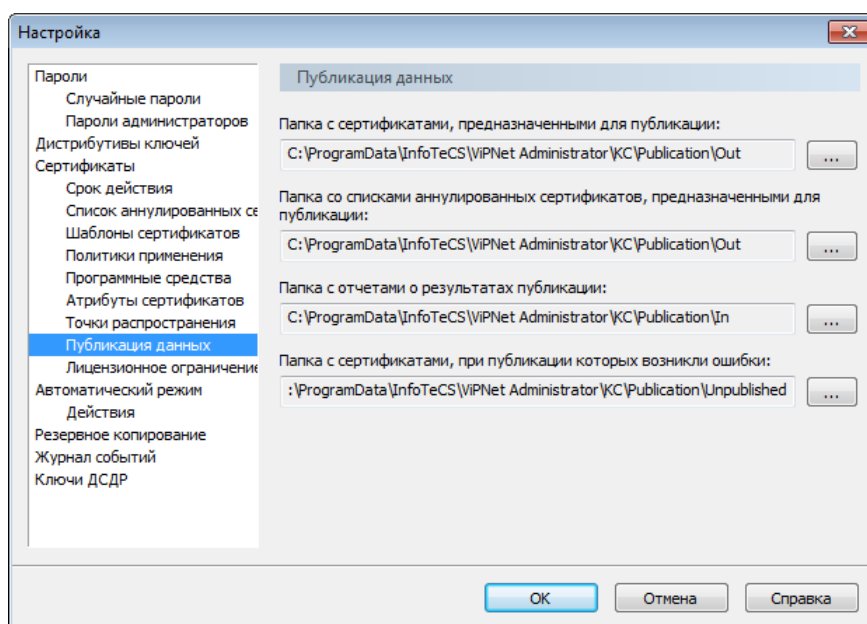


Рисунок 104. Настройка папок обмена данных

3 В соответствующих полях укажите с помощью кнопки  папки для обмена данными с программой ViPNet Publication Service. По умолчанию заданы следующие папки обмена:

- Папка данных, предназначенных для публикации: `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Publication\Out.`
- Папка для списков аннулированных сертификатов: `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Publication\Out.`

Для публикации обновленных CRL в указанную папку убедитесь, что в разделе **Список аннулированных сертификатов** на вкладке **Своя сеть** установлен флажок **Публиковать список аннулированных сертификатов**.

- Папка для приема данных и отчетов из сервиса публикации:
`C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Publication\In.`
- Папка для файлов, при публикации которых возникли ошибки:
`C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Publication\Unpublished.`

В программе ViPNet Publication Service необходимо настроить обмен данными с УКЦ через папки, заданные в программе ViPNet Удостоверяющий и ключевой центр. Подробнее см. документ «ViPNet Publication Service. Руководство администратора», глава «Настройка взаимодействия УКЦ и Сервиса публикации», раздел «Настройка папок обмена».

Настройка списка точек распространения

Списки аннулированных сертификатов (CRL) и сертификаты издателей (администраторов) с помощью программы ViPNet Publication Service могут публиковаться в **точках распространения данных**. Через точки распространения пользователи могут получать доступ к нужным им сертификатам издателей и CRL. Точкой распространения данных может быть, например, FTP- или HTTP-сервер. Также точкой распространения может выступать сервер онлайн-проверки статуса сертификатов — **OCSP-сервер**.

Если в соответствии с **инфраструктурой PKI**, развернутой в вашей организации, сертификаты администраторов и CRL размещаются в точках распространения, то информация об этих точках должна помещаться в издаваемые сертификаты пользователей. Для этого в программе ViPNet Удостоверяющий и ключевой центр должен быть сформирован список этих точек распространения. Если сертификаты и CRL публикуются на OCSP-сервер, то в программе должен быть задан адрес доступа к нему.

Точки распространения и адрес доступа к OCSP-серверу задаются в настройках программы. Точки распространения также могут задаваться при издании сертификата администратора (см. **Издание сертификата администратора**). В этом случае задается точка распространения для издаваемого сертификата или для его CRL. Точки распространения, заданные при издании сертификатов администраторов, сохраняются в настройках программы.

Чтобы в настройках УКЦ создать точку распространения или задать адрес доступа к OCSP-серверу:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.

2 В появившемся окне на панели навигации выберите раздел **Точки распространения**.

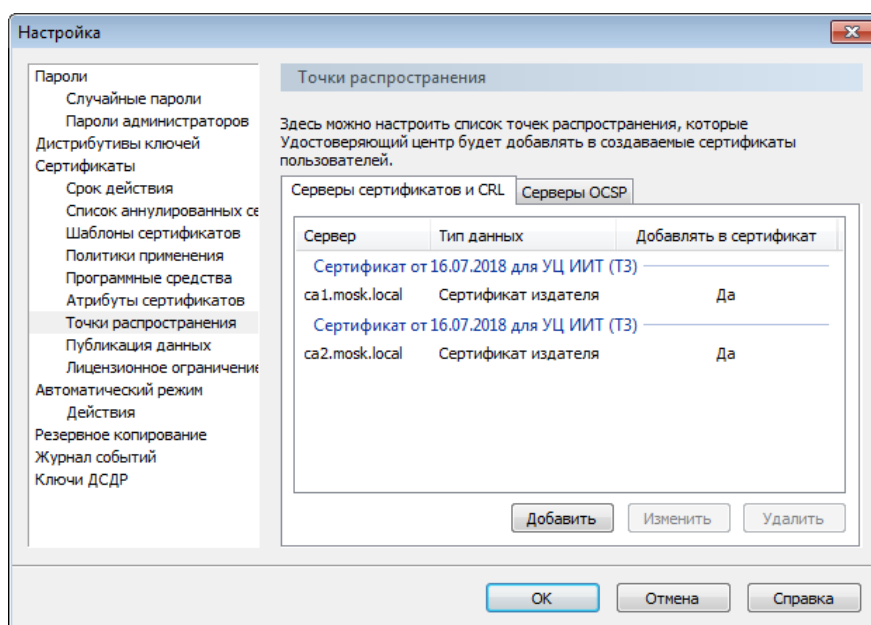


Рисунок 105. Настройка списка точек распространения

3 Чтобы создать точку распространения сертификата администратора или точку распространения CRL:

3.1 На вкладке **Серверы сертификатов и CRL** нажмите кнопку **Добавить**.

3.2 В появившемся окне укажите следующие параметры:

- **Сертификат издателя** — сертификат администратора. В зависимости от того, какой тип точки распространения вы укажете (см. параметр ниже), в созданной точке будет опубликован этот сертификат или соответствующий ему CRL.
- **Имя сервера** — имя точки распространения.
- **Сетевой путь** — URL-адрес сетевого ресурса, на котором будет размещаться данная точка распространения. В качестве URL-адреса может быть указан один из следующих адресов:

HTTP-адрес, например: `http://www.infotecs.ca.ru/10A1_rem.crl`.

FTP-адрес, например: `ftp://192.168.12.158/crl/5606-kid939/10A1_rem.crl`.

LDAP-адрес, например: `ldap://192.168.45.144:389/CN=CDP,DC=kd,DC=local`.

- **Тип точки распространения**. Для публикации в точке распространения выбранного сертификата администратора укажите тип **Сертификат издателя**. Для публикации CRL, который соответствует выбранному сертификату, укажите **Список аннулированных сертификатов**.
- Для добавления информации о точке распространения в издаваемые сертификаты пользователей установите флажок **Добавлять в сертификаты пользователей**.



Примечание. В некоторых случаях может потребоваться не добавлять в сертификаты пользователей адрес точки распространения, в которой опубликован сертификат их издателя или CRL. Например, если точка распространения в будущем будет заменена OCSP-сервером и не будет использоваться. В этих случаях вам следует снять флажок в параметрах точки.

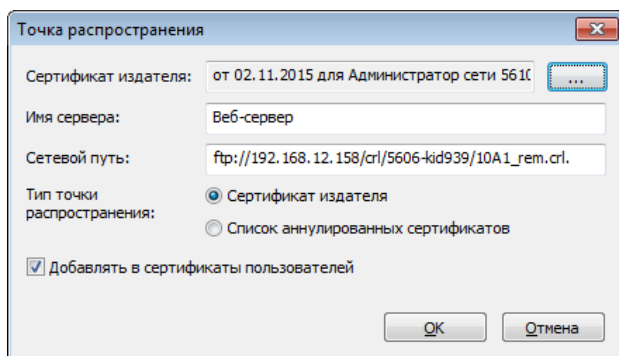


Рисунок 106. Добавление точки распространения

3.3 Нажмите кнопку **ОК**. В списке появится новая точка распространения.

4 Чтобы задать адрес доступа к OCSP-серверу:

4.1 На вкладке **Серверы OCSP** нажмите кнопку **Добавить**.

4.2 В появившемся окне укажите следующие параметры:

- **Имя сервера** — имя OCSP-сервера.
- **Сетевой путь** — URL-адрес OCSP-сервера, например, `http://infotecs.ru/ocsp/ocsp.srf`.
- Для добавления информации об OCSP-сервере в издаваемые сертификаты пользователей установите флажок **Добавлять в сертификаты пользователей**.



Примечание. В некоторых случаях может потребоваться не добавлять в сертификаты пользователей адрес доступа к OCSP-серверу, на котором размещается сертификат их издателя или CRL. Например, если OCSP-сервер используется в тестовом режиме или на какое-то время прекращена его эксплуатация. В этих случаях вам следует снять флажок в параметрах доступа к OCSP-серверу.

4.3 Нажмите кнопку **ОК**. В списке появится новый адрес доступа к OCSP-серверу.

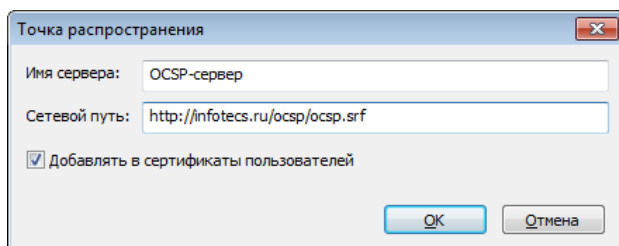


Рисунок 107. Добавление адреса доступа к OCSP-серверу

- 5 Для сохранения созданных точек распространения или адресов доступа к OCSP-серверу нажмите кнопку **ОК**.

Чтобы изменить параметры точки распространения (или адреса доступа к OCSP-серверу), выберите ее в списке и нажмите кнопку **Изменить**, затем в окне **Точка распространения** внесите необходимые коррективы (см. выше) и нажмите кнопку **ОК**. Чтобы удалить точку распространения (или адрес доступа), выберите ее в списке и нажмите кнопку **Удалить**.

11

Установление доверительных отношений с другими удостоверяющими центрами

Общая информация	221
Установление доверительных отношений с вышестоящим или подчиненным удостоверяющим центром	223
Установление доверительных отношений с равнозначным удостоверяющим центром	233
Установление доверительных отношений с удостоверяющим центром Минкомсвязи России	242

Общая информация

Между несколькими удостоверяющими центрами могут быть установлены доверительные отношения. Удостоверяющие центры, функционирующие на базе программного обеспечения ViPNet Удостоверяющий и ключевой центр, могут устанавливать отношения не только между собой, но и с удостоверяющими центрами, использующими программное обеспечение других производителей.

Установление доверительных отношений осуществляется путем кросс-сертификации. Кросс-сертификация, как правило, проводится на основе иерархической либо распределенной модели.

- В иерархической модели доверительных отношений удостоверяющие центры объединяются в древовидную структуру, в основании которой находится **головной удостоверяющий центр**. Головной удостоверяющий центр выдает кросс-сертификаты подчиненным ему центрам, тем самым обеспечивая доверие к ключам проверки электронной подписи этих центров. Каждый удостоверяющий центр вышестоящего уровня аналогичным образом делегирует право выпуска сертификатов подчиненным ему центрам. В результате доверие к сертификату каждого удостоверяющего центра основано на заверении его ключом вышестоящего центра. Сертификат головного удостоверяющего центра (**корневой сертификат**) является самоподписанным. В остальных удостоверяющих центрах администраторы не имеют собственных корневых сертификатов и для установления доверительных отношений формируют запросы на кросс-сертификат к своим вышестоящим удостоверяющим центрам.

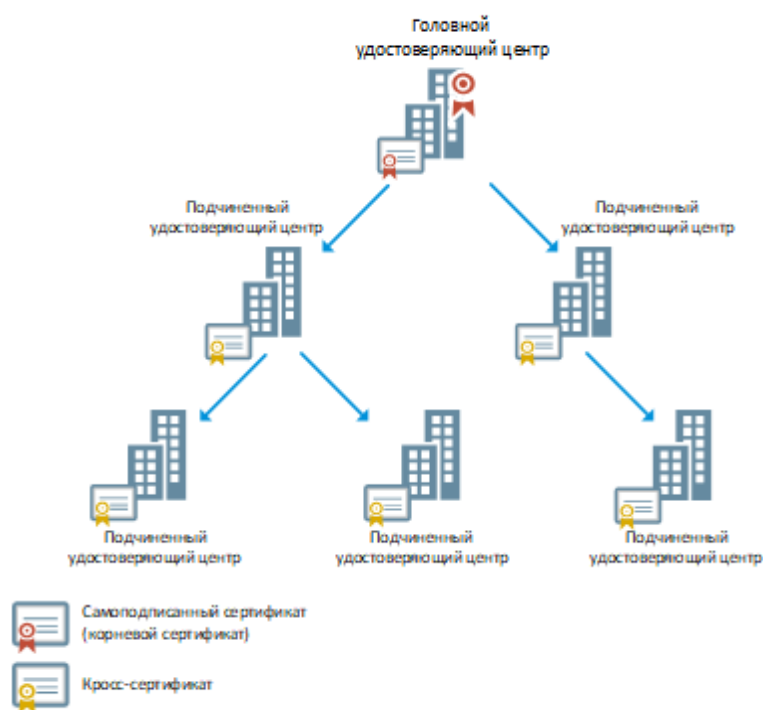


Рисунок 108. Иерархическая модель доверительных отношений

- В распределенной модели доверительных отношений все удостоверяющие центры равнозначны: в каждом удостоверяющем центре администратор имеет свой корневой (самоподписанный) сертификат. Доверительные отношения между удостоверяющими центрами в этой модели устанавливаются обычно путем двусторонней кросс-сертификации, когда два удостоверяющих центра издают кросс-сертификаты друг для друга. Взаимная кросс-сертификация проводится попарно между всеми удостоверяющими центрами. В результате в каждом удостоверяющем центре в дополнение к корневому сертификату имеются кросс-сертификаты, изданные для администраторов в других удостоверяющих центрах.

Для подписания сертификатов пользователей каждый удостоверяющий центр продолжает пользоваться своим корневым сертификатом, а кросс-сертификат, изданный для другого удостоверяющего центра, использует для проверки сертификатов пользователей другой сети. Это возможно в силу того, кросс-сертификат для доверенного удостоверяющего центра издается на базе его корневого сертификата и содержит сведения о его ключе проверки электронной подписи. Поэтому в сети, отправившей запрос, нет необходимости переиздавать сертификаты пользователей.

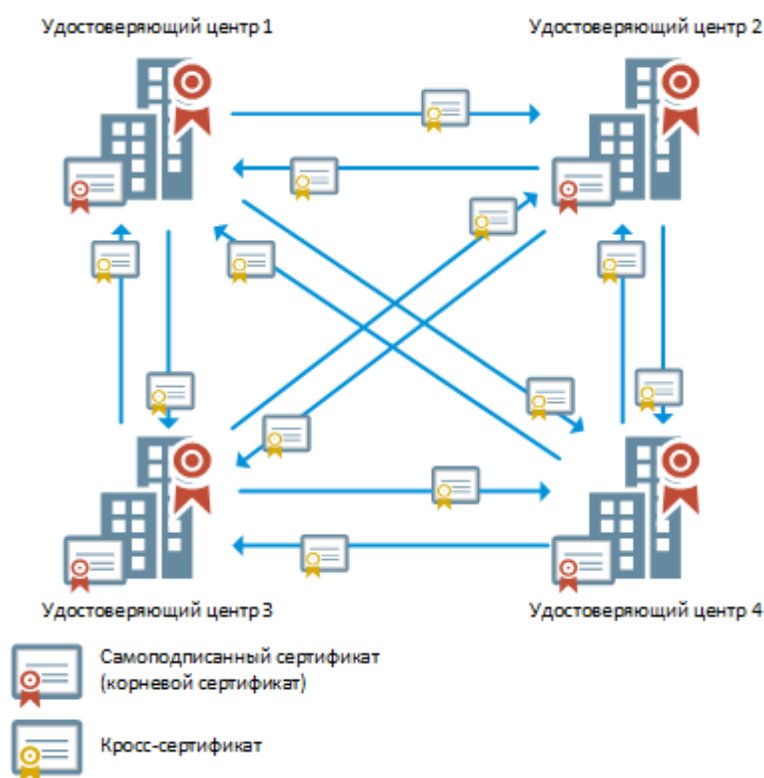


Рисунок 109. Распределенная модель доверительных отношений

О том, как установить доверительные отношения на основе данных моделей, см. в разделах ниже.

Установление доверительных отношений с вышестоящим или подчиненным удостоверяющим центром

Если вам требуется установить доверительные отношения с удостоверяющим центром (назовем его удостоверяющий центр А) на основе иерархической модели и ваш удостоверяющий центр является [подчиненным по отношению к нему](#), выполните следующие действия:

- 1 Сформируйте запрос на сертификат к вышестоящему удостоверяющему центру для администратора программы ViPNet Удостоверяющий и ключевой центр. Подробнее см. раздел [Создание запроса на сертификат к вышестоящему удостоверяющему центру](#). Если администраторов в программе несколько, сформируйте запрос для каждого из них.
- 2 Сформированный запрос (или запросы, если их было создано несколько) передайте администратору удостоверяющего центра А лично либо любым защищенным способом.

Администратор удостоверяющего центра А должен издать в соответствии с полученным от вас запросом [кросс-сертификат](#) — сертификат администратора подчиненного удостоверяющего центра, после чего экспортировать его и передать вам вместе с сертификатом издателя, которым он был заверен, и соответствующим [списком аннулированных сертификатов \(CRL\)](#).



Внимание! Если удостоверяющий центр А не является [головным](#), то вам также должны быть переданы сертификаты и CRL вышестоящих удостоверяющих центров по отношению к удостоверяющему центру А, включая корневой сертификат и соответствующий ему CRL головного удостоверяющего центра. В противном случае изданный сертификат не сможет быть импортирован (см. пункт ниже) по причине отсутствия информации для его проверки.

- 3 Импортируйте полученные от администратора удостоверяющего центра А данные в следующей последовательности:
 - 3.1 Импортируйте сертификат издателя (см. [Импорт сертификатов администраторов, полученных из вышестоящего удостоверяющего центра](#)). Если соответствующий CRL содержится в одном файле с сертификатом, он также будет автоматически импортирован.
 - 3.2 Если CRL, соответствующий сертификату издателя, был передан в отдельном файле, импортируйте его (см. [Импорт списков аннулированных сертификатов, полученных из вышестоящего удостоверяющего центра](#)).
 - 3.3 Импортируйте изданный для вас сертификат (см. [Импорт сертификата, выданного вышестоящим удостоверяющим центром](#)).

4. Импортированный сертификат администратора сделайте текущим (см. [Выбор текущего сертификата администратора](#)). В процессе данной операции для сертификата будет сформирован соответствующий CRL.

В результате доверительные отношения между вашим и вышестоящим удостоверяющим центром будут установлены. Сертификатом администратора начнут подписываться все сертификаты, издаваемые в вашем удостоверяющем центре.

Если ваш удостоверяющий центр является по отношению к другому удостоверяющему центру (назовем его удостоверяющий центр В) **вышестоящим**, и удостоверяющий центр В хочет установить с вами доверительные отношения, то в этом случае выполните следующие действия:

1. В соответствии с полученным из удостоверяющего центра В запросом (или запросами) издайте сертификат (или сертификаты). При издании сертификат будет заверен вашим текущим сертификатом. Подробнее см. раздел [Издание кросс-сертификата по запросу](#).
2. Экспортируйте изданный сертификат. Подробнее см. раздел [Экспорт кросс-сертификата](#). Кроме этого, аналогичным образом экспортируйте тот сертификат, которым был заверен изданный сертификат, и соответствующий этому сертификату CRL.



Внимание! Если ваш удостоверяющий центр не является головным, то вы также должны экспортировать и передать сертификаты издателей и CRL вышестоящих по отношению к вам удостоверяющих центров, включая корневой сертификат и соответствующий ему CRL головного удостоверяющего центра. В противном случае администратор удостоверяющего центра В не сможет импортировать изданный сертификат по причине отсутствия информации для его проверки.

3. Экспортированные сертификаты и CRL передайте администратору удостоверяющего центра В лично либо любым защищенным способом.

Администратор удостоверяющего центра В должен импортировать все полученные от вас данные.

На этом установка доверительных отношений между вашим удостоверяющим центром и удостоверяющим центром В будет считаться завершенной.

Создание запроса на сертификат к вышестоящему удостоверяющему центру

Для получения сертификата (кросс-сертификата) в вышестоящем удостоверяющем центре требуется сформировать запрос. Сформировать запрос может администратор, учетная запись которого является текущей (см. [Смена текущей учетной записи администратора](#)).



Примечание. При создании запроса на сертификат к вышестоящему удостоверяющему центру формируется контейнер ключей, в который помещается ключ электронной подписи. Сертификат, изданный по запросу, в процессе импорта сопоставляется с данным ключом электронной подписи (см. [Импорт сертификата, выданного вышестоящим удостоверяющим центром](#)).

Чтобы создать запрос на сертификат к вышестоящему удостоверяющему центру:

- 1 В окне программы на панели навигации выберите представление **Администрирование** и перейдите в раздел **Кросс-сертификация > Запросы в вышестоящий УЦ**.
- 2 На панели просмотра нажмите кнопку **Создать**.

Будет запущен мастер создания запроса на сертификат в вышестоящий удостоверяющий центр, следуйте его указаниям.
- 3 На начальных страницах мастера укажите необходимую информацию, криптопровайдер и параметры алгоритма подписи, место хранения ключа электронной подписи, ограничения и расширения сертификата, на который создается запрос. Данные сведения указываются таким же способом, как и при издании обычного сертификата администратора (см. [Издание сертификата администратора](#)).



Примечание. В запросе вы также можете задать основные ограничения сертификата. Это может быть ограничение на длину цепочки. Длина цепочки определяет количество издателей — других удостоверяющих центров, которые могут следовать за вашим удостоверяющим центром. Этим издателям будет доверять удостоверяющий центр, в который вы отправите запрос. Если длина будет равна 0, то удостоверяющий центр, в который вы отправите запрос, будет доверять только вашему удостоверяющему центру.

- 4 На странице **Файл запроса** задайте путь и имя файла, в котором будет сохранен запрос на сертификат в вышестоящий УЦ, после чего нажмите кнопку **Далее**.

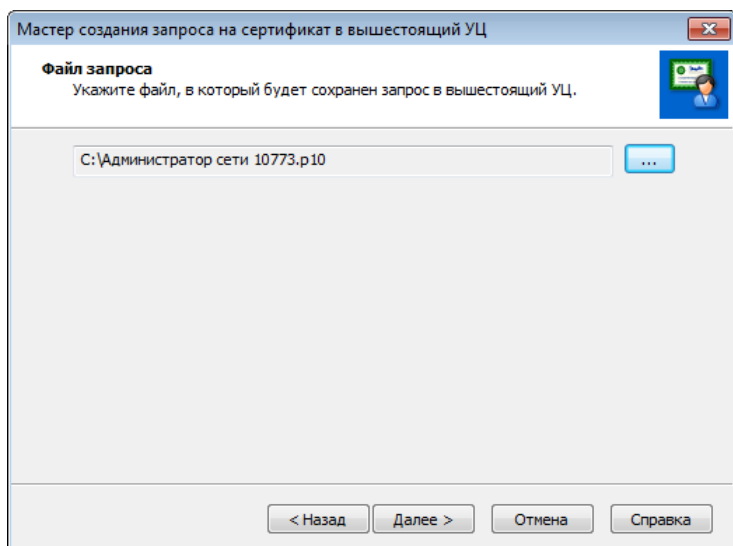


Рисунок 110. Указание места хранения файла с запросом на сертификат к вышестоящему удостоверяющему центру

- 5 На странице готовности к созданию запроса на сертификат убедитесь в правильности параметров, заданных на предыдущих страницах мастера, и нажмите кнопку **Далее**. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.
- 6 Появится **электронная рулетка**, если она еще не запускалась в текущем сеансе работы. Следуйте указаниям в окне **Электронная рулетка**. После этого будет запущен процесс создания запроса на сертификат.
- 7 На последней странице мастера при успешном создании и сохранении запроса появится соответствующее сообщение и значок  напротив каждой операции. Нажмите кнопку **Заккрыть**.

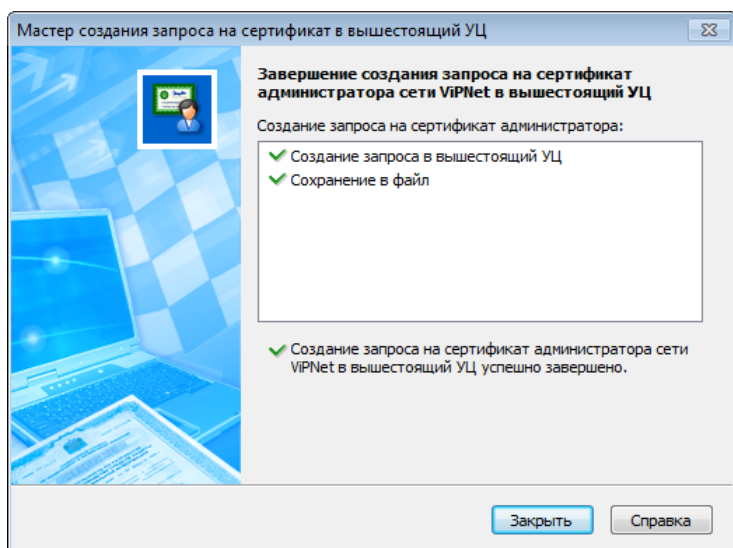


Рисунок 111. Результат создания запроса на сертификат к вышестоящему удостоверяющему центру

В результате для вас будет сформирован запрос на сертификат к вышестоящему удостоверяющему центру в формате PKCS#10 (файл *.p10). Передайте его администратору вышестоящего удостоверяющего центра для издания сертификата (кросс-сертификата).

Созданный запрос будет добавлен в список запросов к вышестоящему удостоверяющему центру и появится в разделе **Кросс-сертификация > Запросы в вышестоящий УЦ**. При необходимости вы можете его там найти и просмотреть (см. [Просмотр запроса на сертификат к вышестоящему удостоверяющему центру](#)).

Импорт сертификатов администраторов, полученных из вышестоящего удостоверяющего центра

Прежде чем импортировать сертификат, изданный в вышестоящем удостоверяющем центре, требуется импортировать сертификат издателя — сертификат администратора вышестоящего удостоверяющего центра, которым заверен ваш сертификат. Также необходимо импортировать соответствующий сертификату издателя список аннулированных сертификатов (CRL). Сертификат издателя и соответствующий CRL требуются для проверки сертификата, изданного вышестоящим удостоверяющим центром.



Примечание. Если удостоверяющий центр, который выдал вам сертификат, не является **головным**, то вам также должны быть переданы сертификаты и CRL вышестоящих по отношению к нему удостоверяющих центров, включая корневой сертификат и соответствующий ему CRL головного удостоверяющего центра. Данные сертификаты и CRL также должны быть импортированы.

Сертификат и соответствующий ему CRL передаются в отдельных файлах, поэтому импортируются отдельно друг от друга. О том, как импортировать CRL, см. в разделе [Импорт списков аннулированных сертификатов, полученных из вышестоящего удостоверяющего центра](#). Чтобы импортировать сертификат администратора вышестоящего удостоверяющего центра:

- 1 В окне программы на панели навигации выберите представление **Администрирование** и перейдите в раздел:
 - **Импортированные сертификаты > Корневые сертификаты** — для импорта корневого сертификата головного удостоверяющего центра.
 - **Импортированные сертификаты > Сертификаты промежуточных УЦ** — для импорта сертификата промежуточного удостоверяющего центра.

После этого на панели просмотра нажмите кнопку **Загрузить из файла**.

- 2 В появившемся окне выберите один или несколько файлов сертификатов, которые требуется импортировать. Выбранные сертификаты будут отображены в окне **Загрузка корневых сертификатов** или **Загрузка кросс-сертификатов**.

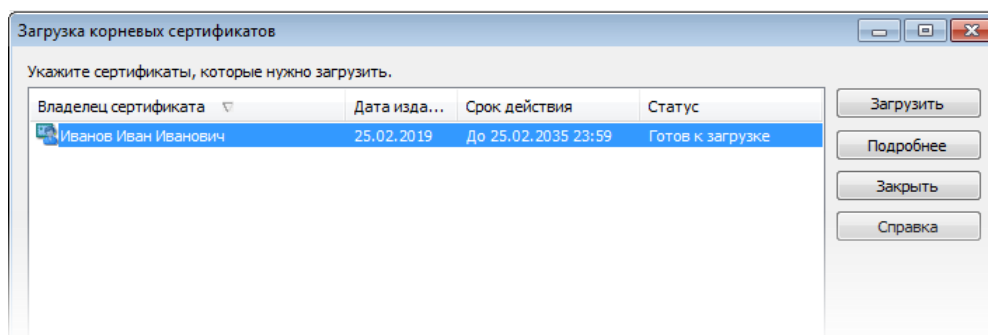


Рисунок 112. Импорт корневых сертификатов



Примечание. В окне **Загрузка корневых сертификатов** невозможно импортировать сертификаты, не являющиеся корневыми. В окне **Загрузка кросс-сертификатов** невозможно импортировать корневые сертификаты. Кроме этого, невозможно импортировать сертификаты, которые уже были импортированы ранее.

- 3 Прежде чем импортировать сертификаты, вы можете просмотреть их содержимое. Для этого выберите нужный сертификат в списке и нажмите кнопку **Подробнее**. Откроется окно просмотра сертификата (см. [Просмотр сертификатов](#)).



Примечание. Сертификаты, которые еще не были импортированы, не являются действительными. В связи с этим при просмотре и проверке этих сертификатов на вкладке **Путь сертификации** отображается информация о том, что нет доверия к корневому сертификату центра сертификации. Данное сообщение не является препятствием для импорта сертификата. При отсутствии других ошибок и совпадении содержимого полей сертификата с содержимым в бумажной копии, сертификат может быть импортирован. После импорта он станет действительным.

- 4 Чтобы импортировать сертификаты, выберите их в списке и нажмите кнопку **Загрузить**. Будет выполнен импорт выбранных сертификатов.
- 5 После импорта сертификатов издателей передайте CRL на узлы вашей сети (см. [Передача CRL на узлы вручную](#)). В составе CRL на узлы будут доставлены сертификаты издателей.

Импорт списков аннулированных сертификатов, полученных из вышестоящего удостоверяющего центра

Список аннулированных сертификатов, соответствующий сертификату администратора вышестоящего удостоверяющего центра, требуется для проверки вашего сертификата, который был издан в этом удостоверяющем центре.

Если списки аннулированных сертификатов поступили вместе с сертификатами администраторов в одном наборе формата PKCS #7, то они будут импортированы автоматически вместе с сертификатами (см. [Импорт сертификатов администраторов, полученных из вышестоящего удостоверяющего центра](#)). Если список аннулированных сертификатов поступил в виде файла *.crl, то для его импорта выполните следующие действия:

- 1 В окне программы на панели навигации выберите представление **Администрирование** и перейдите в раздел **Импортированные сертификаты > Списки аннулированных сертификатов**, затем нажмите кнопку **Загрузить из файла**.
- 2 В появившемся окне выберите один или несколько файлов, содержащих списки аннулированных сертификатов. Выбранные списки будут отображены в окне **Загрузка списков аннулированных сертификатов**.

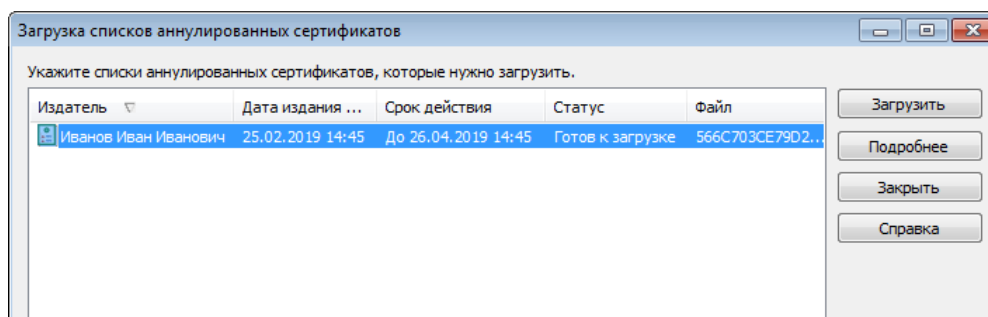


Рисунок 113. Импорт списков аннулированных сертификатов

- 3 Прежде чем импортировать списки аннулированных сертификатов, вы можете просмотреть их содержимое. Для этого выберите нужный список и нажмите кнопку **Подробнее**. Откроется окно просмотра CRL.
- 4 Чтобы импортировать списки аннулированных сертификатов, выберите их и нажмите кнопку **Загрузить**. Будет выполнен импорт выбранных списков.



Примечание. Невозможно импортировать списки аннулированных сертификатов, если ранее не были импортированы соответствующие им сертификаты администраторов. Также невозможно импортировать списки аннулированных сертификатов, срок действия которых истек.

- 5 После импорта списков аннулированных сертификатов передайте их на узлы вашей сети (см. [Передача CRL на узлы вручную](#)).

Импорт сертификата, выданного вышестоящим удостоверяющим центром

Чтобы использовать сертификат (кросс-сертификат), полученный из вышестоящего удостоверяющего центра, в своем удостоверяющем центре, вам его требуется импортировать.

Импортировать сертификат может администратор, учетная запись которого является текущей (см. [Смена текущей учетной записи администратора](#)).



Внимание! Импорт сертификата вы сможете выполнить только после того, как были импортированы сертификат его издателя — сертификат, которым он был подписан при издании, и соответствующий ему список аннулированных сертификатов (CRL).

В процессе импорта сертификат (а точнее ключ проверки электронной подписи, который содержится в сертификате) сопоставляется с ключом электронной подписи, который был создан при формировании запроса на данный сертификат (см. [Создание запроса на сертификат к вышестоящему удостоверяющему центру](#)).

Для импорта сертификата, изданного в вышестоящем удостоверяющем центре:

- 1 В окне программы на панели навигации выберите представление **Администрирование** и перейдите в раздел **Кросс-сертификация > Сертификаты от вышестоящего УЦ**, затем нажмите кнопку **Загрузить из файла**.
- 2 В появившемся окне выберите файл с изданным сертификатом, предварительно указав тип его расширения. Выбранный сертификат появится в окне **Загрузка сертификатов изданных в вышестоящем УЦ**.



Примечание. Изданный сертификат может быть передан в файле *.p7b, *.cer или *.crt.

- 3 Прежде чем импортировать загруженный сертификат, вы можете просмотреть его содержимое. Для этого выберите сертификат в списке и нажмите кнопку **Подробнее**. Откроется окно просмотра сертификата (см. [Просмотр сертификатов](#)).

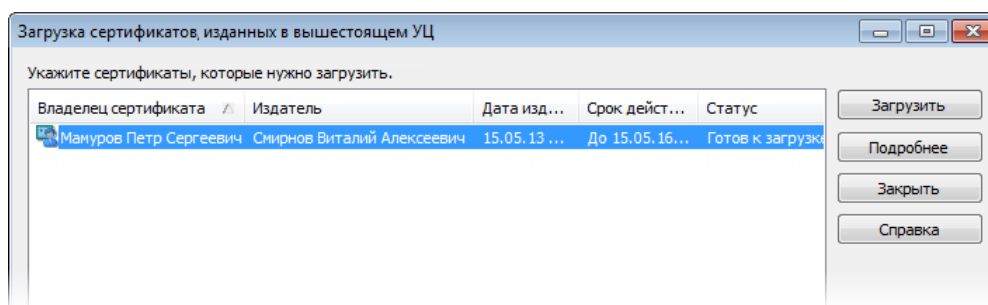


Рисунок 114. Импорт сертификата, изданного вышестоящим удостоверяющим центром

- 4 Для импорта сертификата нажмите кнопку **Загрузить**.

В результате сертификат, полученный из вышестоящего удостоверяющего центра, будет импортирован (появится в списке сертификатов в разделе **Кросс-сертификация > Сертификаты от вышестоящего УЦ**). Запрос, в соответствии с которым был издан данный сертификат, будет считаться удовлетворенным, его статус изменится на **Удовлетворен вышестоящим УЦ**. Кроме этого, будет создан список аннулированных сертификатов,

соответствующий импортированному сертификату. Данный список появится в разделе **Кросс-сертификация > Список аннулированных сертификатов**.

- 5 Импортированный сертификат, полученный из вышестоящего удостоверяющего центра, назначьте текущим сертификатом администратора (см. [Выбор текущего сертификата администратора](#)). Появится окно о необходимости отправить CRL на узлы своей сети, нажмите **ОК**.
- 6 Передайте CRL на узлы своей сети (см. [Передача CRL на узлы вручную](#)).

При наличии межсетевого взаимодействия выполните экспорт служебных данных (см. [Экспорт межсетевой информации](#)). В составе CRL ваш новый сертификат, а также сертификат его издателя и список аннулированных сертификатов, будут доставлены на сетевые узлы, в составе экспорта — в доверенные сети.

Просмотр запроса на сертификат к вышестоящему удостоверяющему центру

Чтобы просмотреть параметры сформированных запросов на сертификаты к вышестоящему удостоверяющему центру:

- 1 В окне программы на панели навигации перейдите в представление **Администрирование** и выберите раздел **Кросс-сертификация > Запросы в вышестоящий УЦ**.
- 2 Дважды щелкните нужный запрос либо в контекстном меню запроса выберите пункт **Открыть запрос**.
- 3 В окне просмотра параметров запроса ознакомьтесь с информацией на следующих вкладках:
 - **Состав запроса** — содержит список расширений запроса, в которых указаны:
 - сведения об администраторе, для которого создан запрос;
 - параметры ключа проверки электронной подписи — алгоритм, который использовался при создании ключа, заявленный срок действия;
 - список назначений, ограничений и политик применения, которые должны быть включены в сертификат.
 - **Изданный сертификат** — содержит информацию о сертификате, изданном по данному запросу: серийный номер, срок действия и статус (**Действителен**, **Недействителен**). С помощью кнопки **Открыть сертификат** можно просмотреть параметры сертификата. Если по запросу не издавался сертификат либо был получен, но не импортировался, то данная вкладка отображаться не будет.

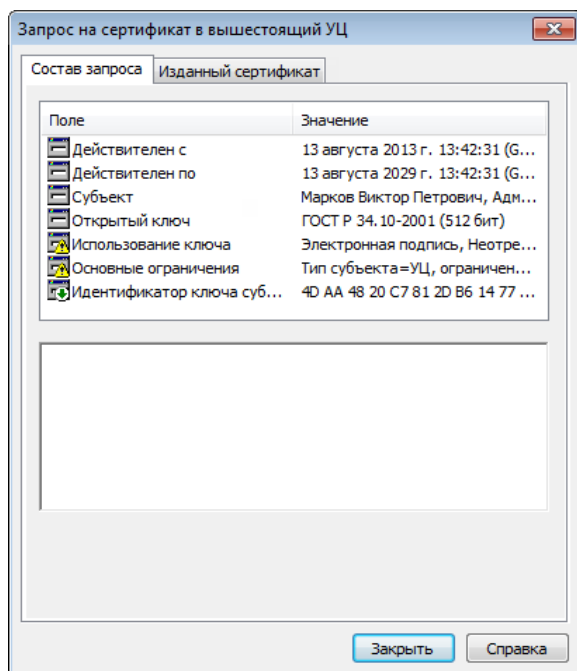


Рисунок 115. Просмотр параметров запроса на сертификат к вышестоящему удостоверяющему центру

Установление доверительных отношений с равнозначным удостоверяющим центром

Если вы хотите, чтобы между вашим и другим удостоверяющим центром (назовем его удостоверяющий центр С) были установлены доверительные отношения по распределенной модели, и администратор удостоверяющего центра С согласен с этим, выполните следующие действия:

- 1 Для каждого действительного сертификата администратора программы ViPNet Удостоверяющий и ключевой центр сформируйте запрос на кросс-сертификат. Подробнее см. в раздел [Создание запроса на кросс-сертификат](#). Если администраторов в программе несколько, то запрос на кросс-сертификат необходимо создать для сертификатов каждого администратора.
- 2 Сформированные запросы передайте администратору удостоверяющего центра С лично либо любым защищенным способом.

Администратор удостоверяющего центра С должен издать в соответствии с полученными от вас запросами кросс-сертификаты, после чего распространить их среди своих пользователей.

В результате удостоверяющий центр С будет доверять вашему удостоверяющему центру, то есть все издаваемые в вашем удостоверяющем центре сертификаты в удостоверяющем центре С будут считаться действительными.

Если администратор удостоверяющего центра С хочет, чтобы ваш удостоверяющий центр также ему доверял, и вы с этим согласны, то в этом случае выполните следующие действия:

- 1 В соответствии с полученными из удостоверяющего центра С запросами издайте кросс-сертификаты. Подробнее см. раздел [Издание кросс-сертификата по запросу](#).
- 2 Распространите изданные кросс-сертификаты между вашими пользователями путем передачи на их узлы CRL (см. [Передача CRL на узлы вручную](#)).

В результате ваш удостоверяющий центр будет доверять удостоверяющему центру С, то есть все сертификаты, издаваемые в удостоверяющем центре С, в вашем удостоверяющем центре будут проверяться и считаться действительными.

Таким образом, будет проведена двусторонняя кросс-сертификация между вашим и удостоверяющим центром С.



Примечание. При установлении доверительных отношений с несколькими удостоверяющими центрами описанную выше процедуру двусторонней кросс-сертификации потребуется провести с каждым из них.

Создание запроса на кросс-сертификат

Чтобы администратор удостоверяющего центра, с которым вы хотите установить доверительные отношения, смог издать кросс-сертификат, вам требуется создать и передать ему запрос на кросс-сертификат. Сформировать запрос на кросс-сертификат может администратор, учетная запись которого является текущей (см. [Смена текущей учетной записи администратора](#)).



Примечание. При создании запроса на кросс-сертификат, в отличие от создания запроса к вышестоящему удостоверяющему центру, ключ электронной подписи не формируется. Запрос на кросс-сертификат подписывается ключом электронной подписи, соответствующим сертификату, на основе которого данный запрос создается.

Чтобы создать запрос на кросс-сертификат:

- 1 В окне программы выберите представление **Администрирование** и перейдите в раздел **Моя сеть > Администраторы**.
- 2 В списке на панели просмотра щелкните вашу учетную запись правой кнопкой мыши и в контекстном меню выберите пункт **Создать запрос на кросс-сертификат**. Будет запущен мастер создания запроса на кросс-сертификат, следуйте его указаниям.
- 3 На странице **Сертификат администратора** выберите сертификат, на основе которого будет создан запрос на кросс-сертификат.

При необходимости просмотрите параметры сертификата с помощью кнопки **Посмотреть сертификат**. Создаваемый запрос впоследствии будет подписан ключом электронной подписи, который соответствует выбранному сертификату.

Нажмите кнопку **Далее**.

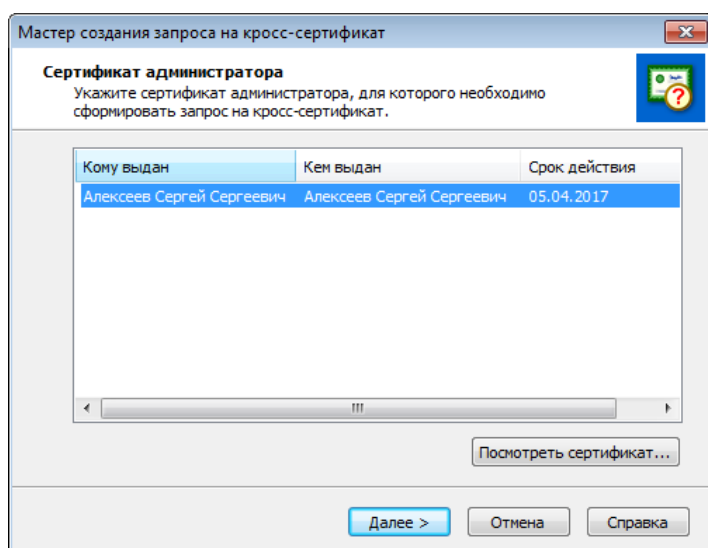


Рисунок 116. Выбор сертификата администратора для создания запроса на кросс-сертификат

- 4 На странице **Назначение кросс-сертификата**, если требуется, добавьте или измените ограничения и расширения, которые будет содержать запрос на кросс-сертификат, а после издания и сам кросс-сертификат. Формирование ограничений и расширений для кросс-сертификата осуществляется так же, как и при издании обычного сертификата администратора (см. [Издание сертификата администратора](#)).

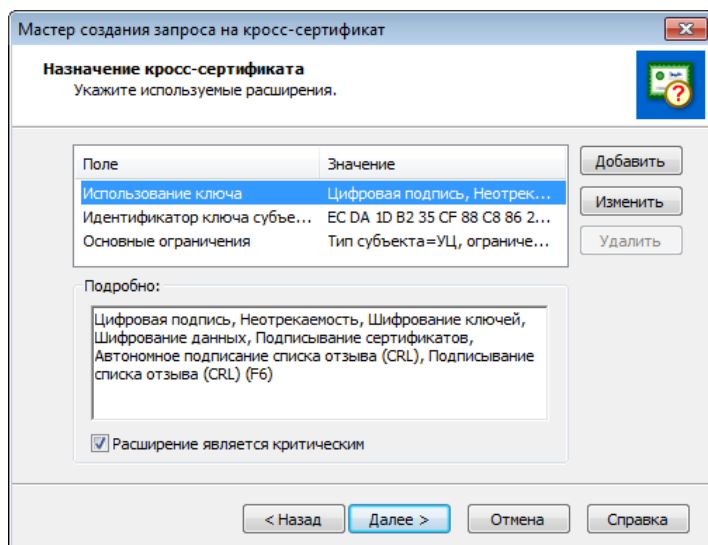


Рисунок 117. Указание расширений кросс-сертификата



Примечание. В запросе вы также можете задать основные ограничения сертификата. Это может быть ограничение на длину цепочки. Длина цепочки определяет количество издателей — других удостоверяющих центров, которые могут следовать за вашим удостоверяющим центром. Этим издателям будет доверять удостоверяющий центр, в который вы отправите запрос. Если длина будет равна 0, то удостоверяющий центр, в который вы отправите запрос, будет доверять только вашему удостоверяющему центру. Длина не может превышать длину, указанную в сертификате администратора, для которого создается запрос.

- 5 После задания параметров кросс-сертификата нажмите кнопку **Далее**.
- 6 На последней странице **Файл запроса** задайте путь и имя файла, в котором будет сохранен запрос, затем нажмите кнопку **Готово**.

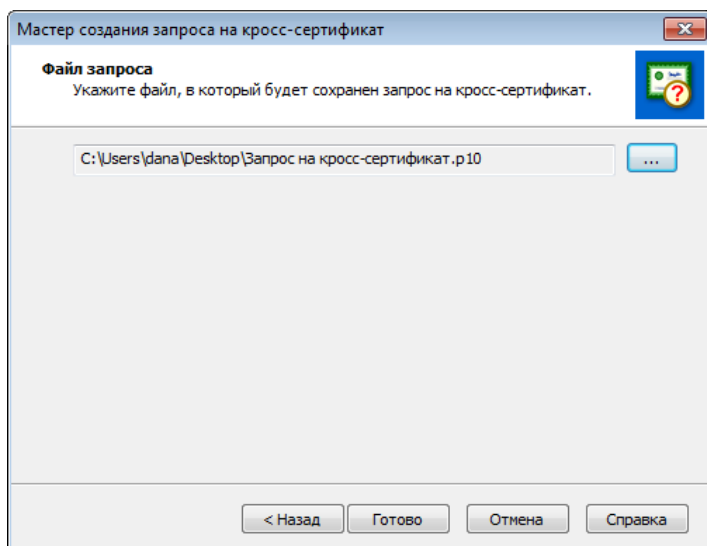


Рисунок 118. Указание места хранения файла с запросом на кросс-сертификат

В результате будет сформирован запрос на кросс-сертификат в формате PKCS#10 (файл *.p10). Передайте запрос администратору удостоверяющего центра, с которым устанавливаются доверительные отношения, для издания кросс-сертификата.

Издание кросс-сертификата по запросу

Если вам поступил запрос на кросс-сертификат, то его требуется обработать — издать по нему кросс-сертификат.

Кроме этого, если по запросу уже когда-то был издан кросс-сертификат, то вы можете издать по нему еще один повторно (например, если срок действия имеющегося кросс-сертификата истекает или если требуется добавить в него дополнительные расширения).



Примечание. Издание кросс-сертификатов производится одинаково как по запросам от подчиненных удостоверяющих центров, так и по запросам от равнозначных удостоверяющих центров.

Чтобы издать кросс-сертификат в соответствии с запросом, полученным из другого удостоверяющего центра:

- 1 В окне программы на панели навигации выберите представление **Администрирование** и перейдите в раздел **Кросс-сертификация > Сертификаты для других УЦ**, затем нажмите кнопку **Загрузить и обработать запрос**.
- 2 В появившемся окне выберите файл *.p10, в котором содержится запрос на кросс-сертификат, и нажмите кнопку **Открыть**. При необходимости вы можете выбрать сразу несколько файлов с запросами.
- 3 В окне **Издание кросс-сертификатов** в списке ознакомьтесь с параметрами запроса, который содержится в файле.

Для запроса указывается следующая информация:

- Кем запрос создан.
- Статус запроса: **Ожидает обработки**, **Действителен**, **Искажен** или **Неверный набор атрибутов**.
- Присутствуют ли в запросе сведения о сертификате, для которого он создавался (только для запросов, поступивших из равнозначных удостоверяющих центров).

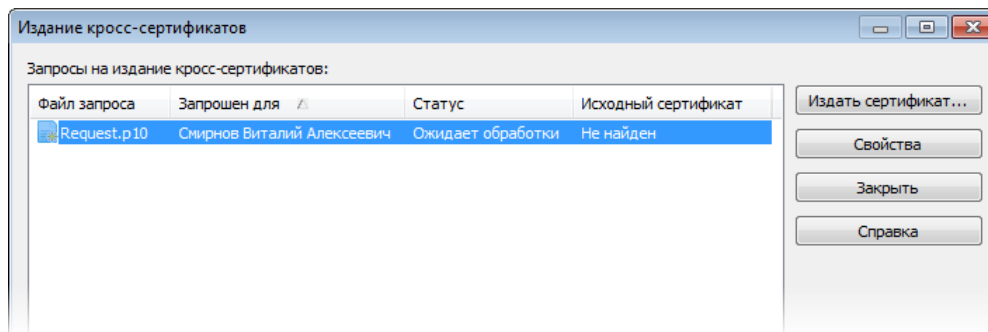


Рисунок 119. Выбор запроса для издания кросс-сертификата

- 4 При необходимости просмотрите параметры запроса с помощью кнопки **Свойства** (см. [Просмотр запроса на кросс-сертификат](#)).
- 5 Выберите запрос в списке, после чего нажмите кнопку **Издать сертификат**.

Примечание. Кнопка **Издать сертификат** будет неактивна в следующих случаях:



- Запрос поврежден (имеет статус **Искажен**).
- В запросе отсутствуют критические расширения (имеет статус **Неверный набор атрибутов**).
- Запрос принадлежит администратору вашего удостоверяющего центра (имеет статус **Не является запросом от другого УЦ**).

- 6 В появившемся мастере на странице **Срок действия кросс-сертификата** задайте срок действия издаваемого кросс-сертификата.

Рисунок 120. Задание срока действия издаваемого кросс-сертификата

- 7 На странице **Назначение кросс-сертификата** добавьте или измените основные ограничения и расширения издаваемого сертификата и нажмите кнопку **Далее**. Данные сведения формируются так же, как и при издании обычного сертификата пользователя (см. [Издание сертификатов](#)).

Рисунок 121. Формирование назначений кросс-сертификата

Если сертификат администратора удостоверяющего центра, на основе которого был создан запрос и для которого соответственно издается кросс-сертификат, включает политики применения, можно добавить расширение **Политики сертификата**. Это расширение позволит установить соответствие между политиками применения, содержащимися в запросе, и политиками применения вашего удостоверяющего центра (см. [Настройка списка политик применения сертификата](#)). Для этого:

- 7.1 На странице **Назначение кросс-сертификата** нажмите кнопку **Добавить**.
- 7.2 В окне **Допустимые расширения** выберите **Политики сертификата** и нажмите кнопку **ОК**.

- 7.3 В окне **Политики сертификата** на левой панели выберите собственную политику, затем нажмите кнопку **Добавить**. Из списка политик запроса укажите ту политику, которую требуется поставить в соответствие выбранной собственной политике, затем нажмите кнопку **ОК**.

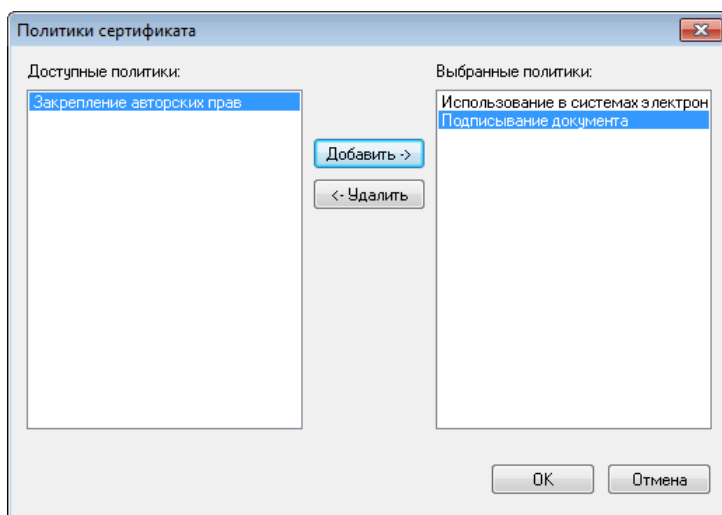


Рисунок 122. Сопоставление политик применения при издании кросс-сертификата

- 8 На странице **Состав кросс-сертификата** убедитесь в правильности параметров издаваемого сертификата, заданных на предыдущих страницах мастера, и нажмите кнопку **Готово**. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.
- 9 В окне сообщения об успешном издании кросс-сертификата нажмите кнопку **ОК**.

После издания кросс-сертификата передайте CRL на узлы вашей сети (см. [Передача CRL на узлы вручную](#)). В составе CRL на узлы будет доставлен изданный кросс-сертификат.

Изданный кросс-сертификат будет сохранен в контейнере кросс-сертификатов, который содержится в файле `issued_cross_cert_issuers_trl.p7s` в папке

`C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Key management\Certificates Issuers`, и появится в разделе **Кросс-сертификация > Сертификаты для других УЦ**. При необходимости вы можете его там найти и просмотреть (см. [Просмотр сертификатов](#)).

Если кросс-сертификат издавался для администратора подчиненного удостоверяющего центра, то его требуется экспортировать в файл для передачи данному администратору (см. [Экспорт кросс-сертификата](#)).

Экспорт кросс-сертификата

Кросс-сертификаты, изданные в процессе установления доверительных отношений с другими удостоверяющими центрами, также как и обычные сертификаты, можно экспортировать в файл (см. [Экспорт сертификатов](#)). Чаще всего экспортировать требуется сертификаты, изданные при установлении отношений по иерархической модели, потому что их необходимо передавать администраторам подчиненных удостоверяющих центров. Сертификаты, изданные при

установлении отношений на основе распределенной модели, как правило, после издания распространяются только среди своих пользователей с помощью отправки файлов CRL на узлы этих пользователей. При необходимости они также могут быть экспортированы.

Чтобы экспортировать изданный кросс-сертификат:

- 1 В окне программы перейдите в представление **Администрирование** и выберите раздел **Кросс-сертификация > Сертификаты для других УЦ**.
- 2 В списке на панели просмотра выберите нужный сертификат.
- 3 Щелкните по сертификату правой кнопкой мыши и в контекстном меню выберите пункт **Экспортировать**.
- 4 В появившемся мастере задайте параметры экспорта сертификата таким же образом, как и при экспорте обычного сертификата.

В результате выбранный сертификат будет экспортирован в файл с указанным расширением и будет готов к передаче.

Просмотр запроса на кросс-сертификат

Прежде чем обработать поступивший запрос на кросс-сертификат, просмотрите его параметры:

- 1 В окне **Издание кросс-сертификатов** в списке выберите запрос и нажмите кнопку **Свойства**.
- 2 В окне просмотра параметров запроса ознакомьтесь с информацией на следующих вкладках:
 - **Общие** — содержит список расширений запроса, в которых указаны параметры ключа проверки электронной подписи; сведения об администраторе, для которого запрошен кросс-сертификат; назначение и использование ключа; основные ограничения и другое.
 - **Сертификат автора запроса** — содержит сведения о сертификате, для которого создавался запрос и которым он был подписан: серийный номер, срок действия и статус (**Действителен**, **Недействителен**). При необходимости можно просмотреть параметры данного сертификата с помощью кнопки **Открыть сертификат из файла** (см. раздел [Просмотр сертификатов](#)).



Примечание. Данные сведения отображаются только для запросов на кросс-сертификаты от равнозначных удостоверяющих центров и только в том случае, если сертификаты, для которых создавались запросы, были предварительно импортированы. Во всех остальных случаях на данной вкладке указано, что сертификат не найден.

- **Изданные сертификаты** — содержит список кросс-сертификатов, которые уже были изданы по данному запросу ранее (в том случае, если по запросу повторно издается кросс-сертификат). Для каждого сертификата отображается имя владельца, срок действия и статус (**Действителен**, **Недействителен**). С помощью кнопки **Подробнее** можно просмотреть параметры каждого сертификата из списка.

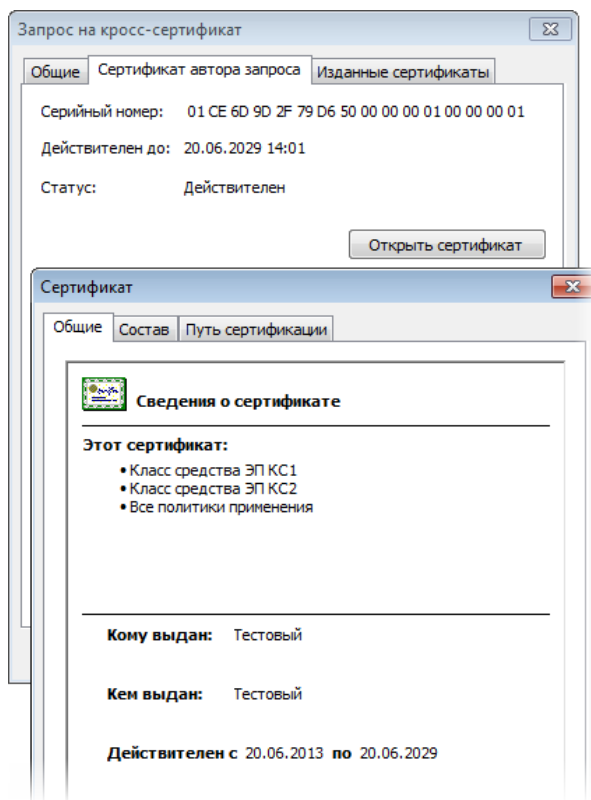


Рисунок 123. Просмотр параметров запроса на кросс-сертификат

Установление доверительных отношений с удостоверяющим центром Минкомсвязи России

Если удостоверяющий центр, функции которого выполняет программа ViPNet Удостоверяющий и ключевой центр, на территории РФ планирует работать в качестве [аккредитованного удостоверяющего центра](#), в процессе его аккредитации требуется установить доверительные отношения между ним и головным аккредитованным удостоверяющим центром, функции которого выполняет уполномоченный федеральный орган. Аккредитованный удостоверяющий центр для подписания от своего имени квалифицированных сертификатов обязан использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром. Аккредитованному удостоверяющему центру запрещается использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, для подписания сертификатов, не являющихся квалифицированными сертификатами.

Чтобы установить доверительные отношения с головным аккредитованным УЦ:

- 1 Для администратора программы ViPNet Удостоверяющий и ключевой центр сформируйте запрос на сертификат к вышестоящему УЦ (см. [Создание запроса на сертификат к вышестоящему удостоверяющему центру](#)).
- 2 Передайте сформированный запрос администратору головного аккредитованного УЦ.
- 3 Получите от администратора головного аккредитованного УЦ подчиненный сертификат, который он издал по вашему запросу, а также сертификат издателя, которым заверен ваш подчиненный сертификат, и соответствующий список аннулированных сертификатов (CRL). Сертификат издателя и соответствующий список аннулированных сертификатов при аккредитации и при смене сертификата издателя должны передаваться доверенным образом.
- 4 Импортируйте в УКЦ сертификат издателя и CRL, полученные от администратора головного аккредитованного УЦ. Подробнее см. разделы [Импорт сертификатов администраторов, полученных из вышестоящего удостоверяющего центра](#) и [Импорт списков аннулированных сертификатов, полученных из вышестоящего удостоверяющего центра](#).
- 5 Импортируйте в УКЦ подчиненный сертификат, изданный для вас в головном аккредитованном УЦ (см. [Импорт сертификата, выданного вышестоящим удостоверяющим центром](#)). Этот сертификат автоматически будет назначен вашим текущим сертификатом.

После этого вы можете издавать для пользователей квалифицированные сертификаты.

12

Работа с данными администратора программы ViPNet Удостоверяющий и ключевой центр

Управление учетной записью администратора	244
Просмотр и изменение данных об администраторе	248
Управление ключами электронной подписи и сертификатом администратора	250
Смена пароля администратора	261
Смена ключа защиты УКЦ	263

Управление учетной записью администратора

Отказ от использования нескольких учетных записей администратора

Начиная с версии 4.0, в программе ViPNet Удостоверяющий и ключевой центр можно использовать только одну учетную запись администратора, создание дополнительных учетных записей невозможно. Если в вашей сети ранее были созданы несколько учетных записей администраторов УКЦ, то при переходе на версию 4.0 и выше они продолжают нормально функционировать. Однако мы настоятельно рекомендуем оставить среди них только одну учетную запись для администрирования УКЦ, а остальные учетные записи — удалить (см. [Удаление учетной записи администратора](#)). Использование нескольких учетных записей администраторов программы ViPNet Удостоверяющий и ключевой центр не рекомендуется по следующим соображениям:

- 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 будет потеряно доверие ко всей цепочке сертификатов, изданных с использованием сертификата этого администратора. Аннулирование, проверка, обновление сертификатов пользователей будут невозможны.
- 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 (отпуск, болезнь), другой администратор с его ведома должен войти в УКЦ с использованием пароля отсутствующего администратора и обновить CRL. Однако передача собственной конфиденциальной информации крайне нежелательна из соображений безопасности.
- При наличии нескольких учетных записей администратора УКЦ и, соответственно, нескольких CRL у каждого CRL после его публикации на внешней точке доступа будет собственный адрес. Собственный адрес необходим, поскольку для проверки разных сертификатов пользователей нужно скачивать разные CRL.

Удаление учетной записи администратора

Если в вашей сети есть несколько учетных записей администраторов, которые были созданы в УКЦ еще до перехода на версию 4.0 и выше, то настоятельно рекомендуется оставить только одну учетную запись, остальные записи следует удалить.

Учетную запись можно удалить только в том случае, если она не является текущей. При необходимости можно удалить сразу несколько учетных записей.

В процессе удаления учетной записи администратора требуется перевыпустить сертификаты пользователей, которые были изданы этим администратором (если срок действия сертификатов этого администратора еще не истек). Потому что после удаления учетной записи будет невозможно обновить [списки аннулированных сертификатов \(CRL\)](#), соответствующих действующим сертификатам подписи этого администратора. Отсутствие актуальных CRL, в свою очередь, приведет к тому, что на узлах сети будет невозможно проверить сертификаты пользователей, выданные этим администратором.

Чтобы удалить учетную запись администратора:

- 1 В окне программы выберите представление **Администрирование** и перейдите в раздел **Моя сеть > Администраторы**.
- 2 Щелкните учетную запись правой кнопкой мыши и в контекстном меню выберите пункт **Удалить**.
- 3 В появившемся окне подтвердите удаление учетной записи.
- 4 Убедитесь, что учетная запись пропала из списка в разделе **Администраторы**.
- 5 Издайте новые сертификаты пользователей на смену сертификатам, которые были изданы администратором с удаленной учетной записью. Изданные сертификаты должны быть заверены вашим действующим сертификатом подписи (см. [Издание сертификатов](#)).
- 6 Если у администратора, учетная запись которого была удалена, останется возможность доступа к программе, настоятельно рекомендуется сменить ключ защиты УКЦ (см. [Смена ключа защиты УКЦ](#)).



Примечание. Если администраторы УКЦ с удаленными учетными записями имели учетные записи пользователей в программе ViPNet Центр управления сетью, то эти учетные записи будут сохранены. Удалите их при необходимости вручную. О том, как в ЦУСе удалить учетную запись пользователя, см. в документе «ViPNet Центр управления сетью. Руководство администратора», в разделе «Изменение списка пользователей сетевого узла».

Смена текущей учетной записи администратора

Под текущей учетной записью администратора понимается учетная запись администратора, сертификатом которого подписываются издаваемые в данный момент сертификаты пользователей. Учетная запись, которая используется для входа в программу ViPNet Удостоверяющий и ключевой центр, становится текущей (см. [Запуск и завершение работы программы](#)). Если в вашей сети есть несколько учетных записей администраторов, которые были созданы в УКЦ еще до перехода на

версию 4.0 и выше, вы можете сменить текущую учетную запись непосредственно в самом сеансе работы с программой (см. ниже).



Внимание! В силу сложности организационных мер по поддержанию работоспособности системы доверительных отношений не рекомендуется использовать в программе ViPNet Удостоверяющий и ключевой центр более одной учетной записи администратора программы (см. [Отказ от использования нескольких учетных записей администратора](#)).

Только одна учетная запись из имеющихся может являться текущей. Список зарегистрированных учетных записей администраторов содержится в представлении **Администрирование** в разделе **Моя сеть > Администраторы**. Текущая учетная запись администратора в списке обозначена значком , остальные учетные записи — значком .

Если в УКЦ зарегистрировано несколько учетных записей администраторов, вы можете сменить текущую учетную запись (текущего администратора), не выходя из программы. Для этого:

- 1 В окне программы в меню **УКЦ** выберите пункт **Сменить администратора**.
- 2 В окне с сообщением о необходимости завершить текущий сеанс работы нажмите кнопку **Да**.
- 3 В появившемся окне выберите учетную запись администратора, под которой будет производиться вход в программу, и введите [пароль](#).



Внимание! Если вы 3 раза ввели неправильный пароль, то дальнейший ввод пароля будет возможен по истечении 40 секунд.

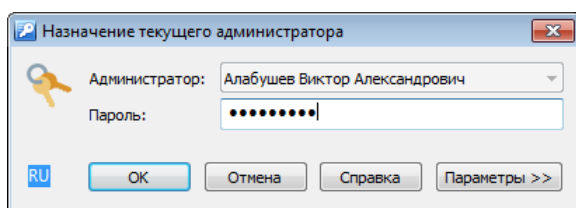


Рисунок 124. Смена текущей учетной записи

- 4 Укажите место хранения [ключей администратора](#) в том случае, если оно было изменено либо если ключи находятся на внешнем устройстве хранения данных. Для этого в окне входа в программу нажмите кнопку **Параметры** и в скрытой ранее группе **Устройство хранения ключей** установите переключатель в положение:
 - **Папка**, если ключи администратора хранятся в папке на компьютере. После этого с помощью кнопки  укажите путь к нужной папке с ключами.
 - **Устройство**, если ключи администратора хранятся на внешнем устройстве (см. [Внешние устройства](#)). После этого подключите устройство хранения ключей, выберите его в соответствующем списке и введите ПИН-код (если требуется).



Примечание. Необходимость ввода ПИН-кода зависит от типа используемого внешнего устройства. Чтобы сохранить ПИН-код и в дальнейшем не вводить его при аутентификации, в окне входа в УКЦ установите соответствующий флажок.

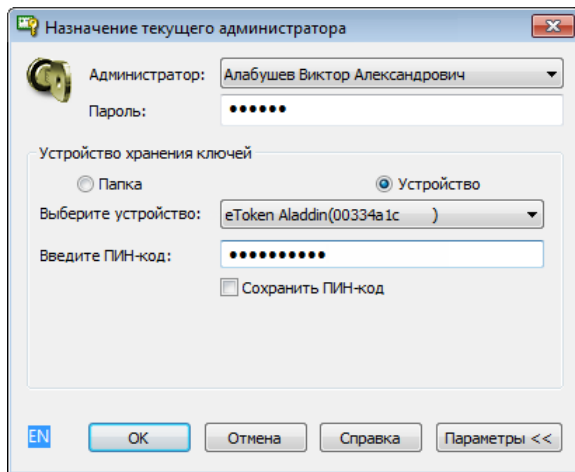


Рисунок 125. Смена текущей учетной записи с указанием места хранения ключей

5 После ввода необходимых для аутентификации данных нажмите кнопку **ОК**.

В результате произойдет смена текущей учетной записи администратора, и все операции в программе будут осуществляться от имени администратора с текущей учетной записью.

Просмотр и изменение данных об администраторе

Для просмотра или изменения информации об администраторах программы ViPNet Удостоверяющий и ключевой центр:

- 1 В окне программы выберите представление **Администрирование** и перейдите в раздел **Моя сеть > Администраторы**.
- 2 В списке на панели просмотра дважды щелкните учетную запись администратора либо в контекстном меню учетной записи выберите пункт **Открыть**.
- 3 В окне просмотра свойств администратора ознакомьтесь с информацией на следующих вкладках:
 - **Общие** — указано имя администратора. На вкладке также имеется кнопка смены пароля (см. [Смена пароля администратора](#)) и кнопка смены ключа защиты УКЦ (см. [Смена ключа защиты УКЦ](#)).
 - **Текущий сертификат** — содержатся сведения о текущем сертификате администратора (сертификате, которым заверяются издаваемые сертификаты пользователей), сроке плановой смены ключа электронной подписи, размещении [контейнера ключей](#).

С помощью кнопок **Подробнее** вы можете узнать подробную информацию о текущем сертификате администратора (см. [Просмотр сертификатов](#)) и просмотреть свойства контейнера ключей (см. [Просмотр контейнера ключей подписи администратора](#)).



Примечание. Если в программе зарегистрировано несколько администраторов, то вкладка **Текущий сертификат** отображается только в том случае, если открыты свойства администратора, учетная запись которого является текущей (см. [Смена текущей учетной записи администратора](#)).

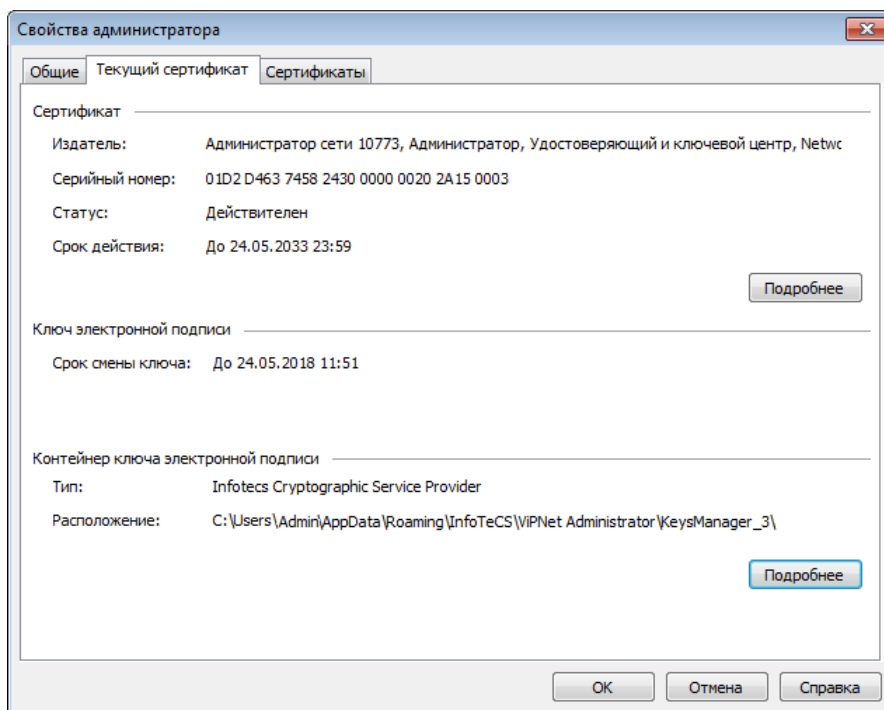


Рисунок 126. Просмотр сведений о текущем сертификате администратора

- 4 Чтобы изменить имя учетной записи администратора, на вкладке **Общие** в поле **Имя** введите новое имя, которое будет использоваться для входа в программу УКЦ, и нажмите кнопку **ОК**.

Для отображения списка всех сертификатов и выбора текущего сертификата администратора перейдите на вкладку **Сертификаты** (см. [Выбор текущего сертификата администратора](#)).

Управление ключами электронной подписи и сертификатом администратора

Издание сертификата администратора

Издание сертификата администратора производится автоматически при первичной инициализации (см. [Установка и первичная инициализация программы ViPNet Удостоверяющий и ключевой центр](#)). Вы также можете вручную издать новый сертификат администратора УКЦ, например, при плановой смене ключа электронной подписи текущего сертификата администратора. Вручную издавать сертификаты администраторов целесообразно в том случае, если ваш удостоверяющий центр не является подчиненным. В противном случае изданные сертификаты нельзя будет использовать для подписи сертификатов пользователей.



Внимание! Как правило, издание сертификатов администраторов должно определяться регламентом работы удостоверяющего центра вашей организации.

В процессе издания сертификата формируется ключ электронной подписи. По истечении срока плановой смены ключ электронной подписи не сможет быть использован для подписи издаваемых сертификатов пользователей. Подпись списка аннулированных сертификатов (CRL) данным ключом электронной подписи при этом будет возможна в течение срока действия ключа электронной подписи. Срок действия ключа электронной подписи зависит от места его хранения.

В сертификате администратора отсутствует расширение «Срок действия закрытого ключа», если он издается на срок меньше, чем допустимый срок действия ключа электронной подписи (см. [Плановая смена ключа электронной подписи и сертификата администратора](#)):

- в файле на компьютере либо на внешнем устройстве без аппаратной поддержки российских криптографических алгоритмов — 4,5 года;
- на устройстве с аппаратной поддержкой российских криптографических алгоритмов — 6 лет.

Срок действия ключа в данном случае будет равен сроку действия сертификата. CRL обновляется в течение всего срока действия сертификата. После того, как срок действия сертификата администратора истек, CRL будет удален.

В сертификате администратора будет расширение «Срок действия закрытого ключа», если он издается на срок равный или больше допустимого срока действия ключа электронной подписи. В данном случае CRL обновляется в течение срока действия ключа электронной подписи. После того, как истечет срок действия ключа электронной подписи, статус CRL будет отображен как **Действителен (текущий, финальный)**. При этом в УКЦ будет запрещено отзывать сертификаты пользователей. После истечения срока действия сертификата CRL будет удален. Таким образом, CRL

своевременно удаляются из УКЦ по истечении допустимого срока действия ключа электронной подписи.

Издать сертификат можно только для администратора, учетная запись которого является текущей (см. [Смена текущей учетной записи администратора](#)).

Совет. Если требуется, чтобы сертификат администратора имел формат квалифицированного сертификата, то перед его изданием необходимо выполнить ряд дополнительных настроек программы (см. [Издание квалифицированных сертификатов](#)).



Кроме этого, в настройках программы вы можете предварительно задать срок, на который должен быть издан сертификат администратора. Как правило, данная настройка полезна в том случае, если при издании сертификата администратора вы не планируете редактирование параметров на страницах мастера. Чтобы задать срок действия сертификата администратора, в настройках программы перейдите в раздел **Срок действия**, в котором в группе **Сертификаты и ключи администраторов** в поле **Срок действия сертификата** укажите срок (в месяцах). Срок не может превышать 192 месяца (16 лет).

Для издания сертификата администратора:

- 1 В окне программы выберите представление **Администрирование** и перейдите в раздел **Моя сеть > Администраторы**.
- 2 Щелкните имя своей учетной записи правой кнопкой мыши и в контекстном меню выберите **Создать корневой сертификат**.
Появится электронная рулетка, если она еще не запускалась в рамках текущего сеанса работы программы. Поводите указателем в пределах окна **Электронная рулетка**.
- 3 На первых страницах мастера **Сведения о владельце сертификата** укажите имя администратора и другие необходимые данные, которые впоследствии будут добавлены в его сертификат, и нажмите кнопку **Далее**.

Рисунок 127. Указание сведений об администраторе, для которого создается сертификат

- 4 На странице **Дополнительные сведения о владельце сертификата** при необходимости отредактируйте дополнительные сведения о владельце. Для этого в списке выберите соответствующие атрибуты, нажмите кнопку **Изменить** и внесите необходимую информацию. Затем нажмите кнопку **Далее**.

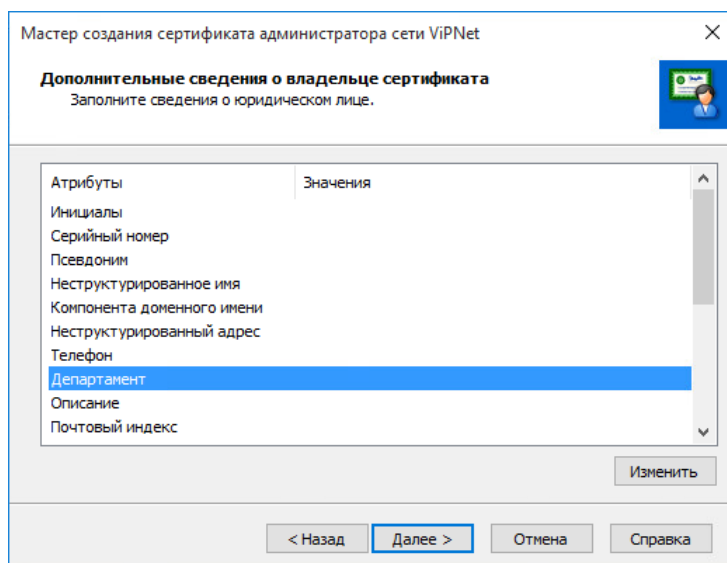


Рисунок 128. Указание дополнительных сведений об администраторе, для которого создается сертификат

- 5 На странице **Параметры ключа электронной подписи** выберите криптопровайдер в соответствии с приведенной ниже таблицей либо другой криптопровайдер, установленный на компьютере. Выбранный криптопровайдер определит алгоритм подписи, по которому будет создаваться ключ электронной подписи и ключ проверки электронной подписи и вычисляться хэш-функция.

Кроме этого, укажите параметры алгоритма подписи. В соответствии с заданными параметрами будет автоматически определена длина ключа проверки электронной подписи и алгоритм хэширования.

Таблица 9. Характеристика криптопровайдеров и алгоритмов электронной подписи

Криптопровайдер и соответствующий ему алгоритм электронной подписи	Параметры алгоритма подписи	Длина ключа проверки электронной подписи и алгоритм хэширования
Infotecs GOST 2012/512	ГОСТ Р 34.10 - 2001. Параметры	512 бит
Cryptographic Service Provider	по умолчанию (рекомендуется)	ГОСТ Р 34.11-2012/256
ГОСТ Р 34.10-2012/512	OID «1.2.643.2.2. 35.1»	
Новый стандарт электронной подписи от 2012 года с длиной ключа электронной подписи 256 бит	ГОСТ Р 34.10 - 2001 Параметры подписи В	
OID «1.2.643.2.2. 35.2»	OID «1.2.643.2.2. 35.2»	
OID «1.2.643.7.1.1.1.1»	ГОСТ Р 34.10 - 2001. Параметры подписи С	
	OID «1.2.643.2.2. 35.3»	
Infotecs GOST 2012/1024	ГОСТ Р 34.10 - 2012/1024. Набор	1024 бит

Криптопровайдер и соответствующий ему алгоритм электронной подписи	Параметры алгоритма подписи	Длина ключа проверки электронной подписи и алгоритм хэширования
Cryptographic Service Provider	параметров А	ГОСТ Р 34.11-2012/512
ГОСТ Р 34.10-2012/1024	ГОСТ Р 34.10 - 2012/1024. Набор параметров В	
Новый стандарт электронной подписи от 2012 года с длиной ключа электронной подписи 512 бит		
OID «1.2.643.7.1.1.1.2»		



Совет. Рекомендуется использовать параметры алгоритма, предлагаемые по умолчанию. Данные параметры характеризуются наибольшей скоростью вычисления и проверки электронной подписи.

Нажмите кнопку **Далее**.

Рисунок 129. Настройка параметров ключа электронной подписи

- 6 На странице **Место хранения контейнера ключей** укажите место хранения контейнера ключей: **В файле** или **На внешнем устройстве**. Нажмите кнопку **Далее**.

Если выбрано хранение ключа на внешнем устройстве, подключите внешнее устройство к компьютеру и выберите его на странице **Место хранения контейнеров ключа электронной подписи и ключа защиты УКЦ**. Если требуется, введите ПИН-код. После этого нажмите кнопку **Далее**.



Примечание. Если устройство не было отформатировано ранее, то может быть отображено окно с предложением отформатировать устройство. В этом случае согласитесь с предложением и дождитесь окончания форматирования.

Подробную информацию о поддерживаемых внешних устройствах хранения данных и особенностях работы с ними читайте в разделе [Внешние устройства](#).

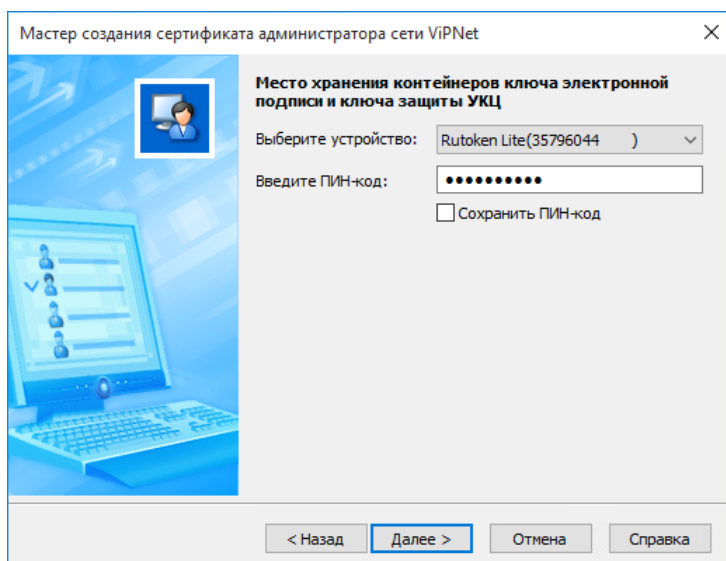


Рисунок 130. Выбор внешнего устройства

В зависимости от выбранного места хранения будет определен срок действия ключа электронной подписи и, соответственно, срок его плановой смены. При хранении ключа электронной подписи в файле на компьютере либо на внешнем устройстве без аппаратной поддержки алгоритма ГОСТ 34.10-2012 плановая смена ключа электронной подписи должна производиться каждые 15 месяцев, период действия ключа электронной подписи для обновления CRL составляет 54 месяца.

Если ключ электронной подписи хранится на устройстве с аппаратной поддержкой ГОСТ Р 34.10-2012 (был непосредственно сформирован на нем), то смена ключа должна производиться каждые 3 года, период действия ключа электронной подписи для обновления CRL составляет 72 месяца.

Место хранения и срок плановой смены ключа электронной подписи должны быть зафиксированы в регламенте работы удостоверяющего центра.

- 7 На странице **Срок действия сертификата** задайте срок действия сертификата администратора, после чего нажмите кнопку **Далее**. Если вы предварительно задавали срок действия сертификата администратора в настройках программы, то редактирование параметров на данной странице мастера вы можете пропустить.

Мастер создания сертификата администратора сети ViPNet

Параметры ключа электронной подписи
Укажите информацию о параметрах ключа электронной подписи.

Криптопровайдер: Infotecs GOST 2012/512 Cryptographic Service Provide

Алгоритм электронной подписи: ГОСТ Р 34.10-2012/512

Параметры алгоритма ЭП: ГОСТ Р 34.10 Параметры по умолчанию

Длина ключа проверки ЭП (бит): 512

Алгоритм хеширования: ГОСТ Р 34.11-2012/256

< Назад **Далее >** Отмена Справка

Рисунок 131. Задание срока действия сертификата администратора

- 8 На странице **Назначение сертификата** укажите ограничения, расширения и политики применения издаваемого сертификата и нажмите кнопку **Далее**. Данные сведения формируются так же, как и при издании обычного сертификата пользователя (см. [Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ](#)).



Примечание. При издании сертификата администратора вы не можете редактировать расширение «Использование ключа».

Мастер создания сертификата администратора сети ViPNet

Назначение сертификата
Укажите используемые расширения.

Поле	Значение
Основные ограничения	Тип субъекта=УЦ, ограничение н...
Тип идентификации	Личное присутствие

Добавить Изменить Удалить

Подробнее:

Тип субъекта=УЦ
Ограничение на длину пути=Отсутствует

☒ Расширение является критическим

< Назад **Далее >** Отмена Справка

Рисунок 132. Указание расширений издаваемого сертификата администратора

- 9 Если требуется, на странице **Сведения о точках распространения** создайте [точку распространения](#) для издаваемого сертификата или для списка аннулированных сертификатов (CRL), который будет сформирован после издания сертификата. Информация о созданных точках будет помещаться в сертификаты пользователей, заверенные данным сертификатом администратора. Кроме этого, заданные точки будут перенесены в настройки программы.

Задать или изменить их вы можете в настройках программы (см. [Настройка списка точек распространения](#)).

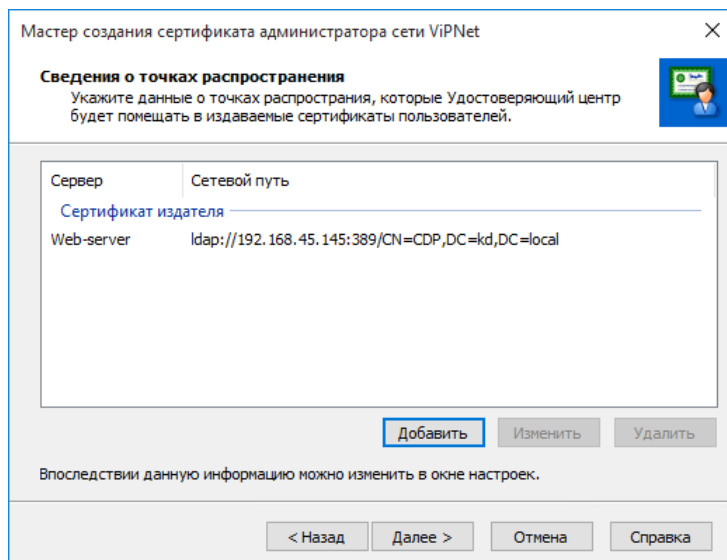


Рисунок 133. Указание точек распространения

На странице готовности к изданию сертификата убедитесь в правильности параметров, заданных на предыдущих страницах мастера, и нажмите кнопку **Далее**. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.

- 10 На последней странице мастера ознакомьтесь с результатом издания сертификата, после чего нажмите кнопку **Готово**. После издания сертификата будет автоматически произведены [экспорт межсетевой информации](#) и передача CRL на узлы вашей сети (см. [Передача CRL на узлы вручную](#)).

При успешном издании сертификата администратора и выполнении всех сопутствующих операций на последней странице мастера появится соответствующее сообщение, и напротив каждой операции будет отображаться значок . Если какие-то операции были выполнены с ошибками, то они будут отмечены значком .

Если в УКЦ установлены доверительные отношения с каким-либо другим удостоверяющим центром на основе распределенной модели, то после издания сертификата администратора УКЦ необходимо, чтобы в удостоверяющем центре, с которым установлены доверительные отношения, был издан новый сертификат, выданный вышестоящим УЦ (подробнее см. раздел [Создание запроса на кросс-сертификат](#)).

Выбор текущего сертификата администратора

Если у вас имеется несколько ключей электронной подписи и соответственно несколько сертификатов ключа проверки электронной подписи, то в каждый момент времени только один из имеющихся ключей и сертификатов может являться текущим и использоваться для подписи издаваемых сертификатов пользователей. В программе ViPNet Удостоверяющий и ключевой центр можно просмотреть список всех сертификатов (см. ниже) и изменить текущий сертификат. При

назначении сертификата текущим ключ электронной подписи, которому он соответствует, также назначается текущим.

Выбирать текущий сертификат может только администратор, учетная запись которого является текущей (см. [Смена текущей учетной записи администратора](#)).

Для смены текущего сертификата:

- 1 В окне программы выберите представление **Администрирование** и перейдите в раздел **Изданные сертификаты** > **Корневые сертификаты** или **Кросс-сертификация** > **Сертификаты от вышестоящего УЦ**.
- 2 Щелкните нужный сертификат правой кнопкой мыши и в контекстном меню выберите пункт **Назначить текущим**.

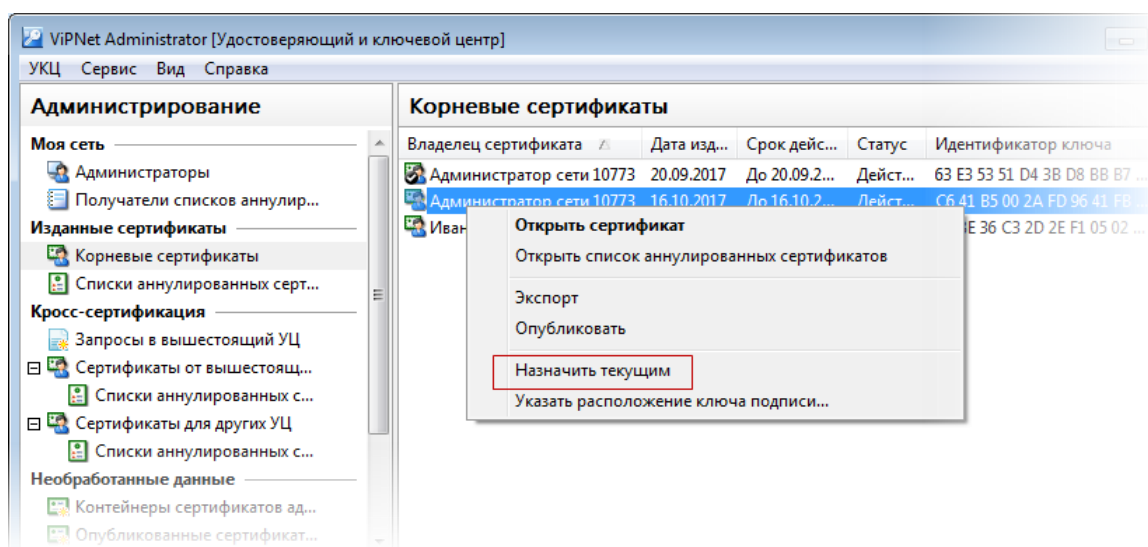


Рисунок 134. Выбор текущего сертификата администратора

Сертификат, назначенный текущим, будет использоваться для подписания сертификатов пользователей, издаваемых данным администратором. В разделе главного окна, в котором отображается данный сертификат, у него будет статус **Действителен (текущий)**.

Плановая смена ключа электронной подписи и сертификата администратора

Из соображений безопасности в процессе работы удостоверяющего центра проводится плановая смена ключа электронной подписи администратора. Срок плановой смены ключа электронной подписи зависит от места его хранения. При хранении ключа электронной подписи в файле на компьютере либо на внешнем устройстве без аппаратной поддержки российских криптографических алгоритмов плановая смена ключа производится каждые 15 месяцев. Если ключ электронной подписи хранится на устройстве с аппаратной поддержкой российских криптографических алгоритмов (был непосредственно сформирован на нем), то срок плановой смены ключа составляет 3 года.

По истечении срока плановой смены электронной подписи ключ электронной подписи администратора не сможет быть использован для подписи издаваемых сертификатов пользователей. Подписание списка аннулированных сертификатов (CRL) данным ключом электронной подписи при этом остается возможным до истечения срока действия ключа электронной подписи в зависимости от места хранения, а именно в течение следующих периодов:

- 54 месяца или 72 месяца, если корневой сертификат был издан на срок больше срока плановой смены ключа электронной подписи;
- срока действия сертификата администратора, если корневой сертификат был издан на срок равный или менее срока плановой смены ключа электронной подписи. Срок действия ключа электронной подписи в данном случае будет равен сроку действия сертификата.

Таблица 10. Срок плановой смены ключа электронной подписи администратора

Место хранения ключа электронной подписи	Срок плановой смены ключа электронной подписи	Срок действия ключа электронной подписи для обновления CRL
Файл на компьютере либо внешнее устройство без аппаратной поддержки российских криптографических алгоритмов	15 месяцев	54 месяца
Устройство с аппаратной поддержкой российских криптографических алгоритмов	36 месяцев	72 месяца

Узнать, в какие устройства встроена аппаратная поддержка криптографических алгоритмов, вы можете в разделе Список поддерживаемых внешних устройств.



Внимание! Место хранения ключа электронной подписи и срок его плановой смены должны быть зафиксированы в регламенте работы удостоверяющего центра вашей организации.

По истечении срока плановой смены ключа электронной подписи появится оповещение о необходимости проведения смены ключа электронной подписи. Количество дней, за которое будет произведено оповещение, задается в настройках программы. Требуется незамедлительно провести плановую смену ключа электронной подписи. Если смена ключа электронной подписи не будет своевременно проведена, издание сертификатов пользователей в программе будет невозможно.

Во время плановой смены требуется создать новый ключ электронной подписи и получить новый сертификат администратора одним из следующих способов:

- издать новый сертификат, если ваш удостоверяющий центр, в роли которого выступает УКЦ, является **ГОЛОВНЫМ**;
- получить новый сертификат по соответствующему запросу в вышестоящем удостоверяющем центре, если ваш удостоверяющий центр является **ПОДЧИНЕННЫМ**.

Настройка оповещений о плановой смене ключа электронной подписи и сертификата администратора

Для настройки оповещений о плановой смене ключа электронной подписи и сертификата администратора:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Сертификаты > Срок действия**.
- 3 В разделе **Срок действия** в группе **Сертификаты и ключи администраторов** в поле **Сообщать о плановой смене ключа ЭП за** введите количество дней (не более 30), за которое следует производить оповещение об истечении срока плановой смены ключа электронной подписи и сертификата администратора.



Примечание. Оповещение об истечении срока плановой смены ключа электронной подписи должно производиться за 15 дней.

- 4 Для сохранения указанных настроек нажмите кнопку **ОК**.

Просмотр контейнера ключей подписи администратора

В процессе первичной инициализации, а также при каждом издании сертификата администратора или создании запроса на сертификат к вышестоящему удостоверяющему центру создается ключ электронной подписи, который помещается вместе с сертификатом в специальный **контейнер ключей**. В свою очередь, контейнер ключей сохраняется либо локально на компьютере (в заданной папке на диске), либо на внешнем устройстве хранения данных и является составной частью **ключей администратора**.

В программе ViPNet Удостоверяющий и ключевой центр вы можете просмотреть подробную информацию о контейнере ключей администратора: имя, место хранения (путь к файлу контейнера ключей на компьютере или название внешнего устройства) и содержимое (сведения о ключе электронной подписи и сертификате ключа проверки электронной подписи). При наличии нескольких контейнеров ключей можно просмотреть информацию только о контейнере, в котором находится ключ электронной подписи, соответствующий его текущему сертификату (см. [Выбор текущего сертификата администратора](#)).

Для просмотра контейнера ключей текущего администратора:

- 1 В окне программы перейдите в представление **Администрирование** и выберите раздел **Моя сеть > Администраторы** и дважды щелкните свою учетную запись.
- 2 В окне **Свойства администратора** перейдите на вкладку **Текущий сертификат** и в группе **Контейнер ключа электронной подписи** нажмите кнопку **Подробнее**.

- 3 В появившемся окне **Свойства контейнера ключей** ознакомьтесь с содержимым контейнера ключей.

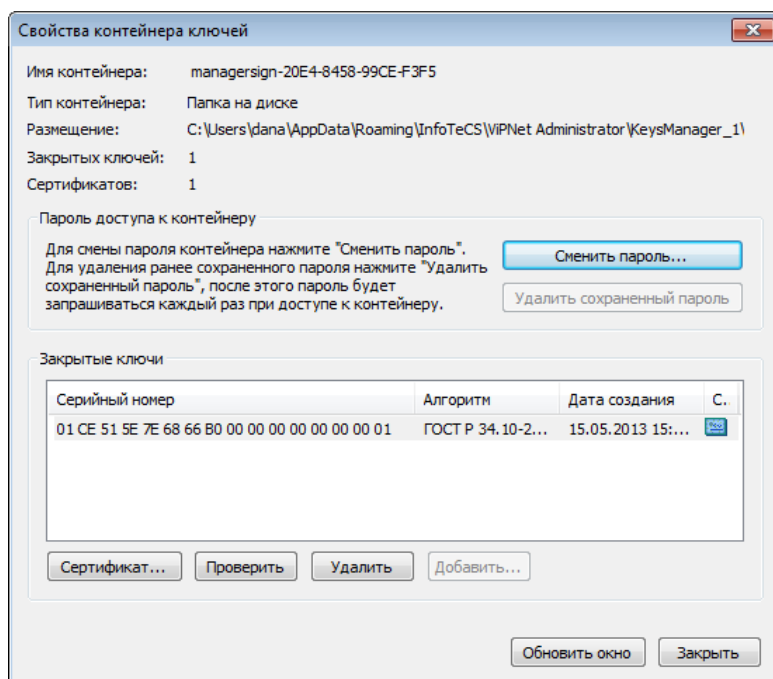


Рисунок 135. Информация о контейнере ключей администратора



Внимание! Кроме просмотра содержимого, не производите никаких действий в данном окне.

Смена пароля администратора

В целях обеспечения безопасности рекомендуется менять пароль администратора программы ViPNet Удостоверяющий и ключевой центр каждые 6 месяцев. По истечении 6 месяцев после создания пароля администратора появится оповещение о необходимости смены пароля. Сменить пароль может только администратор, учетная запись которого является текущей (см. [Смена текущей учетной записи администратора](#)).

Чтобы сменить пароль администратора:

- 1 В окне программы выберите представление **Администрирование** и перейдите в раздел **Моя сеть > Администраторы**.
- 2 Выполните одно из действий:
 - В контекстном меню вашей учетной записи выберите пункт **Сменить пароль администратора**.
 - В контекстном меню вашей учетной записи выберите пункт **Открыть** и в окне просмотра свойств администратора на вкладке **Общие** нажмите кнопку **Сменить пароль**.
- 3 В окне **Смена пароля и ключа защиты администратора** укажите свой текущий пароль.
- 4 В группе **Новый пароль** задайте тип нового пароля:
 - **Собственный** — пароль, задаваемый вами вручную. Пароль данного типа должен включать в себя не менее 8 символов.
 - **На основе парольной фразы** — [пароль, формируемый автоматически на основе парольных фраз](#) согласно параметрам, заданным в настройках программы (см. [Настройка параметров случайных паролей](#)).

После этого в зависимости от выбранного типа пароля, выполните соответствующие действия:

- Если вы выбрали тип пароля **Собственный**, задайте и подтвердите пароль.
- Если вы выбрали тип пароля **На основе парольной фразы**, появится электронная рулетка, если она еще не запускалась в рамках текущего сеанса работы программы. Поводите указателем в пределах окна **Электронная рулетка**.

Если вы выбрали тип пароля **На основе парольной фразы**, то появится автоматически сформированный пароль с парольной фразой, помогающей запомнить пароль.

При необходимости измените параметры или длину случайного пароля на основе парольной фразы с помощью кнопки **Свойства**, после чего создайте другой пароль, нажав кнопку **Другой**.



Совет. Рекомендуется задавать сложные пароли, в состав которых входят буквы в разных регистрах, цифры и специальные символы.

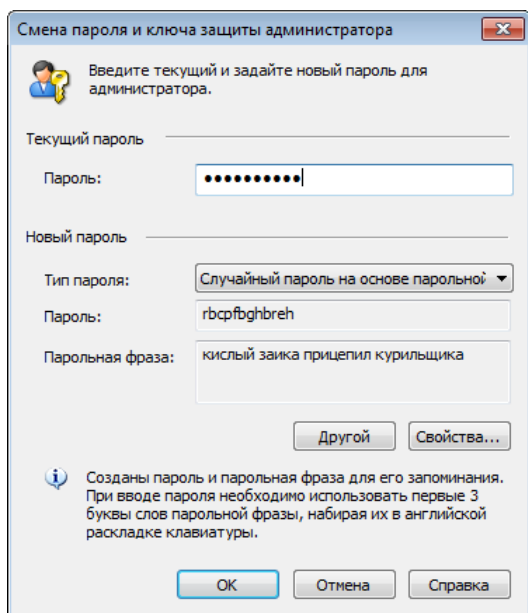


Рисунок 136. Смена пароля администратора

- 5 Для завершения смены пароля нажмите кнопку **ОК**.

В результате ваш пароль будет изменен.



Внимание! Запомните новый пароль (парольную фразу). При утере данный пароль невозможно будет восстановить.

При следующей аутентификации используйте новый пароль.

Смена ключа защиты УКЦ

Вся информация, хранящаяся в программе ViPNet Удостоверяющий и ключевой центр, зашифрована на [ключе защиты УКЦ](#). Данный ключ входит в состав ключей каждого администратора УКЦ, которые могут находиться в локальной папке или на внешнем устройстве. Ключ защиты УКЦ зашифрован на ключе защиты администратора.

Рекомендуется проводить плановую смену ключа защиты УКЦ не реже одного раза в 15 месяцев. По истечении 15 месяцев после создания ключа защиты УКЦ появится оповещение о необходимости его смены. Также рекомендуется менять ключ защиты УКЦ после удаления учетной записи администратора УКЦ (см. [Удаление учетной записи администратора](#)).

Перед сменой ключа защиты УКЦ автоматически создается резервная копия текущей конфигурации программы (см. [Работа с резервными копиями конфигураций сети](#)). С ее помощью можно будет восстановить работу УКЦ в случае, если смена ключа защиты будет проведена некорректно.



Внимание! Если база данных SQL и программа ViPNet Удостоверяющий и ключевой центр установлены на разных компьютерах, то резервная копия может быть создана только при соответствующей настройке программы (см. [Настройка параметров создания резервных копий](#)). В противном случае она не сможет быть создана. При этом если резервная копия не будет создана, смена ключа защиты УКЦ не будет выполнена.

Для смены ключа защиты УКЦ:

- 1 Выполните одно из действий:
 - В окне программы в меню **УКЦ** выберите пункт **Сменить ключ защиты УКЦ**.
 - В окне программы выберите представление **Администрирование** и перейдите в раздел **Моя сеть > Администраторы**. Затем в контекстном меню вашей учетной записи выберите пункт **Открыть** и в окне просмотра свойств администратора на вкладке **Общие** нажмите кнопку **Сменить ключ защиты УКЦ**.
- 2 В окне с сообщением о том, что будет создан новый ключ защиты УКЦ, нажмите кнопку **Продолжить**.

В результате будет запущен процесс смены ключа защиты. Дождитесь его завершения. Смена ключа защиты может занимать продолжительное время, поскольку в процессе смены производится перешифрование всей хранимой в УКЦ информации. Поэтому чем больше размер базы данных программы, тем больше времени займет смена ключа защиты УКЦ.

При успешной смене ключа защиты появится соответствующее сообщение.



Внимание! Если процесс смены ключа защиты не был завершен успешно, не выходите из программы и сразу выполните восстановление конфигурации из резервной копии, которая была автоматически сделана до смены ключа защиты (см. [Восстановление конфигурации](#)). В случае выхода из программы возобновить работу с ней будет невозможно.

Если с УКЦ работают несколько администраторов, сразу после смены ключа защиты УКЦ поочередно назначьте учетную запись каждого из них текущей (см. [Смена текущей учетной записи администратора](#)). При вводе пароля администратора в момент назначения учетной записи текущей новый ключ защиты УКЦ будет включен в состав ключей данного администратора и зашифрован на его ключе защиты, после чего станет для администратора доступным. Администраторы, для которых данное перешифрование не будет произведено, не смогут войти в программу.

13

Административные функции

Работа с резервными копиями конфигураций сети	266
Работа с журналом событий	274
Проверка текущих данных	278
Учет ключей ДСДР	282

Работа с резервными копиями конфигураций сети

В программе ViPNet Удостоверяющий и ключевой центр существует возможность создания резервных копий конфигурации сети, позволяющая при необходимости осуществлять возврат к более ранним конфигурациям.

В состав резервной копии конфигурации сети (файл *.zip или *.rp) входят следующие данные:

- Резервная копия базы данных ViPNet Administrator, в которой содержится информация о структуре сети ViPNet, сведения о лицензии, сертификатах и списках аннулированных сертификатов, изданных в УКЦ, и другие данные.
- Копия папки, в которой хранится служебная информация УКЦ:
C:\ProgramData\Infotecs\ViPNet Administrator\KC.



Примечание. По требованиям безопасности в резервную копию конфигурации сети не включаются копии контейнеров ключей администраторов УКЦ. Резервные копии контейнеров ключей требуется создавать отдельно.

Также в резервную копию не включаются справочники и ключи узлов, при необходимости они могут быть созданы после восстановления конфигурации сети.

Резервные копии создаются на компьютере, на котором установлена база данных, но хранятся на компьютере с УКЦ. Если база данных и программа ViPNet Удостоверяющий и ключевой центр установлены на разных компьютерах, то созданная резервная копия автоматически перемещается на компьютер с УКЦ в папку по умолчанию C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore. При необходимости вы можете изменить путь к этой папке (см. [Изменение места хранения резервных копий, используемого по умолчанию](#)). Чтобы обеспечить перенос резервных копий с одного компьютера на другой, необходимо в УКЦ настроить доступ к папке, в которую помещаются резервные копии на компьютере с базой данных (см. [Настройка параметров создания резервных копий](#)). В случае, если база данных установлена на одном компьютере с УКЦ, такая настройка не требуется.

Резервные копии могут создаваться двумя способами:

- Автоматически с определенной периодичностью согласно настройкам (см. [Настройка параметров создания резервных копий](#)). В этом случае при работе УКЦ в автоматическом режиме создание резервной копии конфигурации сети попадает в очередь автоматически выполняемых операций. Если администратор производит в программе какие-либо действия, за 30 секунд до создания резервной копии появится окно с сообщением, с помощью которого администратор при необходимости может отменить создание резервной копии, нажав кнопку **Отмена**.

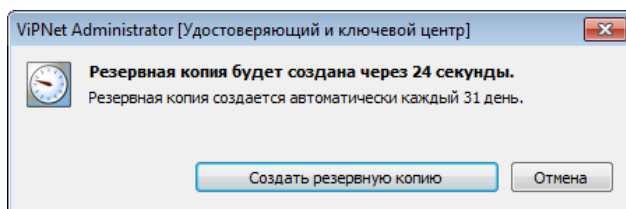


Рисунок 137. Сообщение о создании резервной копии конфигурации сети по расписанию

При смене ключа защиты УКЦ (см. [Смена ключа защиты УКЦ](#)) резервная копия всегда создается автоматически независимо от настроек программы.

- Вручную с использованием мастера восстановления конфигурации (см. [Создание резервной копии текущей конфигурации](#)). Таким способом рекомендуется создавать резервную копию каждый раз перед обновлением программного обеспечения ViPNet Administrator. Данную резервную копию можно будет использовать для восстановления конфигурации сети в случае нарушения ее работоспособности после обновления.

Внимание! Следует иметь в виду, что:



- Если резервная копия была создана в более поздней версии УКЦ по сравнению с установленной, эту резервную копию невозможно использовать для восстановления конфигурации сети.
- При удалении одной из учетных записей администратора рекомендуется сменить ключ защиты УКЦ и удалить те резервные копии, которые были созданы данным администратором.

Создание резервной копии текущей конфигурации

Резервная копия конфигурации создается для того, чтобы в случае необходимости можно было восстановить определенную конфигурацию сети.



Примечание. Если для создания резервной копии конфигурации недостаточно свободного пространства на диске, программа выдаст сообщение об этом. Для создания резервной копии необходимо освободить больше пространства на диске.

Чтобы создать резервную копию текущей конфигурации:

- 1 В окне программы ViPNet Administrator в меню **Сервис** выберите пункт **Резервное копирование и восстановление**. Будет запущен мастер **Резервное копирование и восстановление конфигурации ViPNet Administrator**.
- 2 На странице **Резервное копирование и восстановление конфигурации ViPNet Administrator** выберите **Создать резервную копию текущей конфигурации**, затем нажмите кнопку **Далее**.

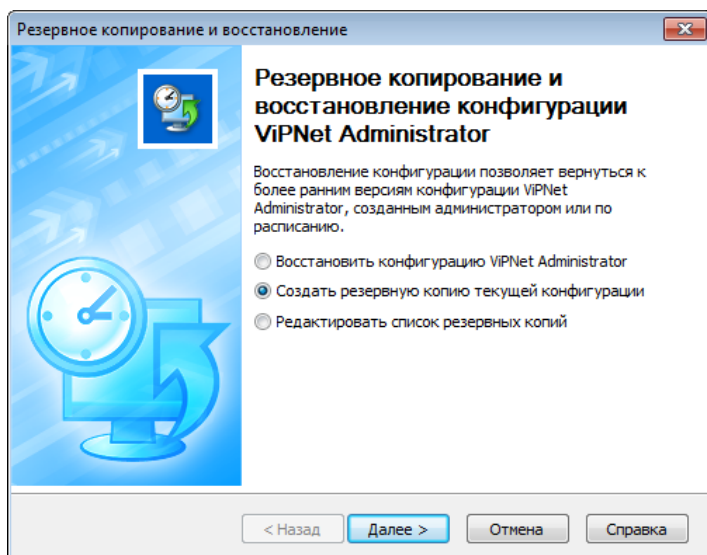


Рисунок 138. Запуск мастера создания и восстановления конфигурации

- 3 На странице **Создание резервной копии** в поле **Комментарий к резервной копии** введите комментарий с описанием конфигурации. Добавление комментария необязательно, но он поможет быстрее найти нужную резервную копию в списке. Комментарий должен содержать не более 200 символов.
- 4 Нажмите кнопку **Далее**. Будет создана резервная копия конфигурации.
Созданная резервная копия конфигурации будет сохранена на компьютере, на котором установлена программа ViPNet Удостоверяющий и ключевой центр, в папке по умолчанию `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore`.
- 5 Чтобы закончить работу мастера, на странице **Завершение создания резервной копии конфигурации** нажмите кнопку **Готово**.
Чтобы выполнить новую операцию с резервными копиями, нажмите кнопку **В начало**.

Редактирование списка резервных копий

Список резервных копий конфигурации можно редактировать: удалять резервные копии или изменять комментарии.

Для редактирования списка резервных копий конфигурации:

- 1 В окне программы ViPNet Administrator в меню **Сервис** выберите пункт **Резервное копирование и восстановление**. Будет запущен мастер **Резервное копирование и восстановление конфигурации ViPNet Administrator**.
- 2 Выберите **Редактировать список резервных копий** и нажмите кнопку **Далее**.
- 3 На странице **Редактирование списка резервных копий** выберите резервную копию, которую необходимо изменить. Чтобы изменить комментарий, нажмите кнопку **Изменить комментарий**. Для удаления резервной копии нажмите кнопку **Удалить**.

Резервные копии конфигурации автоматически сортируются по дате и времени создания. Чтобы изменить порядок сортировки, щелкните заголовок столбца **Дата и время создания** или **Комментарий**.

- 4 Чтобы завершить редактирование, нажмите кнопку **Далее**.
- 5 Чтобы закончить работу мастера, на странице **Завершение создания резервной копии конфигурации** нажмите кнопку **Готово**.

Чтобы выполнить новую операцию с резервными копиями, нажмите кнопку **В начало**.

Восстановление конфигурации

С помощью восстановления конфигурации вы можете вернуться к определенному состоянию сети ViPNet или восстановить работоспособность сети после сбоя. При восстановлении конфигурации сети выполняется также восстановление конфигурации программ ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр.

В результате восстановления конфигурации структура сети ViPNet, параметры сетевых объектов, данные о ключах и сертификатах, настройки программ ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр будут возвращены к состоянию, которое было актуально в момент создания резервной копии.

В резервную копию конфигурации не входят ключи электронной подписи администратора. Поэтому вы можете восстановить конфигурацию ViPNet Administrator из ранее созданной резервной копии только в период работы одних и тех же мастер-ключей (с одинаковой серией). Если была смена мастер-ключей, восстановление конфигурации к состоянию до смены мастер-ключей приведет к неработоспособности сети. Чтобы восстановить конфигурацию к состоянию до смены мастер-ключей, требуется резервная копия ключей электронной подписи администратора, созданная до смены мастер-ключей. См. «ViPNet Administrator 4. Руководство по смене мастер-ключей в сети ViPNet», раздел «Создание резервной копии ключей подписи администратора».

Чтобы восстановить конфигурацию из ранее созданной резервной копии:

- 1 В окне программы ViPNet Administrator в меню **Сервис** выберите пункт **Резервное копирование и восстановление**. Будет запущен мастер **Резервное копирование и восстановление конфигурации ViPNet Administrator**.
- 2 На странице **Резервное копирование и восстановление конфигурации ViPNet Administrator** выберите **Восстановить конфигурацию ViPNet Administrator**, затем нажмите кнопку **Далее**.
- 3 На странице **Выбор резервной копии** представлен список резервных копий конфигураций.

Резервные копии, созданные автоматически, могут иметь следующие комментарии:

- Создана при восстановлении конфигурации.
- Создана автоматически по расписанию.

Выберите резервную копию конфигурации, которую требуется восстановить, и нажмите кнопку **Далее**. Начнется процесс восстановления выбранной конфигурации сети.

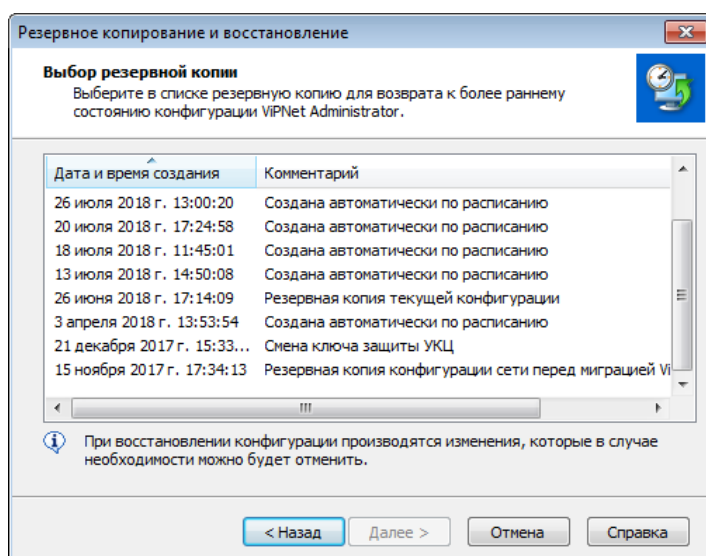


Рисунок 139. Восстановление конфигурации из резервной копии

- 4 Если база данных и УКЦ установлены на разных компьютерах, потребуется авторизация администратора SQL-сервера (подробнее см. в документе «ViPNet Administrator. Руководство по установке», в главе «Установка программного обеспечения ViPNet Administrator», в разделе «Информация для администратора SQL»). В появившемся окне укажите имя учетной записи и пароль администратора SQL-сервера. Иначе будет отказано в доступе к данным SQL-сервера и, следовательно, в доступе к базе данных ViPNet Administrator, и конфигурация не сможет быть восстановлена.

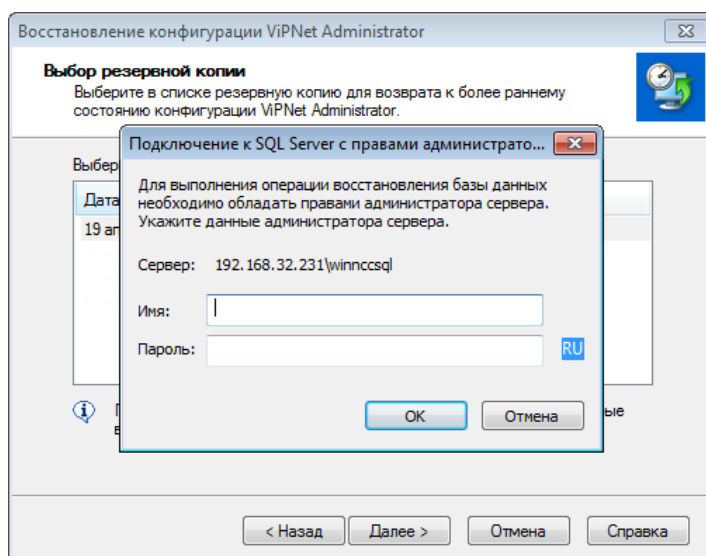


Рисунок 140. Ввод данных администратора SQL-сервера для получения доступа к базе данных ViPNet Administrator

- 5 Если база данных и УКЦ установлены на разных компьютерах и отсутствует доступ к данным SQL-сервера:
 - 5.1 Для экземпляра SQL-сервера создайте учетную запись администратора с проверкой подлинности SQL Server и правами суперадминистратора sysadmin. Для работы с SQL-сервером вы можете использовать Microsoft SQL Server Management Studio.

5.2 Повторите подключение к базе данных с учетными данными созданного администратора SQL-сервера.

- 6 Если была смена мастер-ключей и вы хотите восстановить конфигурацию к состоянию до смены мастер-ключей, то используйте копию ключей электронной подписи администратора, созданную до смены мастер-ключей.

См. «ViPNet Administrator 4. Руководство по смене мастер-ключей в сети ViPNet», раздел «Восстановление конфигурации после смены мастер-ключей».

- 7 Чтобы закончить работу мастера, на странице **Завершение восстановления конфигурации ViPNet Administrator** нажмите кнопку **Заккрыть**.
- 8 После восстановления конфигурации войдите в программу и убедитесь, что восстановленная конфигурация работоспособна. В случае необходимости вы можете отменить восстановление конфигурации.
- 9 После успешного восстановления конфигурации сети из резервной копии отправьте на сетевые узлы [ключи узлов](#) и [пользователей](#).

В том случае если в процессе работы с программой изменялось местоположение или имя папок обмена с программой ViPNet Publication Service, после восстановления конфигурации следует проверить, правильно ли заданы параметры взаимодействия с программой ViPNet Publication Service (см. [Настройка параметров публикации данных](#)).

Настройка параметров создания резервных копий

Вы можете настроить автоматическое создание резервных копий конфигурации с определенной периодичностью в заданное время. При переходе УКЦ в автоматический режим создание резервных копий конфигурации будет включено в список выполняемых операций в этом режиме. При выходе из программы УКЦ автоматическое создание резервных копий конфигурации не будет выполняться.

Кроме того, если база данных и программа ViPNet Удостоверяющий и ключевой центр установлены на разных компьютерах, для возможности получения резервных копий конфигурации вам необходимо настроить доступ к папке на компьютере с базой данных, в которой будет размещаться резервная копия базы данных. Эта папка используется программой УКЦ для переноса резервных копий с компьютера с базой данных на компьютер с УКЦ при создании и восстановлении резервных копий конфигурации.

Чтобы настроить указанные параметры создания резервных копий конфигурации:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Резервное копирование**.

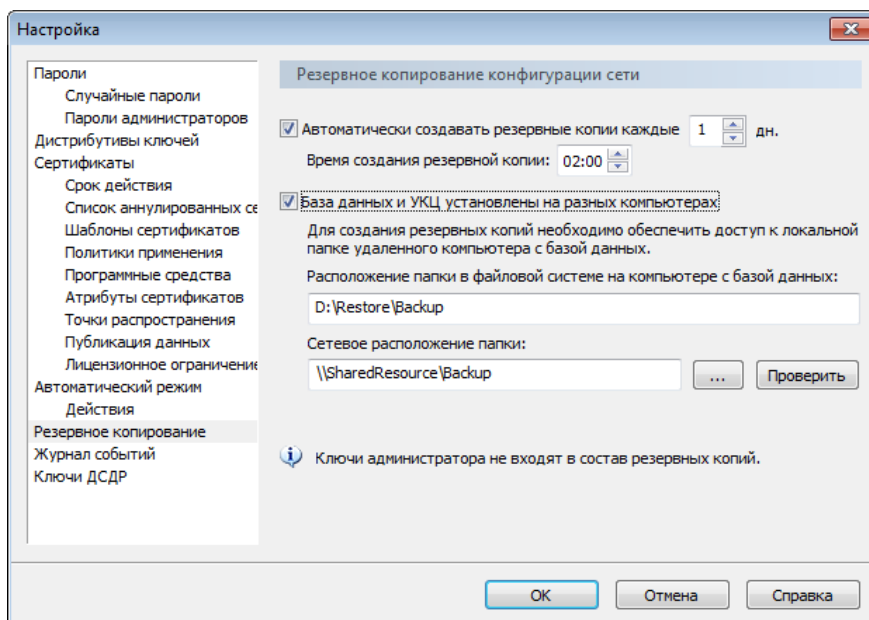


Рисунок 141. Настройка параметров восстановления конфигурации

- 3 Чтобы создание резервных копий выполнялось с определенной периодичностью в заданное время, укажите соответствующие значения в полях **Автоматически создавать резервные копии каждые** и **Время создания резервной копии**. По умолчанию резервные копии создаются ежедневно в 2 часа ночи.

Чтобы отключить автоматическое создание резервных копий, снимите соответствующий флажок.
- 4 Если база данных расположена на отдельном компьютере, установите флажок **База данных и УКЦ установлены на разных компьютерах** и укажите:
 - 4.1 В поле **Расположение папки в файловой системе на компьютере с базой данных** укажите полный путь к общей папке на компьютере с базой данных ПО ViPNet Administrator. Например, D:\Restore\Backup.
 - 4.2 В поле **Сетевое расположение папки** обеспечьте сетевой доступ к общей папке на компьютере с базой данных ПО ViPNet Administrator одним из двух способов:
 - укажите сетевой путь в следующем формате: \\<Имя сервера>\<Имя общей папки>, где
 <Имя сервера> — имя в WINS или DNS-имя (предпочтительнее), или IP-адрес компьютера с базой данных ПО ViPNet Administrator;
 <Имя общей папки> — название общей папки на компьютере с базой данных ПО ViPNet Administrator.

 Например, \\SharedResource\Backup. Имя общей папки (например, Backup) может отличаться от полного пути на компьютере (например, D:\Restore\Backup).
 - укажите букву сетевого диска, по которому подключена к компьютеру с УКЦ общая папка компьютера с базой данных ПО ViPNet Administrator, например, z:\. Вы можете указать сетевой диск с помощью кнопки .

Чтобы убедиться, что папка задана верно, нажмите кнопку **Проверить**.



Примечание. Общая папка задана верно, только если она существует и у вас есть права на чтение и запись данных в эту папку.

5 Для сохранения настроек нажмите кнопку **ОК**.

Если база данных и УКЦ расположены на одном компьютере, флажок **База данных и УКЦ установлены на разных компьютерах** должен быть снят, в этом случае резервные копии конфигурации сети сохраняются в папку по умолчанию `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore`. При необходимости вы можете изменить папку сохранения резервных копий на компьютере (см. [Изменение места хранения резервных копий, используемого по умолчанию](#)).

Изменение места хранения резервных копий, используемого по умолчанию

Резервные копии конфигурации сети могут занимать большой объем на диске `C:`, особенно если копии создаются автоматически с большой периодичностью. В этом случае вы можете изменить место хранения резервных копий конфигурации сети по умолчанию

`C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore`.

Чтобы изменить место хранения файлов резервных копий конфигурации сети, используемого по умолчанию:

- 1 Откройте для редактирования файл конфигурации УКЦ `KC.ini`, который находится в папке `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\ini`.
- 2 В секции `[Archive]` добавьте следующую строку:
`Configuration backup folder=<Локальный путь к папке сохранения резервных копий>.`
- 3 Чтобы все текущие резервные копии конфигурации сети были доступны для восстановления по новому пути, перенесите все содержимое папки автоматического сохранения резервных копий конфигурации сети `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore` в папку сохранения резервных копий по новому пути.
- 4 Чтобы применить изменения, перезапустите программу ViPNet Удостоверяющий и ключевой центр.

Работа с журналом событий

Информация о событиях, возникающих при работе программы ViPNet Удостоверяющий и ключевой центр, фиксируется в журнале событий, который находится в системном журнале Windows. Настройка журнала событий описана в разделе [Настройка параметров журнала событий](#).

Просмотр событий в журнале событий

Для мониторинга работы ViPNet Удостоверяющий и ключевой центр:

- 1 На **Панели управления** в категории **Администрирование** дважды щелкните значок **Просмотр событий**.
- 2 В окне **Просмотр событий** на панели навигации выберите **Журналы приложений и служб > ViPNet Administrator KCA**.

В результате на панели просмотра отобразится список зарегистрированных событий.

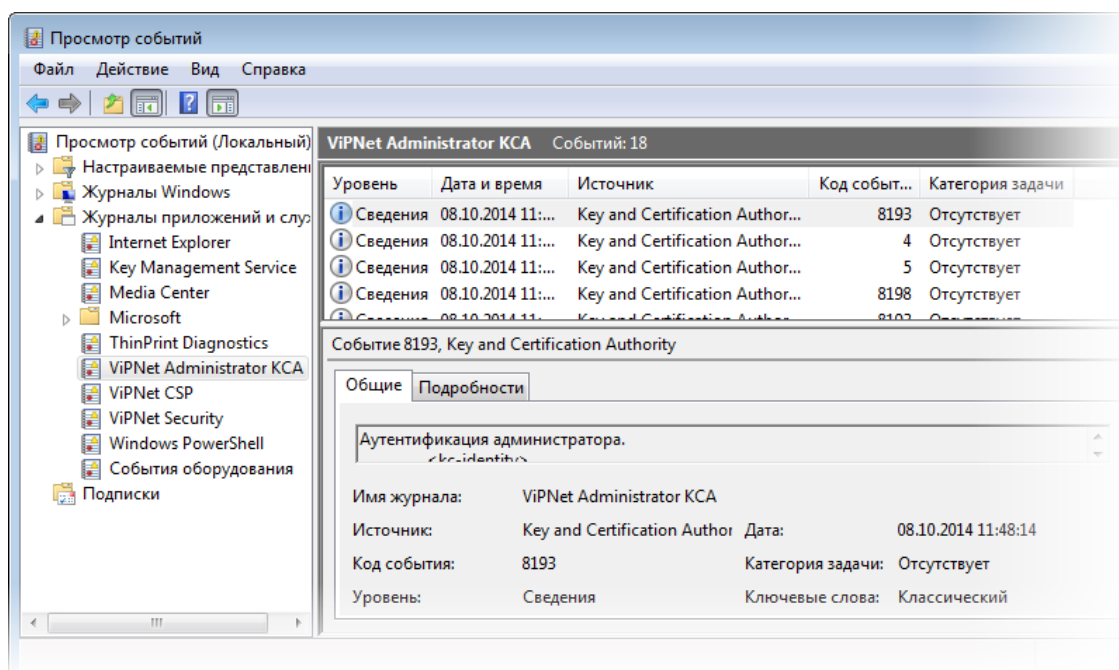


Рисунок 142. Просмотр событий в системном журнале событий УКЦ

Настройка параметров журнала событий

По умолчанию в журнале событий фиксируется наиболее важная информация о работе программы ViPNet Удостоверяющий и ключевой центр (издание сертификата подписи, издание списка аннулированных сертификатов, удовлетворение либо отклонение запроса на сертификат или его аннулирование и другое). В программе ViPNet Удостоверяющий и ключевой центр вы

можете изменить степень детализации записей журнала либо отключить ведение журнала, если нет необходимости в мониторинге работы программы. Параметры хранения файла журнала событий настраиваются с помощью компонента Microsoft Windows Панель управления.

Для настройки параметров хранения файла журнала событий:

- 1 Нажмите кнопку **Пуск** и выберите пункт **Панель управления**.
- 2 На панели управления в категории **Администрирование** дважды щелкните значок **Просмотр событий**.
- 3 В окне **Просмотр событий** на панели навигации выберите **Журналы приложений и служб > ViPNet Administrator KCA**, щелкните **ViPNet Administrator KCA** правой кнопкой мыши и в меню выберите пункт **Свойства**.
- 4 В окне свойств журнала при необходимости измените:
 - Путь к папке для хранения и имя файла журнала.
 - Максимальный размер файла журнала (по умолчанию — 300 Мбайт).
 - Действие при достижении максимального размера файла журнала:
 - **Переписывать события при необходимости (сначала старые события)** — новые записи заносятся в журнал, при этом каждая новая запись заменяет в журнале наиболее старую.
 - **Архивировать журнал при заполнении; не перезаписывать события** (выбран по умолчанию) — файл журнала автоматически архивируется и сохраняется в папку, выбранную для хранения журнала.
 - **Не перезаписывать события (очистить журнал вручную)** — журнал очищается вручную.

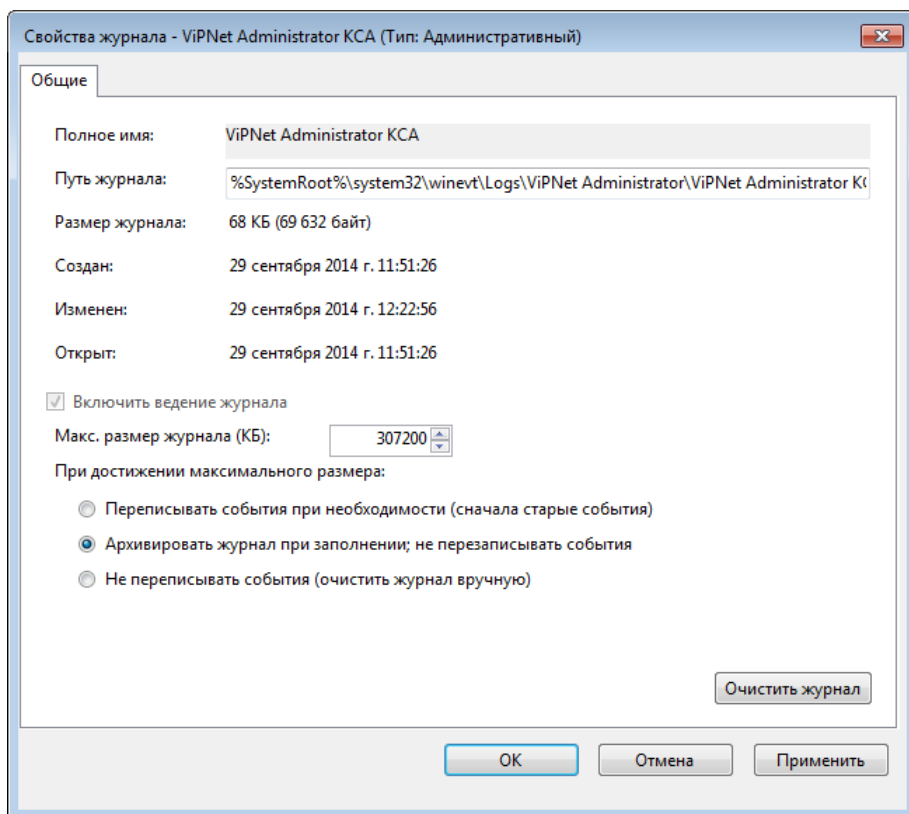


Рисунок 143. Настройка параметров сохранения журнала событий

Чтобы изменить степень детализации записей журнала событий или отключить ведение журнала в программе ViPNet Удостоверяющий и ключевой центр:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Журнал событий**.

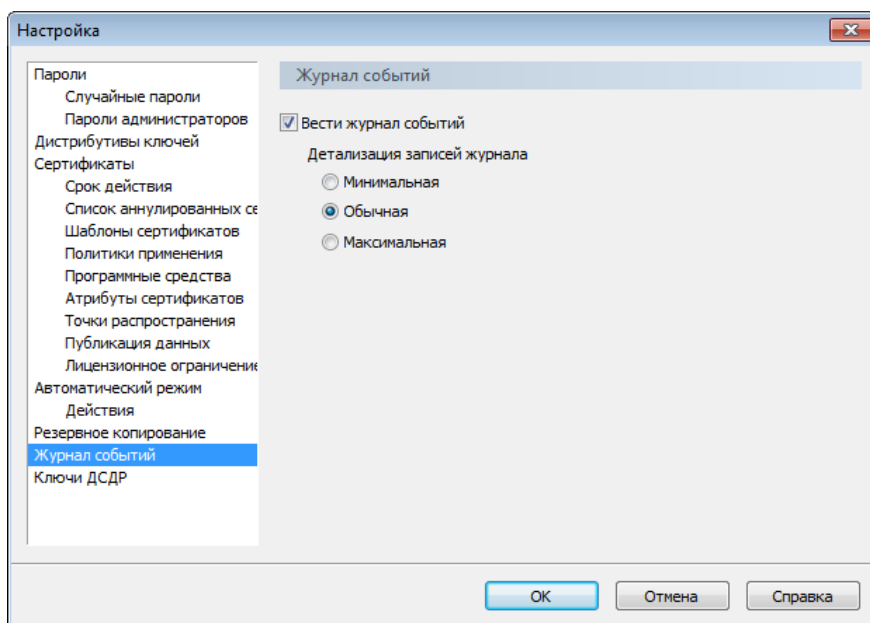


Рисунок 144. Настройка параметров журнала событий

- 3 Если требуется отключить ведение журнала событий, снимите флажок **Вести журнал событий**. Если данный флажок снят, настройка детализации записей журнала недоступна.



Примечание. Если в программе ViPNet Удостоверяющий и ключевой центр отключено ведение журнала, то в журнал событий **ViPNet Administrator KCA** записываются только события запуска и завершения работы программы.

- 4 В группе **Детализация записей журнала** выберите один из пунктов:

- **Минимальная** — фиксируются основные события, такие как: аутентификация администратора УКЦ, регистрация нового администратора, издание сертификата администратора, создание мастер-ключа своей сети, завершение работы УКЦ.

Обычная (выбран по умолчанию) — фиксируется наиболее важная информация, например: издание сертификата подписи, издание списка аннулированных сертификатов, удовлетворение либо отклонение запроса на сертификат или его аннулирование.

- **Максимальная** — фиксируется вся информация.

Полный список событий УКЦ представлен в приложении [Перечень событий УКЦ, регистрируемых в журнале событий Windows](#).

- 5 Чтобы сохранить настройки, нажмите кнопку **ОК**.

Проверка текущих данных

При запуске и в процессе работы программы ViPNet Удостоверяющий и ключевой центр автоматически производится проверка текущих данных на наличие следующих ошибок:

- **Критические** — ошибки, при которых программа не может продолжать свою работу и закрывается.
- **Аномальные** — ошибки, при которых некоторые функции программы либо недоступны, либо неуспешны. Например, могут быть недоступны операции с сертификатами (издание, аннулирование, импорт и прочее) вследствие истечения срока действия списка аннулированных сертификатов администратора или невозможны операции по созданию ключей для узлов, пароли администраторов которых искажены или недействительны.



Примечание. Проверку данных на наличие аномальных ошибок также можно выполнить вручную (см. [Проверка текущих данных вручную](#)).

- **Рабочие** — ошибки, возникающие в рабочем порядке и не влияющие на функциональность программы.

Если в ходе проверки данных будет установлен факт возникновения какой-либо ошибки, будет выдано соответствующее сообщение с его описанием.

Перечень возможных критических, аномальных и рабочих ошибок, а также описание действий администратора при возникновении данных ошибок приведены ниже в таблице.

Таблица 11. Описание ошибок, которые могут возникнуть при проверке текущих данных

Описание ошибки и форма оповещения	Рекомендуемые действия администратора программы
Критические	
Нарушение целостности или повреждение исполняемых модулей программы. Контроль целостности осуществляется путем вычисления имитозащитной вставки. При обнаружении повреждений появляется сообщение о найденном несоответствии, и программа завершает свою работу.	Поставьте в известность должностное лицо, ответственное за безопасность эксплуатации сети ViPNet, и выявите причины появления данной ошибки. Особое внимание рекомендуется уделить исключению возможностей несанкционированного доступа к компьютеру и умышленного искажения файлов. Восстановление работоспособности программы в данном случае возможно только путем ее переустановки.

Описание ошибки и форма оповещения	Рекомендуемые действия администратора программы
Нарушение целостности ключей ViPNet (ключа защиты УКЦ, ключа электронной подписи текущего администратора). При обнаружении нарушения целостности появляется сообщение об ошибке инициализации администратора.	Выявите причины возникновения подобной ошибки. В зависимости от того, какой ключ был поврежден, устранение ошибки возможно будет либо путем восстановления конфигурации программы из резервной копии (см. Восстановление конфигурации), либо путем переиздания сертификата администратора (см. Плановая смена ключа электронной подписи и сертификата администратора).
Аномальные	
Истечение срока действия списка аннулированных сертификатов. За определенное количество дней до истечения срока действия (если установлена опция в настройках программы) либо при истечении срока действия появляется соответствующее сообщение с предложением сформировать новый список аннулированных сертификатов.	Обновите список аннулированных сертификатов (см. Обновление CRL вручную).
Истечение срока плановой смены ключа электронной подписи администратора. За определенное количество дней до истечения срока плановой смены ключа электронной подписи появляется сообщение о том, что необходимо обновить ключ электронной подписи и сертификат администратора. В противном случае издание сертификатов пользователей станет невозможным.	Выполните плановую смену ключа электронной подписи администратора (см. Плановая смена ключа электронной подписи и сертификата администратора).
Искажение паролей администраторов сетевых узлов. При обнаружении искаженных паролей администраторов сетевых узлов появляется соответствующее сообщение. Создание ключей для узлов с такими паролями невозможно.	Смените (см. Создание и смена пароля администратора сетевого узла или группы узлов) или сбросьте такие пароли администраторов (см. Сброс пароля администратора сетевого узла).
Истечение срока действия паролей администраторов сетевых узлов или групп узлов. За определенное количество дней до истечения срока действия (если установлена опция в настройках программы) либо при истечении срока действия паролей появляется соответствующее сообщение. Создание ключей для узлов с такими паролями невозможно.	Смените (см. Создание и смена пароля администратора сетевого узла или группы узлов) или сбросьте такие пароли администраторов (см. Сброс пароля администратора сетевого узла).

Описание ошибки и форма оповещения	Рекомендуемые действия администратора программы
Найдены искаженные межсетевые мастер-ключи или ключи, срок действия которых истек. Сообщение появляется, если обнаружены действующие межсетевые мастер-ключи, которые используются более 1 года. Рекомендуется выполнить смену указанных межсетевых мастер-ключей.	Выполните смену межсетевых мастер-ключей, указанных в сообщении (см. Смена межсетевого мастер-ключа).
Рабочие	
Истечение срока действия сертификата пользователя своей сети. За определенное количество дней до истечения срока действия (если установлена опция в настройках программы) либо при истечении срока действия появляется сообщение о том, что истекает (истек) срок действия сертификата для следующего пользователя (списка пользователей).	Для пользователя, указанного в сообщении, сформируйте новые ключи (см. Создание и передача ключей пользователей в ЦУС).
Наличие искажений в межсетевой информации (сертификатах администраторов доверенных сетей ViPNet, информации о пользователях и сетевых узлах, межсетевых мастер-ключах и прочем). При обнаружении искажений в процессе обращения к поврежденной информации появляется соответствующее сообщение об ошибке. До устранения неполадок выполнение ряда операций в программе будет невозможно.	Получите у администратора этой доверенной сети ViPNet обновленную межсетевую информацию и импортируйте ее.
Закончились лицензии на издание сертификатов пользователей в соответствии с лицензионным файлом. Если число изданных сертификатов станет равным числу, указанному в настройках программы, либо максимальному числу, заявленному в лицензионном файле, появляется соответствующее сообщение. При достижении лимита издание сертификатов становится невозможным.	Обратитесь к представителю компании ИнфоТеКС с запросом на расширение текущей лицензии.
В программе появились необработанные контейнеры сертификатов, полученные от администраторов доверенных сетей ViPNet. Выдается сообщение с предложением обработать контейнеры сертификатов.	Выполните обработку контейнеров сертификатов. Поступившие контейнеры сертификатов находятся в представлении Администрирование в разделе Необработанные данные > Контейнеры сертификатов администраторов сетей ViPNet.

Описание ошибки и форма оповещения	Рекомендуемые действия администратора программы
Получены файлы с запросами на издание сертификатов от пользователей либо из центра регистрации или файлы с запросами на аннулирование сертификатов. Выдается сообщение с предложением обработать поступившие запросы.	Обработайте поступившие запросы. Запросы отображаются в представлении Удостоверяющий центр. Подробнее см. соответствующие разделы в главе Управление сертификатами.
Из доверенной сети ViPNet поступила обновленная межсетевая информация (файлы с информацией о появившихся сетевых узлах и их связях). Выдается сообщение о том, что требуется создать ключи узлов, связанных с новыми узлами доверенной сети.	Сформируйте и отправьте новые ключи узлов (см. Создание и передача ключей узлов в ЦУС).

Проверка текущих данных вручную

В программе ViPNet Удостоверяющий и ключевой центр вы можете вручную выполнить проверку текущих данных на наличие аномальных ошибок. Описание возможных аномальных ошибок приведено в разделе [Проверка текущих данных](#).

Чтобы вручную выполнить проверку данных, в окне программы в меню **Сервис** выберите пункт **Проверка текущих данных**. Если аномальные ошибки отсутствуют, появится соответствующее сообщение.

Учет ключей ДСДР

Если в сети ViPNet в качестве координаторов используются программно-аппаратные комплексы (ПАК) ViPNet Coordinator KB (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 KB (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.

Ключи ДСДР имеют срок действия, после истечения которого необходимо использовать новую серию ключей, следующую за текущей серией ключей ДСДР. Если наступила дата завершения срока действия следующей серии ключей ДСДР, зарегистрируйте новую серию ключей ДСДР. Вы можете зарегистрировать до двух серий ключей ДСДР одновременно. По истечении срока действия текущей серии ключей ДСДР автоматически будет использована следующая серия.

Внимание! Для корректной работы сети ViPNet при автоматической смене серии ключей ДСДР обновите все ViPNet Coordinator KB до версии 4.3.0 и выше.



ViPNet Coordinator KB версии 4.3.0 и выше поддерживает функцию автоматической смены серии ключей ДСДР по истечении срока действия. Если в сети ViPNet параллельно используются ViPNet Coordinator KB версии 4.3.0 и выше и ViPNet Coordinator KB более ранних версий, не поддерживающих данную функцию, то после автоматической смены серии ключей ДСДР связь между ними будет нарушена.

Номер серии ключей, указанный на обложке диска ДСДР, состоит из 8 цифр: первые 2 цифры обозначают год изготовления (не вводятся в УКЦ) и 6 цифр серии ключей. Чтобы в УКЦ ввести серию ключей ДСДР, используйте последние 6 цифр номера, указанного на обложке ДСДР, без указания года.



Внимание! После смены роли для узла с ПАК ViPNet Coordinator KB, например, при замене на более новое исполнение, в УКЦ назначьте заново номер комплекта ключей ДСДР.

Для регистрации ключей ДСДР:

- 1 В окне программы в меню **Сервис** выберите пункт **Настройка**.
- 2 В появившемся окне на панели навигации выберите раздел **Ключи ДСДР**.

Примечание. Раздел **Ключи ДСДР** в настройках программы отображается только в том случае, если лицензией разрешено использование следующих ролей:



- «Coordinator KB100»;
- «Coordinator KB1000»;
- «Coordinator KB2000»;
- «Coordinator KB5000»;
- «L2-10G»;
- «L2-100G»;
- «Failover KB100».

Подробнее см. документ «ViPNet Центр управления сетью. Руководство администратора», раздел «Роли сетевых узлов».

3 Установите флажок **Использовать ключи ДСДР**.

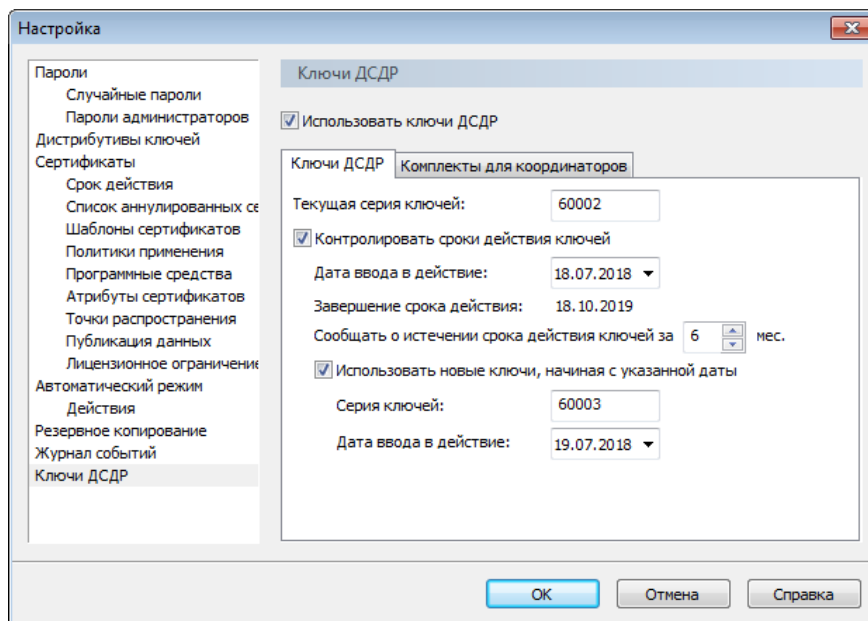


Рисунок 145. Настройка контроля срока действия ключей ДСДР

- 4 В поле **Текущая серия ключей** введите серию ключей ДСДР, которая будет использована первой.
- 5 Чтобы управлять использованием ключей ДСДР, установите флажок **Контролировать сроки действия ключей** и укажите дату ввода в действие ключей ДСДР.
- 6 Чтобы получать оповещение об окончании срока действия ключей ДСДР, в поле **Сообщать об истечении срока действия ключей за мес** установите необходимое значение. По умолчанию установлено значение 6 месяцев.
- 7 Чтобы по окончании срока действия текущей серии ключей ДСДР автоматически использовать следующую серию, установите флажок **Использовать новые ключи, начиная с указанной даты** и введите номер следующей серии ключей ДСДР и дату ввода в действие.

По окончании срока действия текущей серии ключей ДСДР в поле **Текущая серия ключей** появится номер следующей серии ключей ДСДР и будет обновлена информация о дате ввода в действие для текущей серии ключей ДСДР. В этом случае до окончания действия второй текущей серии ключей зарегистрируйте новую следующую серию ключей ДСДР.

8 На вкладке **Комплекты для координаторов** каждому координатору из списка назначьте номер комплекта ключей одним из следующих способов:

- При добавлении нового координатора в сеть ViPNet вручную присвойте номер комплекта ключей ДСДР. Для этого в списке выберите координатор и нажмите кнопку **Задать номер комплекта**. В появившемся окне установите флажок **Использовать комплект ключей** и укажите номер комплекта (в диапазоне от 1 до 9999), после чего нажмите кнопку **ОК**. В том случае если указанный номер комплекта ключей уже задан для другого координатора, появится соответствующее сообщение о необходимости задать другой номер комплекта.
- При первичном развертывании сети ViPNet присвойте номера комплектов ключей сразу всем координаторам автоматически. Для этого нажмите кнопку **Задать номера автоматически**. Присвоение номеров произойдет для всех координаторов в порядке, в котором они расположены в списке. Новый номер комплекта ключей будет назначен в том числе и для координаторов, у которых он уже был.



Внимание! Не задавайте номера комплектов ключей автоматически, если в сети уже развернуты другие координаторы с ПАК ViPNet Coordinator KB. Это изменит их номера комплектов ключей и нарушит связь с остальными узлами. Для восстановления работоспособности сети ViPNet потребуется установка дистрибутивов ключей для всех узлов заново.

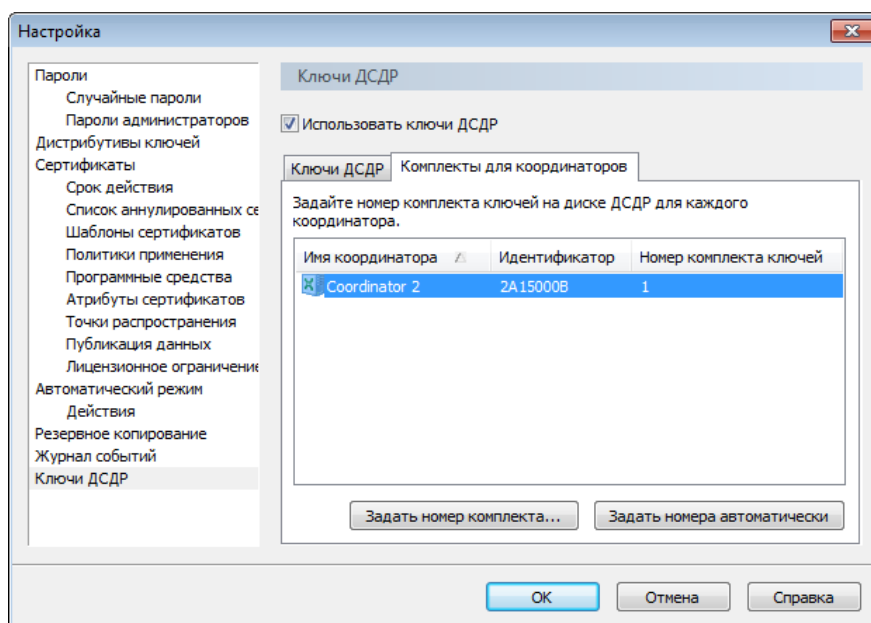


Рисунок 146. Назначение координатору комплекта ключей ДСДР



Примечание. В списке отображаются имена и идентификаторы всех зарегистрированных в программе ViPNet Центр управления сетью ПАКов ViPNet Coordinator KB. По умолчанию номера комплектов ключей для них не заданы.

- 9 Чтобы сохранить настройки, нажмите кнопку **ОК**.
- 10 После регистрации ключей ДСДР создайте для координаторов дистрибутивы ключей (см. [Создание дистрибутива ключей для ПАК ViPNet Coordinator KB](#)) либо создайте и отправьте на координаторы новые ключи узлов (см. [Создание и передача ключей узлов в ЦУС](#)).
- 11 Из ЦУСа отправьте обновления ключей с отложенной датой вступления в действие.



Примечание. Убедитесь, что обновления ключей будут доставлены на все координаторы с ПАК ViPNet Coordinator KB до наступления даты применения обновлений на узлах, указанной в настройках УКЦ.



Возможные неполадки

Не удастся войти в программу ViPNet Удостоверяющий и ключевой центр

Если вам не удастся войти в программу ViPNet Удостоверяющий и ключевой центр, проблема может иметь следующие причины:

- **Изменились параметры подключения к SQL-серверу**

При запуске УКЦ могут возникнуть следующие ошибки подключения к SQL-серверу:

- выбранный SQL-сервер недоступен;
- на SQL-сервере изменились учетные данные пользователя, имеющего доступ к базе данных;
- изменились настройки подключения или настройки проверки подлинности SQL-сервера;
- изменился IP-адрес или имя SQL-сервера и прочее.

В случае возникновения указанных ошибок появится окно подключения к SQL-серверу.

Укажите параметры подключения, как описано в разделе [Подключение к SQL-серверу при запуске программы](#).

- **Учетная запись Windows, которую вы используете, не имеет прав доступа к SQL-серверу**

Например, эта проблема может возникнуть в том случае, если компьютер с УКЦ ввели в домен Active Directory.

Для решения проблемы:

- Удалите файл `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\ini\sqllogininfo.dat`.
- Перезапустите программу ViPNet Удостоверяющий и ключевой центр. Появится окно **Подключение к SQL Server**.

- Укажите параметры подключения по имени и паролю пользователя SQL-сервера (см. [Подключение к SQL-серверу при запуске программы](#)).
- **Не найден контейнер ключей администратора УКЦ**

По умолчанию контейнер ключей администратора УКЦ находится в папке: `C:\Users\<имя учетной записи Windows>\AppData\Roaming\Infotecs\ViPNet Administrator\KeysManager_1`.

Причина проблемы может быть в том, что контейнер ключей администратора УКЦ перемещен или учетная запись Windows, которую вы используете, не имеет прав доступа к контейнеру. В случае перемещения контейнера ключей администратора УКЦ укажите место его хранения.

Не удастся посмотреть пароль, сохраненный в файле

Пароли пользователей сохраняются в графическом виде в файлы формата `xps`. Просмотреть файлы `*.xps` вы можете в том случае, если на компьютере установлена программа Средство просмотра XPS.

Программа Средство просмотра XPS по умолчанию не установлена на компьютерах с операционными системами Windows Server 2012 R2 или Windows Server 2016. Поэтому если на вашем компьютере используется одна из указанных ОС, установите Средство просмотра XPS вручную. Ниже описан сценарий установки компонента Средство просмотра XPS на Windows Server 2012. Установка компонента на других ОС включает в себя аналогичные действия, но мастер установки может иметь другой внешний вид.

Чтобы установить компонент Средство просмотра XPS вручную:

- 1 Запустите консоль **Диспетчер серверов (Server Manager)**.
- 2 В окне консоли в меню **Управление (Manage)** выберите пункт **Добавить роли и компоненты (Add roles and Features)**. Будет запущен мастер добавления ролей и компонентов, следуйте его указаниям.
- 3 На странице **Тип установки (Select installation type)** выберите **Установка ролей или компонентов (Role-based or feature-based installation)**.
- 4 На странице **Компоненты (Select features)** в списке компонентов установите флажок напротив **Средство просмотра XPS (XPS Viewer)**.

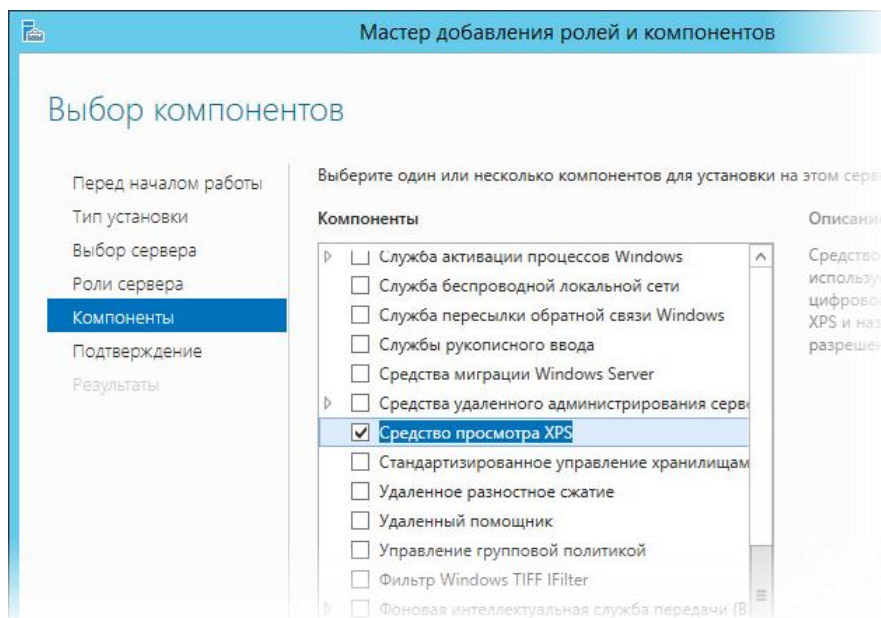


Рисунок 147. Добавление компонента Средство просмотра XPS

- 5 На странице **Подтверждение (Confirmation)** нажмите кнопку **Установить (Install)**.
- 6 На последней странице мастера ознакомьтесь с результатом установки компонента и убедитесь, что в процессе установки не возникло ошибок. После этого завершите работу с мастером.

Теперь вы можете просматривать файлы с паролями пользователей.

Не удастся выполнить обновление списка аннулированных сертификатов

Проблема с обновлением списка аннулированных сертификатов может возникнуть, если было изменено место размещения контейнера с ключом электронной подписи, соответствующим этому списку аннулированных сертификатов. Например, путь к папке с контейнерами ключей мог измениться при миграции ПО ViPNet Administrator с одного компьютера на другой.

Чтобы указать корректный путь к папке с контейнером ключей:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр на панели навигации выберите представление **Администрирование**, и затем выберите раздел **Изданные сертификаты > Корневые сертификаты**.
- 2 Выберите корневой сертификат, соответствующий обновляемому списку аннулированных сертификатов, вызовите контекстное меню и выберите команду **Указать расположение ключа подписи**.
- 3 В открывшемся окне программы ViPNet CSP установите переключатель в положение **Папка на диске** и укажите путь к папке с контейнером ключей.

- 4 В списке **Имя контейнера** выберите контейнер, содержащий нужный ключ электронной подписи, и нажмите кнопку **OK**.

В

История версий

В приложении описаны основные изменения в предыдущих версиях ViPNet Administrator.

Что нового в версии 4.6.9 R3

Обзор изменений в версии 4.6.9 R3 по сравнению с 4.6.9 R2.

- **Управление временем обновления и публикации CRL**

Раньше если время было не синхронизировано, то на компьютерах пользователей возникали ошибки при проверке действительности CRL. Теперь вы можете управлять временем обновления CRL (полем «Действителен с»), задавая его до 10 минут раньше системного времени. Также чтобы получить новый CRL и начать заранее опрашивать точку распространения CRL, вы можете управлять временем публикации следующего CRL (полем «Следующая публикация») до 24 часов. Подробнее см. [Управление временем обновления и публикации CRL](#).

- **Изменения в работе с квалифицированными сертификатами**

Теперь в режиме аккредитованного УЦ нельзя приостанавливать действие квалифицированных сертификатов и возобновлять их, вы можете только аннулировать их.

- **Поддержка ViPNet CSP 4.4.4**

Теперь ViPNet Administrator поддерживает новую версию криптопровайдера ViPNet CSP 4.4.4, в которой устранена несовместимость с обновлением Microsoft Windows 10 KB5009543 (версии 20H2, 21H1, 21H2).

Что нового в версии 4.6.10

- **Управление временем обновления и публикации CRL**

Раньше если время было не синхронизировано, то на компьютерах пользователей возникали ошибки при проверке действительности CRL. Теперь в УКЦ вы можете управлять временем обновления CRL (полем «Действителен с»), задавая его до 10 минут раньше системного времени. Также чтобы получить новый CRL и начать заранее опрашивать точку распространения CRL, вы можете управлять временем публикации следующего CRL (полем «Следующая публикация») до 24 часов. Подробнее см. [Управление временем обновления и публикации CRL](#).

- **Изменения в работе с квалифицированными сертификатами**

Теперь в УКЦ в режиме аккредитованного УЦ нельзя приостанавливать действие квалифицированных сертификатов и возобновлять их, вы можете только аннулировать их.

- **Поддержка ViPNet CSP 4.4.4**

В ViPNet Administrator поддержана новая версия криптопровайдера ViPNet CSP 4.4.4, в которой устранена несовместимость с обновлением Microsoft Windows 10 KB5009543 (версии 20H2, 21H1, 21H2).

Что нового в версии 4.6.9 R2

- **Поддержка ViPNet CSP 4.4.2**

- **Поддержка Windows Server 2019**

Что нового в версии 4.6.9 R1

- **Поддержка внешних устройств JaCarta-2**

Теперь в состав программы входит новая версия криптопровайдера ViPNet CSP 4.4.0 с поддержкой устройств JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ (см. Список поддерживаемых внешних устройств).

- **Поддержка Windows Server 2016**

- **Совместимость с Microsoft SQL Server 2017 и Windows SQL Server 2019**

- **Изменения в списке поддерживаемых операционных систем**

В связи с тем, что компания Microsoft прекратила общую поддержку операционных систем Windows 7 (32/64-разрядная), Windows 8 (32/64-разрядная), Windows Server 2008 R2 (64-разрядная), Windows Server 2012 (64-разрядная), Windows 8.1 (32/64-разрядная), работа

программы ViPNet Удостоверяющий и ключевой центр на компьютерах с этими операционными системами также более не поддерживается ИнфоТеКС.

- **Поддержка изменений приказа ФСБ России №795**

В УКЦ поддержаны изменения приказа Федеральной службы безопасности Российской Федерации от 29.01.2021 № 31 «О внесении изменений в приказ ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»:

- **Отображение типа владельца сертификата при издании сертификатов по входящим запросам**

Теперь при издании сертификатов вручную по запросам внешних пользователей (из файлов *.p10 и *.csc), так и при издании сертификата из входящего запроса отображается тип владельца сертификата.

Если в запросе на сертификат указаны атрибуты, которые однозначно характеризуют владельца сертификата как индивидуального предпринимателя, физическое или юридическое лицо, то есть в запросе были заданы поля ОГРНИП, ИНН ФЛ или ИНН ЮЛ соответственно, то при издании сертификатов отображается тип владельца в заголовке первой страницы мастера издании сертификатов.

Если такие поля не были заданы в запросе, то при издании сертификатов необходимо выбрать тип владельца сертификата. В зависимости от выбранного типа будет предложено заполнить поля сертификата. Например, если выбрать **Индивидуальный предприниматель**, то будут доступны поля для ИП (ОГРНИП и другие). А при выборе **Юридическое лицо** появится новое поле — **ИНН ЮЛ** (расширение INNLE), в котором задается ИНН из 10 символов. Раньше был один общий формат ИНН из 12 символов для всех типов владельцев сертификата и для юридических лиц добавлялись два нуля в начало ИНН в издаваемых сертификатах. Чтобы продолжить использовать старый формат ИНН ЮЛ, внесите изменения в конфигурационный файл УКЦ.

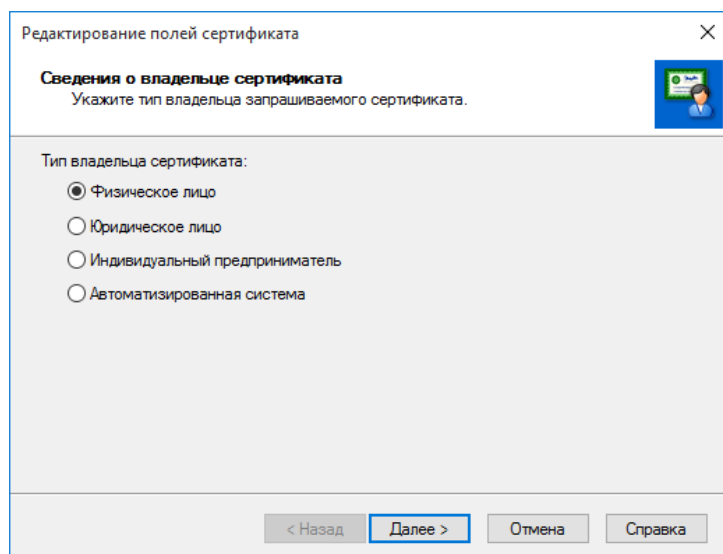


Рисунок 148. Выбор типа владельца сертификата при удовлетворении запроса на сертификат

- **Возможность указания типа идентификации владельца сертификата**

Теперь при издании квалифицированных сертификатов необходимо добавлять расширение «Тип идентификации». Это нужно для того, чтобы определить, как идентифицировал себя пользователь при создании запроса на сертификат. Возможны следующие типы идентификации:

- **Личное присутствие.**
- **Действующий сертификат.**
- **Заграничный паспорт.**
- **ЕСИА/ЕБС** (Единая система идентификации и аутентификации/Единая биометрическая система).

Указанное расширение должно добавляться в запросы на квалифицированные сертификаты или в издаваемые квалифицированные сертификаты, его наличие не является обязательным для простых и неквалифицированных сертификатов.

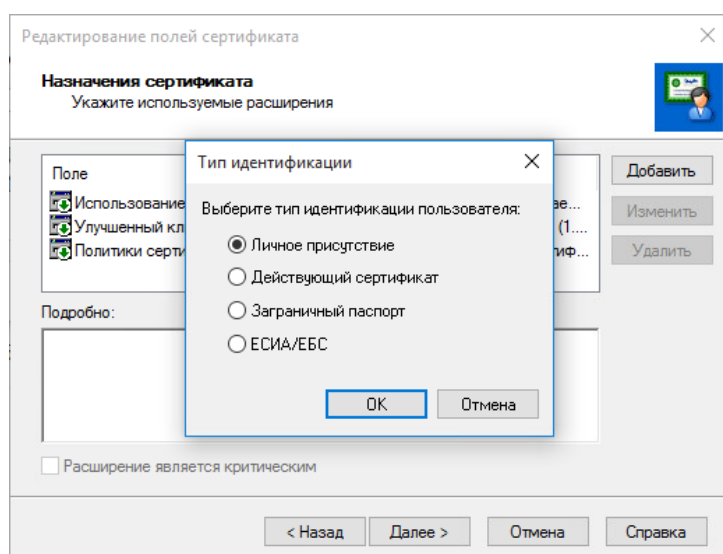


Рисунок 149. Указание типа идентификации владельца сертификата

- **Улучшение внутренней функциональности**

Исправлены ошибки, выявленные в процессе эксплуатации программы ViPNet Удостоверяющий и ключевой центр версии 4.6.7.

Что нового в версии 4.6.7

- **Управление параметрами ключей ДСДР для программно-аппаратных комплексов ViPNet L2**

Для координаторов с ролями «L2-10G» и «L2-100G» добавлено управление параметрами ключей ДСДР (см. [Учет ключей ДСДР](#)).

- **Улучшение внутренней функциональности**

Исправлены ошибки, выявленные в процессе эксплуатации программы ViPNet Удостоверяющий и ключевой центр версии 4.6.6.

Что нового в версии 4.6.6

- **Смена пароля администратора сети ViPNet каждые 6 месяцев**

Раньше вы меняли пароль администратора программы ViPNet Удостоверяющий и ключевой центр каждые 15 месяцев. Теперь по требованиям безопасности необходимо менять пароль администратора программы ViPNet Удостоверяющий и ключевой центр каждые 6 месяцев.

- **Исправление ошибок**

Исправлены ошибки, выявленные в процессе эксплуатации программы ViPNet Удостоверяющий и ключевой центр версии 4.6.5.

Что нового в версии 4.6.5

- **Увеличение срока действия ключа электронной подписи администратора до 6 лет и срока его плановой смены до 3 лет**

Теперь при хранении ключа электронной подписи администратора на устройстве с аппаратной поддержкой ГОСТ Р 34.10-2001/2012 вы можете использовать ключ электронной подписи для издания сертификатов пользователей в течение 3 лет и обновления списка аннулированных сертификатов (CRL) в течение 6 лет. Подробнее см. в разделе [Плановая смена ключа электронной подписи и сертификата администратора](#).

- **Передача всех CRL в автоматическом режиме работы программы**

Раньше вы могли в автоматическом режиме программы распространять CRL только из доверенных сетей ViPNet. Теперь вы можете автоматически по расписанию распространять все CRL, которые присутствуют в программе, включая CRL из других удостоверяющих центров.

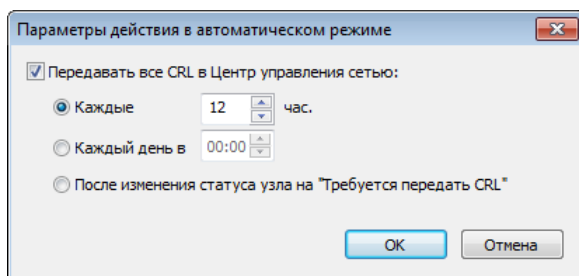


Рисунок 150. Настройка автоматической отправки CRL на все узлы

Обновление CRL происходит при каждом отзыве сертификатов пользователей. После обновления CRL всем сетевым узлам присваивается статус CRL. При работе в автоматическом режиме работы программы отправка обновления CRL на большое количество узлов занимает много времени. Также теперь при необходимости вы можете отключить передачу CRL на узлы

после обновления CRL в автоматическом режиме работы программы (см. [Настройка автоматической передачи CRL](#)).

Что нового в версии 4.6.4

- **Отказ от использования случайного цифрового пароля**

С целью повышения безопасности паролей пользователей, администраторов сетевых узлов и администратора УКЦ отменена возможность использовать случайный цифровой пароль. Теперь в УКЦ отсутствует возможность выбирать тип пароля «Случайный цифровой пароль». В случае если в настройках программы УКЦ вы использовали случайный цифровой пароль, то после обновления ПО автоматически будет задано использование пароля на основе парольной фразы. Созданные ранее случайные цифровые пароли можно будет продолжать использовать после обновления.

- **Повторное использование свободных идентификаторов сетевых узлов, если был присвоен максимальный идентификатор объекту сети ViPNet**

В сети ViPNet может быть создано большое число объектов сети ViPNet — сетевых узлов и пользователей, а также групп узлов и групп пользователей, и при частом удалении объектов мог быть достигнут максимальный идентификатор объекта — 65535. Новому объекту не мог быть присвоен новый идентификатор объекта сети ViPNet. При удалении объекта идентификатор освобождался и не использовался. Теперь при достижении максимального идентификатора объекта вы можете создавать новые объекты сети ViPNet благодаря повторному использованию идентификаторов ранее удаленных объектов сети ViPNet. При этом неповторяемость ключей, создаваемых в УКЦ, обеспечивается за счет автоматического изменения варианта ключей узла или варианта персонального ключа пользователя (увеличение на единицу от последнего номера варианта, имевшегося в РНПК пользователя).

- **Улучшен интерфейс мастера издания сертификатов по запросам от пользователей**

Раньше при удовлетворении запроса на сертификат в мастере редактирования полей сертификата вы могли сразу издать сертификат без просмотра его параметров, нажав кнопку **Готово**. Теперь на странице **Источник параметров сертификата мастера** добавлен новый флажок **Показывать параметры сертификата**, который установлен по умолчанию, при этом из интерфейса страницы удалена кнопка **Готово**. Это позволяет просмотреть остальные страницы мастера с параметрами сертификата и при необходимости изменить их, и только после этого издать сертификат.

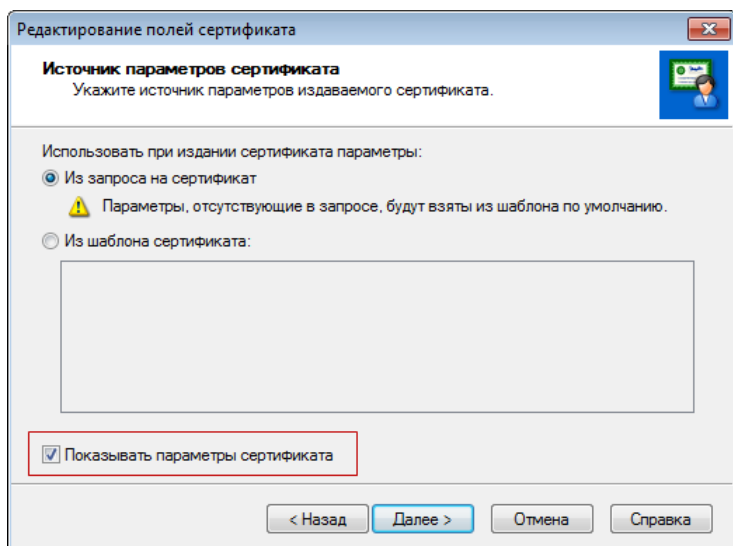
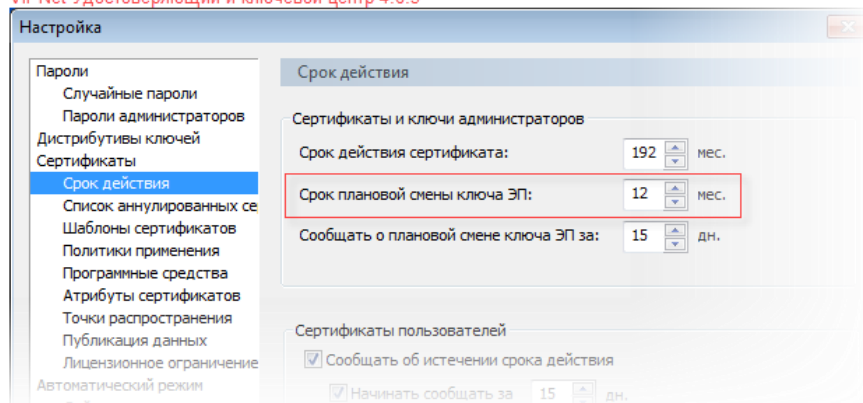


Рисунок 151. Управление просмотром параметров сертификатов по запросам от пользователей

- **Контроль срока действия ключа электронной подписи уполномоченного лица УЦ**

Раньше срок плановой смены ключа электронной подписи указывался вручную в настройках программы в разделе **Сертификаты > Срок действия группы Сертификаты и ключи администраторов**. Теперь срок плановой смены ключа электронной подписи задан автоматически в программе и составляет 15 месяцев (1 год и 3 месяца). Этот срок нельзя изменить, а вам не нужно выполнять дополнительной настройки этого срока.



ViPNet Удостоверяющий и ключевой центр 4.6.4

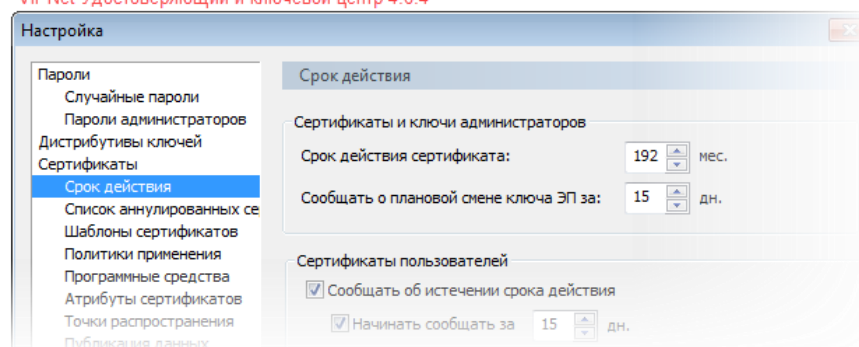


Рисунок 152. Отмена возможности самостоятельно задавать срок плановой смены ключа электронной подписи

Также теперь вы можете просматривать срок действия ключа электронной подписи администратора УКЦ или вышестоящего УЦ, не открывая сам сертификат. В представлении **Администрирование** в разделах **Изданные сертификаты** > **Корневые сертификаты** и **Кросс-сертификация** > **Сертификаты от вышестоящего УЦ** в соответствующие таблицы со списками сертификатов добавлен столбец **Срок действия ключа ЭП**.

Корневые сертификаты					
Владелец сертификата	Дата издания	Срок действия	Срок действия ключа ЭП	Статус	
Администратор сети 10773	21.11.2017	До 21.11.2023 14:40	До 21.11.2020 14:40	Действителен (текущий)	
Администратор сети 10773	21.11.2017	До 21.12.2017 12:14	До 21.12.2017 12:14	Действителен	
Администратор сети 10773	20.11.2017	До 20.11.2020 23:59	До 20.11.2020 19:54	Действителен	
Администратор сети 10773	20.11.2017	До 20.11.2033 23:59	До 20.11.2020 19:01	Действителен	

Рисунок 153. Просмотр срока действия ключа электронной подписи в списке корневых сертификатов

- Поиск корневых сертификатов и CRL по идентификатору ключа

Раньше при просмотре и поиске изданных корневых сертификатов и сертификатов из вышестоящих УЦ или CRL было сложно различить сертификаты одного и того же владельца сертификата или издателя CRL. Теперь в представлении **Администрирование** вы можете найти необходимый корневой сертификат или CRL по идентификатору ключа электронной подписи владельца сертификата (идентификатору ключа субъекта), отобразив столбцы с дополнительной информацией.

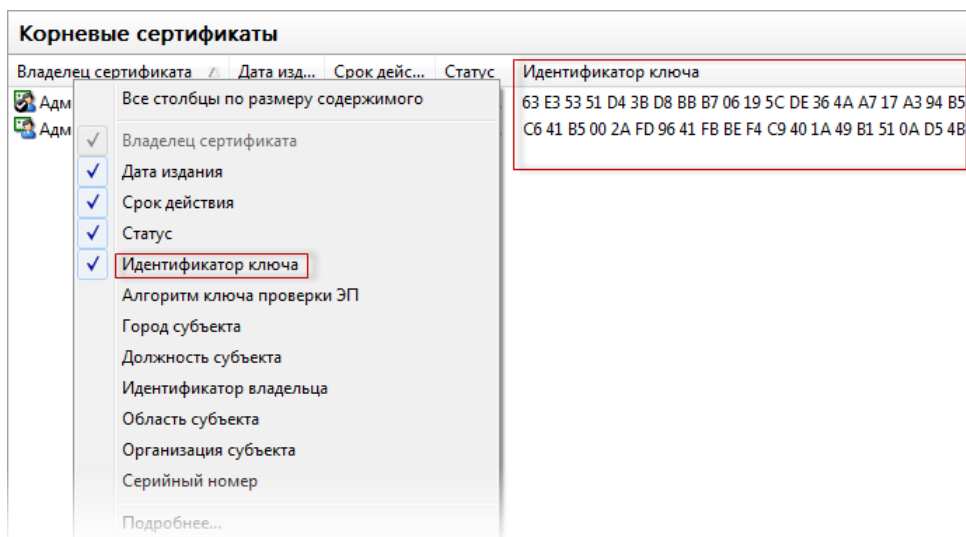


Рисунок 154. Включение отображения идентификатора ключа электронной подписи владельца сертификата

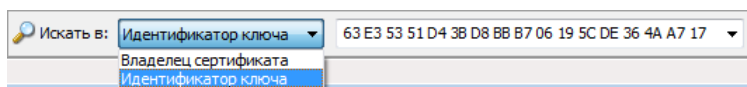


Рисунок 155. Поиск корневого сертификата по идентификатору ключа владельца сертификата

- Поиск по всем столбцам в представлении Ключевой центр

Раньше в представлении **Ключевой центр** при просмотре разделов **Пользователи**, **Запросы на дистрибутивы ключей**, **Сетевые узлы** и **Группы узлов** вы могли найти необходимый объект только по его имени. Теперь в представлении **Ключевой центр** для этих разделов вы можете задать поиск по всем столбцам.

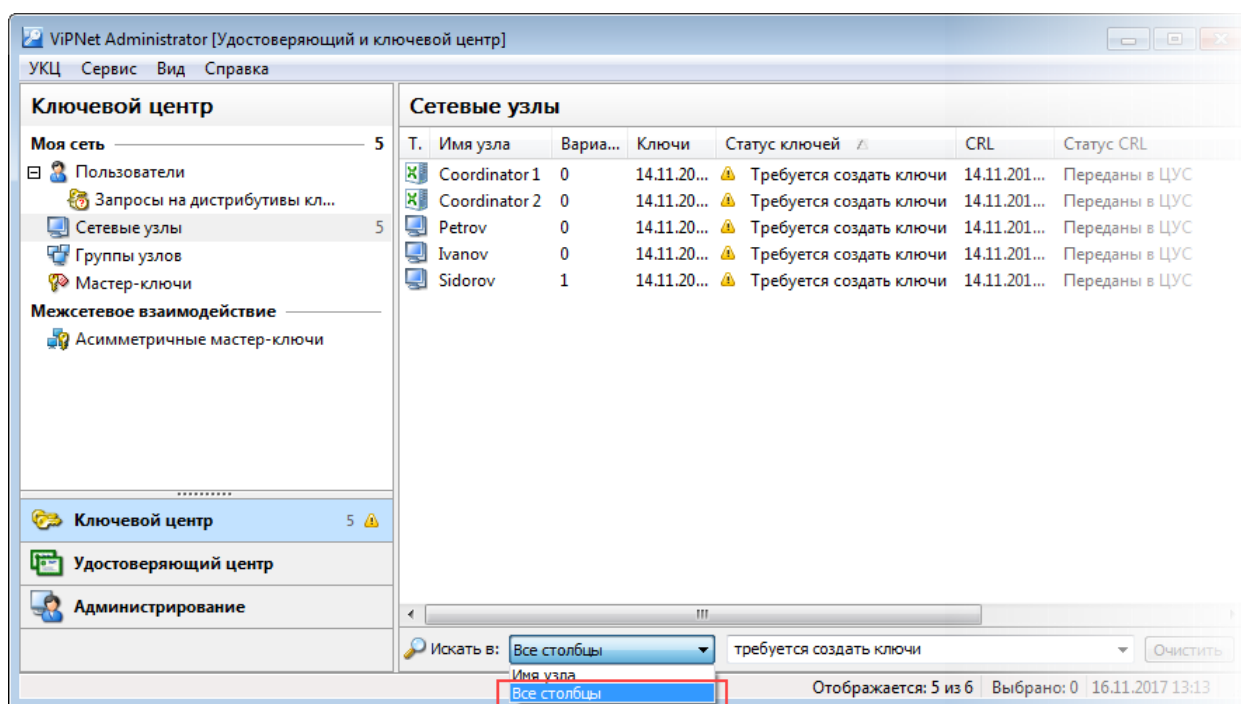


Рисунок 156. Поиск по всем столбцам разделов в представлении Ключевой центр

- Ввод в действие текущего сертификата администратора из контекстного меню

Раньше для смены текущего сертификата администратора вы выполняли действия в разделе **Моя сеть** > **Администраторы** в окне свойств администратора на вкладке **Сертификаты**. Теперь для удобства работы вы можете выбрать текущий сертификат администратора в списке корневых сертификатов или сертификатов из вышестоящего УЦ и в контекстном меню пункт **Назначить текущим**.

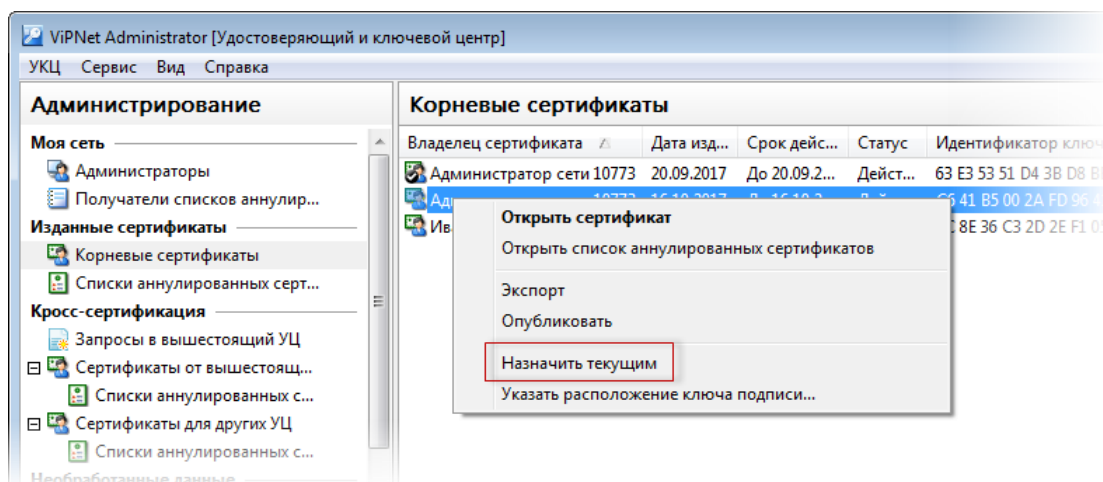


Рисунок 157. Выбор текущего сертификата администратора

- Смена имени учетной записи администратора УКЦ

Теперь вы можете изменять имя учетной записи администратора УКЦ, используемое для входа в программу УКЦ, в окне **Свойства администратора**. Подробнее см. в разделе [Просмотр и изменение данных об администраторе](#).

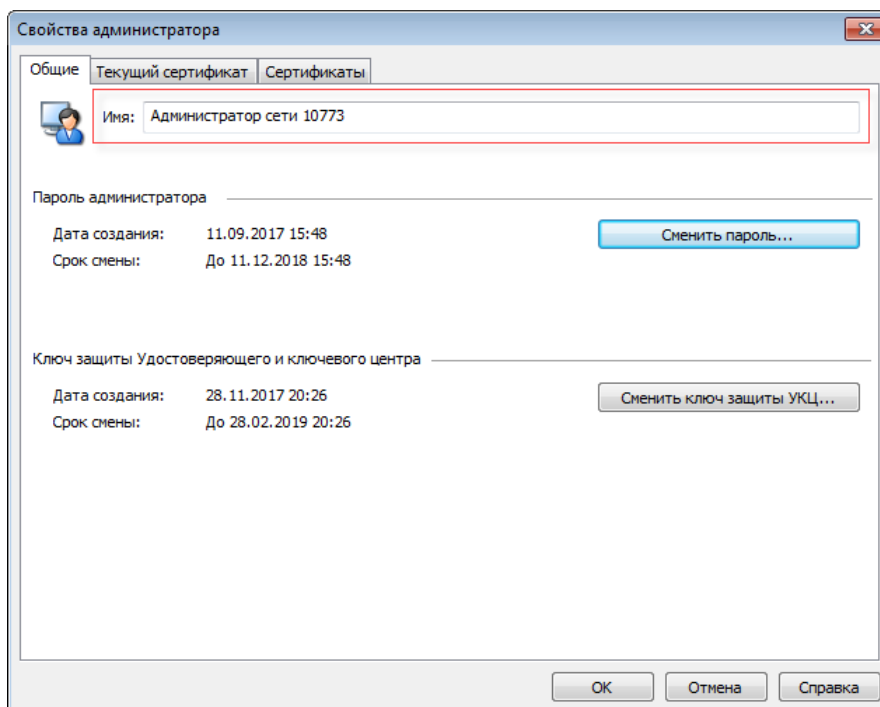


Рисунок 158. Изменение имени учетной записи администратора УКЦ

- **Исправление ошибок**

В ViPNet Удостоверяющий и ключевой центр 4.6.4 были исправлены ошибки, обнаруженные при эксплуатации предыдущей версии программы.

Что нового в версии 4.6.3

- **Непрерывная работа ПАК ViPNet Coordinator KB2 при смене ключей ДСДР**

В предыдущей версии программы ViPNet Удостоверяющий и ключевой центр 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.

Чтобы исключить время простоя при смене ключей ДСДР и снизить вероятность пропуска срока обновления ключей ДСДР, в новой версии УКЦ реализованы следующие возможности:

- контроль сроков действия ключей ДСДР для узлов ПАК ViPNet Coordinator KB2;
- настройка оповещения об окончании срока действия ключей ДСДР;
- автоматическая смена ключей ДСДР при регистрации двух серий ключей ДСДР.

Теперь вы можете зарегистрировать до двух серий ключей ДСДР одновременно. По истечении срока действия текущей серии ключей ДСДР автоматически будет использована следующая серия. Это позволит вам реже обновлять ключи ДСДР.

- **Новый формат архивного файла и хранение файлов по указанному пути при резервном копировании конфигурации сети**

Теперь при создании резервных копий используется новый формат архивного файла ZIP (раньше — LZH). Файл резервной копии имеет расширение *.zip (раньше — *.rp). При этом мастер восстановления конфигурации сети поддерживает оба формата.

По умолчанию резервные копии конфигурации сети ViPNet сохраняются на системном диске C: в папку C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore. Вы не могли задавать путь хранения файлов резервных копий конфигураций сети. Теперь вы можете настроить сохранение резервных копий по заданному пути (см. [Изменение места хранения резервных копий, используемого по умолчанию](#)), например, в случае если заканчивается объем системного диска C:.

- **Новая папка для публикации CRL**

Появилась возможность настроить расположение папки со списками аннулированных сертификатов для обмена между программами ViPNet Удостоверяющий и ключевой центр и ViPNet Publication Service.

Также в окне **Сервис > Настройка** раздел **Папки обмена** переименован в **Публикация данных**.

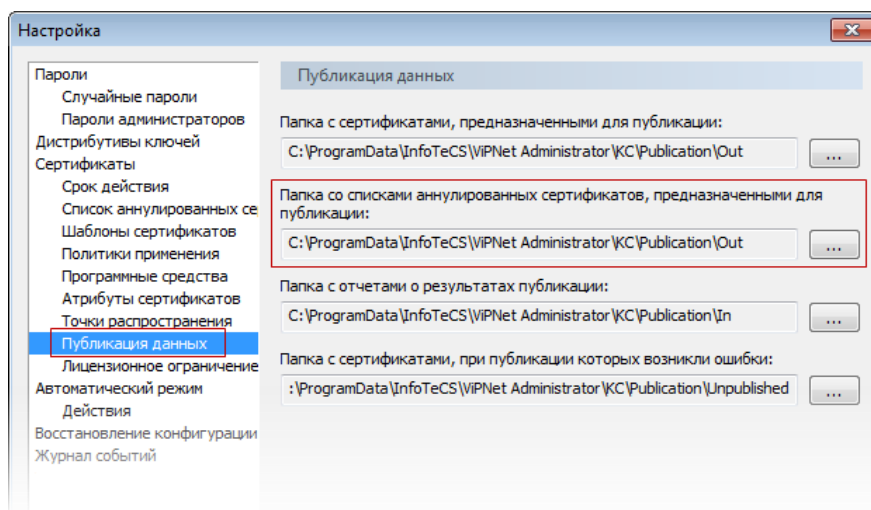


Рисунок 159. Настройка папки со списками аннулированных сертификатов, предназначенных для публикации

- **Улучшение управления сертификатами пользователя**

Раньше чтобы аннулировать сертификат в представлении **Удостоверяющий центр**, нужно было найти сертификат в списке изданных сертификатов пользователей сети. В случае если для одного пользователя было найдено несколько сертификатов, было сложно определить правильный сертификат, который нужно аннулировать. Поиск сведений о текущем сертификате пользователя отнимал дополнительное время. Теперь вы можете аннулировать сертификат пользователя непосредственно в окне **Свойства пользователя** на вкладке **Сертификаты**. Подробнее см. в разделе [По инициативе администратора УКЦ](#).

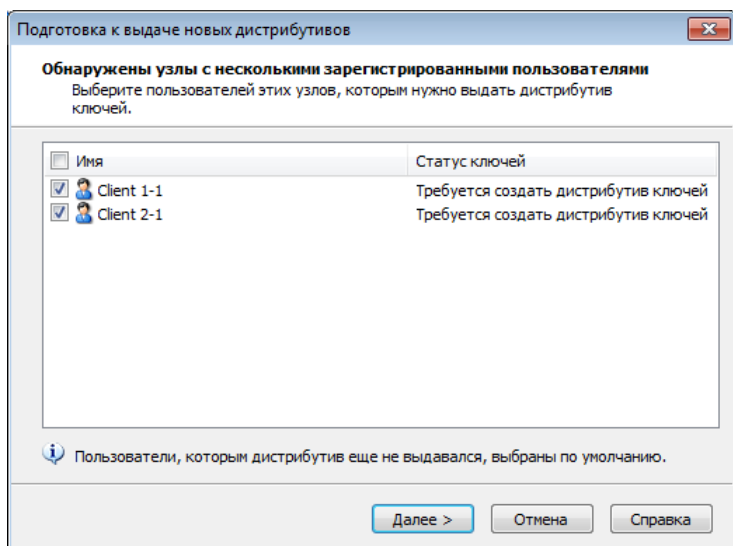


Рисунок 162. Выбор пользователей при выдаче дистрибутива ключей

- **Исправление ошибок**

В ViPNet Удостоверяющий и ключевой центр 4.6.3 были исправлены ошибки, обнаруженные при эксплуатации предыдущей версии программы.

Что нового в версии 4.6.2

- **Новый способ аутентификации пользователей по сертификату**

Реализован новый способ аутентификации по сертификату, который не требует передачи контейнера ключей пользователя администратору УКЦ для настройки способа аутентификации в ПО ViPNet. Данный способ аутентификации удобно использовать в организациях, в которых у пользователей 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. Подробнее о способах аутентификации пользователей см. в разделе [Задание способа аутентификации пользователя](#).

Также теперь способ аутентификации отображается в списке пользователей напротив их имен в столбце **Способ аутентификации**.

Пользователи					
Имя	Ключи	Статус ключей	Резервные наб...	Ключи электр...	Способ аутентификации
Coordinator 1		Требуется соз...			Пароль
Coordinator 2		Требуется соз...			Пароль
Coordinator 3		Требуется соз...			Пароль
Client 1-1	08.09....	Переданы в дист...	08.09.2015 1...	08.09.2015 15:38	Пароль
Client 1-2	09.09....	Переданы в ЦУС	08.09.2015 1...	09.09.2015 16:01	Сертификат
Client 1-3	08.09....	Переданы в дист...	08.09.2015 1...	08.09.2015 15:45	Сертификат
Client 2-1		Требуется соз...			Пароль
Client 2-2		Требуется соз...			Пароль

Рисунок 163. Отображение способов аутентификации пользователей

- **Изменения в процедуре создания дистрибутивов ключей**

В процедуру создания дистрибутивов ключей (см. [Создание дистрибутивов ключей](#)) были внесены следующие изменения:

- Теперь дистрибутивы ключей сразу после создания автоматически сохраняются программой ViPNet Удостоверяющий и ключевой центр в специальную 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.
- 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 данные ключи на внешние устройства, а для остальных — поместить в дистрибутив ключей.
- Теперь **резервный набор персональных ключей** включается в состав каждого создаваемого дистрибутива ключей, независимо от того, первично он создается для пользователя или повторно. В предыдущих версиях программы резервные наборы включались только в состав первого дистрибутива ключей, создаваемого для пользователя. Это изменение исключает ситуацию, когда на узле после развертывания повторно созданного дистрибутива ключей удаляется резервный набор ключей, вследствие чего невозможно удаленное обновление ключей при смене мастер-ключей в сети или компрометации ключей пользователя.

- **Изменения в процедуре создания резервных наборов персональных ключей**

Теперь резервные наборы персональных ключей сразу после создания сохраняются в папку по указанному вами пути. В связи с этим в представлении **Ключевой центр** на панели навигации был удален раздел **Пользователи > Резервные наборы персональных ключей**, из контекстного меню пользователей был удален пункт **Резервные наборы персональных ключей > Сохранить в файл**. Пункт контекстного меню **Резервные наборы персональных ключей > Создать** был изменен на пункт **Создать и сохранить РНПК в файл**.

- **Настройка параметров выдачи дистрибутивов ключей**

В связи с изменениями в процедуре выдачи дистрибутивов ключей были введены новые настройки программы ViPNet Удостоверяющий и ключевой центр и добавлен раздел **Дистрибутивы ключей** в окне **Настройка**. В данном разделе настраивается путь к папке для сохранения дистрибутивов ключей, а также включаются функции выбора способа аутентификации пользователей и способа сохранения ключей электронной подписи пользователей (см. [Настройка параметров создания дистрибутивов ключей](#)).

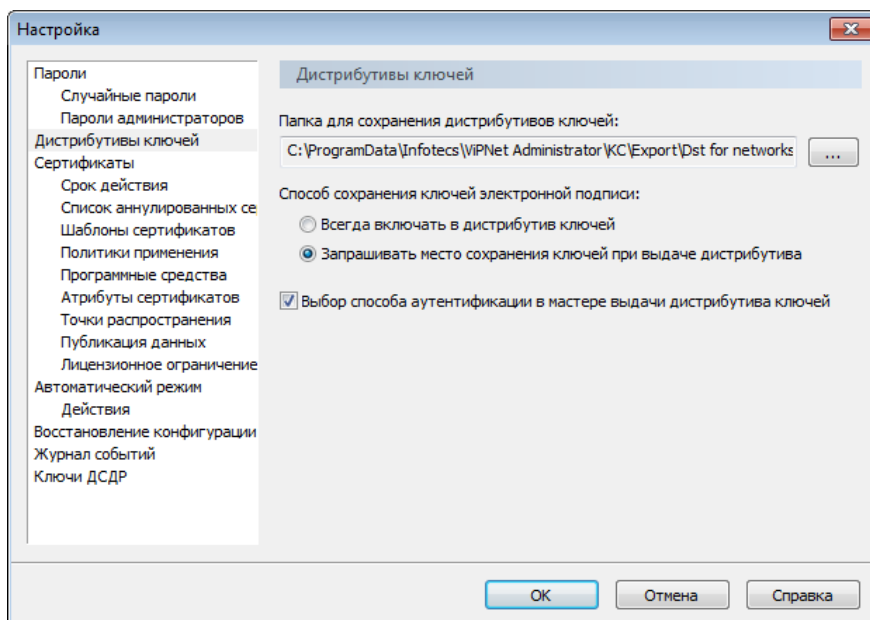


Рисунок 164. Настройка параметров выдачи дистрибутивов ключей

- **Выдача паролей пользователей**

В предыдущих версиях пароль пользователю ViPNet всегда выдавался в текстовом файле (*.txt). В новой версии программы по требованиям безопасности появилась возможность печати паролей пользователей на специальных ПИН-конвертах, в которых пароли содержатся в запечатанной части. Это сделано для защищенной передачи паролей пользователям с целью исключения доступа к паролям посторонних лиц.

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

Подробнее о способах выдачи паролей пользователей см. в разделе [Выдача паролей пользователей](#).

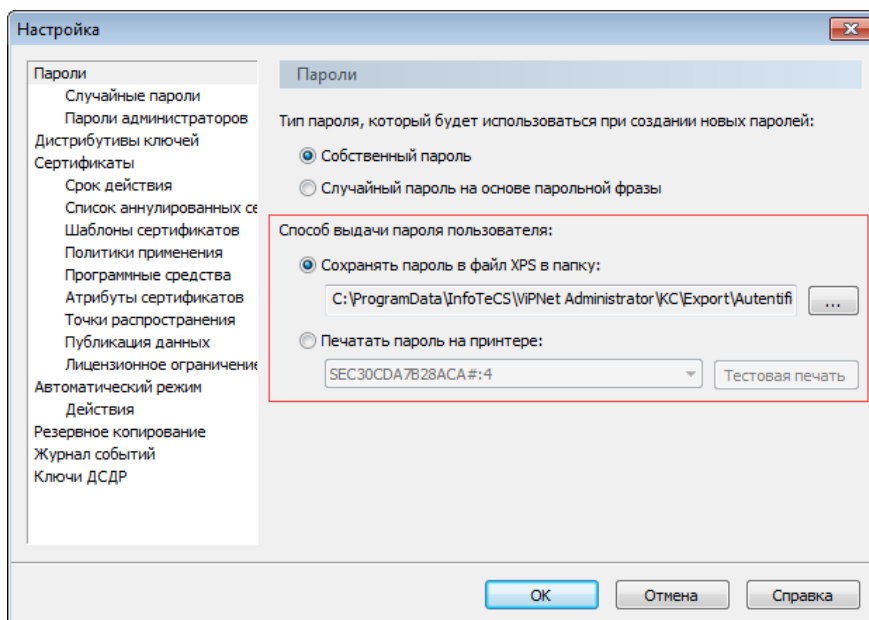


Рисунок 165. Настройка способа выдачи паролей пользователей

- **Повышение криптостойкости случайных паролей**

Теперь в настройках случайных паролей вы можете включить добавление цифр в начало пароля и использование заглавных букв в начале слов парольной фразы.

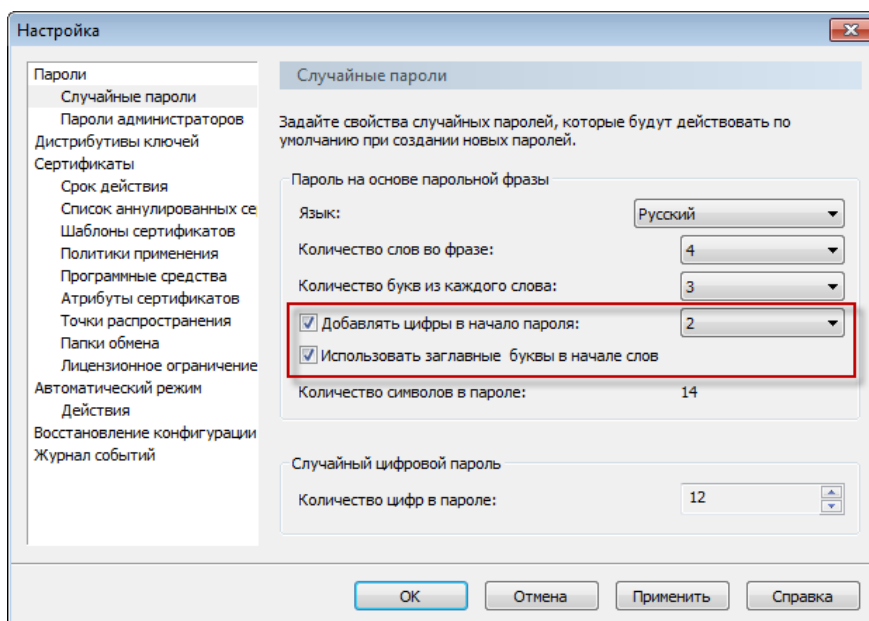


Рисунок 166. Настройка параметров случайных паролей

- **Настройка подключения к базе данных**

В программе ViPNet Удостоверяющий и ключевой центр реализована возможность настройки подключения к конкретной базе данных на SQL-сервере. Данная функция может понадобиться, если в организации имеется несколько сетей ViPNet и для каждой из них используется отдельная база данных ПО ViPNet Administrator на общем SQL-сервере.

- **Изменены сценарии действий администратора при компрометации ключей**

Раньше действия в случае компрометации выполнялись отдельно для ключей пользователя и ключей сетевого узла. Теперь они объединены в единую процедуру (см. [Действия в случае компрометации ключей 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.

Также реализована возможность изменения варианта персонального ключа пользователя и ключей узла (см. [Изменение вариантов 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.

- **Изменения настроек точек распространения**

В новой версии для удобства параметры точек распространения сертификатов издателей и CRL и адресов доступа к OCSP-серверам настраиваются на разных вкладках.

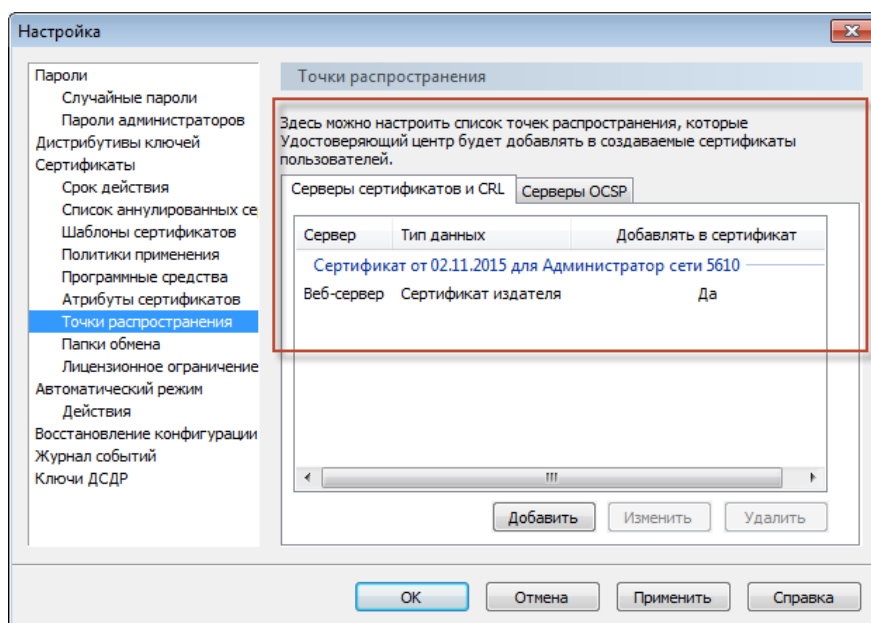


Рисунок 167. Настройка точек распространения и адресов доступа к OCSP-серверам

Кроме этого, появилась возможность задания точки распространения сертификата издателя или соответствующего сертификату CRL непосредственно при издании этого сертификата.

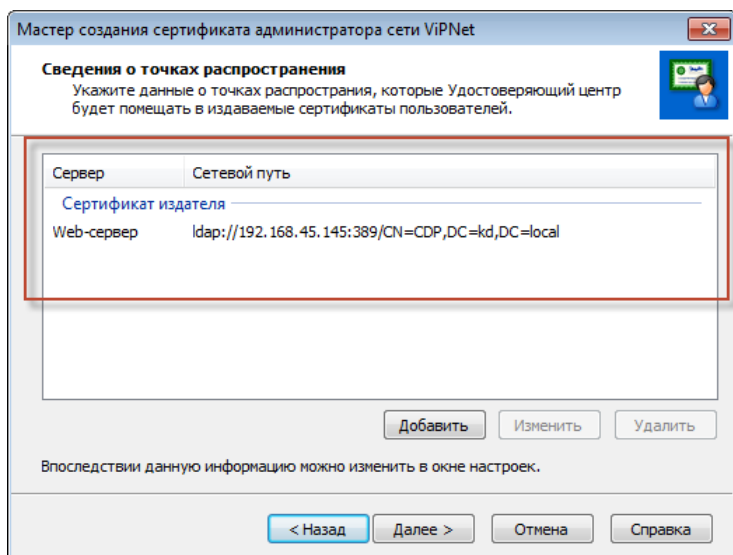


Рисунок 168. Задание точки распространения при издании сертификата издателя

- Улучшен интерфейс поиска и работы с объектами

- Для поиска объектов в строке поиска теперь не нужно нажимать кнопку Найти (не считая поиска по дате). Достаточно выбрать столбец, по данным которого нужно осуществлять поиск, и ввести сочетание букв. Поиск произойдет автоматически через несколько секунд.

Кроме этого, теперь при поиске по дате можно указать интервал времени. Раньше можно было организовать поиск только по конкретному числу.

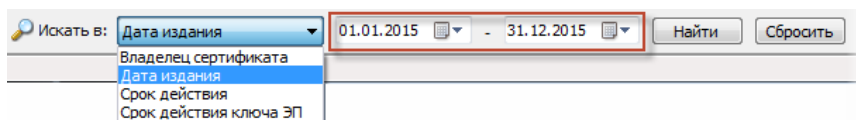


Рисунок 169. Поиск объектов по дате

Также теперь строка поиска отсутствует в тех разделах, в которых не может содержаться большое количество объектов, например, в разделе **Мастер-ключи**, **Администраторы** и другие.

- В предыдущей версии в подразделах раздела **Изданные сертификаты** всегда отображалось не более 100 сертификатов. Теперь можно увеличить количество отображаемых сертификатов с помощью настройки файла `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Ini\KC.ini`. Для этого в указанный файл требуется добавить параметр `Certificates cache capacity` с нужным количеством сертификатов. Максимальное количество отображаемых сертификатов составляет 10000. При этом стоит учитывать, что при увеличении количества сертификатов будет снижаться скорость отображения списка сертификатов в программе.

Возможность настройки количества отображаемых сертификатов может быть удобна в том случае, если на базе ViPNet Удостоверяющий и ключевой центр функционирует удостоверяющий центр, который осуществляет массовое издание сертификатов.

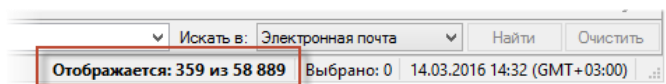


Рисунок 170. Увеличение количества отображаемых сертификатов

- В разделе **Опубликованные списки аннулированных сертификатов других УЦ** появился новый столбец, в котором отображается количество аннулированных сертификатов, содержащихся в CRL. По данной информации можно определять примерный размер CRL.

Издатель	Дата издания списка	Срок действия	Содержит сертификатов
CA 5611	26.03.2016 18:59	До 12.04.2016 19:01	72976
CA TAXCOM	04.08.2015 16:01	До 24.08.2027 16:21	65391

Рисунок 171. Отображение количества сертификатов в CRL

- В окне **Свойства пользователя** на вкладке **Сертификаты** теперь отображаются сертификаты пользователя. Раньше для просмотра списка сертификатов нужно было перейти в отдельное окно. Кроме этого, теперь сертификаты в списке группируются в соответствии с тем, каким сертификатом издателя они подписаны. То есть сертификаты, заверенные разными сертификатами издателей, находятся в разных группах. Также в списке значком  отмечается сертификат, изданный последним для пользователя. Из последнего сертификата берутся сведения о владельце (пользователе) при издании для него новых сертификатов.

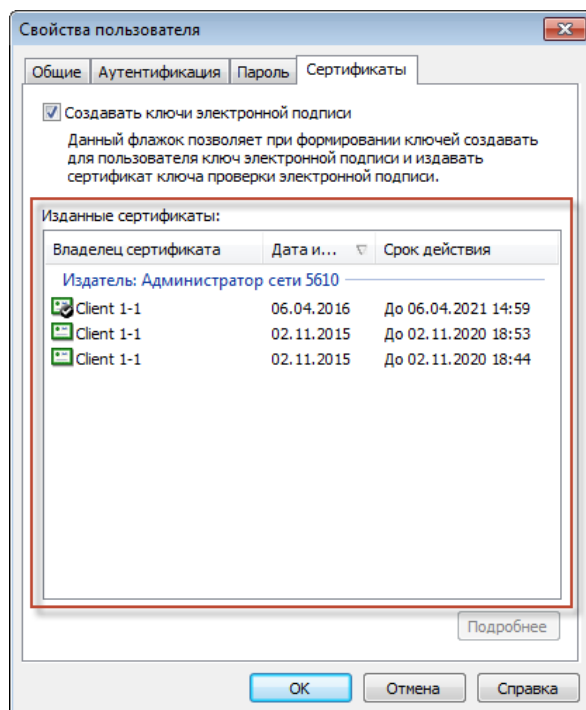


Рисунок 172. Список сертификатов в окне просмотра свойств пользователя

Что нового в версии 4.5

- Настройка параметров работы в автоматическом режиме при первичной инициализации

Теперь при первичной инициализации УКЦ вы можете настроить параметры работы программы в автоматическом режиме: задать время неактивности администратора, по истечении которого будет производиться переход в автоматический режим, и выбрать операции для выполнения в автоматическом режиме.

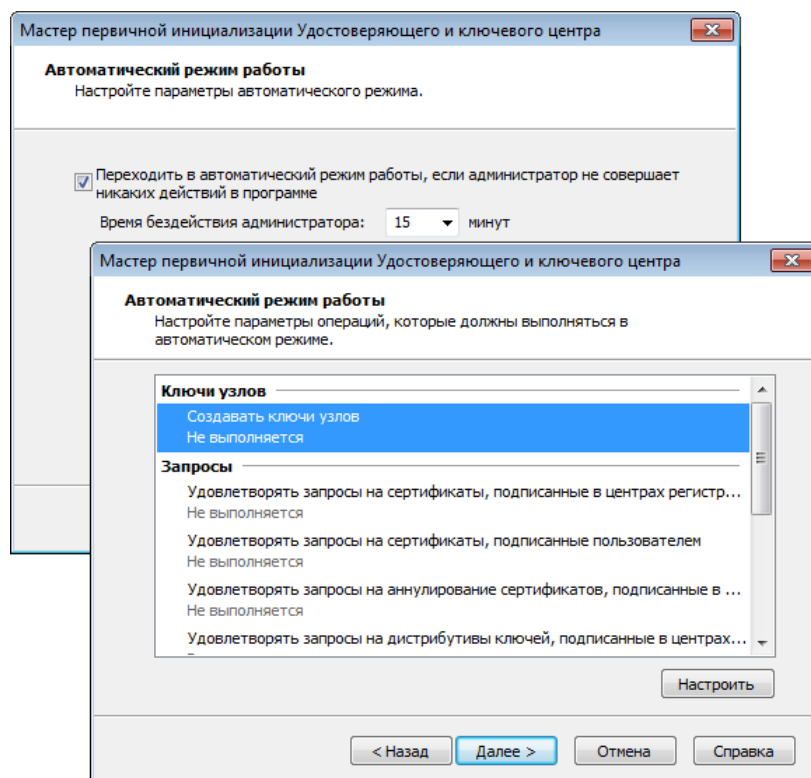


Рисунок 173. Настройка параметров работы в автоматическом режиме при первичной инициализации

- **Дополнительные возможности автоматического режима работы**

Раньше при наличии межсетевого взаимодействия после обновления списков аннулированных сертификатов (CRL) в автоматическом режиме работы УКЦ вам необходимо было отправлять CRL и корневой сертификат в доверенные сети вручную. Теперь это действие выполняется автоматически.

Кроме того, раньше после загрузки CRL из доверенных сетей ViPNet они сразу отправлялись на сетевые узлы, что могло быть неудобно в случае наличия межсетевого взаимодействия с большим количеством доверенных сетей. Теперь вы можете настроить расписание отправки CRL, полученных из доверенных сетей ViPNet, на узлы: раз в несколько минут или часов после загрузки CRL, каждый день в конкретное время или сразу после загрузки CRL.

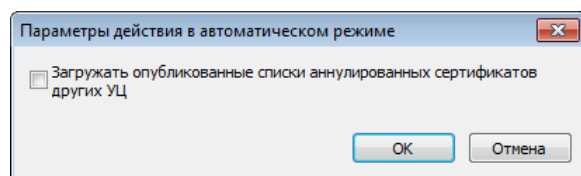


Рисунок 174. Настройка автоматической загрузки CRL

- **Плановая смена пароля администратора и ключа защиты УКЦ**

Раньше в целях обеспечения безопасности мы рекомендовали менять пароль администратора и ключ защиты УКЦ не реже одного раза в год. При этом никаких уведомлений о необходимости их смены предусмотрено не было. Теперь по истечении 15 месяцев со дня начала действия пароля администратора и ключа защиты УКЦ вы будете получать уведомление о необходимости их смены. Просмотреть информацию о рекомендуемых сроках смены ключа защиты УКЦ, пароля администратора, а также ключа электронной подписи администратора вы можете в представлении **Администрирование** в разделе **Администраторы**.

- **Смена ключа защиты УКЦ в окне просмотра свойств администратора**

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

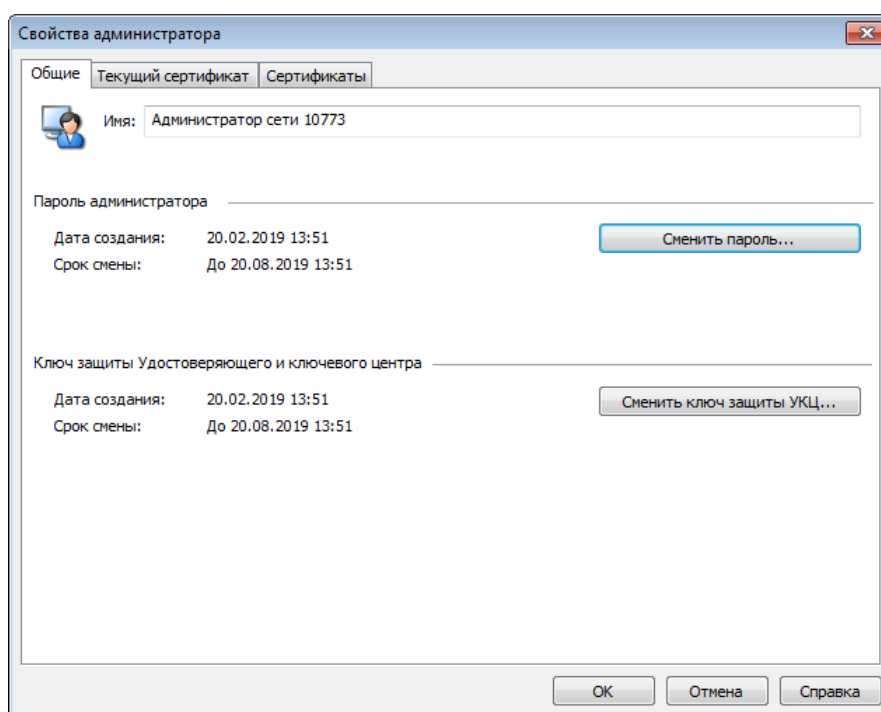


Рисунок 175. Смена ключа защиты УКЦ

- **Обработка запросов на дистрибутивы ключей**

Теперь перед обработкой запроса на дистрибутив ключей вы можете просмотреть информацию о том, кем и когда этот запрос был создан, а также сведения о пользователе, для которого он был создан. Кроме того, в случае удовлетворения такого запроса при соответствующих настройках программы ViPNet Удостоверяющий и ключевой центр вы можете отредактировать поля издаваемого сертификата с помощью мастера.

- **Изменены сценарии работы с ключами пользователей**

Раньше можно было создать ключи пользователя с резервным набором персональных ключей или без него и затем передать их в ЦУС или сохранить в файл. Теперь после создания ключей они автоматически либо передаются в ЦУС, либо сохраняются в файл. Причем включить резервный набор персональных ключей в состав ключей пользователей можно только в случае создания и сохранения ключей пользователя в файл.

Кроме того, раньше создать ключи электронной подписи для пользователя можно было только в процессе формирования его ключей или дистрибутива ключей. Теперь при необходимости можно создать ключи электронной подписи отдельно, при этом они автоматически сохраняются в файл.

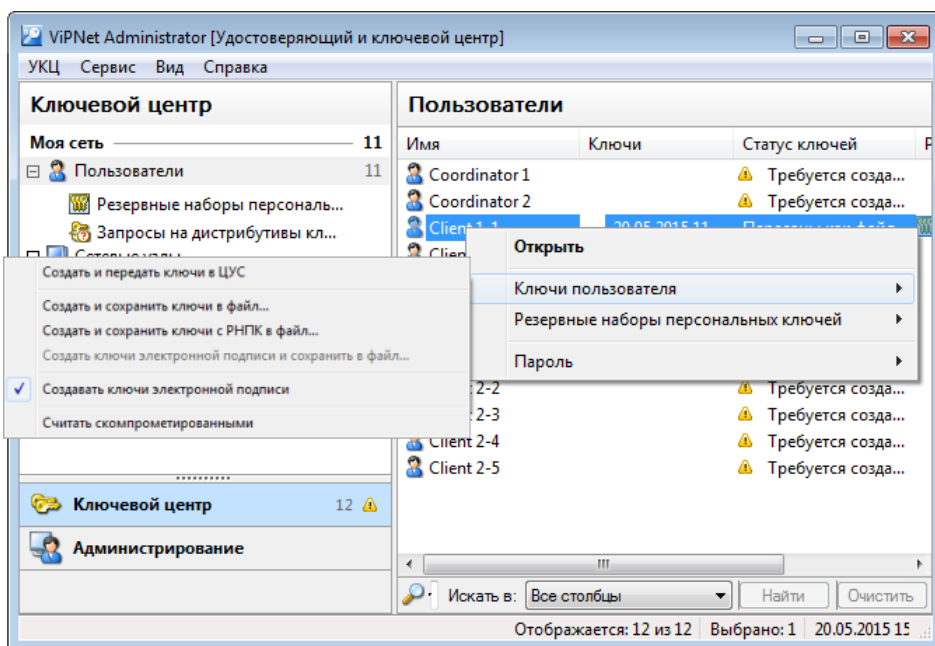


Рисунок 176. Работа с ключами пользователя

Что нового в версии 4.4

- **Автоматическая установка криптопровайдера ViPNet CSP**

Теперь криптопровайдер ViPNet CSP, необходимый для работы УКЦ, автоматически устанавливается вместе с УКЦ. Это позволяет упростить и ускорить процесс установки программного обеспечения. Обновление ViPNet CSP по-прежнему может производиться независимо от обновления программы ViPNet Удостоверяющий и ключевой центр.

- **Реализация системного журнала событий**

В предыдущих версиях журнал событий был организован непосредственно в самой программе. Теперь регистрация событий, возникающих в процессе работы УКЦ, осуществляется в системном журнале Windows, который защищен от модификации и удаления обычным пользователем, не имеющим прав администратора Windows.

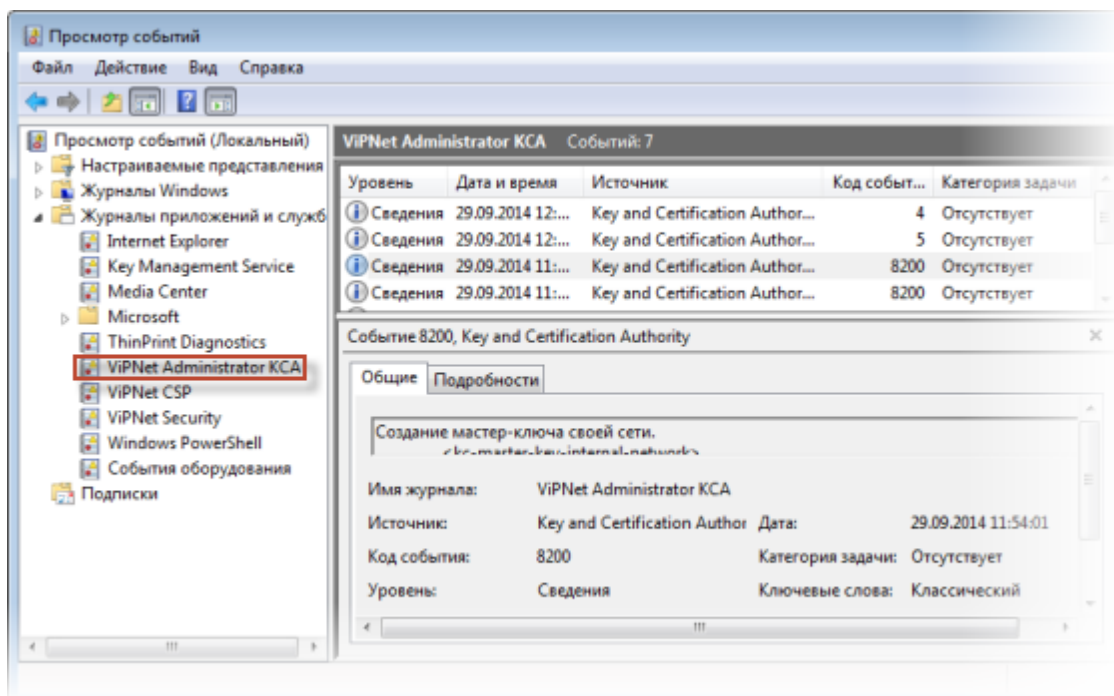


Рисунок 177. Системный журнал событий УКЦ

- **Автоматическое создание резервной копии конфигурации сети по расписанию**

В предыдущих версиях была возможность автоматического создания резервной копии конфигурации сети ViPNet 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. Теперь вы можете гибко настроить создание резервных копий — с определенной периодичностью (от 1 до 31 дней) и в любое время суток.

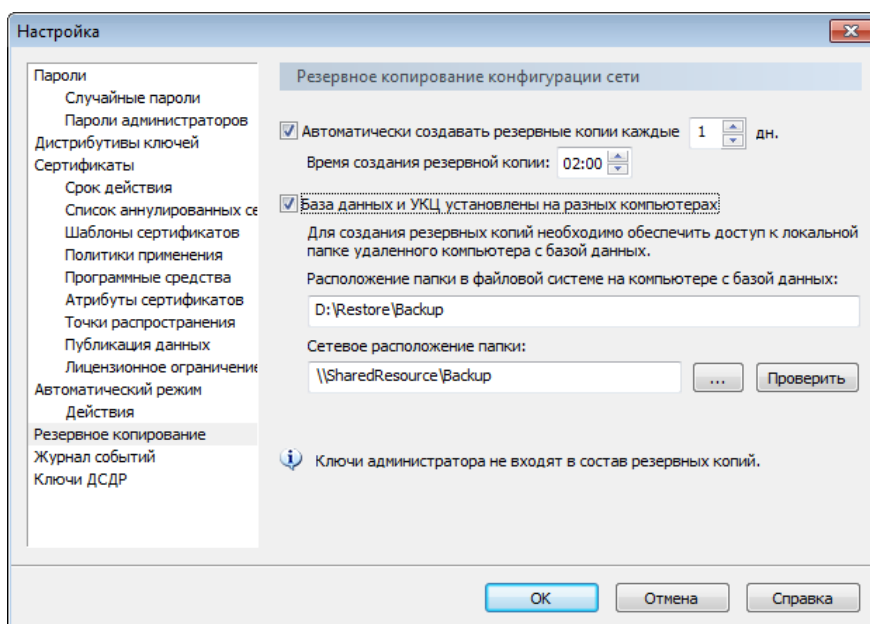


Рисунок 178. Автоматическое создание резервных копий конфигурации по расписанию

- **Оптимизация процесса создания резервной копии конфигурации сети**

Теперь информация о файлах, полученных и отправленных сетевыми узлами, хранится в специальной базе и при создании резервной копии конфигурации сети ViPNet в нее не включаются. Справочники и ключи узлов, которые всегда могут быть созданы в текущей конфигурации сети, также больше не сохраняются в файл резервной копии конфигурации. Это позволяет значительно сократить время, необходимое для создания резервной копии конфигурации сети и последующего восстановления конфигурации сети из резервной копии.

- **Восстановление из резервной копии после обновления программного обеспечения**

В предыдущих версиях 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. Теперь в случае возникновения проблем в сети после обновления программного обеспечения ViPNet Administrator вы можете восстановить конфигурацию сети, используя резервную копию, созданную в более ранней версии УКЦ.

- **Отказ от использования обновлений ключей узлов**

В УКЦ перестали использоваться обновления ключей узлов для доставки на узлы списков аннулированных сертификатов (CRL), сертификатов администраторов и служебной информации. Списки аннулированных сертификатов и сертификаты администраторов теперь передаются на узлы в комплексах CRL. Служебная информация передается в составе ключей узла. Эти изменения сделаны для того, чтобы разделить информацию для работы в инфраструктуре PKI от служебной информации, определяющей работу в защищенной сети ViPNet, и передавать ее в составе разных объектов.

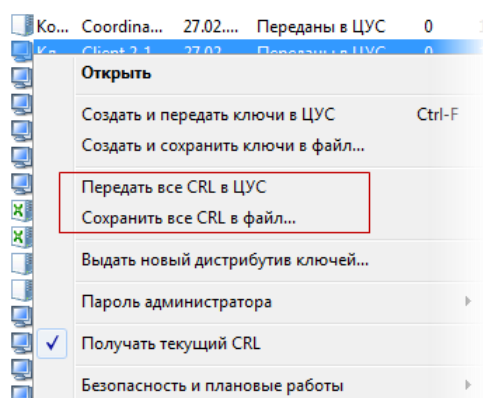


Рисунок 179. Передача CRL на узлы сети вместо обновлений ключей узлов

- **Задание срока действия CRL в часах**

Раньше можно было задать в настройках программы (см. [Настройка срока действия CRL](#)) срок действия списка аннулированных сертификатов только в днях. Теперь 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.

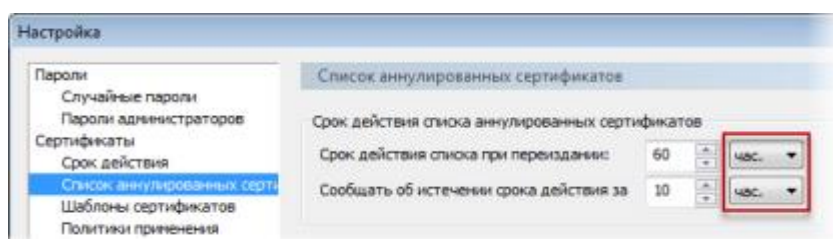


Рисунок 180. Срок действия CRL в часах

- Просмотр данных удостоверяющего центра в автоматическом режиме

Появилась возможность в автоматическом режиме работы открыть окно просмотра изданных сертификатов пользователей. Это позволяет администратору УКЦ отслеживать, какие сертификаты издаются в автоматическом режиме по запросам, при необходимости просматривать их параметры.

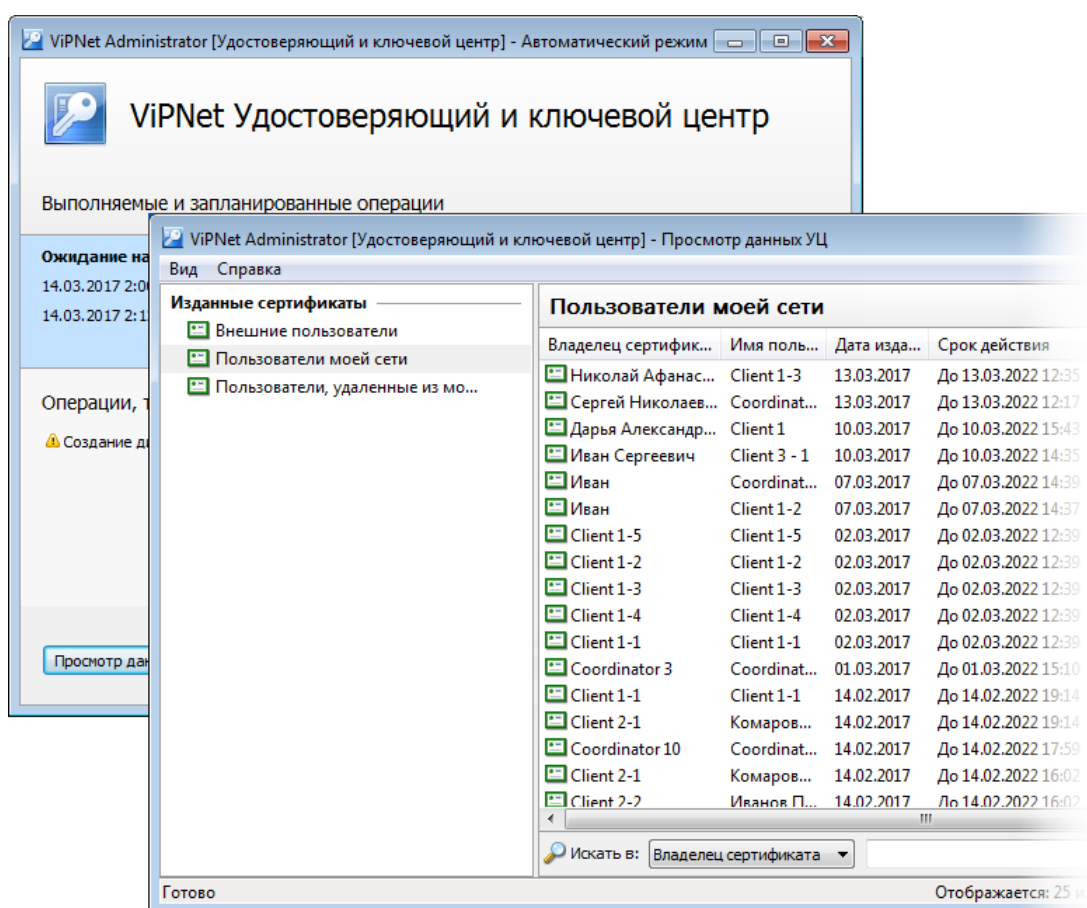


Рисунок 181. Возможность просмотра изданных сертификатов при работе в автоматическом режиме

- 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. Раньше в УКЦ при обработке таких запросов

заданный срок действия ключа электронной подписи не учитывался, и в сертификате задавался срок 1 год. Теперь 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.

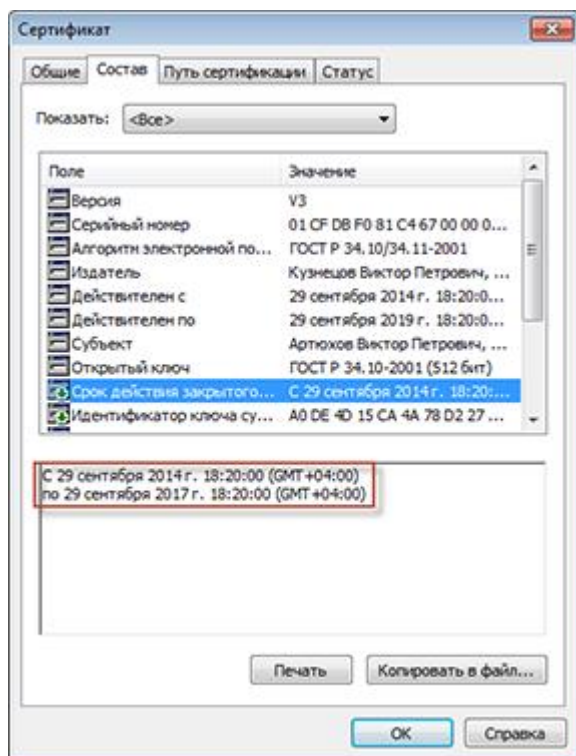


Рисунок 182. Возможность издания сертификатов со сроком действия ключа электронной подписи больше 1 года

- **Отображение дополнительной информации в разделах со списками сертификатов**

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.

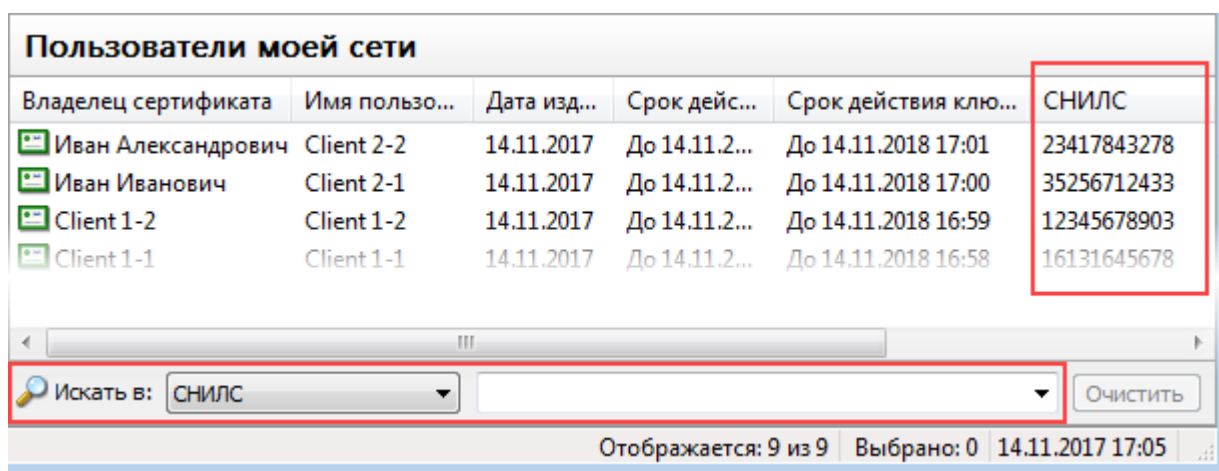


Рисунок 183. Возможность поиска сертификатов по дополнительным полям

- **Работа с сертификатами пользователей, удаленных из сети ViPNet**

Раньше в случае удаления пользователя из сети ViPNet его сертификат перемещался в раздел **Изданные сертификаты > Внешние пользователи**, при этом в лицензионных ограничениях увеличивалось количество изданных сертификатов внешних пользователей. Теперь сертификаты пользователей, удаленных из сети ViPNet, перемещаются в специальный раздел **Изданные сертификаты > Пользователи, удаленные из моей сети**, и количество изданных сертификатов внешних пользователей не изменяется.

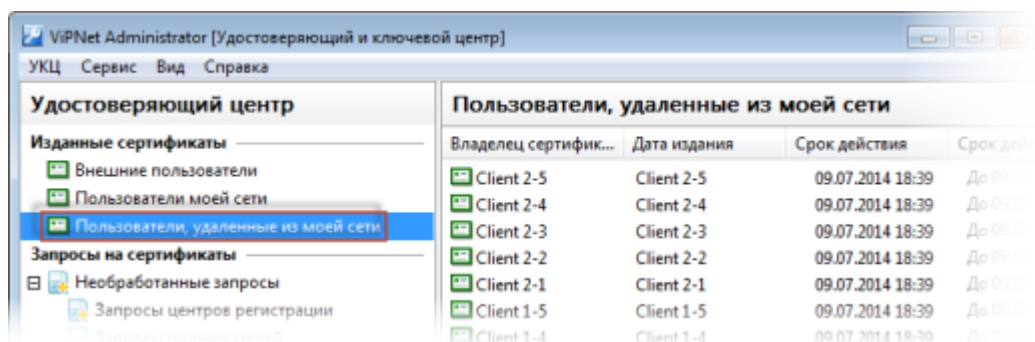


Рисунок 184. Сертификаты пользователей, удаленных из сети ViPNet

В случае необходимости администратор сети может аннулировать, приостановить действие или возобновить действие сертификатов пользователей, удаленных из сети ViPNet.

- **Возможность печати сертификата на нескольких листах**

В новой версии программы возможна печать сертификата на нескольких листах, если его содержимое не помещается на одном листе. Кроме этого, если текст полей сертификата не помещается на одной строке, то он переносится на другую строку. В предыдущих версиях программы текст обрезался по ширине страницы и сертификат мог быть распечатан только на одном листе независимо от его размера.

- **Улучшение внутренней функциональности**

Исправлены незначительные ошибки, выявленные в процессе эксплуатации версии 4.4.

- **Обновление документации и справки**

Доработаны документация и справка для программы ViPNet Удостоверяющий и ключевой центр.

Более подробную информацию о новых возможностях программы см. в документе «Новые возможности ViPNet Administrator. Приложение к документации».

Что нового в версии 4.3

- **Возможность работы в УКЦ в автоматическом режиме**

В новой версии программы появился режим работы, автоматизирующий действия администратора (см. [Режимы работы УКЦ](#)). Данный режим позволяет освободить администратора от выполнения некоторых однообразных операций, а также продолжать работу во время отсутствия администратора на рабочем месте.

При работе в автоматическом режиме формируется очередь операций, блокируются любые действия администратора. Все это позволяет избежать одновременного выполнения нескольких операций, тем самым предотвращая возникновение конфликтов. В предыдущих версиях автоматические операции выполнялись в случайном порядке, параллельно с ними могли выполняться операции вручную. Вследствие этого могли возникать некоторые конфликты (например, могли одновременно создаваться ключи узлов по команде администратора и обновления ключей узлов по расписанию и тому подобное).

Кроме этого, раньше автоматические операции выполнялись в фоновом режиме и администратор об их выполнении мог узнать только из журнала событий. Теперь все автоматические операции отображаются в специальном окне, что позволяет администратору УКЦ следить за ходом их выполнения.

Также настройки всех автоматических операций теперь объединены в одном месте: раздел **Автоматический режим > Действия**. В связи с этим появились изменения в остальных разделах окна **Настройка**. Список автоматических операций был расширен: теперь могут автоматически создаваться ключи узлов; обновляться списки аннулированных сертификатов; импортироваться списки аннулированных сертификатов (CRL) из доверенных сетей и CRL, загруженные сервисом публикации из точек распространения других удостоверяющих центров (описание последних двух функций см. ниже) и другие.

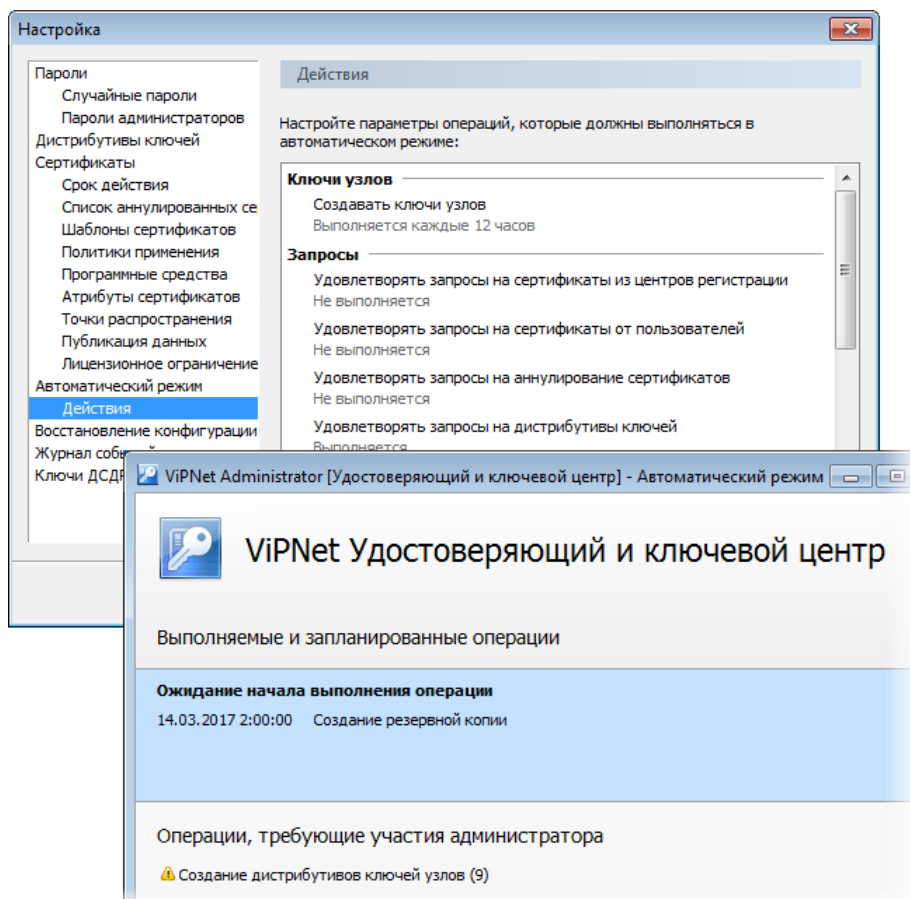


Рисунок 185. Использование автоматического режима работы УКЦ

- **Возможность создания и восстановления резервных копий конфигурации сети при любых способах размещения УКЦ и базы данных SQL**

В новой версии программы реализована 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 только дополнительная настройка программы (см. [Настройка параметров создания резервных копий](#)). Таким образом, теперь создание и восстановление резервных копий конфигурации доступны всегда, независимо от способа размещения программы и базы данных.

- **Управление импортом опубликованных сертификатов и CRL, полученных из программы ViPNet Publication Service**

В предыдущих версиях программы импорт опубликованных сертификатов и CRL, полученных из программы ViPNet Publication Service, выполнялся автоматически, без участия администратора УКЦ. В новой версии администратор может управлять импортом вручную. Это позволяет ему фильтровать данные и импортировать только те, которые необходимы для дальнейшей рассылки на сетевые узлы. Для списков аннулированных сертификатов также предусмотрена возможность настройки автоматического импорта.

- **Выбор криптопровайдера при создании ключей подписи**

В программе ViPNet Удостоверяющий и ключевой центр версии 4.x могут издаваться сертификаты по различным алгоритмам подписи, в том числе по новому алгоритму ГОСТ

34.10-2012. Поскольку каждый алгоритм подписи реализуется конкретным криптопровайдером, в текущей версии программы 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 подписи. Кроме того, теперь при выборе криптопровайдера в процессе издания сертификата администратора, помимо алгоритма подписи, определяется алгоритм хэширования.

- **Задание срока действия сертификата администратора**

В предыдущих версиях программы ViPNet Удостоверяющий и ключевой центр была возможность задания начала и окончания срока действия сертификата администратора УКЦ. В связи с этим могла возникать ситуация, когда для издаваемого сертификата администратора задавалась дата начала действия в будущем, что означало вступление сертификата администратора в действие только по истечении определенного времени. Для сертификата администратора такая ситуация недопустима. Сертификат администратора должен вступать в действие сразу после издания, так как он используется для подписи издаваемых сертификатов пользователей. Поэтому в новой версии программы ViPNet Удостоверяющий и ключевой центр срок действия сертификата администратора УКЦ может быть задан только с настоящего момента.

- **Изменены некоторые термины и названия элементов интерфейса, содержащие эти термины, в соответствии с Федеральным законом 06.04.2011 №63-ФЗ «Об электронной подписи»**

Старый термин	Новый термин	Название элемента интерфейса
Подпись	Электронная подпись	ЭП
Закрытый ключ	Ключ электронной подписи	Ключ ЭП
Открытый ключ	Ключ проверки электронной подписи	Ключ проверки ЭП
Сертификат открытого ключа подписи пользователя	Сертификат ключа проверки электронной подписи	Сертификат
Владелец сертификата	Владелец сертификата ключа проверки электронной подписи	Владелец сертификата
Список отозванных сертификатов (СОС)	Список аннулированных сертификатов (CRL)	CRL
Отзыв сертификата	Аннулирование сертификата	—

В связи с изменениями переработан интерфейс программы.

- **Локализация интерфейса программы**

Новая версия программы ViPNet Удостоверяющий и ключевой центр доступна на русском и английском языках. Для каждой локализации предусмотрен отдельный установочный файл.

- **Возможность обработки запросов на дистрибутивы ключей вручную**

В предыдущих версиях программы обработка запросов на дистрибутивы ключей, созданных в программе ViPNet Registration Point, выполнялась автоматически, без участия администратора УКЦ. В новой версии у администратора появилась возможность обработать запросы вручную (удовлетворить или отклонить). Это позволяет контролировать создание дистрибутивов ключей, поскольку в ЦУСе, через который запросы передаются в УКЦ, отсутствует фильтрация и контроль запросов. Способ обработки запросов зависит от настройки автоматического режима работы программы (см. [Настройка автоматического режима](#)).

Что нового в версии 4.2

- **Настройка плановой смены ключа электронной подписи администратора**

В новой версии появилась функция плановой смены ключа электронной подписи администратора. Срок плановой смены ключа электронной подписи задается администратором в настройках программы и зависит от места хранения ключа электронной подписи. По истечении срока плановой смены производится оповещение и администратор должен создать новый ключ электронной подписи и получить новый сертификат ключа электронной подписи. В противном случае издание сертификатов пользователей в программе становится невозможным.

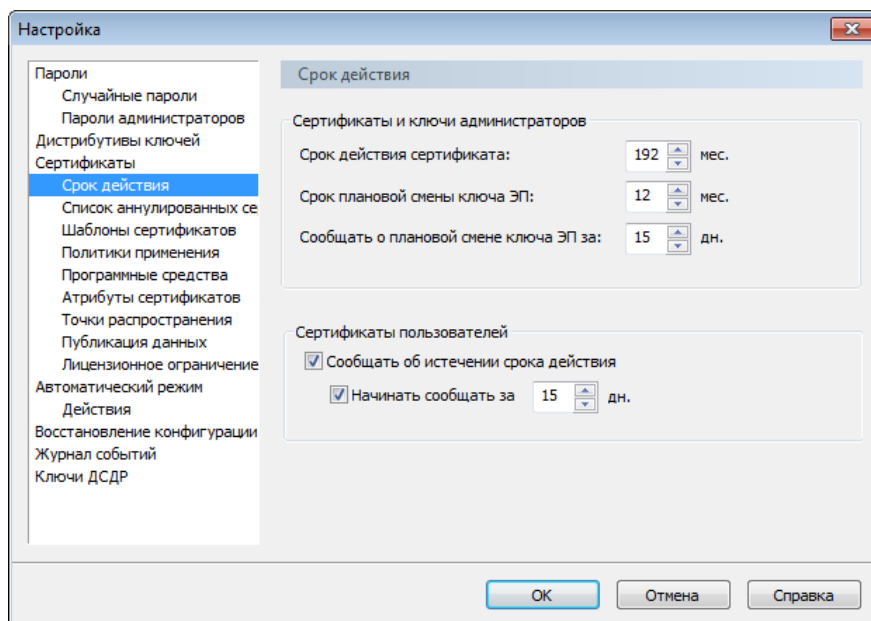


Рисунок 186. Настройка плановой смены ключа электронной подписи администратора

- **Оповещения в главном окне программы**

В новой версии программы 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 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.

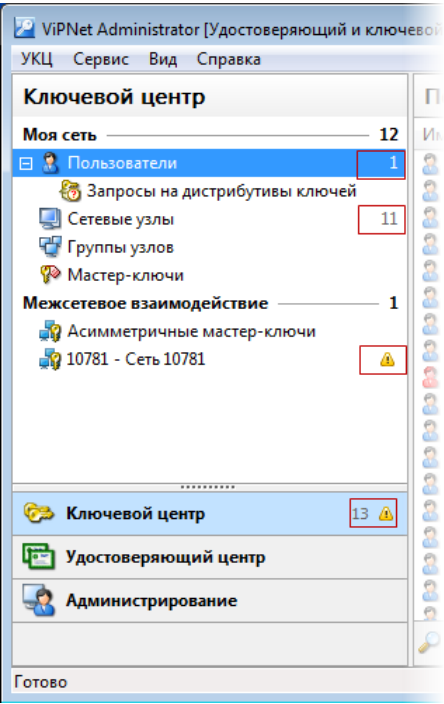


Рисунок 187. Оповещения о необходимости проведения важных операций

- **Работа с большими списками объектов**

В новой версии программы оптимизирована работа с большими списками объектов: сертификатов пользователей, удовлетворенных и отклоненных запросов на сертификаты.

Раньше при запуске программы списки указанных объектов загружались из базы данных полностью. Списки, состоящие более чем из миллиона объектов, не могли быть загружены, поскольку это требовало большого объема оперативной памяти на компьютере УКЦ.

Теперь такие списки загружаются по частям. Каждый раз загружается допустимое количество объектов из списка — 100 объектов. В строке состояния главного окна программы при этом показывается, сколько всего объектов данного типа содержится в базе данных. Просмотреть остальные объекты списка можно только путем их поиска с помощью строки поиска 🔍.

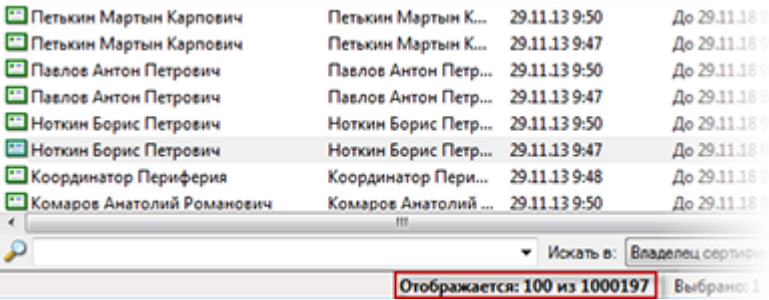


Рисунок 188. Отображение информации о количестве загруженных объектов в строке состояния

- **Сохранение ключа электронной подписи и ключа проверки электронной подписи в файл**

Появилась возможность сохранить ключ электронной подписи и ключ проверки электронной подписи в отдельный файл, если они были созданы при формировании дистрибутива ключей или ключей пользователя. Отдельный файл с ключом электронной подписи и ключом проверки электронной подписи может потребоваться, например, в том случае, если у пользователя нет в наличии внешнего устройства, но при этом ему необходимо получить эти ключи в виде отдельного файла на съемном диске, а не в составе ключей или дистрибутива ключей.



Примечание. Контейнер ключей в виде отдельного файла требуется при работе в программе ViPNet CryptoFile и при разворачивании службы ViPNet CA WebService.

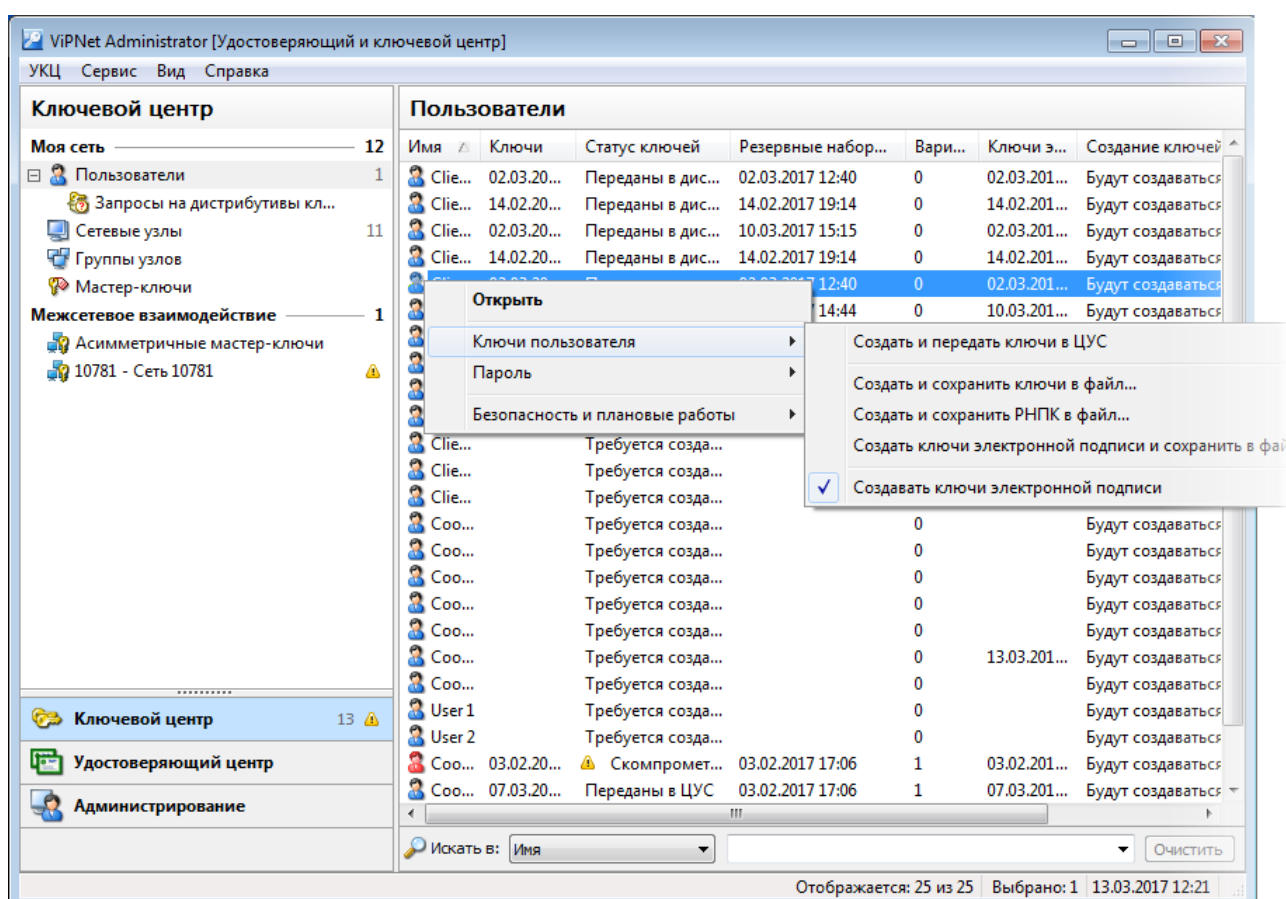


Рисунок 189. Возможность сохранения ключа ЭП и ключа проверки ЭП пользователя в файл

- **Добавление информации о центрах регистрации в издаваемые сертификаты пользователей**

Появилась возможность включать в сертификаты, издаваемые по запросам из центров регистрации, информацию об этих центрах — имя и серийный номер сертификата администратора центра регистрации. Для этого в настройках программы требуется установить соответствующий флажок.

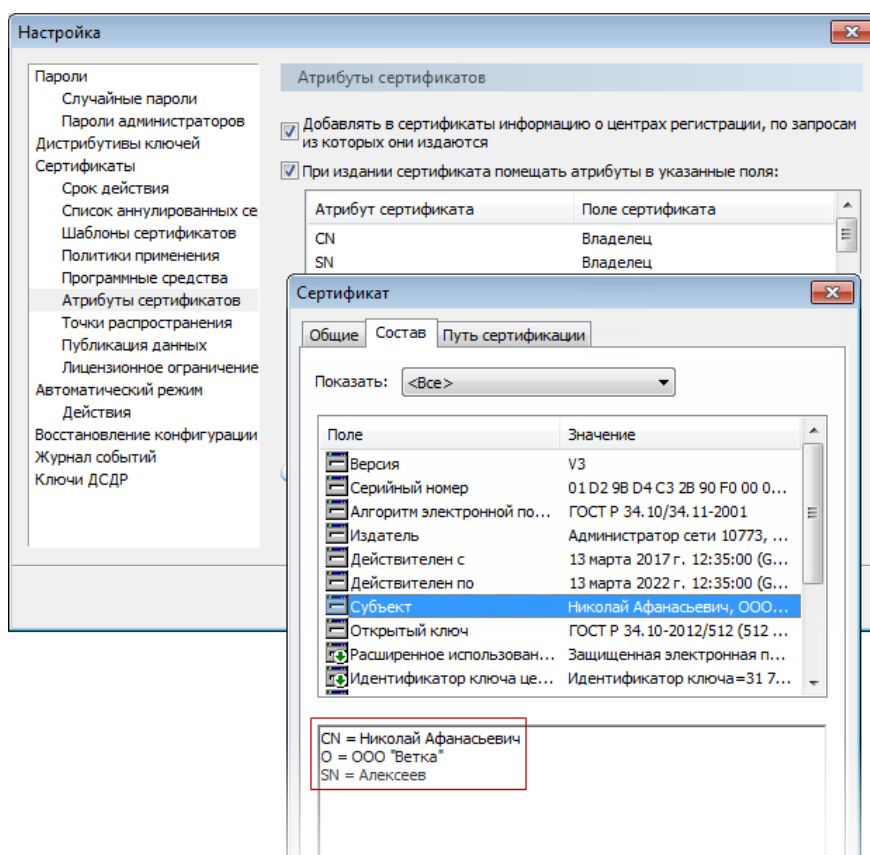


Рисунок 190. Добавление информации о центре регистрации в сертификаты пользователей

- **Возможность печати нескольких сертификатов пользователей**

Появилась возможность отправки на печать сразу нескольких сертификатов пользователей. В предыдущих версиях на печать можно было вывести только один сертификат с помощью кнопки **Печать** в окне просмотра сертификата.

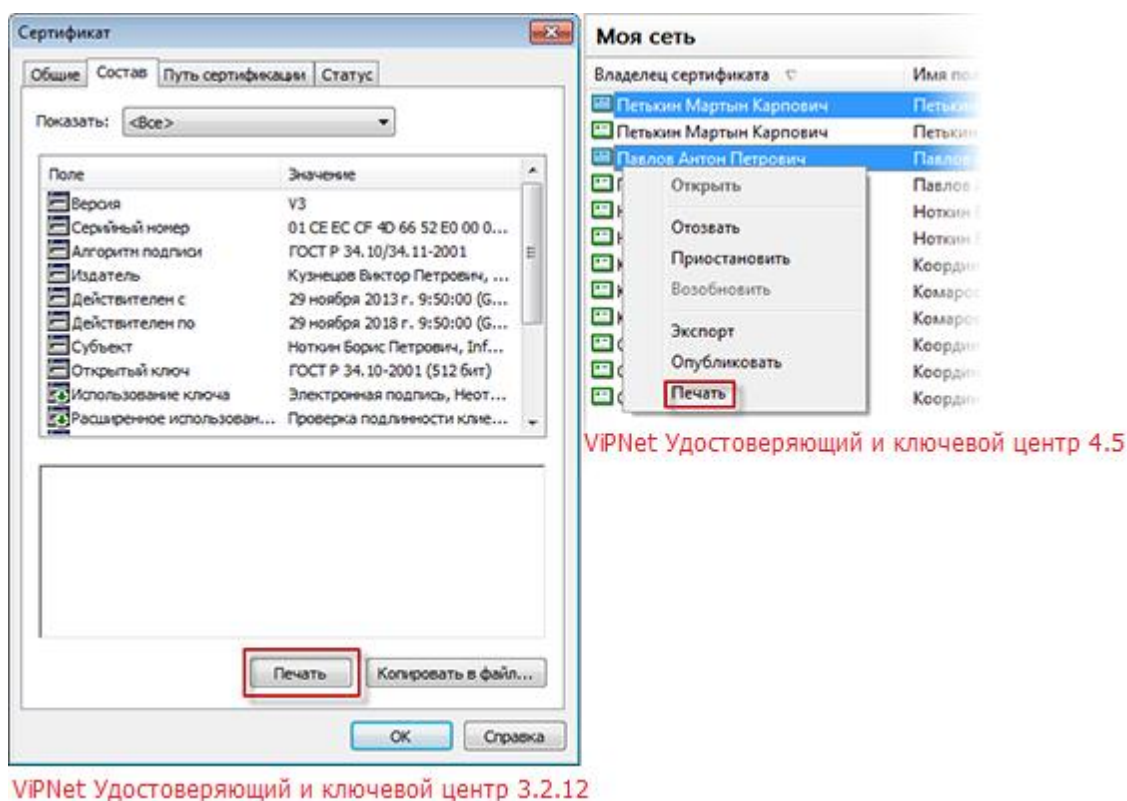


Рисунок 191. Возможность отправки на печать нескольких сертификатов

- Сброс паролей администраторов сетевых узлов

Появилась возможность сброса (удаления) паролей администраторов сетевых узлов. Данная операция может потребоваться в том случае, если пароль искажен или недействителен и если не требуется создавать вместо него новый пароль (менять пароль). В предыдущих версиях пароль можно было только сменить.

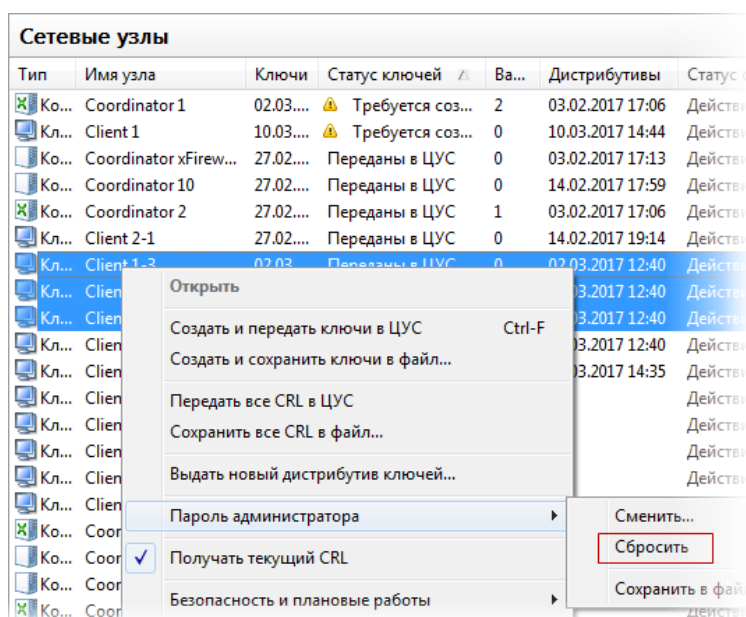


Рисунок 192. Возможность сброса паролей администраторов сетевых узлов и групп узлов

- **Изменение в сценарии смены пароля администратора УКЦ**

Теперь при смене пароля администратора УКЦ требуется указывать текущий пароль. Ранее данная операция была не нужна.

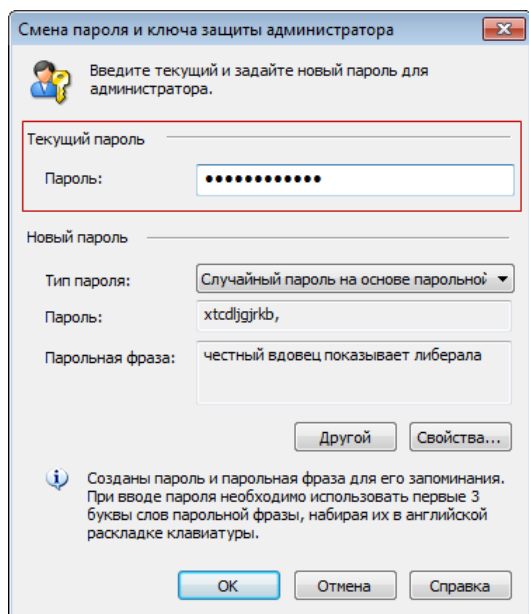


Рисунок 193. Задание текущего пароля администратора УКЦ

- **Изменение в сценарии компрометации ключей пользователя или сетевого узла**

В предыдущих версиях программы при компрометации ключей пользователя автоматически компрометировались ключи его сетевого узла (или узлы, если он зарегистрирован на нескольких узлах), при компрометации ключей узла — ключи всех пользователей, которые на нем зарегистрированы. Теперь компрометация ключей узла при компрометации ключей пользователя и компрометация ключей пользователя при компрометации ключей узла не является обязательным условием. Решение о компрометации ключей того или иного объекта принимается администратором УКЦ.

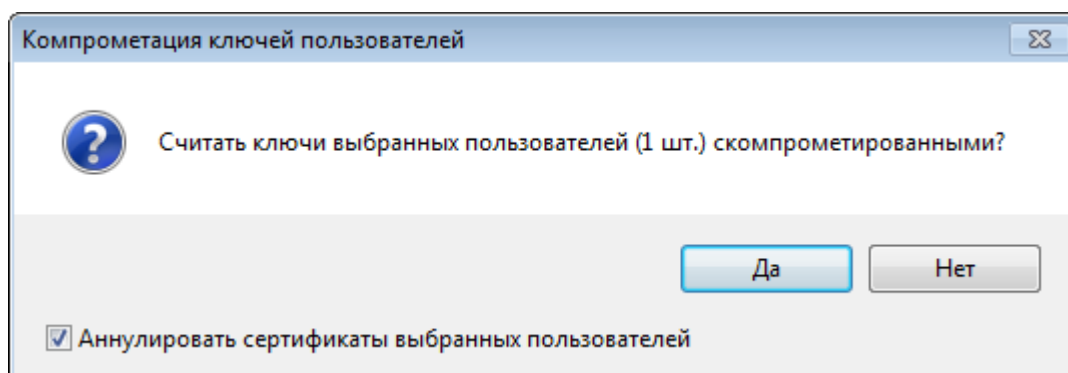


Рисунок 194. Компрометация ключей пользователя вместе с компрометацией ключей его узла

Кроме этого, удалена операция создания ключей при компрометации. В новой версии программы после компрометации требуется создавать стандартные ключи пользователей и ключи узлов. Также теперь при компрометации ключей узла могут создаваться ключи для других узлов, имеющих с ним связь.

Что нового в версии 4.1

- Для более удобной работы с сертификатами и запросами на сертификаты при построении доверительных отношений с другими удостоверяющими центрами вместо подразделов **Изданные сертификаты > Кросс-сертификаты** и **Импортированные сертификаты > Кросс-сертификаты** был создан новый раздел **Кросс-сертификация**, включающий ряд отдельных подразделов.

В раздел **Импортированные сертификаты** был также добавлен подраздел **Сертификаты промежуточных УЦ**, включающий сертификаты всех вышестоящих удостоверяющих центров цепочки сертификации, кроме головного.

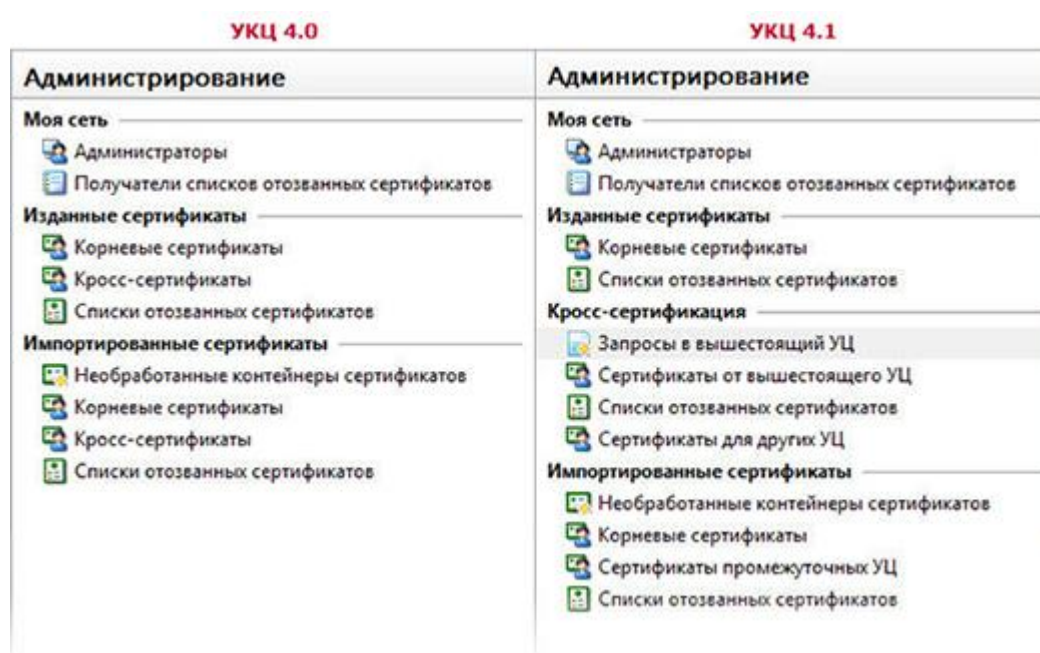


Рисунок 195. Изменение интерфейса в представлении «Администрирование»

- Блокировка отдельных операций со стороны ViPNet Центр управления сетью

Программы ViPNet Удостоверяющий и ключевой центр и ViPNet Центр управления сетью при работе используют одну и ту же базу данных. Из-за этого одновременное выполнение некоторых операций невозможно. В таком случае появляется предупреждение, и выполнение действия блокируется.

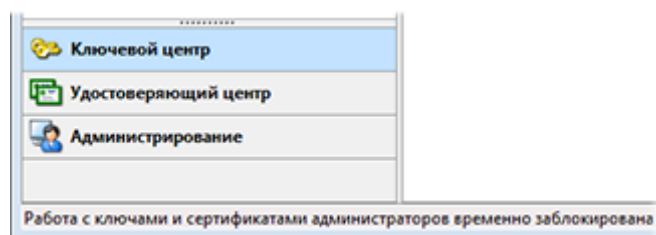


Рисунок 196. Сообщение о временной блокировке работы ViPNet Удостоверяющий и ключевой центр

- **Учёт ключей ДСДР**

В программе ViPNet Удостоверяющий и ключевой центр 4.1 реализована функция учета ключей ДСДР, которая была доступна в версии 3.x. Ключи ДСДР используются, если в состав сети ViPNet входят программно-аппаратные комплексы «ViPNet Координатор-KB2».

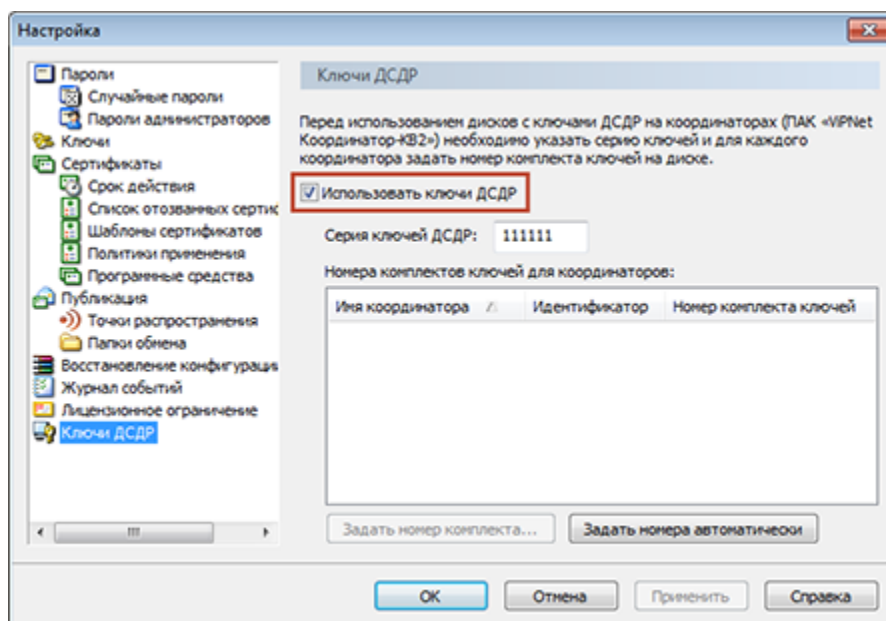


Рисунок 197. Настройка работы с ключами ДСДР

Что нового в версии 4.0

- **Реализация новой архитектуры программного обеспечения ViPNet Administrator**

Реализована новая архитектура программного обеспечения ViPNet Administrator. Теперь УКЦ взаимодействует с программой ViPNet Центр управления сетью только через [базу данных SQL](#). В базе данных хранится вся информация о структуре и настройках сети ViPNet.

- **Изменение графического интерфейса**

Графический интерфейс пользователя значительно переработан. Содержание главного окна программы сгруппировано согласно основным функциям программы.

- **Выделение криптопровайдера ViPNet CSP в отдельную программу**

Из программы установки ViPNet Удостоверяющий и ключевой центр выделена установка криптопровайдера ViPNet CSP. Теперь ViPNet CSP устанавливается только как отдельная программа, что обеспечивает удобство ее обновления независимо от программы ViPNet Удостоверяющий и ключевой центр. Наличие на компьютере установленной программы ViPNet CSP по-прежнему обязательно для работы программы ViPNet Удостоверяющий и ключевой центр.

- **Поддержка новых алгоритмов**

В программе ViPNet Удостоверяющий и ключевой центр 4.0 появилась возможность создавать ключ электронной подписи и ключ проверки электронной подписи, а также асимметричные ключи обмена по алгоритмам нового стандарта ГОСТ Р 34.10-2012.

- **Упрощение процедуры создания ключей пользователей и ключей узлов**

Теперь при создании новых ключей пользователей и ключей узлов нет необходимости каждый раз заново передавать справочники (файлы связи) из ЦУСа в УКЦ. Дата создания ключей сетевых узлов, ключей пользователей, резервных наборов персональных ключей стала доступной для просмотра.

- **Возможность передачи резервных наборов персональных ключей (РНПК) в составе ключей пользователя**

В версии 4.0 появилась возможность создавать ключи пользователя вместе с **резервным набором персональных ключей**. При передаче ключей пользователя на сетевой узел созданный таким образом резервный набор также передается пользователю. В данном случае резервный набор зашифрован не на пароле, а на персональном ключе, и поэтому может быть передан пользователю этим способом.

Для упрощения работы с РНПК теперь нет необходимости в настройке параметров их создания. В версии 4.0 резервный набор всегда содержит 20 персональных ключей, а минимальное число ключей, которые должны оставаться неиспользованными, всегда равно 1.

- **Отказ от операций распаковки ключей и дистрибутивов ключей**

В программе ViPNet Удостоверяющий и ключевой центр версии 3.x можно было выполнить распаковку ключей или дистрибутивов ключей. В связи с невостребованностью данных операций в версии 4.0 они были исключены из списка доступных операций.

- **Изменение настройки параметров аутентификации пользователя и поддерживаемых способов аутентификации**

В версии 4.0 способ аутентификации пользователя настраивается в окне свойств пользователя. Теперь для пользователя можно задать новый тип аутентификации **Устройство**. Кроме того, теперь невозможно задать способ аутентификации с вводом пароля с внешнего устройства (**Пароль на устройстве**), поскольку этот способ перестал отвечать требованиям безопасности.

- **Изменение сроков действия сертификатов**

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. Это изменение внесено в соответствии с требованиями Приказа ФСБ РФ № 796 от 27 декабря 2011 года о том, что срок действия ключа проверки электронной подписи не должен превышать срок действия соответствующего ключа электронной подписи более чем на 15 лет.

- **Увеличение минимальной допустимой длины паролей**

В соответствии с требованиями безопасности минимальная допустимая длина паролей, задаваемых в версии 4.0, увеличена до 8 символов.

- **Отказ от использования универсальных межсетевых мастер-ключей**

В версии 4.0 не поддерживаются универсальные симметричные межсетевые мастер-ключи. Это сделано для обеспечения более высокого уровня безопасности межсетевого

взаимодействия. Универсальные межсетевые мастер-ключи удаляются при конвертации базы данных УКЦ в процессе миграции с версии 3.x.

- **Возможность выбора сертификатов администраторов и списков аннулированных сертификатов, переданных в доверенную сеть**

В программном обеспечении ViPNet Administrator версии 3.x сертификаты администраторов и списки аннулированных сертификатов (CRL) передаются в доверенную сеть в едином контейнере сертификатов. В программе ViPNet Удостоверяющий и ключевой центр версии 4.0 при обработке контейнера сертификатов можно выбрать отдельные сертификаты и соответствующие им списки CRL для применения.

- **Отказ от использования нескольких учетных записей администратора**

В программе ViPNet Удостоверяющий и ключевой центр версии 3.x использование нескольких учетных записей администратора программы было затруднительно по ряду причин. В связи с этим в версии 4.0 заблокирована функция создания нескольких учетных записей администратора УКЦ. Тем не менее, если в вашей сети ранее были созданы несколько учетных записей администратора, при переходе на версию 4.0 они продолжают нормально функционировать.

- **Возможность задания произвольных папок обмена с программой ViPNet Publication Service**

В программе ViPNet Удостоверяющий и ключевой центр версии 3.x для обмена данными с сервисом публикации (узлом, на котором установлена программа ViPNet Publication Service) использовались папки с предопределенными и неизменяемыми именами. В версии 4.0 реализована возможность произвольно назначать папки (в том числе и папки на сетевых дисках).

- **Перенос ряда функций из ЦУСа в УКЦ**

Функции, которые раньше выполнялись в ЦУСе и теперь перенесены в УКЦ:

- назначение права подписи пользователя;
- выбор узлов для рассылки [списков аннулированных сертификатов](#);
- [компрометация ключей](#).

- **Изменение терминологии**

В связи с изменением функциональности и логики работы программы ViPNet Удостоверяющий и ключевой центр изменились некоторые термины и названия элементов интерфейса.

С

Внешние устройства

Общие сведения

Внешние устройства предназначены для хранения [контейнеров ключей](#), которые вы можете использовать для аутентификации, формирования [электронной подписи](#) или для других целей.

На внешнем устройстве могут храниться ключи, созданные по различным алгоритмам в программном обеспечении ViPNet или в сторонних программах. Максимальное количество контейнеров ключей, которое может храниться на одном внешнем устройстве, зависит от объема памяти устройства.

Все операции с контейнерами ключей и внешними устройствами вы можете выполнить в программе ViPNet CSP. Чтобы использовать какое-либо внешнее устройство, на компьютер необходимо установить драйверы этого устройства. Перед записью ключей на устройство убедитесь, что оно отформатировано.

Список поддерживаемых внешних устройств

Таблица 12. Поддерживаемые внешние устройства

Название семейства устройств в ViPNet CSP	Типы и полные названия устройств	Условия и особенности использования семейства устройств
ESMART Token	Смарт-карты и токены типов: • ESMART Token, • ESMART Token ГОСТ.	На компьютере должно быть установлено ПО ESMART PKI Client для Windows (рекомендуемая версия — 4.11). Устройства типа ESMART Token необходимо отформатировать с помощью ПО ESMART PKI Client для Windows с профилем ViPNet2. Перенос ключей подписи с устройства и на устройство ESMART Token ГОСТ невозможен, так как на устройстве используется аппаратная криптография с неизвлекаемым ключом.
Infotecs Software Token	ViPNet SoftToken — программная реализация стандарта PKCS#11.	На компьютере должен быть установлен компонент ViPNet SoftToken (входит в состав ПО ViPNet OpenSSL). С помощью программы <code>token_manager.exe</code> должен быть создан программный токен. Подробнее см. в документе «ViPNet SoftToken. Руководство разработчика» > «Использование утилиты <code>token_manager</code> для работы с программными токенами».
SafeNet eToken (eToken Aladdin)	Персональные электронные ключи и смарт-карты производства компаний Gemalto (SafeNet) и «Аладдин Р.Д.»: • Gemalto SafeNet eToken 5100/5105, 5200/5205, 7300, • eToken PRO, • eToken NG-OTP, NG-FLASH, • eToken 5300, • SafeNet eToken 5110, • Gemalto SafeNet eToken 4100.	На компьютере с Windows 10 должен быть установлен SafeNet Authentication Client (рекомендуемая версия — 10.6.146). На компьютере с другой ОС — PKI Client версии 5.1 SP1 или SafeNet Authentication Client (рекомендуемая версия — 10.6.146). Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC-совместимым устройством считывания карт. Примечание. Установка «Единый Клиент JaCarta» и SafeNet Authentication Client на один компьютер не рекомендуется производителем. Это может вызвать ошибки при выполнении криптографических операций с использованием устройств из семейства SafeNet eToken (eToken Aladdin).

Название семейства устройств в ViPNet CSP	Типы и полные названия устройств	Условия и особенности использования семейства устройств
ViPNet HSM	Программно-аппаратный комплекс ViPNet HSM 3.3 производства АО «ИнфоТеКС».	На компьютере должно быть установлено ViPNet HSM SDK. В ViPNet CSP необходимо задать параметры подключения к серверу ViPNet HSM.
JaCarta	Персональные электронные ключи и смарт-карты производства компании «Аладдин Р.Д.»: • JaCarta-2 SE, • JaCarta-2 SF, • JaCarta SF/ГОСТ, • JaCarta-2 SE/PKI/ГОСТ, • JaCarta-2 PKI/BIO/ГОСТ, • JaCarta PKI/BIO, • JaCarta PKI, • JaCarta LT, • JaCarta PKI/ГОСТ, • JaCarta PRO, • JaCarta-2 PKI/ГОСТ, • JaCarta-2 ГОСТ, • JaCarta-2 PRO/ГОСТ.	Рекомендуемая версия прошивки для устройств JaCarta-2 — 2.5.5. На компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая минимальная версия — 2.13). Перенос ключей подписи с апплетов «Криптотокен» и «Криптотокен 2 ЭП» (модели JaCarta со словом «ГОСТ» в названии) и на эти апплеты невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом. Работа с апплетом PRO через ПО «Единый Клиент JaCarta» версии 2.12 не поддерживается. Необходимо установить последнее обновление ПО «Единый Клиент JaCarta» с сайта производителя либо обратиться в службу поддержки компании «Аладдин Р.Д.».
Rutoken	Электронные идентификаторы производства компании «Актив»: • Рутокен ЭЦП 2.0 Flash, • Рутокен ЭЦП 2.0 Touch, • Рутокен ЭЦП 2.0, • Рутокен ЭЦП 2.0 3000, • Рутокен Lite, • Рутокен ЭЦП PKI (2.0), • Рутокен ЭЦП 2.0 2100, • Рутокен ЭЦП 3.0 3100, • Рутокен ЭЦП 3.0 3220.	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.13.0.0). Перенос ключей подписи с устройств, а также на устройства Рутокен ЭЦП 2.0 невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.

Название семейства устройств в ViPNet CSP	Типы и полные названия устройств	Условия и особенности использования семейства устройств
Rutoken S	Электронные идентификаторы Рутокен S производства компании «Актив».	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.13.0.0).
Foros	Смарт-карты и токены R301 Foros для ViPNet CSP производства компании «СмартПарк».	На компьютере должен быть установлен драйвер ForosMaster (рекомендуемая версия — 1.0.0.12). Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.



Примечание. Список поддерживаемых операционных систем для каждого из приведенных устройств см. на официальном сайте производителя этого устройства.

Алгоритмы и функции, поддерживаемые внешними устройствами

Таблица 13. Алгоритмы и функции, поддерживаемые внешними устройствами

Название семейства устройств в ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Работа с ДСЧ в ViPNet CSP	Поддержка PKCS#11
ESMART Token	ESMART Token — отсутствует; ESMART Token ГОСТ — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ 256 бит)	ESMART Token — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 ESMART Token ГОСТ — отсутствует	Да	Да
Infotecs Software Token	Изолированная программная реализация: ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012		Нет	Да
SafeNet eToken (eToken Aladdin)	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
ViPNet HSM	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	отсутствует	Нет	Да
JaCarta (устройства JaCarta PKI, JaCarta SE, JaCarta LT, JaCarta PKI/ГОСТ и JaCarta-2 PKI/ГОСТ с апплетом Laser)	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да

Название семейства устройств в ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Работа с ДСЧ в ViPNet CSP	Поддержка PKCS#11
JaCarta (устройства JaCarta PKI/ГОСТ и JaCarta-2 PKI/ГОСТ с апплетом ГОСТ, JaCarta-2 ГОСТ)	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ 256 бит)	отсутствует	Да	Да
Rutoken	Рутокен ЭЦП 2.0 — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012; Рутокен Lite — отсутствует	Рутокен ЭЦП 2.0 — отсутствует; Рутокен Lite — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	ЭЦП 2.0 — да; Lite — нет	Да
Rutoken S	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да

Стандарт PKCS#11 (также известный как Cryptoki) — один из стандартов семейства PKCS (Public Key Cryptography Standards — криптографические стандарты ключа проверки электронной подписи), разработанных компанией RSA Laboratories. Стандарт определяет независимый от платформы интерфейс API для работы с криптографическими устройствами идентификации и хранения данных.

Выработка ключей шифрования (функция `C_DeriveKey` интерфейса PKCS#11) поддерживается не всеми перечисленными устройствами. Для получения более подробной информации см. документацию к устройству.



Получение CRL из локальных точек распространения

В процессе электронного документооборота для проверки подписи требуется наличие актуальных списков аннулированных сертификатов (CRL). В зависимости от того, каким образом устроен электронный документооборот в сети, получение CRL может производиться по-разному, например:

- путем скачивания из внешних точек распространения, указанных в сертификатах, при проверке электронной подписи;
- с помощью рассылки в составе обновлений ключей узлов;
- с помощью периодического опроса точек распространения, заданных администратором сети или локально на узле;
- с помощью сетевых хранилищ CRL.

Первый способ является стандартным способом для сетей с инфраструктурой PKI. Второй способ является стандартным для сетей ViPNet, использующих такие средства электронного документооборота, как ViPNet Деловая почта, ViPNet CryptoService, ViPNet Dispatcher и другие. Однако при большом масштабе сетей ViPNet этот способ может быть весьма затратным вследствие массовых рассылок CRL (особенно при невысокой скорости передачи данных в сети). Третий и четвертый способы используются, когда первые два способа получения CRL неприменимы: точки распространения в сертификатах не указаны или отсутствует доступ к ним, либо сеть ViPNet достаточно велика для рассылки CRL.

Если во взаимодействующих организациях используется различное ПО для документооборота, то может использоваться комбинация нескольких способов получения CRL. Если документооборот осуществляется между организациями, в которых развернуты защищенные сети ViPNet, то они могут обмениваться CRL с помощью передаваемой межсетевой информации, и затем распространять обновления CRL на сетевые узлы.

Рассмотрим подробнее использование третьего и четвертого способов получения CRL на следующем примере.

Имеются две организации А и В, между которыми осуществляется электронный документооборот. Из организации В в организацию А с определенной периодичностью поступают почтовые сообщения, заверенные электронной подписью. В организации А развернута защищенная сеть ViPNet с большим количеством узлов. В организации В развернута только PKI-инфраструктура, при этом ПО ViPNet не используется.

Передача актуальных CRL из организации В в организацию А с помощью межсетевой информации невозможна — в организации В нет развернутой сети ViPNet, которая могла бы стать доверенной для сети в организации А. Поэтому получить CRL, выпущенные удостоверяющим центром организации В, можно в специальной внешней точке распространения. Но при этом узлы сети ViPNet, на которые поступают почтовые сообщения, доступа к внешней точке распространения не имеют. Импорт списков из внешней точки распространения в сеть ViPNet организовать возможно, но их распространение по узлам сети будет трудоемким. Как в данном случае можно обеспечить получение CRL узлами сети ViPNet организации А из внешней точки распространения?

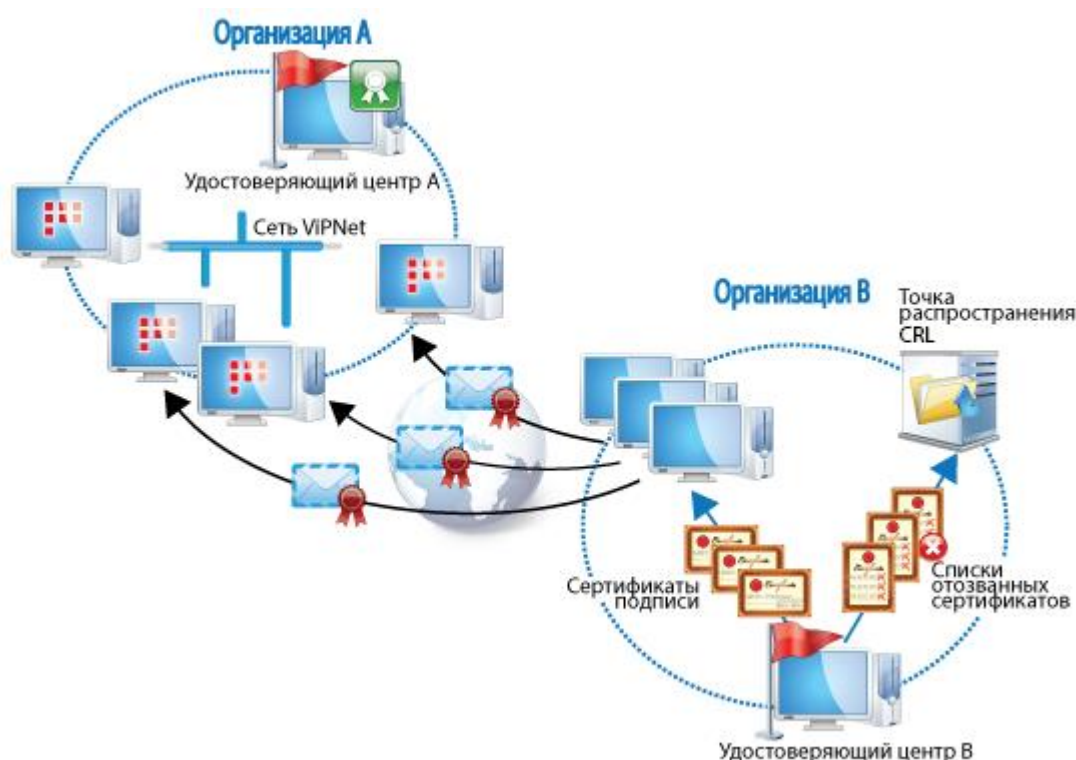


Рисунок 198. Пример организации электронного документооборота между несколькими организациями

С помощью технологии ViPNet данную задачу можно решить третьим способом, а именно: создать в сети организации А точку распространения или сетевое хранилище — место размещения CRL, к которому будут иметь доступ остальные узлы, и с помощью сервиса публикации публиковать в него CRL, скачанные из внешней точки. При этом информирование узлов сети о том, что при проверке подписи следует обращаться к данному месту хранения для получения CRL (если внешняя точка распространения недоступна), будет производиться с помощью файла `crl-update-setting.ini`.

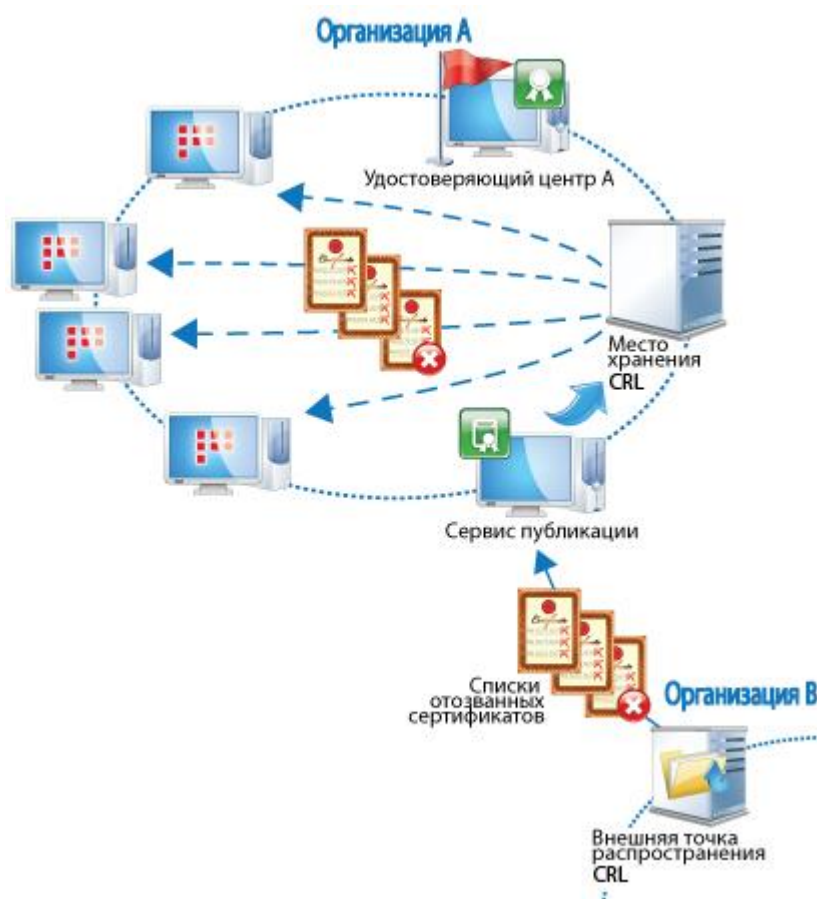


Рисунок 199. Пример реализации скачивания СОС из внешних точек распространения

Файл `crl-update-setting.ini` формируется на узле администратора сети (в процессе первичной инициализации программы ViPNet Удостоверяющий и ключевой центр) и на остальные узлы передается при рассылке CRL. В нем указываются точки распространения и сетевые хранилища, к которым могут обращаться узлы сети для получения списков отозванных сертификатов, а также задаются параметры поиска CRL в них.

Таким образом, для реализации описанной выше схемы получения CRL требуется выполнить следующие действия:

- 1 Организовать место хранения списков отозванных сертификатов в сети ViPNet.
- 2 С помощью сервиса публикации организовать регулярное скачивание CRL сторонних удостоверяющих центров из внешней точки распространения в место хранения CRL, доступное внутри организации. См. указания в документе «ViPNet Publication Service. Руководство администратора».
- 3 Подготовить файл `crl-update-setting.ini`. См. указания в разделах ниже.
- 4 На все узлы сети разослать CRL. См. указания в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

Подготовка файла crl-update-settings.ini

В файле `crl-update-setting.ini` вы можете указать информацию о местах размещения списков аннулированных сертификатов и настроить параметры поиска CRL в них следующим образом:

- 1 Откройте файл `crl-update-settings.ini` в текстовом редакторе. Файл расположен в папке установки ViPNet Удостоверяющий и ключевой центр в подпапке `\ViPNet Administrator\KC\ini`.

- 2 Чтобы добавить информацию о месте хранения CRL, выполните следующие действия:

Если в качестве места хранения выступает сетевое хранилище:

- Создайте секцию с названием `[NetworkCrlStore-n]`, где `n` в названии секции — номер хранилища. Нумерация секций (хранилищ) должна начинаться с нуля: `[NetworkCrlStore-0]`, `[NetworkCrlStore-1]`. В противном случае не все секции будут учитываться при обработке.
- В созданной секции в виде параметра `URL` укажите сетевой путь, по которому доступно хранилище. Количество вводимых символов не должно быть меньше 6 и больше 2083. Например, сетевой путь может быть таким:
`URL=ldap://192.168.45.144:389/CN=CDP,DC=kd,DC=local`

Если в качестве места хранения выступает точка распространения:

- Создайте секцию с названием `[CDP-n]`, где `n` в названии секции — номер точки. Нумерация секций (точек) должна начинаться с нуля: `[CDP-0]`, `[CDP-1]`. В противном случае не все секции будут учитываться при обработке.
- В созданной секции в виде параметра `URL` укажите сетевой путь, по которому доступна точка распространения. Количество вводимых символов не должно быть меньше 6 и больше 2083. Например, сетевой путь может быть таким:
`URL=ftp://192.168.12.158/crl/5606-kid939FB75998C4D8044A4E341C024C4D73650C0AD6/revokedCerts.crl.`
- При необходимости для указанной точки распространения задайте следующие дополнительные параметры:
 - `IntervalInMinutes` — интервал опроса данной точки распространения (в минутах). По умолчанию значение параметра равно 1440 (1 сутки), минимальное значение равно 1.
 - `NextUpdate` — дата и время следующего опроса.
 - `Enabled` — параметр отключения, либо включения точки распространения в момент опроса. Если `Enabled=1`, то точка доступа будет опрашиваться. Если `Enabled=0`, то опрос данной точки осуществляться не будет.
 - `IssuerName` — имя издателя CRL в формате X.500. Фактически данный параметр не используется и может содержать любое имя в формате X.500, которое может и не

соответствовать реальному издателю. Для простоты можно указать в качестве значения «cn=x». Пустое значение данного параметра недопустимо.

3 В секции [CrlUpdateAtSigVerification] задайте параметры поиска CRL при проверке электронной подписи:

- Укажите значение параметра `AllowCrlUpdate` равным 1, чтобы расширить поиск CRL в заданных местах хранения. Если значение параметра будет равно 0, то поиск CRL производиться не будет.
- Укажите значение параметра `ForceCrlUpdate` равным 1, чтобы форсировать поиск CRL (то есть производить поиск CRL даже при его наличии на узле с неистекшим сроком действия). Рекомендуется указывать такое значение в том случае, если производится частое обновление CRL (в основном это зависит от политики безопасности, применяемой в компании).
- Укажите значение параметра `AllowUsingCDP` равным 1 для возможности опроса точек распространения, заданных в сертификатах. Если установить значение 0, то опрос точек распространения производиться не будет.
- Укажите значение параметра `AllowUsingNetworkCRLStores` равным 1 для возможности опроса сетевых хранилищ, заданных в данном файле. Если установить значение 0, то опрос хранилищ данных производиться не будет.

4 В секции [PeriodicallyCrlUpdate] задайте параметры периодического обновления CRL, не в момент проверки электронной подписи:

- Укажите значение параметра `AllowCrlUpdate` равным 1 для выполнения периодического обновления CRL на узле. В этом случае будет производиться опрос точек распространения, заданных в данном файле.
- Укажите значение параметра `CollectLocallyDetectedCdp` равным 1 для автоматического добавления найденных при проверке электронной подписи точек распространения в список опроса, который хранится в специальном отдельном файле `locally-detected-cdp.ini`. То есть если при проверке электронной подписи была найдена новая точка распространения, то в этом случае она будет добавлена в список для дальнейшего периодического опроса.

5 Сохраните внесенные изменения и закройте файл.

С примером составления файла `crl-update-settings.ini` вы можете ознакомиться в разделе ниже.

Пример составления файла crl-update-settings.ini

Ниже приведен пример того, как может быть составлен файл `crl_update_settings.ini`:

```
[CrlUpdateAtSigVerification]
AllowCrlUpdate=1
ForceCrlUpdate=0
AllowUsingCDP=1
AllowUsingNetworkCRLStores=1

[PeriodicallyCrlUpdate]
AllowCrlUpdate=1
CollectLocallyDetectedCdp=0

[NetworkCrlStore-0]
URL=ldap://192.168.45.144:389/CN=CDP,DC=kd,DC=local

[CDP-0]
URL=ftp://192.168.12.158/crl/5606-kid939FB75998C4D8044A4E341C024C4D73650C0AD6/revokedCerts.crl
IssuerName=O="ООО Ветка",OU=Удостоверяющий и ключевой центр,Т=Администратор,СN=Беляев
Виталий Петрович
Enabled=1
NextUpdate=1344591938
IntervalInMinutes=1

[CDP-1]
URL=ldap://192.168.45.144/CN=kidF7CBBC571746304F0709C8C5EC7FF0B73AC9AF95,CN=9996,CN=CDP,DC=kd,DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint
IssuerName=O="ООО Ветка",OU=Удостоверяющий и ключевой центр,Т=Администратор,СN=Беляев
Виталий Петрович
Enabled=1
NextUpdate=1344591879
IntervalInMinutes=1
```



Региональные настройки

Для корректного отображения русской локализации интерфейса программ ViPNet в русифицированных ОС Microsoft Windows английской локализации необходимо установить поддержку кириллицы для программ, не поддерживающих Юникод. Эти настройки рекомендуется производить до установки самой программы.

Данные настройки также понадобятся сделать, если установлен русскоязычный MUI (Multilanguage User Interface). Это значит, что ядро операционной системы английское, а русский язык для интерфейса и файлов справки был установлен позже. В этом случае региональные настройки по умолчанию английские и требуют изменения.



Внимание! Для изменения региональных настроек вы должны обладать правами администратора операционной системы.

Региональные настройки в Windows

Чтобы установить поддержку кириллицы:

- 1 Откройте панель управления (Control Panel) и в категории **Часы, язык и регион (Clock, Language, and Region)** выберите параметр **Изменение форматов даты, времени и чисел (Change date, time, or number formats)**.
- 2 В окне **Регион (Region)** перейдите на вкладку **Дополнительно (Administrative)**.

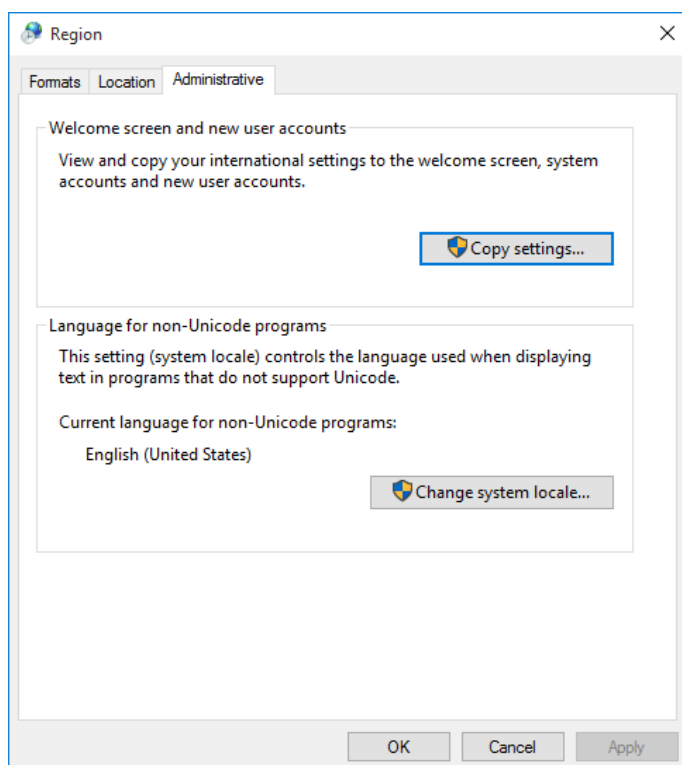


Рисунок 200. Дополнительные языковые параметры

- 3 На вкладке **Дополнительно (Administrative)** нажмите кнопку **Изменить язык системы (Change system locale)**.
- 4 В появившемся окне в списке выберите **Русский (Россия) (Russian (Russia))**.

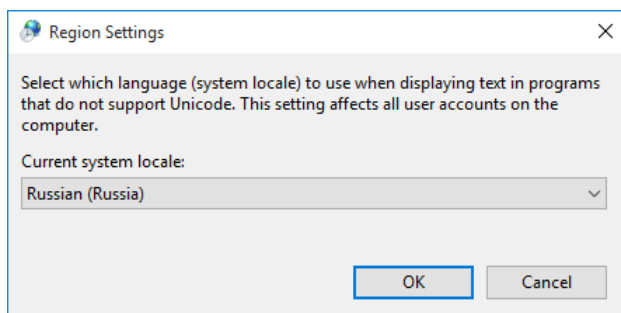


Рисунок 201. Выбор языка системы

- 5 Нажмите кнопку **ОК**. Перезагрузите компьютер.
- 6 Дождитесь завершения перезагрузки компьютера, откройте панель управления (Control Panel) и в категории **Часы, язык и регион (Clock, Language, and Region)** выберите параметр **Изменение форматов даты, времени и чисел (Change date, time, or number formats)**.
- 7 В окне **Регион (Region)** перейдите на вкладку **Дополнительно (Administrative)**.
- 8 На вкладке **Дополнительно (Administrative)** нажмите кнопку **Копировать параметры (Copy settings)**.
- 9 В открывшемся окне в списке **Копировать текущие параметры в (Copy your current settings to)** установите флажок **Экран приветствия и системные учетные записи (Welcome screen and system accounts)** и нажмите кнопку **ОК**.

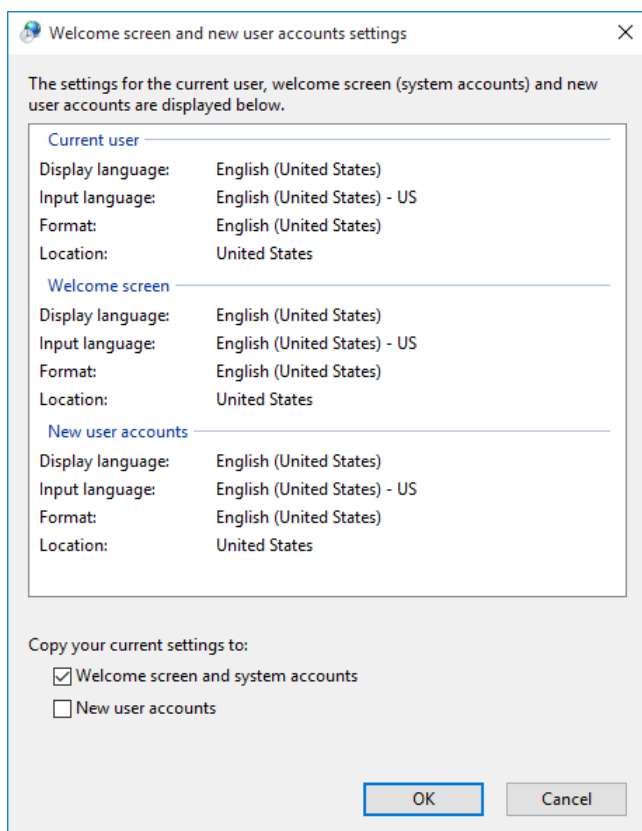


Рисунок 202. Копирование параметров

Также для исключения проблем с кодировкой в некоторых системах мы рекомендуем выполнить следующие действия:

- 1 В окне **Регион (Region)** на вкладке **Форматы (Formats)** в списке **Формат (Format)** выберите **Русский (Россия) (Russian (Russia))**.

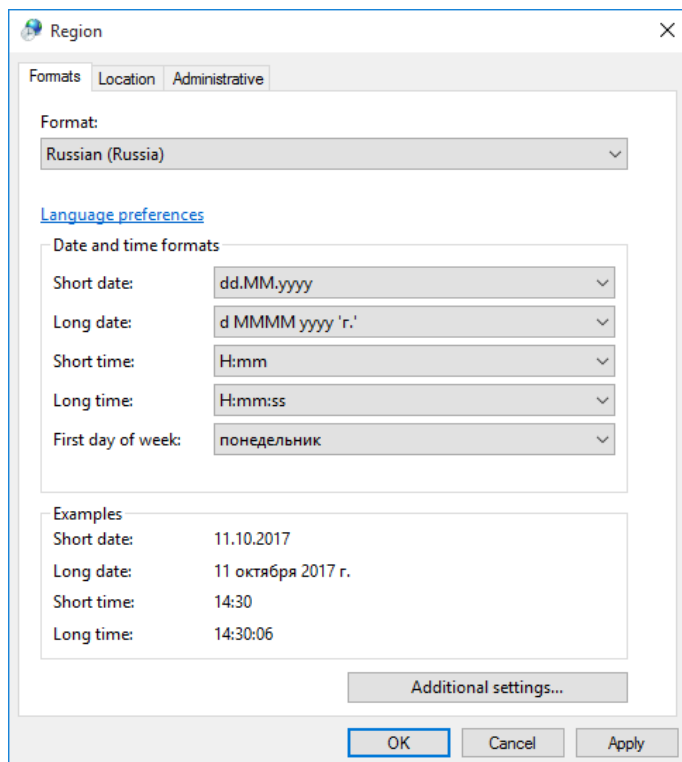


Рисунок 203. Настройка форматов

- 2 В окне **Регион (Region)** на вкладке **Местоположение (Location)** в списке **Основное расположение (Home location)** выберите **Россия (Russia)**.



Примечание. В Windows 10 версии 1809 и выше нет вкладки **Location**, поэтому указанный параметр настраивать не нужно.

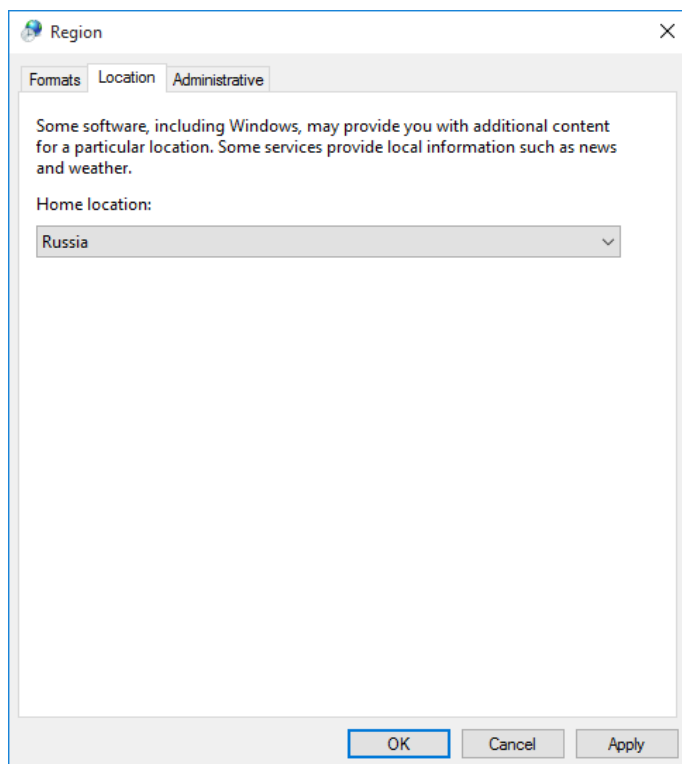


Рисунок 204. Выбор текущего расположения



Перечень событий УКЦ, регистрируемых в журнале событий Windows

В этом приложении представлен перечень всех событий программы ViPNet Удостоверяющий и ключевой центр, регистрируемых в журнале событий, для разной степени детализации записей. Настройка журнала событий описана в разделе [Настройка параметров журнала событий](#).

Таблица 14. События УКЦ для различных уровней детализации записей журнала событий

Название события	Минимальная	Обычная	Максимальная
Запущен процесс аудита событий	•	•	•
Завершен процесс аудита событий	•	•	•
Введен неверный пароль при аутентификации	•	•	•
Вход в систему	•	•	•
Выход из системы	•	•	•
Вход в режим администратора	•	•	•
Выход из режима администратора	•	•	•
Введен неверный пароль администратора	•	•	•
Проведено обновление ключей узла	•	•	•
Проведено обновление ключей пользователя	•	•	•
Ошибка при обновлении ключей узла	•	•	•

Название события	Минимальная	Обычная	Максимальная
Ошибка при обновлении ключей пользователя	•	•	•
Автоматический перезапуск приложения для применения обновления ключей	•	•	•
Автоматический вход в систему для применения обновления ключей	•	•	•
Изменен текущий сертификат ключа проверки электронной подписи пользователя	•	•	•
Ошибка при смене текущего сертификата ключа проверки электронной подписи пользователя	•	•	•
Сертификат введен в действие	•	•	•
Ошибка при вводе в действие сертификата	•	•	•
Смена места хранения ключа электронной подписи пользователя	•	•	•
Ошибка при смене места хранения ключа электронной подписи пользователя	•	•	•
Изменены настройки параметров безопасности	•	•	•
Ошибка при изменении настроек параметров безопасности	•	•	•
Изменен способ аутентификации	•	•	•
Ошибка при изменении способа аутентификации	•	•	•
Аутентификация администратора	•	•	•
Неудачная аутентификация администратора	•	•	•
Создание администратора	•	•	•
Ошибка создания администратора	•	•	•
Удаление администратора	•	•	•
Нормальное завершение работы УКЦ	•	•	•
Повторный запуск УКЦ	•	•	•
Создание мастер-ключа своей сети	•	•	•
Ошибка создания мастер-ключа своей сети	•	•	•
Создание сертификата администратора	•	•	•
Ошибка создания сертификата администратора	•	•	•
Смена ключевого носителя администратора	•	•	•
Ошибка смены ключевого носителя администратора	•	•	•

Название события	Минимальная	Обычная	Максимальная
Создание запроса на кросс-сертификат	•	•	•
Ошибка создания запроса на кросс-сертификат	•	•	•
Создание для сертификата администратора запроса к вышестоящему УЦ	•	•	•
Ошибка создания для сертификата администратора запроса к вышестоящему УЦ	•	•	•
Смена пароля администратора	•	•	•
Ошибка смены пароля администратора	•	•	•
Смена ключа защиты УКЦ	•	•	•
Ошибка смены ключа защиты УКЦ	•	•	•
Смена пароля администратора группы сетевых узлов	•	•	•
Ошибка смены пароля администратора группы сетевых узлов	•	•	•
Смена варианта персонального ключа пользователя	•	•	•
Смена варианта ключей сетевого узла	•	•	•
Компрометация ключей пользователя	•	•	•
Конфигурация восстановлена из резервной копии	•	•	•
Ошибка восстановления конфигурации из резервной копии	•	•	•
Инициализация приложения успешно пройдена	•	•	•
Неуспешная инициализация приложения	•	•	•
Смена имени администратора	•	•	•
Выдача нового дистрибутива ключей сетевого узла	•	•	•
Ошибка при выдаче нового дистрибутива ключей сетевого узла	•	•	•
Издан сертификат пользователя		•	•
Ошибка издания сертификата пользователя		•	•
Принят запрос на сертификат пользователя		•	•
Ошибка принятия запроса на издание сертификата		•	•
Дубликат запроса на сертификат пользователя		•	•
Отклонен запрос на издание сертификата		•	•
Принят запрос на аннулирование сертификата		•	•

Название события	Минимальная	Обычная	Максимальная
Ошибка принятия запроса на аннулирование сертификата		•	•
Дубликат запроса на аннулирование сертификата		•	•
Отклонен запрос на аннулирование сертификата		•	•
Издан CRL		•	•
Удовлетворен запрос на аннулирование сертификата		•	•
Ошибка создания ключевого набора сетевого узла		•	•
Созданы ключи узла		•	•
Ошибка создания обновления информации CRL для сетевого узла		•	•
Создано обновление информации CRL для сетевого узла		•	•
Сертификат аннулирован		•	•
Сертификат приостановлен		•	•
Сертификат возобновлен		•	•
Удовлетворен запрос на сертификат		•	•
Создана резервная копия		•	•
Ошибка создания резервной копии		•	•
Смена пароля администратора сетевого узла		•	•
Ошибка смены пароля администратора сетевого узла		•	•
Переключение в автоматический режим		•	•
Переключение в ручной режим		•	•
Смена пароля пользователя		•	•
Изменение прав пользователей			•
Созданы и переданы в ЦУС ключи пользователя			•
Созданы и переданы в ЦУС ключи узла			•
Создан межсетевой мастер-ключ			•
Импортирован межсетевой мастер-ключ			•
Импортирован сертификат администратора доверенной сети			•
Импортирован CRL доверенной сети			•
Ключи узла сохранены в файл			•

Название события	Минимальная	Обычная	Максимальная
Ошибка создания ключевого диска пользователя			•
Ошибка создания ключевого набора сетевого узла			•
Ошибка создания межсетевого мастер-ключа			•
Ошибка импортирования межсетевого мастер-ключа			•
Ошибка импортирования сертификата администратора доверенной сети			•
Ошибка импортирования CRL доверенной сети			•
Ошибка экспортирования ключевого носителя			•
Печать пароля пользователя			•
Ошибка при печати пароля пользователя			•
Смена способа аутентификации пользователя			•
Смена сертификата аутентификации пользователя			•
Удаление межсетевого мастер-ключа			•
Ошибка удаления межсетевого мастер-ключа			•



Основы криптографии

Криптография используется для решения трех основных задач:

- обеспечение конфиденциальности данных;
- контроль целостности данных;
- обеспечение подлинности авторства данных.

Первая задача решается с помощью симметричных алгоритмов шифрования. Для решения второй и третьей задач требуется использование асимметричных алгоритмов и электронной подписи.

В данном разделе содержится упрощенное описание алгоритмов с симметричным ключом, с асимметричным ключом, электронной подписи, а также приводятся примеры использования этих алгоритмов в информационных системах (приведенные примеры не относятся к технологии ViPNet).

Симметричное шифрование

В симметричных алгоритмах для зашифрования и расшифрования применяется один и тот же криптографический ключ. Для того чтобы и отправитель, и получатель могли прочесть исходный текст (или другие данные, не обязательно текстовые), обе стороны должны знать ключ алгоритма.

На схеме ниже изображен процесс симметричного зашифрования и расшифрования.

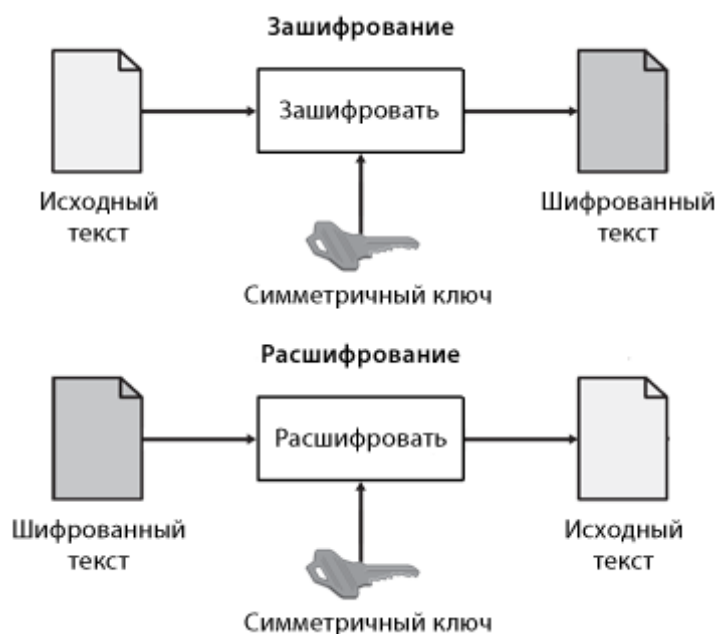


Рисунок 205. Зашифрование и расшифрование на симметричном ключе

Симметричные алгоритмы шифрования способны обрабатывать большое количество данных за короткое время благодаря использованию для зашифрования и расшифрования одного и того же ключа, а также благодаря простоте симметричных алгоритмов по сравнению с асимметричными. Поэтому симметричные алгоритмы часто используют для шифрования больших массивов данных.

Для шифрования данных с помощью симметричного алгоритма криптографическая система использует симметричный ключ. Длина ключа (обычно выражаемая в битах) зависит от алгоритма шифрования и программы, которая использует этот алгоритм.

С помощью симметричного ключа исходный (открытый) текст преобразуется в шифрованный (закрытый) текст. Затем шифрованный текст отправляется получателю. Если получателю известен симметричный ключ, на котором зашифрован текст, получатель может преобразовать шифрованный текст в исходный вид.



Примечание. На практике симметричный ключ нужно передать получателю каким-либо надежным способом. Обычно создается симметричный ключ парной связи, который передается получателю лично. Затем для шифрования используются случайные (сессионные) симметричные ключи, которые зашифровываются на ключе парной связи и в таком виде передаются по различным каналам вместе с зашифрованным текстом.

Наибольшую угрозу безопасности информации при симметричном шифровании представляет перехват симметричного ключа парной связи. Если он будет перехвачен, злоумышленники смогут расшифровать все данные, зашифрованные на этом ключе.

Асимметричное шифрование

Асимметричные алгоритмы шифрования используют два математически связанных ключа: открытый ключ и закрытый ключ. Для зашифрования применяется открытый ключ, для расшифрования — закрытый ключ.

Открытый ключ распространяется свободно. Закрытым ключом владеет только пользователь, который создает пару асимметричных ключей. Закрытый ключ следует хранить в секрете, чтобы исключить возможность его перехвата.

Использование двух различных ключей для зашифрования и расшифрования, а также более сложный алгоритм делают процесс шифрования с помощью асимметричных ключей гораздо более медленным, чем шифрование с помощью симметричных ключей.

Открытый ключ может быть использован любыми лицами для отправки зашифрованных данных владельцу закрытого ключа. При этом парой ключей владеет только получатель зашифрованных данных. Таким образом, только получатель может расшифровать эти данные с помощью имеющегося у него закрытого ключа.

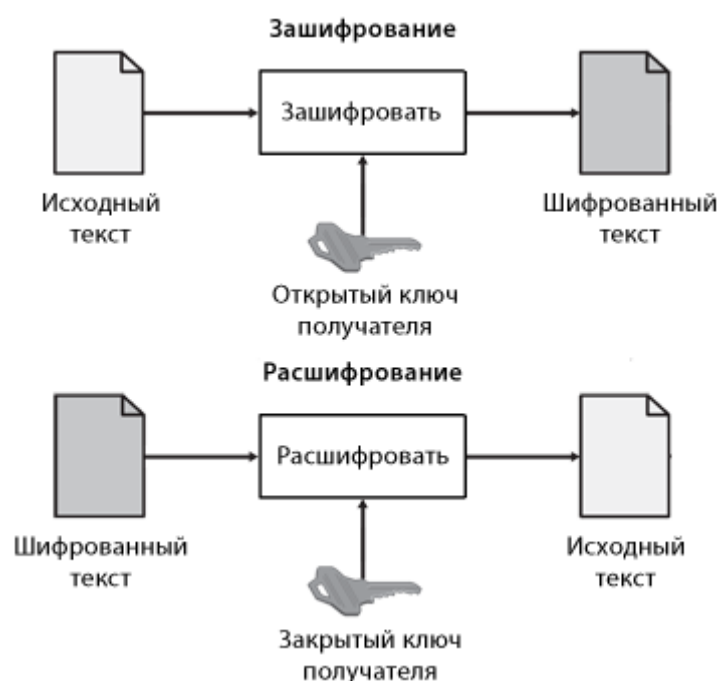


Рисунок 206. Зашифрование и расшифрование на асимметричном ключе



Примечание. На практике асимметричные алгоритмы в чистом виде используются очень редко. Обычно данные зашифровываются с помощью симметричного алгоритма, а затем с помощью асимметричного алгоритма зашифровывается только симметричный ключ. Комбинированные (гибридные) криптографические алгоритмы рассматриваются ниже (см. [Сочетание симметричного и асимметричного шифрования](#)).

Сочетание симметричного и асимметричного шифрования

В большинстве приложений симметричные и асимметричные алгоритмы применяются совместно, что позволяет использовать преимущества обоих алгоритмов.

В случае совместного использования симметричного и асимметричного алгоритмов:

- Исходный текст преобразуется в шифрованный с помощью симметричного алгоритма шифрования. Преимущество этого алгоритма заключается в высокой скорости шифрования.
- Для передачи получателю симметричный ключ, на котором был зашифрован текст, зашифровывается с помощью асимметричного алгоритма. Преимущество асимметричного алгоритма заключается в том, что только владелец закрытого ключа сможет расшифровать симметричный ключ.

На следующем рисунке изображен процесс шифрования с помощью комбинированного алгоритма.

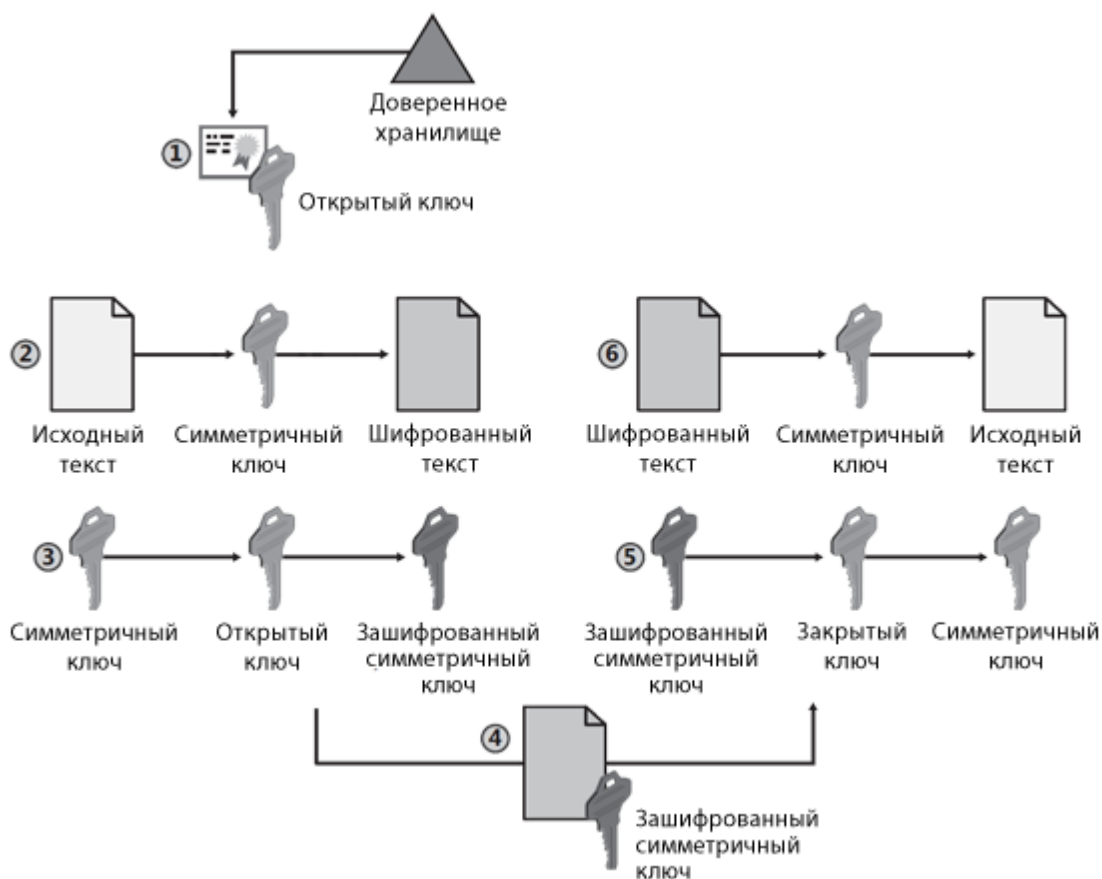


Рисунок 207. Шифрование с помощью комбинированного алгоритма

- 1 Отправитель запрашивает открытый ключ получателя из доверенного хранилища.

- 2 Отправитель создает симметричный ключ и зашифровывает с его помощью исходный текст.
- 3 Симметричный ключ зашифровывается на открытом ключе получателя, чтобы предотвратить перехват ключа во время передачи.
- 4 Зашифрованный симметричный ключ и зашифрованный текст передаются получателю.
- 5 С помощью своего закрытого ключа получатель расшифровывает симметричный ключ.
- 6 С помощью симметричного ключа получатель расшифровывает зашифрованный текст, в результате он получает исходный текст.

Сочетание хэш-функции и асимметричного алгоритма электронной подписи

Электронная подпись защищает данные следующим образом:

- Для подписания данных используется хэш-функция, с помощью которой определяется хэш-сумма исходных данных. По хэш-сумме можно определить, имеют ли место какие-либо изменения в этих данных.
- Полученная хэш-сумма подписывается электронной подписью, позволяя подтвердить личность подписавшего. Кроме того, электронная подпись не позволяет подписавшему лицу отказаться от авторства, так как только оно владеет ключом электронной подписи, использованным для подписания. Невозможность отказаться от авторства называется неотретаемостью.

Большинство приложений, осуществляющих электронную подпись, используют сочетание хэш-функции и асимметричного алгоритма подписи. Хэш-функция позволяет проверить целостность исходного сообщения, а электронная подпись защищает полученную хэш-функцию от изменения и позволяет определить личность автора сообщения.

Приведенная ниже схема иллюстрирует применение хэш-функции и асимметричного алгоритма в электронной подписи.

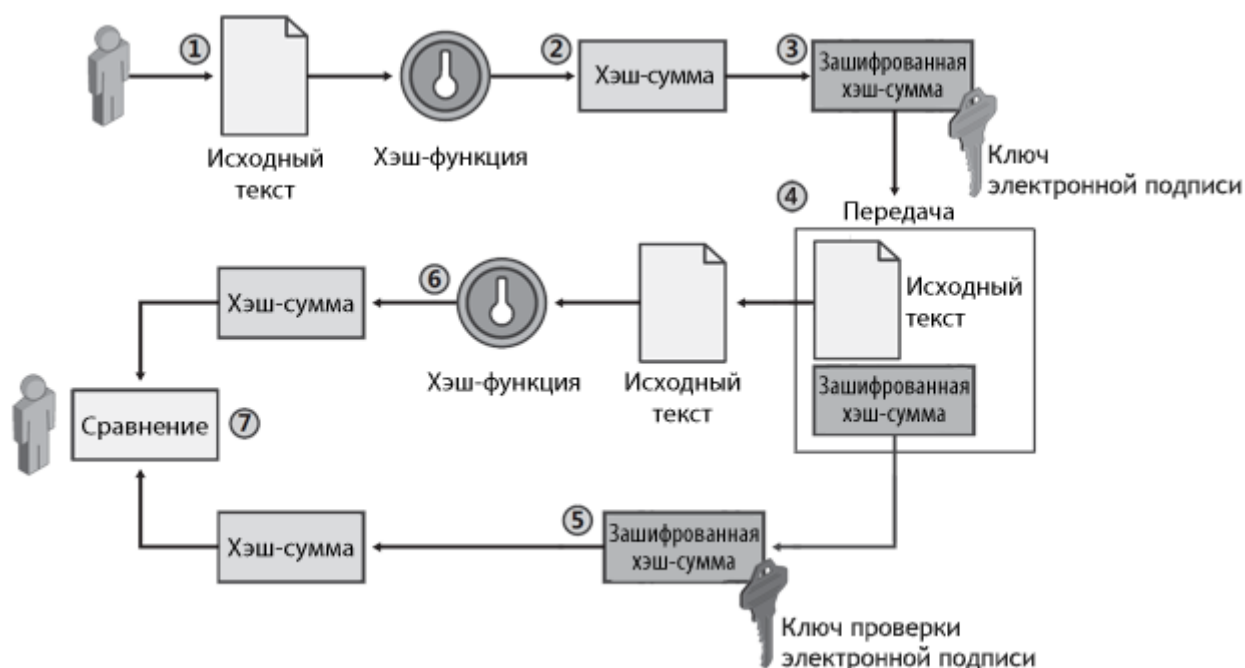


Рисунок 208. Применение хэш-функции и асимметричного криптографического алгоритма в электронной подписи

- 1 Отправитель создает файл с исходным сообщением.
- 2 Программное обеспечение отправителя вычисляет хэш-сумму исходного сообщения.
- 3 Полученная хэш-сумма зашифровывается с помощью ключа электронной подписи отправителя.
- 4 Исходное сообщение и зашифрованная хэш-функция передаются получателю.



Примечание. При использовании электронной подписи исходное сообщение не зашифровывается. Само сообщение может быть изменено, но любые изменения сделают хэш-сумму, передаваемую вместе с сообщением, недействительной.

- 5 Получатель расшифровывает хэш-сумму сообщения с помощью ключа проверки электронной подписи отправителя. Ключ проверки электронной подписи может быть передан вместе с сообщением или получен из доверенного хранилища.
- 6 Получатель использует ту же хэш-функцию, что и отправитель, чтобы вычислить хэш-сумму полученного сообщения.
- 7 Вычисленная хэш-сумма сравнивается с хэш-суммой, полученной от отправителя. Если эти хэш-суммы различаются между собой, то сообщение или хэш-сумма были изменены при передаче.



Термины и сокращения

Microsoft Access

Система управления реляционными базами данных. Входит в состав Microsoft Office.

Microsoft SQL Server

Система управления реляционными базами данных. Используется для работы с базами данных различного размера.

Object Identifier (OID)

Набор символов в десятично-точечной нотации, идентифицирующий атрибуты объектов (например, политики сертификата или криптографические алгоритмы).

OCSP-сервер

Сервер в составе доверенного субъекта инфраструктуры открытых ключей, предоставляющего информацию о статусах сертификатов по запросам в режиме онлайн.

ODBC (Open Database Connectivity)

Стандартный программный интерфейс (Application Programming Interface, API) доступа к различным источникам данных (базам данных), разработанный компанией Microsoft.

PKI (Public Key Infrastructure)

Инфраструктура открытых ключей — комплекс аппаратных и программных средств, политик и процедур, обеспечивающих доверие к открытым ключам (в том числе ключам проверки электронной подписи) путём издания сертификатов ключей проверки электронной подписи и поддержания их жизненного цикла.

SQL-сервер

Сервер базы данных, который работает под управлением программного обеспечения Microsoft SQL Server.

TSP-сервер

Сервер в составе доверенного субъекта инфраструктуры открытых ключей, обладающего точным и надёжным источником времени и предоставляющего штампы времени по запросам.

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 Publication Service

Программное обеспечение для публикации сертификатов и списков аннулированных сертификатов в общедоступных хранилищах данных.

ViPNet Registration Point

Программное обеспечение, предназначенное для регистрации пользователей ViPNet и хранения их регистрационных данных, а также для выдачи сертификатов и дистрибутивов ключей, создаваемых по запросам в ViPNet Удостоверяющий и ключевой центр.

ViPNet Центр управления сетью (ЦУС)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для Удостоверяющего и ключевого центра;
- задание полномочий пользователей сетевых узлов ViPNet.

Администратор сети ViPNet

Лицо, отвечающее за управление сетью ViPNet, создание и обновление справочников и ключей для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями и обладающее правом доступа к программе ViPNet Центр управления сетью и (или) ViPNet Удостоверяющий и ключевой центр.

Администратор УКЦ

Лицо, обладающее правом доступа к программе ViPNet Удостоверяющий и ключевой центр (УКЦ), отвечающее за создание ключей для сетевых узлов ViPNet, создание и обслуживание сертификатов ViPNet, обеспечение взаимодействия с доверенными сетями ViPNet.

Аккредитованный удостоверяющий центр

Удостоверяющий центр, аккредитованный уполномоченным федеральным органом исполнительной власти и издающий квалифицированные сертификаты.

Аннулирование сертификата

Признание сертификата недействительным до истечения его срока действия (например, в случае компрометации соответствующего ключа электронной подписи).

Аутентификация

Процесс односторонней или двусторонней (взаимной) проверки подлинности между клиентом (пользователем) и системой (сервером), например, с использованием учётных данных или сертификатов ключей проверки электронной подписи.

Вариант персонального ключа пользователя

Номер персонального ключа пользователя из резервного набора персональных ключей (РНПК). Изменение варианта персонального ключа пользователя означает, что номер персонального ключа был увеличен на единицу и для создания новых ключей пользователя будет использоваться следующий персональный ключ из РНПК.

Внешний пользователь

Лицо, которое не является пользователем сетевого узла ViPNet и для которого в программе ViPNet Удостоверяющий и ключевой центр издан сертификат ключа проверки электронной подписи.

Возобновление действия сертификата

Возврат сертификату ключа проверки электронной подписи статуса действительного после того, как его действие было приостановлено.

Вышестоящий удостоверяющий центр

Удостоверяющий центр в иерархической системе доверия, не являющийся головным, но имеющий один или несколько подчиненных удостоверяющих центров, для которых он издает сертификаты, тем самым обеспечивая доверие к ним.

Головной удостоверяющий центр

Удостоверяющий центр в иерархической системе доверия, который имеет корневой (самоподписанный) сертификат, и издает сертификаты для подчиненных удостоверяющих центров, тем самым обеспечивая доверие к ним.

Группа узлов

Множество сетевых узлов ViPNet, объединенное под общим именем для удобства администрирования. Например, позволяет задать единый пароль администратора для всех сетевых узлов ViPNet, входящих в данную группу.

Дистрибутив ключей

Файл с расширением *.dst, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии для первичного запуска и последующей работы программы ViPNet на сетевом узле. Для работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Доверенная сеть

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

Доверенное лицо удостоверяющего центра (администратор УЦ)

Лицо, уполномоченное действовать от имени удостоверяющего центра (в том числе издавать, аннулировать сертификаты ключей проверки электронной подписи).

Запрос на сертификат

Документ с информацией, которая требуется для издания сертификата ключа проверки электронной подписи в удостоверяющем центре (владелец, срок действия, назначение сертификата и прочее).

Идентификатор ключа субъекта

Идентификатор (уникальный номер) ключа электронной подписи владельца сертификата.

Иерархическая система доверия между удостоверяющими центрами

Система, в которой каждый удостоверяющий центр издает сертификаты для подчиненных удостоверяющих центров, тем самым обеспечивая доверие к ним. Применяется в аккредитованных удостоверяющих центрах России.

Квалифицированный сертификат

Сертификат ключа проверки электронной подписи, изданный аккредитованным удостоверяющим центром или уполномоченным федеральным органом исполнительной власти.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключ защиты

Ключ, на котором шифруется другой ключ.

Ключ защиты УКЦ

Ключ, на котором зашифрована вся информация, хранящаяся в программе ViPNet Удостоверяющий и ключевой центр (список администраторов УКЦ, мастер-ключи, пароли пользователей ViPNet, ключи пользователей, узлов и прочее).

Ключ защиты УКЦ входит в состав ключей администратора УКЦ и зашифрован на ключе защиты данного администратора.

Ключ обмена

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

Ключ проверки электронной подписи (ключ проверки ЭП)

Несекретный (открытый) ключ из пары асимметричных ключей, который представляет собой уникальную последовательность символов, однозначно связанную с секретным ключом (ключом электронной подписи или закрытым ключом) и предназначенную для проверки подлинности электронной подписи.

Ключ электронной подписи (ключ ЭП)

Секретный (закрытый) ключ из пары асимметричных ключей, который представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Ключевой блокнот ДСДР

Ключевой блокнот ДСДР содержит последовательности случайных чисел, которые используются при шифровании конфиденциальной информации. ДСДР предназначен для средств криптографической защиты данных, не содержащих сведений, составляющих государственную тайну.

Ключи администратора УКЦ

Формируются при создании учетной записи администратора УКЦ и включают в себя:

- ключ защиты администратора, зашифрованный на пароле администратора;
- ключ защиты УКЦ, зашифрованный на ключе защиты администратора;
- контейнеры с ключами подписи.

Ключи пользователя ViPNet

Совокупность ключей, которые необходимы пользователю для аутентификации в сети ViPNet и шифрования других ключей, и к которым имеет доступ только данный пользователь.

Ключи пользователя могут содержать:

- действующий персональный ключ пользователя;
- ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи;
- хэш пароля пользователя.

Содержимое ключей пользователя формируется в зависимости от типа аутентификации пользователя.

Ключи узла ViPNet

Совокупность ключей, с использованием которых производится шифрование трафика, служебной информации и писем программы ViPNet Деловая почта.

Компрометация ключей

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

Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

Контейнер сертификатов администраторов

Файл формата PKCS #7, который может содержать списки сертификатов издателей (администраторов удостоверяющего центра) и соответствующие им списки аннулированных сертификатов. В программе ViPNet Удостоверяющий и ключевой центр используется для установки межсетевого взаимодействия.

Контрольная сумма

Значение, используемое для проверки целостности информации.

Корневой сертификат

Самоподписанный сертификат головного удостоверяющего центра. Используется для подписи сертификатов, издаваемых головным удостоверяющим центром, с целью обеспечения доверия к ним.

Кросс-сертификат

Сертификат, который один удостоверяющий центр издает на базе своего сертификата для другого удостоверяющего центра с целью обеспечения доверия между этими удостоверяющими центрами. Используется в распределенной системе доверия между удостоверяющими центрами.

Лицензия на сеть

Разрешение на пользование определенным набором функций продуктовой линейки ViPNet. В частности, лицензия на сеть ViPNet определяет следующее: номер сети, максимальное количество координаторов и клиентов, максимальное суммарное количество адресов, туннелируемых координаторами сети, максимальное количество узлов, на которые можно добавить ту или иную роль, максимальную разрешенную версию программного обеспечения ViPNet, срок действия лицензии и другие параметры.

Мастер-ключ

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

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

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

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.

Основной узел пользователя

Первый узел, на котором зарегистрирован пользователь в программе ViPNet Центр управления сетью.

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.

Пароль пользователя на основе парольной фразы

Пароль пользователя необходим для входа в любую программу ViPNet. Случайный пароль создается на основе парольной фразы, которую можно использовать для запоминания пароля. Парольные фразы могут быть созданы на нескольких языках. Фразы представляют собой грамматически корректные конструкции, однако слова, составляющие фразу, выбираются случайным образом из большого по объему словаря. Парольная фраза может содержать 3 или 4 слова, при желании пароль может быть создан из двух парольных фраз.

Чтобы получить пароль из парольной фразы, достаточно набрать без пробелов в раскладке латиницей первые X букв из каждого слова парольной фразы, содержащей Y слов. Пользователь сам задает параметры X и Y, а также язык парольной фразы.

Например, при использовании трех первых букв из каждого слова парольной фразы «Затейливый ювелир утащил сдобу» получим пароль «pfn.dtenfclj».

Парольная фраза

Набор грамматически согласованных между собой слов, выбираемых случайным образом из специальных словарей. Парольная фраза формируется при создании паролей и служит для их запоминания. Пароль из парольной фразы получается по следующему правилу: в латинской раскладке клавиатуры набираются по N первых букв от каждого из M слов парольной фразы без пробелов, где N определяется длиной пароля.

Например, парольной фразе «**служащий латает рельс**» соответствует пароль «ске;kfnfhftkm». В данном случае, при вводе пароля необходимо набирать по 4 первых буквы каждого слова парольной фразы.

Персональный ключ пользователя

Главный ключ защиты ключей, к которым имеет доступ пользователь. Действующий персональный ключ необходимо хранить в безопасном месте, так как компрометация этого ключа означает компрометацию всех других ключей пользователя, а также ключей защиты, на которых зашифрованы ключи обмена.

См. также: [Ключи пользователя ViPNet](#), [Компрометация ключей](#), [Пользователь ViPNet](#), [Резервный набор персональных ключей \(РНПК\)](#), ViPNet Удостоверяющий и ключевой центр (УКЦ).

Подчиненный (промежуточный) удостоверяющий центр

Удостоверяющий центр в иерархической системе доверия, у которого есть сертификат, изданный головным или вышестоящим удостоверяющим центром и обеспечивающий доверие к нему.

Политика применения сертификата

Совокупность правил применения сертификата ключа проверки электронной подписи, определяющих, в каких случаях допустимо или следует использовать данный сертификат в соответствии с требованиями безопасности.

Полномочия пользователя

Разрешения на определенные действия пользователей на сетевом узле ViPNet по изменению настроек некоторых программ ViPNet.

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

Пользователь ViPNet

Лицо, которое использует программное обеспечение ViPNet и имеет ключи для работы с ним.

Приостановление действия сертификата

Временное признание сертификата ключа проверки электронной подписи недействительным до истечения срока его действия.

Публикация

Размещение сформированной в удостоверяющем центре информации в хранилищах данных, доступных по стандартным прикладным протоколам (например, FTP, LDAP).

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.

Сертификат издателя

Сертификат ключа проверки электронной подписи, принадлежащий удостоверяющему центру и служащий для подписи сертификатов, издаваемых удостоверяющим центром.

Сертификат ключа проверки электронной подписи

Документ, изданный удостоверяющим центром 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 управляющем ПО.

Сеть ViPNet

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

Симметричный ключ

Последовательность битов заданной длины (для алгоритма ГОСТ 28147-89 — 256 бит), используемая как для зашифрования, так и для расшифрования информации.

В программном обеспечении ViPNet симметричные ключи используются для зашифрования и расшифрования IP-трафика, информации приложений (в том числе почтовой), служебных и прикладных конвертов.

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.

Справочники

Набор файлов, содержащих информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях. Эти файлы формируются в программе ViPNet Центр управления сетью, предназначенной для создания структуры и конфигурирования сети ViPNet.

Справочники и ключи

Справочники, [ключи узла](#) и ключи пользователя.

Структура сети ViPNet

Упорядоченная совокупность связей между компонентами сети ViPNet, такими как:

- рабочее место администратора сети ViPNet;
- координаторы;
- клиенты.

Каждый клиент должен быть зарегистрирован на координаторе. Связи между координаторами и рабочим местом администратора, а также между координатором и его клиентами обязательны. Остальные связи создаются в соответствии с корпоративной политикой безопасности.

Точка распространения списков аннулированных сертификатов (CDP)

Хранилище, в которое удостоверяющий центр публикует актуальные списки аннулированных сертификатов. URL таких точек указываются в соответствующем расширении сертификатов, издаваемых удостоверяющим центром.

Транспортный сервер MFTP

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

Удостоверяющий центр (УЦ)

Организация, уполномоченная издавать сертификаты ключа проверки электронной подписи для физических и юридических лиц, а также управлять жизненным циклом этих сертификатов.

Шаблон сертификата

Структура, которая определяет набор полей для информации о владельце сертификата и позволяет упростить создание запросов на сертификаты.

Электронная подпись (ЭП)

Созданная криптографической операцией дополнительная информация, с помощью которой можно подтвердить авторство и неизменность основной информации.

Электронная рулетка

Встроенный компонент программного обеспечения ViPNet, позволяющий инициализировать датчик случайных чисел по действиям пользователя. Полученная последовательность используется при формировании криптографических ключей.

Изменения в документации

В разделе перечислены изменения в документации после выпуска ViPNet Administrator версии 4.6.11.

- **18.01.2024 — выпущена документация к версии 4.6.11**
- **25.09.2024 — обновлены документы:**
 - «ViPNet УКЦ 4. Руководство администратора»

Добавлена информация о создании нового дистрибутива ключей при изменении варианта персонального ключа пользователя, если вариант персонального ключа пользователя равен единице, в разделы «Когда следует создавать дистрибутивы ключей», «Действия в случае компрометации ключей пользователя», «Изменение вариантов персонального ключа пользователя и ключей узла».

Добавлена информация о создании нового дистрибутива ключей при смене мастер-ключа персональных ключей, если вариант персонального ключа пользователя равен двум и более, в разделы «Когда следует создавать дистрибутивы ключей», «Смена мастер-ключа персональных ключей».
 - «ViPNet Administrator 4. Смена мастер-ключей»

Добавлена информация о создании нового дистрибутива ключей при смене мастер-ключа персональных ключей, если вариант персонального ключа пользователя равен двум и более, в раздел «Смена мастер-ключей».
- **05.03.2025 — обновлены документы:**
 - «ViPNet УКЦ 4. Руководство администратора»

В раздел «Установка и первичная инициализация программы ViPNet Prime Удостоверяющий и ключевой центр» добавлена информация о том, что пользователь, от имени которого будет производиться установка, первичная инициализация и работа, должен обладать правами администратора.
 - «ViPNet Administrator 4. Руководство по установке»

В раздел «Порядок установки компонентов ПО ViPNet Administrator» добавлена информация о том, что пользователь, от имени которого будет производиться установка, первичная инициализация и работа, должен обладать правами администратора.

- «ViPNet ЦУС 4. Руководство администратора»

В раздел «Возможные неполадки», «Не удастся установить соединение с сервером ViPNet Центр управления сетью» добавлена рекомендация по устранению проблемы недостаточного объема дискового пространства.

- «ViPNet Administrator 4. Руководство по смене мастер-ключей в сети ViPNet»

В раздел «Порядок действий» добавлена информация о том, что порядок смены мастер-ключей ViPNet Coordinator KB 4 необходимо смотреть в документации на координатор.