



ViPNet Publication Service 4.6

Руководство администратора

© ОАО «ИнфоТеКС», 2019

ФРКЕ.00113-05 32 01

Версия продукта 4.6.6

Этот документ входит в комплект поставки ViPNet Publication Service, и на него распространяются все условия лицензионного соглашения.

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

ViPNet® является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

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

ОАО «ИнфоТеКС»

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

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

Веб-сайт: <https://infotecs.ru>

Служба технической поддержки: hotline@infotecs.ru

Содержание

Введение.....	7
О документе.....	8
Для кого предназначен документ	8
Соглашения документа.....	8
О программе	10
Ограничения незарегистрированной версии	10
Системные требования.....	11
Комплект поставки.....	11
Новые возможности версии 4.6.6.....	12
Обратная связь.....	13
 Глава 1. Установка, удаление и обновление программы ViPNet Publication Service.....	14
Установка программы	15
Обновление программы	17
Удаление программы.....	18
 Глава 2. Начало работы с программой ViPNet Publication Service	19
Запуск и завершение работы с программой	20
Настройка параметров работы программы.....	21
 Глава 3. Регистрация ViPNet Publication Service	22
Зачем нужно регистрировать ViPNet Publication Service	23
Начало регистрации	24
Получение серийного номера	26
Получение кода регистрации	27
Получение кода регистрации через Интернет.....	27
Получение кода регистрации по электронной почте.....	30
Получение кода регистрации по телефону.....	31
Регистрация через файл.....	32
Регистрация ViPNet Publication Service.....	34
Сохранение регистрационных данных	35
Если конфигурация вашего компьютера изменилась	36
 Глава 4. Назначение публикаций	37
Публикация сертификатов и CRL	38

Виды хранилищ и типы публикуемых данных	39
Импорт CRL из доверенных сетей ViPNet и сторонних УЦ	40
Настройка публикации данных в хранилище: порядок действий	41
Глава 5. Подготовка хранилищ данных	42
AD LDS.....	43
Расширение схемы AD LDS.....	43
Создание контейнеров для размещения опубликованных данных	44
Создание учетной записи для публикации	45
Создание группы учетных записей для публикации	46
Добавление учетной записи для публикации в группу	46
Задание прав на публикацию и удаление данных	47
Разрешение анонимного доступа к опубликованным данным	48
AD DS.....	51
FTP-сервер	53
Практическое использование FTP	53
Настройка FTP-сервера	54
Структура папок при размещении данных на FTP	56
Глава 6. Настройка взаимодействия программ ViPNet Удостоверяющий и ключевой центр и ViPNet Publication Service.....	58
Настройка папок обмена	59
Подготовка публикуемых данных в УКЦ	61
Глава 7. Добавление публикаций.....	63
Публикация в AD LDS.....	64
Публикация в AD DS.....	67
Публикация сертификатов	67
Публикация CRL.....	69
Публикация на FTP-сервер.....	71
Изменение параметров публикации	73
Отключение и удаление публикации	74
Глава 8. Контроль опубликованных данных	75
Поиск и просмотр опубликованных данных.....	76
Поиск опубликованных сертификатов пользователей и сертификатов издателей	76
Поиск и просмотр опубликованных CRL	77
Просмотр статистики публикаций.....	79
Просмотр журнала публикаций	80

Экспорт опубликованных сертификатов.....	83
Глава 9. Настройка автоматической загрузки CRL	85
Добавление точки распространения	86
Опрос точек распространения.....	88
Глава 10. Экспорт и импорт настроек программы ViPNet Publication Service	89
Зачем нужны экспорт и импорт настроек программы.....	90
Экспорт настроек	91
Импорт настроек.....	92
Приложение А. Часто задаваемые вопросы по настройке публикации в AD DS.....	93
Использование контейнеров для разных версий ViPNet Publication Service.....	94
Общие вопросы и проблемы	95
Как с помощью стороннего приложения, установленного на компьютере не входящем в домен, получить доступ к опубликованным данным?	95
Где находится журнал событий (лог) для ViPNet Publication Service?	96
Ошибка: Не удалось подключиться.....	96
Ошибка: Не удалось определить права	97
Обращение в службу поддержки «ИнфоТеКС»	98
Проблемы публикации сертификатов.....	99
Ошибка: Нет прав на публикацию сертификата.....	99
Ошибок нет, но сертификаты не публикуются	99
Проблемы публикации CRL	102
Ошибка: Нет прав на публикацию списков отзыва	102
Ошибка: Не удалось подключиться, ErrorCode: 0x80072030. There is no such object on the server	103
Ошибка: Не удалось подключиться. ErrorCode: 0x8007202B. A referral was returned from the server	103
Ошибка: Не удалось подключиться. ErrorCode: 0x80005000(E_ADS_BAD_PATHNAME) или E_ADS_BAD_PATHNAME	104
Приложение В. Региональные настройки	105
Региональные настройки в ОС Windows 7, Windows Server 2008 R2	106
Региональные настройки в ОС Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10	110
Приложение С. История версий.....	114
Что нового в версии 4.6	114
Что нового в версии 4.4	114

Что нового в версии 4.3	114
Что нового в версии 4.2	116
Что нового в версии 3.2.10	118
Что нового в версии 3.2.9.....	118
Что нового в версии 3.2.5.....	126
Что нового в версии 3.2.3.....	127
Что нового в версии 3.2.2.....	127
Что нового в версии 3.2.0.....	128
 Приложение D. Глоссарий	 131



Введение

О документе	8
О программе	10
Новые возможности версии 4.6.6	12
Обратная связь	13

О документе

В данном документе описывается назначение и применение программы ViPNet Publication Service, основные возможности программы, принципы работы с программой и описание пользовательского интерфейса.

Для кого предназначен документ

Документ предназначен для администраторов сетей, которым необходимо организовать автоматическую публикацию сертификатов и списков аннулированных сертификатов (далее — CRL) в хранилища для общего доступа к ним всех участников документооборота, использующих опубликованные сертификаты для шифрования и проверки подлинности электронной подписи.

Соглашения документа

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

Таблица 1. Обозначения, используемые в примечаниях




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

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.

Обозначение	Описание
Код	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

О программе

Программное обеспечение ViPNet Publication Service входит в состав программного комплекса ViPNet УЦ и предназначено для публикации сертификатов и [CRL](#) (см. глоссарий, стр. 133) в общедоступных хранилищах данных.

В программе реализованы следующие функции:

- Автоматическая и ручная публикации данных:
 - сертификаты пользователей;
 - сертификаты издателей (корневые и кросс-сертификаты);
 - CRL сетей ViPNet;
 - CRL сторонних удостоверяющих центров (далее — УЦ);
- Поиск и просмотр опубликованных данных.
- Экспорт опубликованных сертификатов.
- Импорт CRL из точек распространения (см. [Настройка автоматической загрузки CRL](#) на стр. 85).

Публикация сертификатов и CRL позволяет обеспечить совместимость клиентских приложений, построенных на базе криптографии ViPNet, с приложениями других производителей.

После установки на компьютер программа ViPNet Publication Service работает в демо-режиме в течение 14 дней. За это время вы можете ознакомиться с возможностями программы и зарегистрировать ее (см. [Регистрация ViPNet Publication Service](#) на стр. 22). После регистрации вы сможете работать с ViPNet Publication Service неограниченное время.

Ограничения незарегистрированной версии

С незарегистрированной версией программного обеспечения ViPNet Publication Service вы можете работать по демо-лицензии.

Особенности демо-лицензии:

- Срок действия: 14 дней.
- Функциональных ограничений нет.

По истечении срока действия демо-лицензии запуск программы ViPNet Publication Service будет невозможен. Для полноценной работы программы потребуется ее регистрация (см. [Регистрация ViPNet Publication Service](#) на стр. 22).

Системные требования

Требования к компьютеру для установки ViPNet Publication Service:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 1 Гбайт.
- Свободное место на жестком диске — не менее 250 Мбайт.
- Сетевой адаптер или модем. Рекомендуется использовать оборудование, обеспечивающее доступ к серверной составляющей со скоростью не менее 1 Мбит/с.
- Операционная система — Windows 7 (32/64-разрядная), Windows Server 2008 R2 (64-разрядная), Windows 8 (32/64-разрядная), Windows Server 2012 (64-разрядная), Windows 8.1 (32/64-разрядная), Windows Server 2012 R2 (64-разрядная), Windows 10 (32/64-разрядная).

Для операционной системы должны быть установлены последние пакеты обновлений.

- При использовании Internet Explorer — версия 7.0 или выше.

Требования к компьютеру, выполняющему функции сервера данных:

Требования к используемому LDAP-серверу:

- AD LDS и Active Directory из состава Windows Server 2008 R2;
- AD LDS и Active Directory из состава Windows Server 2012 и Windows Server 2012 R2.

Требования к используемому FTP-серверу:

Формально допустим любой стандартный FTP-сервер, однако, рекомендуется использовать:

- ProFTPD версии 1.3 или выше на любой ОС;
- Microsoft IIS FTP-сервер из состава Windows Server 2008 R2, Windows Server 2012 и Windows Server 2012 R2.

Комплект поставки

Комплектность поставки варьируется в зависимости от заказа. Как правило, в базовый комплект поставки ViPNet Publication Service входит:

- Установочный файл программы.
- Документация в формате PDF, в том числе:
 - «ViPNet Publication Service. Руководство администратора».
 - «ViPNet Publication Service. Форматы хранения опубликованных данных».

Новые возможности версии 4.6.6

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Publication Service версии 4.6.6 по сравнению с версией 4.6.0. Информация об изменениях в предыдущих версиях программы приведена в приложении [История версий](#) (на стр. 114).

- **Изменен список поддерживаемых операционных систем**

Начиная с версии 4.6.6, добавлена поддержка ОС Windows 8 (32/64-разрядная), Windows Server 2012 (64-разрядная), Windows 8.1 (32/64-разрядная), Windows Server 2012 R2 (64-разрядная), Windows 10 (32/64-разрядная).

Прекращена поддержка ОС Windows Server 2003, Windows Server 2003 R2 и Windows Vista в связи с прекращением их поддержки производителем.

- **Изменен список публикуемых данных**

Начиная с версии 4.6.6 прекращена поддержка публикации обновлений УЦ «Верба-сертификат МВ».

Обратная связь

Дополнительная информация

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

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

Контактная информация

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

- Единый многоканальный телефон:
+7 (495) 737-6192,
8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба технической поддержки: hotline@infotecs.ru.

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

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

- Отдел продаж: soft@infotecs.ru.

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



1

Установка, удаление и обновление программы ViPNet Publication Service

Установка программы	15
Обновление программы	17
Удаление программы	18


Установка программы

Перед установкой ViPNet Publication Service убедитесь, что на компьютере выполнены стандартные сетевые настройки, а также правильно заданы часовой пояс, дата и время.

Если ViPNet Publication Service устанавливается на компьютер с операционной системой Windows, локализация которой отличается от русской, для правильного отображения кириллицы в интерфейсе ViPNet Publication Service нужно изменить региональные настройки Windows (см. [Региональные настройки](#) на стр. 105).

Установку должен выполнять пользователь, обладающий правами администратора в ОС Windows.

Для установки ПО ViPNet Publication Service выполните следующие действия:

- 1 Запустите установочный файл программы , используя учетную запись с полномочиями администратора. Дождитесь, пока завершится подготовка к установке ViPNet Publication Service.
- 2 Ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок и нажмите кнопку **Продолжить**.
- 3 Если вы хотите настроить параметры установки, нажмите кнопку **Настроить** и укажите:
 - путь к папке установки программы ViPNet Publication Service;
 - имя пользователя и название организации;
 - название папки для программы ViPNet Publication Service в меню **Пуск**.

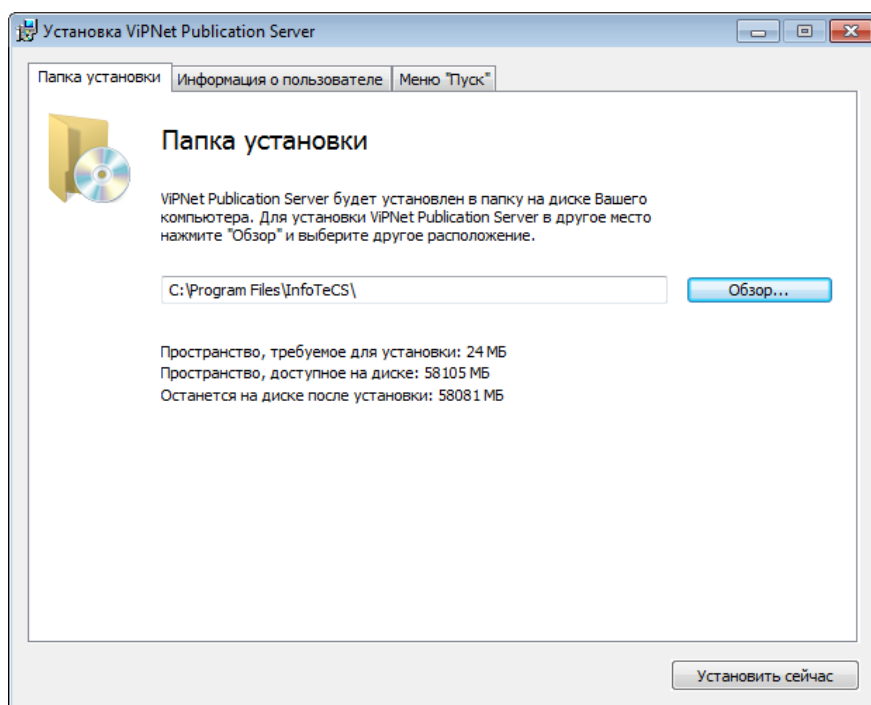


Рисунок 1. Настройка параметров установки ViPNet Publication Service


- 4 Чтобы начать установку ViPNet Publication Service, нажмите кнопку **Установить сейчас**.
- 5 Если после завершения установки появится сообщение о необходимости перезагрузить компьютер, выполните перезагрузку.

Обновление программы



Примечание. В ViPNet Publication Service 3.2 не реализованы импорт и экспорт настроек (см. [Зачем нужны экспорт и импорт настроек программы](#) на стр. 90). Поэтому, если вы хотите применить настройки программы после обновления до версии 4.0 и выше, сохраните содержимое папки `\\%ProfileName%\AppData\Local\InfoTeCS\ViPNet Publication Service\1.0\`. Где `%ProfileName%` — имя учетной записи Windows, под которой запускалась программа ViPNet Publication Service.

Для обновления программы ViPNet Publication Service получите установочный файл новой версии программного обеспечения. Затем выполните следующие действия:

- 1 Завершите работу программы ViPNet Publication Service.
- 2 Запустите установочный файл программы . Дождитесь, пока завершится подготовка к установке ViPNet Publication Service.
- 3 В окне **Установка ViPNet Publication Service** нажмите кнопку **Начать обновление**.
- 4 По окончании процесса обновления нажмите кнопку **Заккрыть**.

Если появится сообщение о необходимости перезагрузить компьютер, выполните перезагрузку.

Внимание! Если программа ViPNet Publication Service версии 3.2.5 (или более ранней версии) была обновлена до текущей версии, то для корректной публикации данных в хранилища AD LDS необходимо расширить схему AD LDS файлами, которые входят в комплект поставки текущей версии ViPNet Publication Service. Подробную информацию о расширении схемы см. в документе «Сетевые хранилища сертификатов 3.0. Руководство администратора».




Если схема AD LDS не будет расширена указанными файлами, публикация будет работать только для сертификатов, не содержащих атрибутов ИНН, ОГРН, СНИЛС. Также при проверке корректности настройки публикации и схемы будет выдаваться сообщение о том, что схема не допускает публикацию сертификатов пользователей.

Если вы обновили программу до текущей версии с версии 4.2 и ниже, то после обновления пройдите процедуру регистрации (см. [Регистрация ViPNet Publication Service](#) на стр. 22). Если регистрация не будет пройдена, вы сможете в течение 14 дней работать в программе в демо-режиме.

Удаление программы

В случае необходимости вы можете удалить с компьютера программу ViPNet Publication Service. При удалении программы ViPNet Publication Service вы можете сохранить пользовательские данные, сформированные и используемые во время работы.

Чтобы удалить программу ViPNet Publication Service, выполните следующие действия:

- 1 Завершите работу программы ViPNet Publication Service.
- 2 Запустите установочный файл программы .
- 3 В открывшемся окне мастера установки ViPNet Publication Service установите переключатель в положение **Удалить все компоненты** и нажмите кнопку **Продолжить**.
- 4 На следующей странице мастера при необходимости установите флажок **Удалить пользовательские данные** и нажмите кнопку **Удалить**.
- 5 Дождитесь завершения удаления программного обеспечения и нажмите кнопку **Заккрыть**.
- 6 Если появится сообщение о необходимости перезагрузить компьютер, выполните перезагрузку.



Совет. Вы также можете полностью удалить ViPNet Publication Service, выбрав в меню **Пуск** пункт **Все программы > ViPNet > ViPNet Publication Service > Установка ViPNet Publication Service**. При этом пользовательские данные не будут сохранены.




2

Начало работы с программой ViPNet Publication Service

Запуск и завершение работы с программой	20
Настройка параметров работы программы	21

Запуск и завершение работы с программой

Чтобы запустить программу ViPNet Publication Service, выполните одно из действий:

- В меню **Пуск** выберите пункт **Все программы > ViPNet > ViPNet Publication Service > ViPNet Сервис Публикации** (во время установки положение программы в меню **Пуск** могло быть изменено).
- Дважды щелкните ярлык  на рабочем столе (ярлык отображается на рабочем столе, если при установке программы была выбрана соответствующая опция).

Если программа ViPNet Publication Service не зарегистрирована, то при запуске появится окно с предложением зарегистрировать программу. Вы можете перейти к регистрации ViPNet Publication Service либо начать работу с ее демо-версией (см. [Ограничения незарегистрированной версии](#) на стр. 10).

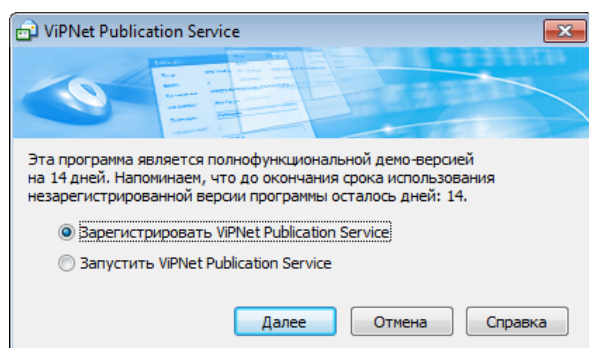



Рисунок 2. Запуск незарегистрированной версии программы

Чтобы выйти из программы ViPNet Publication Service, выполните одно из действий:

- Нажмите кнопку **Заккрыть**  в правом верхнем углу окна.
- Нажмите сочетание клавиш **Alt+F4**.
- В главном окне программы нажмите кнопку **Выход**.

Настройка параметров работы программы

Для настройки параметров работы программы ViPNet Publication Service выполните следующие действия:

- 1 В главном окне программы на панели навигации перейдите в раздел **Настройки**.

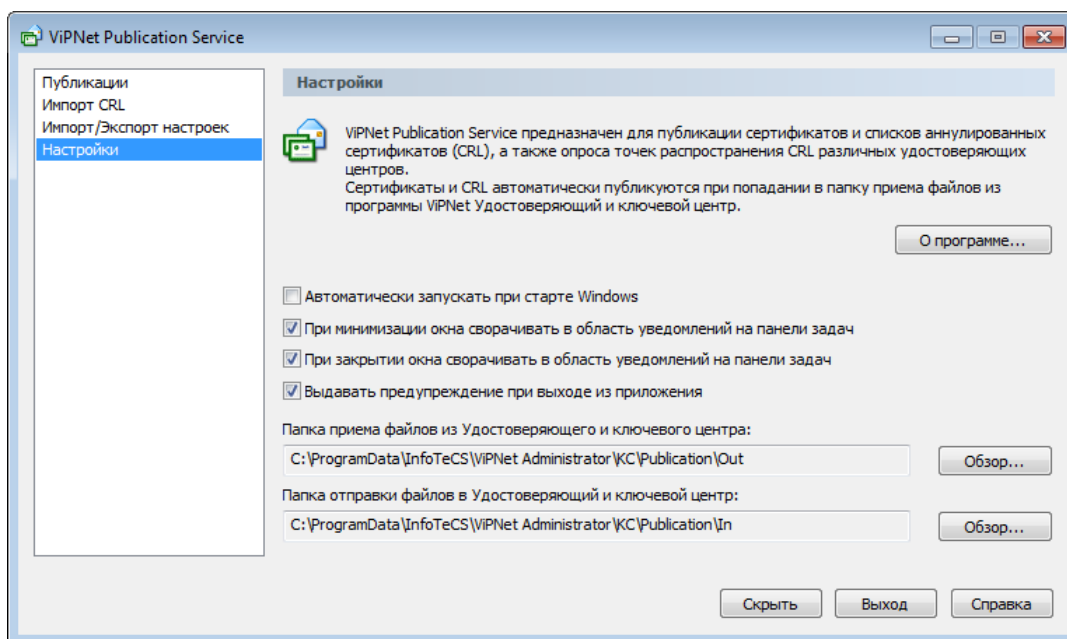




Рисунок 3. Настройка параметров программы

- 2 На панели просмотра при необходимости выполните следующие действия:
 - Чтобы при входе в ОС Windows программа ViPNet Publication Service запускалась автоматически, установите флажок **Автоматически запускать при старте Windows**.
 - Чтобы при нажатии на кнопку **Свернуть**  главное окно программы сворачивалось в область уведомлений, установите флажок **При минимизации окна сворачивать в область уведомлений на панели задач**.
 - Чтобы при нажатии на кнопку **Закрыть**  главное окно программы сворачивалось в область уведомлений, установите флажок **При закрытии окна сворачивать в область уведомлений на панели задач**.
 - Чтобы при выходе из программы появлялось соответствующее предупреждение, установите флажок **Выдавать предупреждение при выходе из приложения**.
 - Для обмена данными между программами ViPNet Удостоверяющий и ключевой центр и ViPNet Publication Service настройте папки обмена (см. [Настройка папок обмена](#) на стр. 59).

В результате измененные параметры программы вступят в силу.

3

Регистрация ViPNet Publication Service

Зачем нужно регистрировать ViPNet Publication Service	23
Начало регистрации	24
Получение серийного номера	26
Получение кода регистрации	27
Регистрация ViPNet Publication Service	34

Зачем нужно регистрировать ViPNet Publication Service

После установки ViPNet Publication Service на компьютер программа работает в демо-режиме (см. [Ограничения незарегистрированной версии](#) на стр. 10). Зарегистрировать программу ViPNet Publication Service вы можете в любой момент, после этого полнофункциональная версия программы будет доступна неограниченное время.

Мы рекомендуем поступить следующим образом:

- установите ViPNet Publication Service и пользуйтесь незарегистрированной версией программы, чтобы оценить возможности и преимущества продукта;
- чтобы работать с полной версией, зарегистрируйте вашу копию ViPNet Publication Service.

Начало регистрации



Примечание. Если программа ViPNet Publication Service повторно установлена на компьютер, на котором она уже была зарегистрирована, вы можете использовать регистрационные данные, сохраненные в файле *.brg (см. [Сохранение регистрационных данных](#) на стр. 35).

Если вы провели обновление конфигурации компьютера, на котором будете использовать ViPNet Publication Service, ознакомьтесь с разделом [Если конфигурация вашего компьютера изменилась](#) (на стр. 36).

Чтобы зарегистрировать ViPNet Publication Service, выполните следующие действия:

- 1 При запуске программы в [окне с предложением зарегистрировать программу](#) (см. рисунок на стр. 20) выберите **Зарегистрировать ViPNet Publication Service** и нажмите кнопку **Далее**. Будет запущен мастер **Регистрация ViPNet Publication Service**.

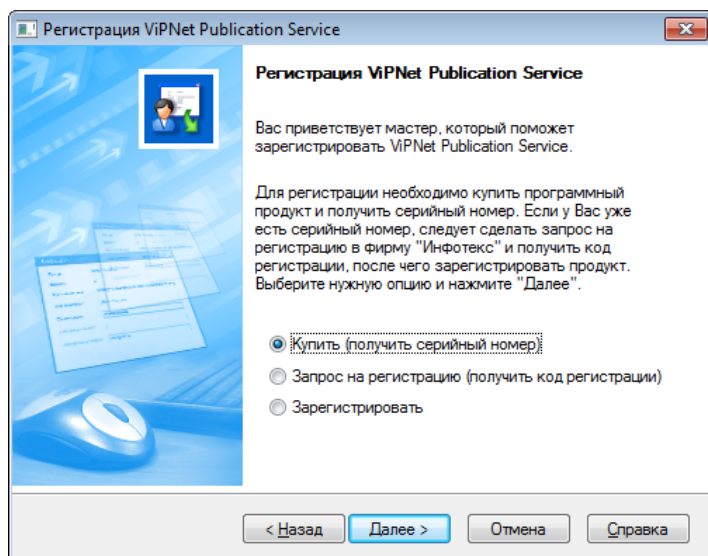


Рисунок 4. Мастер регистрации

- 2 Выполните одно из действий:
 - Если вы не приобрели ViPNet Publication Service, выберите **Купить (получить серийный номер)** (см. [Получение серийного номера](#) на стр. 26).
 - Если вы уже приобрели ViPNet Publication Service и имеете серийный номер, выберите **Запрос на регистрацию (получить код регистрации)** (см. [Получение кода регистрации](#) на стр. 27).



Примечание. Если вы сделаете запрос на регистрацию через Интернет, регистрация ViPNet Publication Service будет проведена автоматически без вашего участия.

- Если вы уже приобрели ViPNet Publication Service и получили код регистрации, выберите **Зарегистрировать** (см. [Регистрация ViPNet Publication Service](#) на стр. 34).

3 Нажмите кнопку **Далее**.

Получение серийного номера

Для получения серийного номера:

- 1 На странице **Регистрация ViPNet Publication Service** выберите **Купить (получить серийный номер)** и нажмите кнопку **Далее**.

В окне вашего браузера откроется страница заказа продуктов ViPNet на сайте компании ОАО «ИнфоТеКС». Приобретите ViPNet Publication Service через веб-сайт и получите серийный номер по электронной почте.

- 2 Получив серийный номер, вернитесь на страницу **Регистрация ViPNet Publication Service** и сделайте запрос на получение кода регистрации (см. [Получение кода регистрации](#) на стр. 27).

Получение кода регистрации

Чтобы запросить код регистрации для ViPNet Publication Service, выполните следующие действия:

- 1 На странице **Регистрация ViPNet Publication Service** выберите **Запрос на регистрацию (получить код регистрации)** и нажмите кнопку **Далее**.
- 2 На странице **Способ запроса на регистрацию** выберите подходящий для вас способ. Для этого установите переключатель в одно из положений:
 - **Через Интернет (online)** (см. [Получение кода регистрации через Интернет](#) на стр. 27).
 - **По электронной почте** (см. [Получение кода регистрации по электронной почте](#) на стр. 30).
 - **По телефону** (см. [Получение кода регистрации по телефону](#) на стр. 31).
 - **Через файл** (см. [Регистрация через файл](#) на стр. 32).

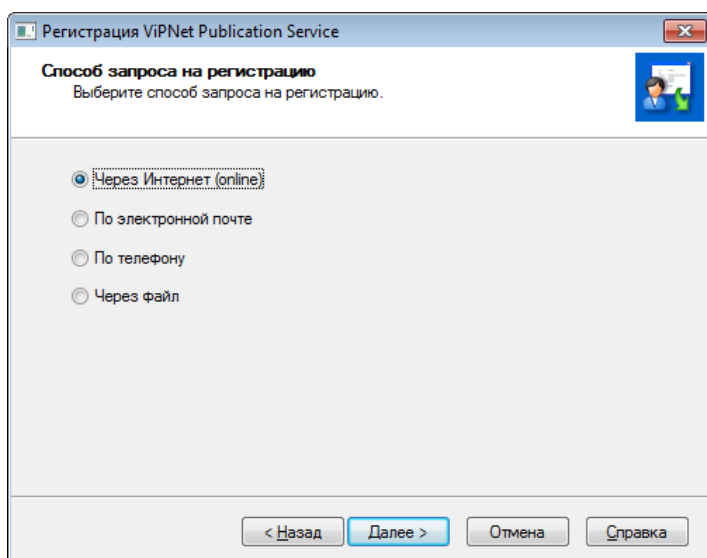


Рисунок 5. Способ запроса на регистрацию

- 3 Нажмите кнопку **Далее**.

Получение кода регистрации через Интернет



Внимание! Для данного способа регистрации необходим доступ в Интернет.

Если вы выбрали способ регистрации **Через Интернет (online)**, откроется страница **Регистрационные данные**.

Рисунок 6. Ввод регистрационных данных

На странице **Регистрационные данные** выполните следующие действия:

- 1 В поле **Серийный номер** введите серийный номер.



Примечание. Если у вас нет серийного номера, сделайте запрос на его получение (см. [Получение серийного номера](#) на стр. 26).

Если вы вводили серийный номер раньше, поле **Серийный номер** будет заполнено автоматически.

- 2 В поле **Пользователь** введите ваше имя. Оно будет использоваться при выпуске лицензии и для обращения к вам. Заполнение этого поля необязательно. По умолчанию в поле **Пользователь** отображается имя, которое вы ввели во время установки ViPNet Publication Service.
- 3 В поле **Организация** введите название вашей организации. Заполнение этого поля необязательно. По умолчанию в поле **Организация** отображается название, которое вы ввели во время установки ViPNet Publication Service.
- 4 В поле **Электронная почта** введите ваш адрес электронной почты, который будет использован для связи с вами в случае необходимости.



Внимание! Мы не будем продавать или распространять ваш адрес электронной почты. ОАО «ИнфоТеКС» ответственно подходит к защите вашей личной информации и принимает все меры для предотвращения несанкционированного доступа или разглашения информации, которую вы нам предоставляете.

- 5 В поле **Дополнительные сведения** вы можете указать любую дополнительную информацию. Например, ваши контактные данные, сообщение о возникшей проблеме или пожелания, касающиеся программного обеспечения ViPNet.

В поле **Код компьютера** отображается код, который однозначно идентифицирует ваш компьютер. Вы не можете изменить значение этого поля.

- Нажмите кнопку **Далее**. Откроется страница, отображающая состояние запроса на регистрацию. На этой странице ведется отсчет времени с начала текущей попытки регистрации. Обратите внимание, что на установление соединения с сервером отводится не более 3 минут.

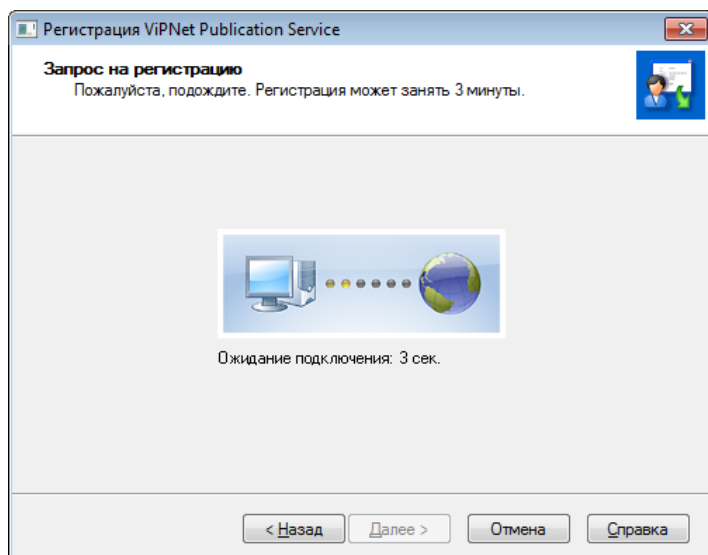


Рисунок 7. Ожидание подключения к серверу регистрации

Если в течение 3 минут соединение с сервером системы регистрации ОАО «ИнфоТеКС» не было установлено, вы увидите соответствующее сообщение.

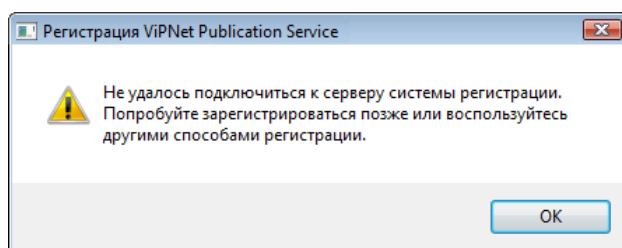


Рисунок 8. Сообщение о неудачной попытке подключения

Если соединение с сервером системы регистрации установлено успешно, но предоставленные вами данные оказались неверными, программа выдаст сообщение об этом.

В окне сообщения нажмите **ОК**, и вы вернетесь на страницу **Регистрационные данные**.

Если вам отказано в регистрации, откроется страница **Регистрационные данные**. Проверьте правильность введенного серийного номера и попробуйте зарегистрироваться снова.

Если регистрация прошла успешно, откроется страница **Регистрация ViPNet Publication Service успешно завершена**. На этой странице дана рекомендация, как безопасно сохранить ваши регистрационные данные (см. [Сохранение регистрационных данных](#) на стр. 35).

- Нажмите кнопку **Готово**.

Получение кода регистрации по электронной почте



Внимание! Для данного способа регистрации необходим доступ в Интернет.

Если вы выбрали способ регистрации **По электронной почте**, откроется страница **Регистрационные данные**. На этой странице выполните следующие действия:

- 1 Введите все данные, как описано в разделе [Получение кода регистрации через Интернет](#) (на стр. 27).
- 2 Нажмите кнопку **Далее**. В вашей почтовой программе будет создано новое сообщение электронной почты, содержащее указанные вами регистрационные данные. Сообщение будет адресовано на электронный почтовый ящик `reg@infotecs.biz`.

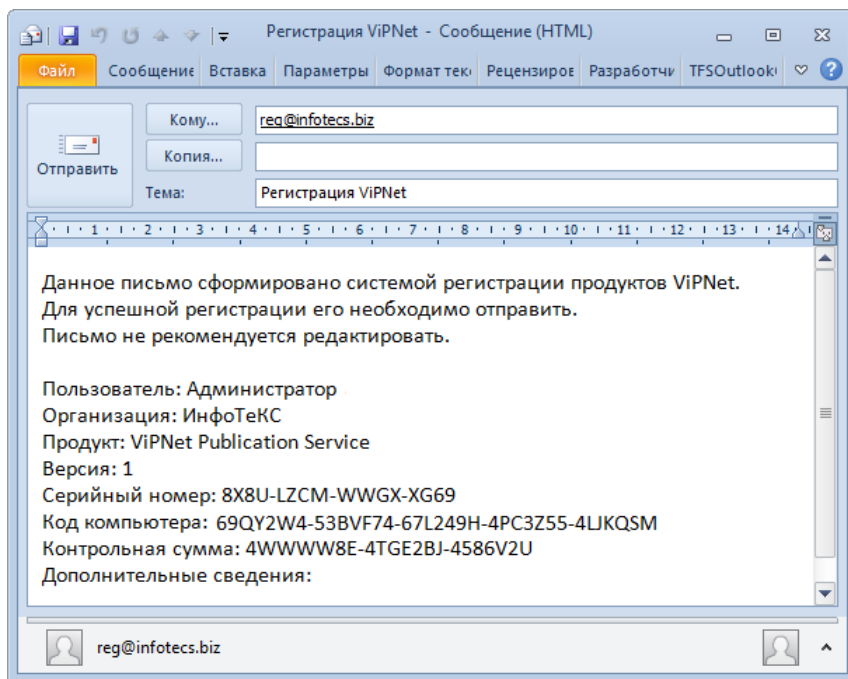


Рисунок 9. Запрос на регистрацию по электронной почте



Внимание! Мы не рекомендуем редактировать сообщение с регистрационными данными.

- 3 Для завершения регистрации отправьте это сообщение. После проверки ваших регистрационных данных вы получите код регистрации по электронной почте.



Внимание! Если в течение нескольких дней вы не получили ответ от компании «ИнфоТеКС», попробуйте снова отправить свое сообщение. Для этого повторите все шаги, описанные в данном разделе. Если после этого вам все же не удалось

зарегистрировать ViPNet Publication Service, обратитесь в службу поддержки ОАО «ИнфоТеКС».

- Получив сообщение с кодом регистрации, зарегистрируйте вашу копию ViPNet Publication Service (см. [Регистрация ViPNet Publication Service](#) на стр. 34).

Получение кода регистрации по телефону

Если вы выбрали способ регистрации **По телефону**, откроется страница **Запрос на регистрацию по телефону**, содержащая данные, которые вы должны будете сообщить сотруднику ОАО «ИнфоТеКС».

The screenshot shows a window titled "Регистрация ViPNet Publication Service" with a sub-header "Запрос на регистрацию по телефону". The main text instructs the user to call OAO "InfoTeKS" at (495) 737-6192 and provide registration information. Below this, a list of fields to be communicated is shown, with most marked as "Сообщается пользователем" (Provided by user). The "Код компьютера" (Computer code) is pre-filled with "69QY2W4-53BVF74-67L249H-4PC3Z55-4LJKQSM". The "Серийный номер" (Serial number) field is marked with a red asterisk and "Сообщается пользователем". A footnote explains that the serial number is provided by the support service. At the bottom are buttons for "< Назад", "Далее >", "Отмена", and "Справка".

Сообщите информацию для регистрации	
Пользователь:	Сообщается пользователем
Организация:	Сообщается пользователем
Продукт:	Сообщается пользователем
Версия программы:	4
Код компьютера:	69QY2W4-53BVF74-67L249H-4PC3Z55-4LJKQSM
Серийный номер *	Сообщается пользователем

* Позвонив в ОАО "ИнфоТеКС", Вы должны сообщить серийный номер, который получают при покупке программы. Если у Вас нет серийного номера, вернитесь в начало мастера регистрации.

Рисунок 10. Запрос на регистрацию по телефону

Выполните следующие действия:

- Позвоните в ОАО «ИнфоТеКС» по телефону, приведенному в верхней части страницы, и сообщите регистрационную информацию. В ответ вам будет сообщен код регистрации.
- Получив код регистрации, нажмите кнопку **Далее**, откроется страница **Зарегистрировать**.

Рисунок 11. Ввод кода регистрации

- 3 На странице **Зарегистрировать** введите ваши серийный номер и код регистрации, затем нажмите кнопку **Далее**.

Если введенные данные верны, откроется страница **Регистрация ViPNet Publication Service** успешно завершена. На этой странице приведены рекомендации, как безопасно сохранить ваши регистрационные данные (см. [Сохранение регистрационных данных](#) на стр. 35).

- 4 Нажмите кнопку **Готово**.

Регистрация через файл

Смысл регистрации через файл состоит в том, что вы перекладываете ответственность за получение кода регистрации на своего системного администратора. Вам не нужно лично запрашивать код регистрации у компании «ИнфоТекС». Вместо этого вы должны воспользоваться мастером **Регистрация ViPNet Publication Service** для формирования файла регистрационных данных и передать файл вашему системному администратору.

После того как администратор получает регистрационные данные от вас и от других пользователей ViPNet, он запрашивает коды регистрации и сообщает их пользователям. Получив от вашего системного администратора код регистрации, вы можете зарегистрировать ViPNet Publication Service.

Чтобы воспользоваться регистрацией через файл:

- 1 На странице **Способ запроса на регистрацию** выберите **Через файл** и нажмите кнопку **Далее**.
- 2 На странице **Регистрационные данные** введите все данные, как описано в разделе [Получение кода регистрации через Интернет](#) (на стр. 27). Нажмите кнопку **Далее**.
- 3 На странице **Сохранение регистрационных данных** нажмите кнопку **Обзор** и укажите папку, в которой будет сохранен файл с вашими регистрационными данными.

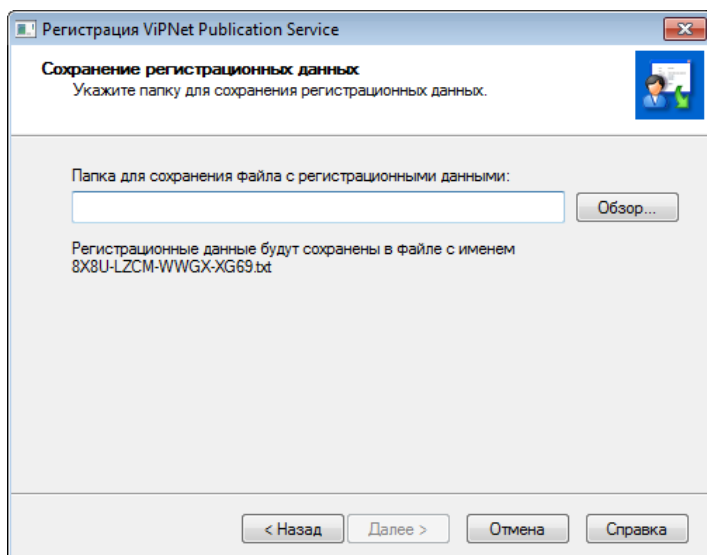


Рисунок 12. Сохранение регистрационных данных

- 4 Указав папку, нажмите кнопку **Далее**. Регистрационные данные будут сохранены в текстовом файле, имя которого совпадает с вашим серийным номером: <серийный номер>.txt.

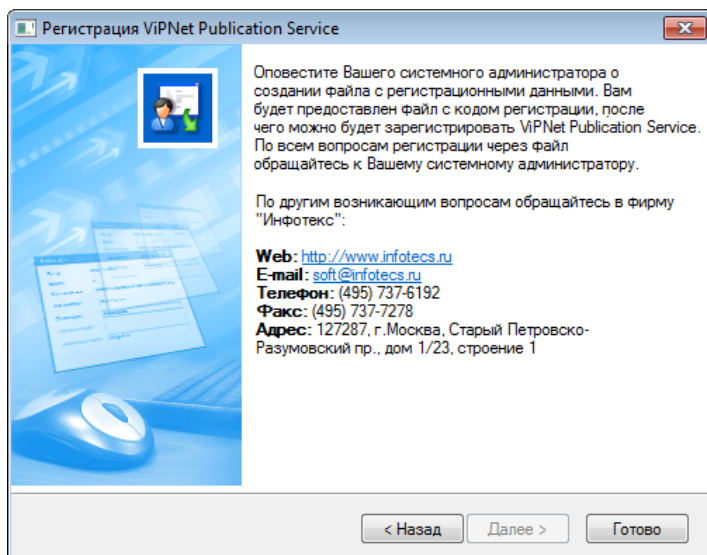


Рисунок 13. Страница с дальнейшими указаниями по групповой регистрации

- 5 На следующей странице мастера нажмите кнопку **Готово**.
- 6 Передайте файл, содержащий регистрационные данные, своему системному администратору.
- 7 Получив от администратора код регистрации, зарегистрируйте свою копию ViPNet Publication Service (см. [Регистрация ViPNet Publication Service](#) на стр. 34).

Регистрация ViPNet Publication Service

Получив от ОАО «ИнфоТекС» код регистрации, вы можете зарегистрировать вашу копию ViPNet Publication Service. Для этого выполните следующие действия:

- 1 Запустите мастер **Регистрация ViPNet Publication Service**.
- 2 На первой странице мастера выберите **Зарегистрировать** и нажмите кнопку **Далее**.
- 3 На странице **Серийный номер** введите ваш серийный номер и нажмите кнопку **Далее**.

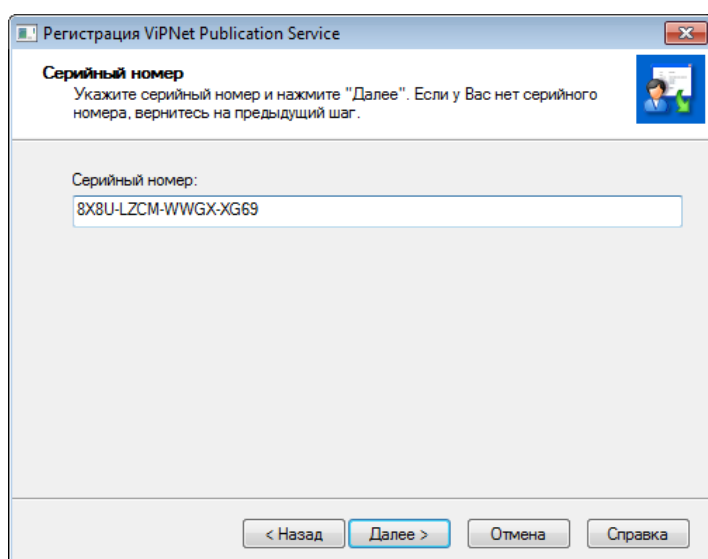


Рисунок 14. Ввод серийного номера



Примечание. Если вы вводили серийный номер раньше, поле **Серийный номер** будет заполнено автоматически.

- 4 На странице **Код регистрации**:
 - Если вы запрашивали код регистрации лично, выберите **Обычная регистрация** и введите код регистрации.
 - Если запрос на регистрацию делал ваш системный администратор, выберите **Регистрация через файл**, затем нажмите кнопку **Обзор** и укажите путь к файлу, содержащему код регистрации.

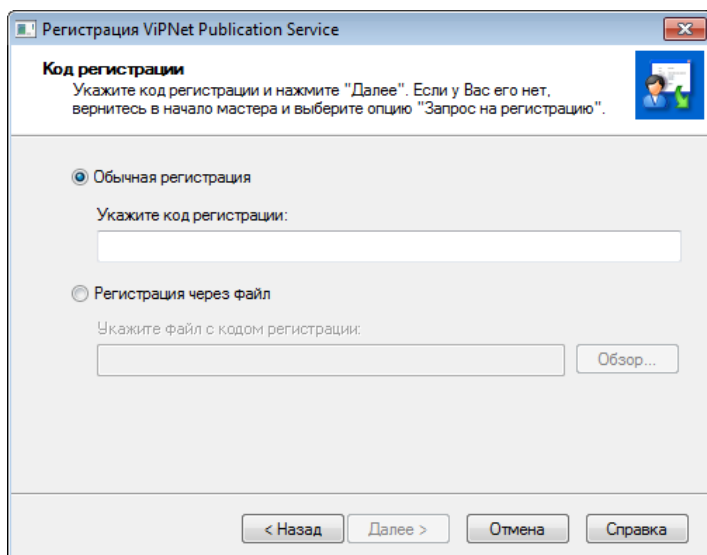


Рисунок 15. Выбор типа регистрации и ввод кода регистрации

- 5 Нажмите кнопку **Далее**. Если указанные вами данные верны, откроется страница **Регистрация ViPNet Publication Service успешно завершена**.

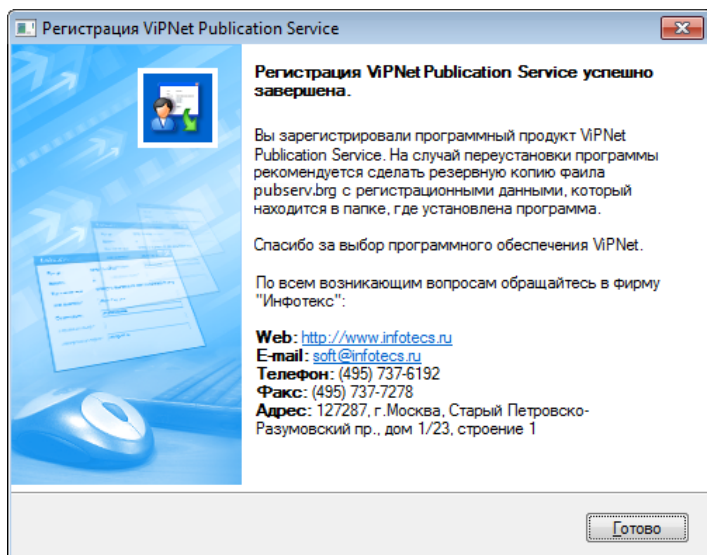


Рисунок 16. Регистрация успешно завершена

- 6 Нажмите кнопку **Готово**.
- 7 Сохраните регистрационные данные (см. [Сохранение регистрационных данных](#) на стр. 35), скопировав в надежное место файл *.brg, находящийся в папке установки программы ViPNet Publication Service.

Сохранение регистрационных данных

После завершения регистрации программа сохраняет регистрационные данные в файле *.brg, который создается в папке C:\ProgramData\InfoTeCS\ViPNet Publication Service\.



Примечание. Имя файла *.brg зависит от версии программного обеспечения ViPNet.

Мы рекомендуем скопировать файл регистрационных данных в надежное место, так как он может быть полезен при повторной установке ViPNet Publication Service (например, если вы хотите переустановить программу в другую папку или снова установить программу после форматирования жесткого диска). В таких случаях следует завершить работу с программой, поместить сохраненный файл *.brg в папки, указанные выше, и заново запустить программу. После запуска программа ViPNet Publication Service будет автоматически зарегистрирована (если регистрационные данные верны и конфигурация компьютера не изменилась).

Данные о регистрации (серийный номер, код компьютера и так далее) также сохраняются в протоколе регистрации `reginfo.txt`, который хранится в той же папке, что и файл с расширением *.brg. Вы можете использовать содержащиеся в этом файле данные, чтобы вручную зарегистрировать программу после переустановки (например, если файл *.brg потерян).

Если конфигурация вашего компьютера изменилась

Обновление конфигурации компьютера, на котором установлена программа ViPNet Publication Service, может сказаться на ее работе. Если изменение конфигурации было значительным (вы заменили большую часть комплектующих), необходимо перерегистрировать вашу копию ViPNet Publication Service (см. [Получение кода регистрации](#) на стр. 27). Если изменения в конфигурации были небольшими, вам не нужно снова регистрировать ViPNet Publication Service.

При первом запуске ViPNet Publication Service после небольшого обновления конфигурации программа выдаст сообщение о том, что в связи с изменением конфигурации компьютера был создан новый файл *.brg. Это значит, что прежний файл регистрационных данных устарел, и вы не можете использовать его для регистрации программы после переустановки.

Скопируйте новый файл *.brg в надежное место. Если вы переустановите ViPNet Publication Service, вам нужно будет скопировать этот файл в папку установки ViPNet Publication Service, и программа будет зарегистрирована.

4

Назначение публикаций

Публикация сертификатов и CRL	38
Импорт CRL из доверенных сетей ViPNet и сторонних УЦ	40
Настройка публикации данных в хранилище: порядок действий	41

Публикация сертификатов и CRL

При организации системы защищенного документооборота возникает потребность в публикации сертификатов и CRL в сетевые хранилища для общего доступа к ним всех участников документооборота. Вы сможете организовать автоматическую публикацию сертификатов и CRL с помощью программы ViPNet Publication Service.

Для публикации данных могут использоваться следующие хранилища (см. [Виды хранилищ и типы публикуемых данных](#) на стр. 39):

- Служба домена Active Directory (AD DS).
- Служба Active Directory облегченного доступа к каталогам (AD LDS).
- FTP-сервер.

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



Рисунок 17. Схема взаимодействия узлов, участвующих в документообороте

Механизм взаимодействия программных компонентов следующий:

- В системе имеется удостоверяющий центр (функции удостоверяющего центра осуществляет программа ViPNet Удостоверяющий и ключевой центр (далее — УКЦ)), который отвечает за формирование сертификатов и CRL. Новые сертификаты и CRL УКЦ помещает в специальную папку обмена.
- Программа ViPNet Publication Service следит за содержанием папки обмена с УКЦ и публикует сертификаты и CRL в соответствии с заданными правилами и в заданные хранилища. В процессе обработки также выполняется формирование файлов отчетов с результатами публикаций и возвращение в УКЦ неопубликованных данных.
- Из хранилищ по мере необходимости пользовательские приложения запрашивают данные сертификатов и CRL — для выполнения операций с документами.

Виды хранилищ и типы публикуемых данных

ViPNet Publication Service позволяет публиковать различные типы сертификатов в трех видах хранилищ. Сопоставление типов публикуемых данных и хранилищ приведено в таблице ниже.

Таблица 3. Виды хранилищ и типы публикуемых данных

Вид хранилища	Типы публикаций
AD DS	<ul style="list-style-type: none">Сертификаты пользователей. Примечание. Доступна только публикация сертификатов для конкретных учетных записей пользователей.CRL сетей ViPNetCRL сторонних УЦ
AD LDS	<ul style="list-style-type: none">Сертификаты пользователейСертификаты издателейCRL сетей ViPNetCRL сторонних УЦ
FTP-сервер	<ul style="list-style-type: none">Сертификаты издателейСертификаты пользователейCRL сетей ViPNetCRL сторонних УЦ

•

Импорт CRL из доверенных сетей ViPNet и сторонних УЦ

Кроме публикации CRL программа ViPNet Publication Service позволяет также выполнять автоматическую загрузку CRL из указанных точек распространения для их последующего импорта в удостоверяющий центр.

Данная возможность используется при необходимости распространения на узлы ViPNet CRL, выпущенных УЦ сетей ViPNet или сторонними УЦ. Распространение CRL на узлы сети ViPNet осуществляется в программе ViPNet Удостоверяющий и ключевой центр посредством функции обновления ключевой информации.

Поэтому, если в системе стоит задача импорта CRL из сторонних УЦ и доверенных сетей ViPNet, в программе ViPNet Publication Service нужно настроить точки распространения CRL (см. [Добавление точки распространения](#) на стр. 86). Эти точки (серверы HTTP, FTP, LDAP) будут опрашиваться программой ViPNet Publication Service с заданной в настройках периодичностью, и обновления CRL будут передаваться в УЦ.



Примечание. Размер импортируемого p7b-файла, содержащего CRL, не должен превышать 80 МБ.

Настройка публикации данных в хранилище: порядок действий

Чтобы настроить публикацию сертификатов или CRL в хранилище, выполните все действия из таблицы ниже в предложенном порядке для нужного типа хранилища.

Таблица 4. Порядок действий при настройке публикаций данных в хранилище

Действие	Ссылка на раздел или документ для использования
<input type="checkbox"/> Подготовьте хранилище данных для публикации.	Подготовка хранилищ данных (на стр. 42)
<input type="checkbox"/> Настройте УКЦ для отправки обновлений сертификатов и CRL в специализированную папку обмена.	Подготовка публикуемых данных в УКЦ (на стр. 61)
<input type="checkbox"/> В ViPNet Publication Service настройте папки приема и отправки данных в УКЦ.	Настройка папок обмена (на стр. 59)
<input type="checkbox"/> В ViPNet Publication Service добавьте публикации в подготовленные хранилища данных.	Добавление публикаций (на стр. 63)

5

Подготовка хранилищ данных

AD LDS	43
AD DS	51
FTP-сервер	53

AD LDS

Стандартная схема AD LDS не позволяет публиковать сертификаты и не содержит структуры для публикации CRL. Чтобы публиковать сертификаты и CRL в AD LDS, выполните следующие действия:

- 1 Расширьте схему AD LDS с помощью файлов, поставляемых с программой ViPNet Publication Service (см. [Расширение схемы AD LDS](#) на стр. 43).
- 2 Создайте контейнеры для размещения опубликованных данных (см. [Создание контейнеров для размещения опубликованных данных](#) на стр. 44).
- 3 Создайте учетную запись для публикации данных (см. [Создание учетной записи для публикации](#) на стр. 45).
- 4 Создайте группу учетных записей для публикации (см. [Создание группы учетных записей для публикации](#) на стр. 46) и добавьте в нее учетную запись, которая будет использоваться для публикации данных (см. [Добавление учетной записи для публикации в группу](#) на стр. 46).
- 5 Задайте права на публикацию и удаление данных (см. [Задание прав на публикацию и удаление данных](#) на стр. 47).
- 6 При необходимости разрешите анонимный доступ к опубликованным данным (см. [Разрешение анонимного доступа к опубликованным данным](#) на стр. 48).

Расширение схемы AD LDS

Для возможности публикации сертификатов и CRL в AD LDS необходимо расширить стандартную схему AD LDS с помощью файлов, поставляемых с программой ViPNet Publication Service. Файлы для расширения схемы AD LDS находятся в папке <Папка установки программы\scheme-update\win2k3-win2k8-adam>.



Примечание. По умолчанию ViPNet Publication Service устанавливается в папку C:\Program Files\InfoTeCS\ViPNet Publication Service в 32-разрядных версиях Windows и C:\Program Files (x86)\InfoTeCS\ViPNet Publication Service в 64-разрядных версиях.

Чтобы расширить схему AD LDS, выполните следующие действия:

- 1 Скопируйте файлы CDP.LDF и MS-InetOrgPerson-update-InfoTeCS.LDF в папку C:\Windows\ADAM.
- 2 Запустите командную строку от имени администратора.
- 3 Перейдите в папку с файлами для расширения с помощью команды `cd C:\Windows\ADAM`.
- 4 Добавьте возможность публикации CRL с помощью команды:

```
ldifde.exe -i -u -f "CDP.LDF" -s <адрес сервера>:<номер порта> -b <имя пользователя>  
<имя домена> <пароль> -k -j . -c "CN=Schema,CN=Configuration,DC=X"  
#schemaNamingContext
```

5 Добавьте возможность публикации сертификатов с помощью команды:

```
ldifde.exe -i -u -f "MS-InetOrgPerson-update-InfoTeCS.LDF" -s <адрес сервера>:<номер порта> -b <имя пользователя> <имя домена> <пароль> -k -j . -c "CN=Schema,CN=Configuration,DC=X" #schemaNamingContext
```

Создание контейнеров для размещения опубликованных данных

Чтобы создать контейнеры для размещения сертификатов и CRL, выполните следующие действия:

- 1 Запустите оснастку **Редактирование AD SI**.
- 2 В меню **Действие** выберите пункт **Подключение к**.
- 3 В открывшемся окне укажите параметры для подключения к каталогу приложений экземпляра AD LDS и нажмите кнопку **ОК**.

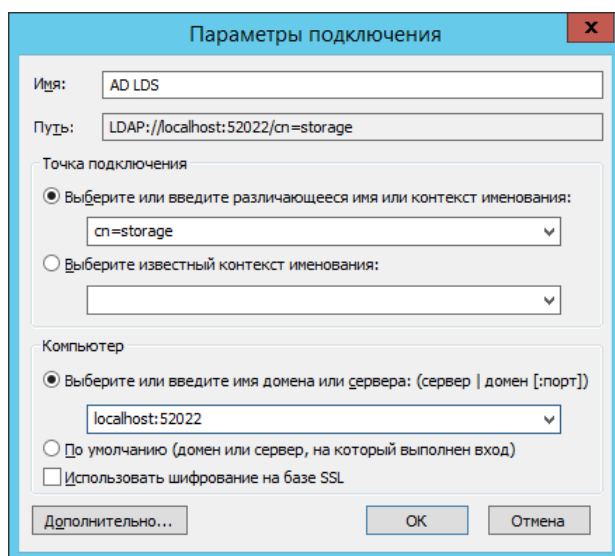


Рисунок 18. Подключение к каталогу приложений экземпляра AD LDS

- 4 В корневом каталоге создайте четыре контейнера с именами `userCerts`, `issuerCerts`, `vipnetCRL`, `nonVipnetCRL`. Для этого в контекстном меню корневого каталога выберите **Создать > Объект** и в окне **Создание объекта** поочередно, на каждой странице укажите ряд параметров. Для перемещения между страницами используйте кнопки **Далее** и **Назад**.
 - Выберите класс **container**.
 - В поле **Значение** задайте имя контейнера.
 - Нажмите кнопку **Готово**.
- 5 Аналогично создайте другие контейнеры.

В этих контейнерах будут размещаться сертификаты пользователей, [сертификаты издателей](#) (см. глоссарий, стр. 133), CRL сетей ViPNet и CRL сторонних УЦ соответственно. Структура раздела каталога примет приблизительно следующий вид:

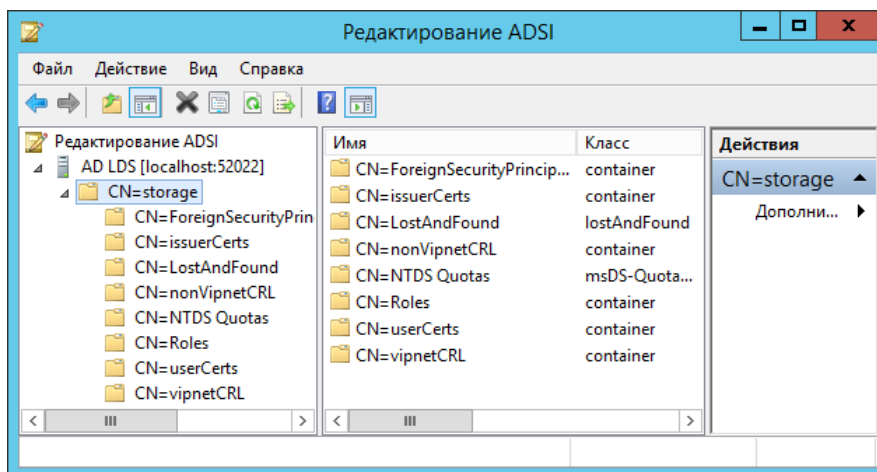


Рисунок 19. Примерная структура раздела каталога после добавления новых контейнеров

В дальнейшем, при настройке публикации в программе ViPNet Publication Service потребуется указать различающееся имя этих контейнеров, которое содержится в атрибуте **distinguishedName**. При настройке публикации для уменьшения вероятности ошибки рекомендуется использовать значение данного атрибута.

Создание учетной записи для публикации

Для публикации данных в AD LDS рекомендуется использовать отдельную учетную запись. Данные этой учетной записи потребуется указать при создании публикации в программе ViPNet Publication Service.

Если AD LDS развернута вне домена, создайте локальную учетную запись Windows.

Если AD LDS развернута в рамках домена, создайте доменную учетную запись. Для этого:

- 1 Запустите **Диспетчер серверов** и в меню **Средства** выберите пункт **Пользователи и компьютеры Active Directory**.
- 2 В контекстном меню каталога **Users** выберите **Создать > Пользователь**.
- 3 На первой странице мастера создания пользователя укажите следующие данные:
 - Имя и фамилию пользователя.
 - Имя пользователя для входа в домен. В данном руководстве будет использоваться имя **vipnetPublisher**.
- 4 На следующей странице мастера выполните следующие действия:
 - Задайте и подтвердите пароль.
 - Снимите флажок **Требовать смены пароля при следующем входе в систему**.
 - Установите флажок **Запретить смену пароля пользователем**.
 - Установите флажок **Срок действия пароля не ограничен**.
- 5 На последней странице мастера нажмите кнопку **Готово**.

Создание группы учетных записей для публикации

Созданную учетную запись, предназначенную для публикации данных, необходимо добавить в группу **Publishers**, которая будет размещаться внутри каталога AD LDS.

Чтобы создать группу учетных записей для публикации, выполните следующие действия:

- 1 Запустите оснастку **Редактирование ADSI**.
- 2 В меню **Действие** выберите пункт **Подключение к**.
- 3 В открывшемся окне укажите параметры для подключения к каталогу приложений экземпляра AD LDS и нажмите кнопку **ОК**.
- 4 В контейнере **cn=Roles,cn=storage** создайте группу с именем **Publishers**. Для этого в контекстном меню контейнера **cn=Roles** выберите **Создать > Объект** и в появившемся окне **Создание объекта** поочередно, на каждой странице укажите ряд параметров. Для перемещения между страницами используйте кнопки **Далее** и **Назад**.
 - Выберите класс **group**.
 - В поле **Значение** задайте имя группы.
 - Нажмите кнопку **Готово**.
- 5 Откройте свойства созданной группы и проверьте, что атрибут **groupType** имеет значение 0x80000002. Если это не так, дважды щелкните этот атрибут и задайте значение -2147483646.

Добавление учетной записи для публикации в группу

Чтобы добавить учетную запись для публикации в группу **Publishers**, выполните следующие действия:

- 1 Запустите оснастку **Редактирование ADSI**.
- 2 В меню **Действие** выберите пункт **Подключение к**.
- 3 В открывшемся окне укажите параметры для подключения к каталогу приложений экземпляра AD LDS и нажмите кнопку **ОК**.
- 4 Перейдите в контейнер **cn=Roles,cn=storage** и откройте свойства группы с именем **Publishers** (см. [Создание группы учетных записей для публикации](#) на стр. 46).
- 5 В списке **Атрибуты** дважды щелкните атрибут **member** и в открывшемся окне нажмите кнопку **Добавить учетную запись Windows**.

- 6 В открывшемся окне в соответствующем поле укажите имя учетной записи для публикации (см. [Создание учетной записи для публикации](#) на стр. 45) и нажмите кнопку **ОК**.
- 7 Сохраните внесенные изменения.

Задание прав на публикацию и удаление данных

Чтобы с помощью учетных записей для публикации можно было публиковать и удалять данные из хранилища AD LDS, группе учетных записей для публикации необходимо задать соответствующие права.



Примечание. Чтобы уменьшить вероятность случайного удаления данных из хранилища, рекомендуется задавать права на удаление данных только в случае действительной необходимости.

Назначение прав доступа осуществляется с помощью консольной утилиты **dscls**.

Чтобы настроить права на публикацию и удаление данных, запустите командную строку от имени администратора и выполните следующие действия:

- Чтобы задать разрешение на чтение опубликованных данных, выполните команду:

```
dscls \\<IP-адрес или DNS-имя экземпляра AD LDS>:<порт экземпляра AD LDS>\cn=storage /I:T /G cn=Publishers,cn=Roles,cn=storage:GR
```
- Чтобы задать разрешение на публикацию сертификатов пользователей, выполните команды:

```
dscls \\<IP-адрес или DNS-имя экземпляра AD LDS>:<порт экземпляра AD LDS>\cn=userCerts,cn=storage /I:S /G cn=Publishers,cn=Roles,cn=storage:GW
```

```
dscls \\<IP-адрес или DNS-имя экземпляра AD LDS>:<порт экземпляра AD LDS>\cn=userCerts,cn=storage /I:T /G cn=Publishers,cn=Roles,cn=storage:CC
```
- Чтобы задать разрешение на удаление опубликованных сертификатов пользователей, выполните команду:

```
dscls \\<IP-адрес или DNS-имя экземпляра AD LDS>:<порт экземпляра AD LDS>\cn=userCerts,cn=storage /I:T /G cn=Publishers,cn=Roles,cn=storage:DC
```
- Чтобы задать разрешение на публикацию сертификатов издателей, выполните команды:

```
dscls \\<IP-адрес или DNS-имя экземпляра AD LDS>:<порт экземпляра AD LDS>\cn=issuerCerts,cn=storage /I:S /G cn=Publishers,cn=Roles,cn=storage:GW
```

```
dscls \\<IP-адрес или DNS-имя экземпляра AD LDS>:<порт экземпляра AD LDS>\cn=issuerCerts,cn=storage /I:T /G cn=Publishers,cn=Roles,cn=storage:CC
```
- Чтобы задать разрешение на удаление опубликованных сертификатов издателей, выполните команду:

```
dscls \\<IP-адрес или DNS-имя экземпляра AD LDS>:<порт экземпляра AD LDS>\cn=issuerCerts,cn=storage /I:T /G cn=Publishers,cn=Roles,cn=storage:DC
```
- Чтобы задать разрешение на публикацию CRL сетей ViPNet, выполните команды:

```
dsaclс \\<IP-адрес или DNS-имя экземпляра AD LDS>:<порт экземпляра AD
LDS>\cn=vipnetCRL,cn=storage /I:S /G cn=Publishers,cn=Roles,cn=storage:GW

dsaclс \\<IP-адрес или DNS-имя экземпляра AD LDS>:<порт экземпляра AD
LDS>\cn=vipnetCRL,cn=storage /I:T /G cn=Publishers,cn=Roles,cn=storage:CC
```

- Чтобы задать разрешение на публикацию CRL сторонних УЦ, выполните команды:

```
dsaclс \\<IP-адрес или DNS-имя экземпляра AD LDS>:<порт экземпляра AD
LDS>\cn=nonVipnetCRL,cn=storage /I:S /G cn=Publishers,cn=Roles,cn=storage:GW

dsaclс \\<IP-адрес или DNS-имя экземпляра AD LDS>:<порт экземпляра AD
LDS>\cn=nonVipnetCRL,cn=storage /I:T /G cn=Publishers,cn=Roles,cn=storage:CC
```

В результате группе учетных записей будут назначены необходимые права.

Разрешение анонимного доступа к опубликованным данным

Анонимный доступ дает возможность стороннему ПО читать опубликованные в хранилище данные без необходимости проходить аутентификацию.

Анонимный доступ подразумевает анонимную привязку к объектам каталога, которая по умолчанию запрещена. Чтобы разрешить анонимный доступ, выполните следующие действия:

- 1 Запустите оснастку **Редактирование ADSI**.
- 2 В меню **Действие** выберите пункт **Подключение к**.
- 3 В открывшемся окне укажите параметры для подключения к каталогу конфигурации экземпляра AD LDS и нажмите кнопку **ОК**.
- 4 Перейдите в контейнер **CN=Windows NT,CN=Services, CN=Configuration,CN={GUID}** и откройте свойства объекта **CN=Directory Service**.
- 5 В списке **Атрибуты** дважды щелкните атрибут **dsHeuristics** и в открывшемся окне задайте значение **0000002**.
- 6 Сохраните внесенные изменения.

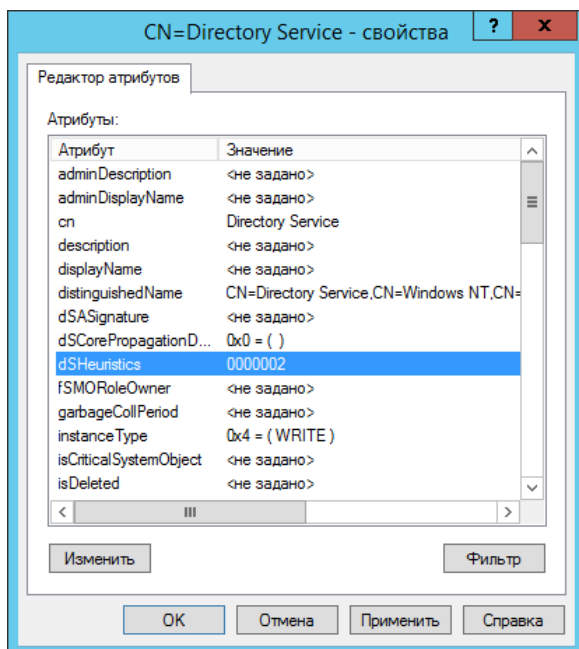


Рисунок 20. Значение атрибута dSHeuristics

Теперь необходимо назначить разрешения на доступ анонимных пользователей к соответствующим объектам в данном каталоге. Для этого:

- 1 Запустите оснастку **Редактирование ADSI**.
- 2 В меню **Действие** выберите пункт **Подключение к...**
- 3 В открывшемся окне укажите параметры для подключения к каталогу приложений экземпляра AD LDS и нажмите кнопку **ОК**.
- 4 Перейдите в контейнер **cn=Roles,cn=storage** и откройте свойства группы **Readers**.
- 5 В списке **Атрибуты** дважды щелкните атрибут **member** и в открывшемся окне нажмите кнопку **Добавить учетную запись Windows**.
- 6 В открывшемся окне нажмите кнопку **Дополнительно**.
- 7 В окне **Выбор** выполните следующие действия:
 - Нажмите кнопку **Размещение** и в качестве места поиска укажите ваш компьютер.
 - Нажмите кнопку **Поиск**.
 - В списке **Результаты поиска** выберите учетную запись **АНОНИМНЫЙ ВХОД** и нажмите кнопку **ОК**.

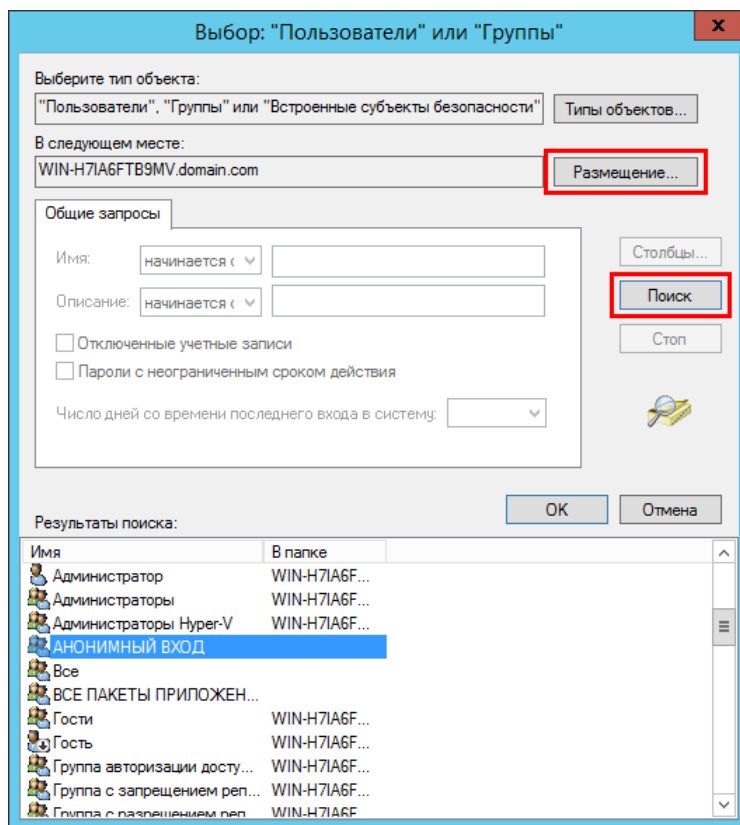


Рисунок 21. Добавление анонимного участника безопасности.

8 Сохраните внесенные изменения.

AD DS



Примечание. Подробную информацию о развертывании и настройке AD DS см. на сайте Microsoft <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-deployment>.

Стандартная структура AD DS позволяет публиковать в хранилище только сертификаты пользователей этого домена. Если требуется публиковать CRL сетей ViPNet и CRL сторонних УЦ в AD DS, необходимо создать соответствующие контейнеры. Для этого:

- 1 Запустите оснастку **Редактирование AD SI**.
- 2 В меню **Действие** выберите пункт **Подключение к**.
- 3 В открывшемся окне укажите параметры подключения к AD DS и нажмите кнопку **ОК**.

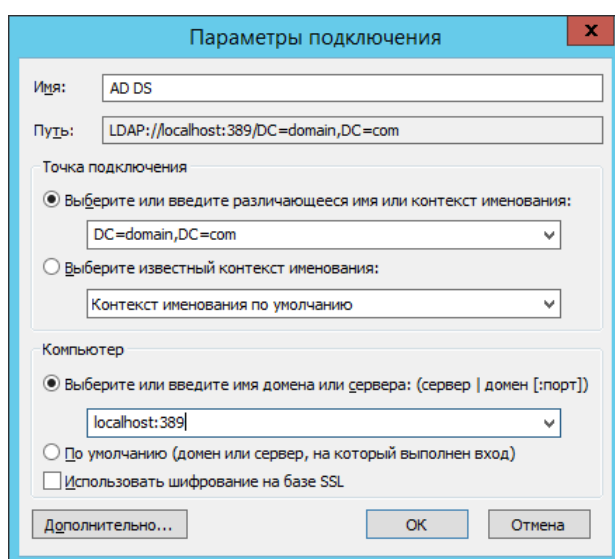


Рисунок 22. Параметры подключения к AD DS

- 4 В корневом каталоге хранилища создайте два контейнера с именами `vipnetCRL` и `nonVipnetCRL`. Для этого в контекстном меню корневого каталога выберите **Создать > Объект** и в окне **Создание объекта** поочередно, на каждой странице укажите ряд параметров. Для перемещения между страницами используйте кнопки **Далее** и **Назад**.
 - Выберите класс **container**.
 - В поле **Значение** задайте имя контейнера.
 - Нажмите кнопку **Готово**.
- 5 Аналогично создайте второй контейнер.

В этих контейнерах будут размещаться CRL сетей ViPNet и CRL сторонних сетей соответственно. Структура раздела каталога примет приблизительно следующий вид:

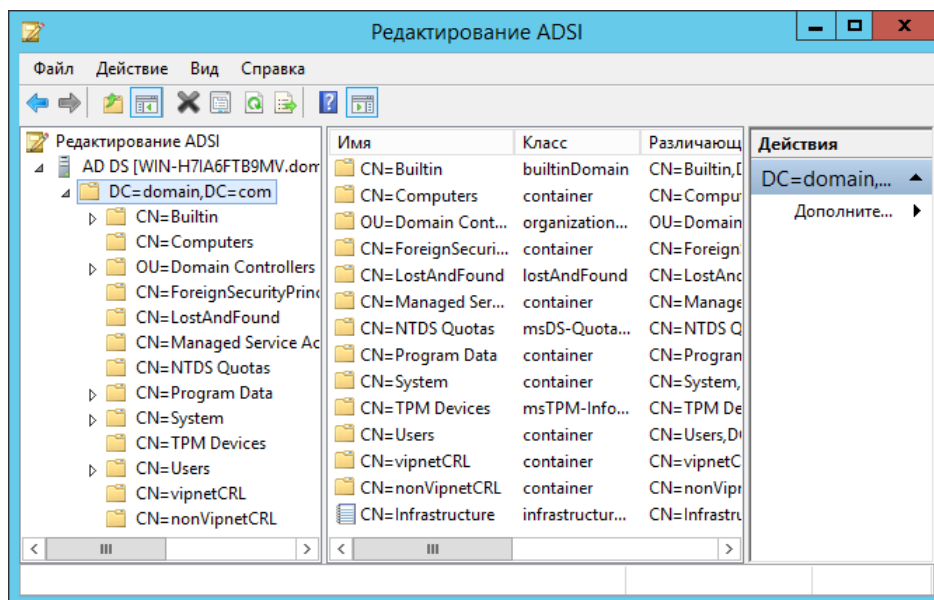


Рисунок 23. Создание контейнера для публикации CRL

В дальнейшем, при настройке публикации в программе ViPNet Publication Service потребуется указать различающееся имя этих контейнеров, которое содержится в атрибуте **distinguishedName** (в нашем примере **CN=vipnetCRL,DC=domain,DC=com** и **CN=nonVipnetCRL,DC=domain,DC=com**). При настройке публикации для уменьшения вероятности ошибки рекомендуется использовать значение данного атрибута.

FTP-сервер

Практическое использование FTP

Программа ViPNet Publication Service позволяет организовать систему автоматической публикации на FTP-сервере следующих типов данных:

- Сертификаты издателей.
- Сертификаты пользователей.
- CRL сетей ViPNet.
- CRL сторонних УЦ.



Примечание. Чтобы избежать возникновения ошибок, публиковать сертификаты пользователей, издателей и CRL необходимо в разных папках на сервере FTP.



Внимание! Публикация сертификатов, в которых не указан идентификатор ключа проверки электронной подписи, не поддерживается. Сертификаты, не содержащие данного поля, можно опубликовать только в хранилище AD LDS.

Типичной причиной, по которой требуется публикация на FTP-сервере, является необходимость обеспечить доступ к сертификатам издателей, пользователей или CRL за пределами локальной сети организации. Такая необходимость может возникнуть при создании защищенного документооборота между двумя и более организациями.

Например, в организации В необходимо проверять электронную подпись документов, полученных из организации А. Для полноценной проверки электронной подписи пользователям в организации В нужно иметь актуальный CRL и сертификат издателя организации А. Доступ пользователей к актуальным CRL и сертификату издателя организации А можно настроить двумя способами.

Если пользователи организации В имеют доступ в Интернет и, следовательно, к опубликованным CRL и сертификату издателя организации А, то можно использовать технологию точек распространения CRL и сертификата издателя. В соответствии с этой технологией в сертификате пользователя прописываются точки распространения, с которых автоматически загружаются сертификат издателя и актуальные CRL.

Если пользователи организации В не имеют доступа в Интернет и, следовательно, к опубликованным CRL и сертификату издателя организации А, то администраторы организаций А и В могут организовать доступ к CRL и сертификату издателя следующим образом:

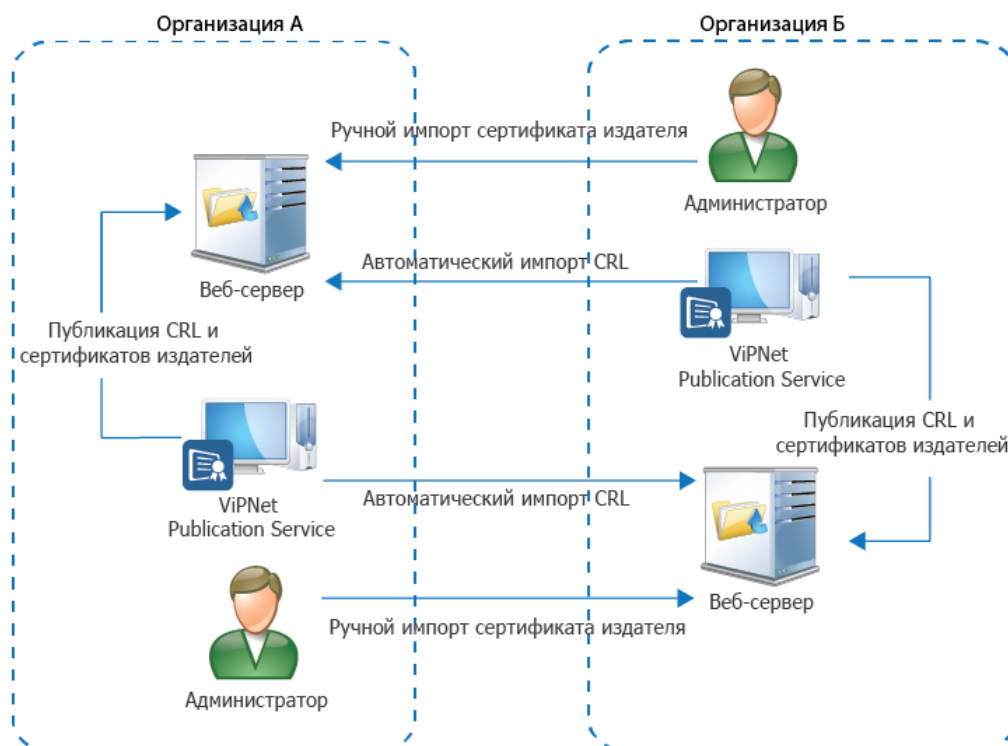


Рисунок 24. Схема организации доступа к CRL и сертификатам издателей

- 1 Администраторы организаций А и В настраивают публикацию своих сертификатов издателей и CRL на своих веб-серверах по FTP-протоколу и делают их доступными по протоколу HTTP (предоставляют возможность скачивать CRL и сертификатов издателей с помощью веб-страницы).
- 2 Администратор организации В загружает сертификат издателя с веб-сайта организации А и распространяет его среди пользователей своей организации.
- 3 Администратор организации В копирует URL-адрес доступа к CRL организации А и настраивает ViPNet Publication Service на импорт CRL по данному адресу (см. [Настройка автоматической загрузки CRL](#) на стр. 85). Загруженные таким образом CRL будут импортированы в удостоверяющий центр. Далее администратор организации В должен разослать импортированные CRL пользователям своей сети.

При использовании ViPNet УКЦ загруженные таким образом CRL будут импортированы в программу ViPNet Удостоверяющий и ключевой центр. С помощью ViPNet УКЦ администратор организации В должен сформировать обновление ключей, которые будут содержать импортированный CRL, и разослать их пользователям своей сети.

- 4 В результате сертификаты издателей и CRL дадут возможность пользователям организации В проверять электронную подпись документов, полученных из организации А.

Настройка FTP-сервера

Информацию по разворачиванию FTP-сервера см. в документации конкретного ПО FTP. Прежде, чем приступить к публикации, необходимо провести настройку FTP-сервера, следуя предложенным

правилам. Для каждого типа публикуемых данных на сервере должна быть выделена отдельная папка:



Примечание. Для некоторых типов FTP-серверов регистр имен папок имеет значение.

- Issuers — папка для сертификатов издателей. В этой папке, кроме самих сертификатов будет храниться связанная с издателем информация.
- UserCerts — папка для сертификатов пользователей.
- CDP — папка для CRL, изданных ViPNet Удостоверяющий и ключевой центр.
- otherCDP — папка для CRL, изданных сторонними УЦ.

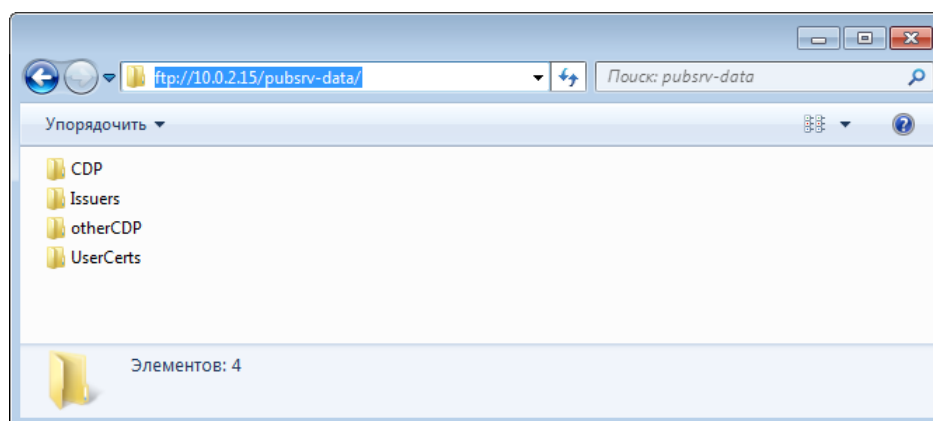


Рисунок 25. Названия папок для публикации на FTP-сервере

Совет. Для публикации рекомендуется создать на FTP-сервере отдельную учетную запись. При ее настройке следует учесть, что публикация подразумевает операции создания, модификации и удаления папок/файлов на FTP-сервере.



Если в дальнейшем планируется организовать анонимный доступ к опубликованным данным по ftp-протоколу, то учетную запись для публикации желательно настроить так, чтобы ее домашний каталог совпадал с домашним каталогом учетной записи anonypous. В этом случае вам скорее всего не придется корректировать автоматически созданные (по отчетам от ViPNet Publication Service) точки распространения CRL и сертификатов издателей в настройках программы ViPNet Удостоверяющий и ключевой центр.

Внимание! При использовании FTP-сервера Serv-U необходимо убедиться в соблюдении следующих условий:



- домашний каталог учетной записи, которая используется для публикации на FTP-сервере, совпадает с домашним каталогом учетной записи anonypous;
 - параметр **Lock user in home directory** настроен одинаково для учетной записи anonypous и учетной записи, которая используется для публикации.
-

При публикации CRL или сертификата издателя создается отчет, который содержит URL-адрес доступа к опубликованным данным. Чтобы в дальнейшем можно было получить доступ к этим данным по протоколу FTP через анонимную учетную запись, которая используется браузерами и программой ViPNet Publication Service при импорте CRL, необходимы указанные выше настройки.

Данные на FTP-сервере размещаются в указанных папках по определенным правилам (подробнее см. раздел [Структура папок при размещении данных на FTP](#) (на стр. 56)).

Структура папок при размещении данных на FTP



Примечание. Каждый сертификат издателя или CRL хранится в отдельной папке, имя которой формируется по определенным правилам.

Более подробная информация о формате размещения данных в хранилище содержится в документе «ViPNet Publication Service. Форматы хранения опубликованных данных».

Для сертификатов издателей папки формируются автоматически на основе идентификатора ключа проверки электронной подписи.

Имя папки = "kid" + Шестнадцатеричное представление идентификатора.

Например: kid131890B2951899E62159569AE7D542AA3766ED3B

Внутри папки размещаются файлы с именами:

- 1 subject — бинарный файл. Хранит имя издателя (владельца) в формате ASN.1
- 2 issuer.crt — бинарный файл. Хранит сертификат издателя в кодировке DER.

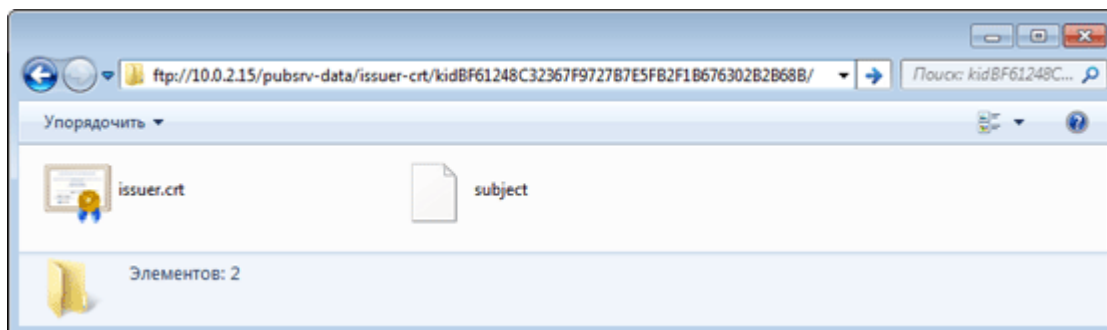


Рисунок 26. Структура хранения сертификатов издателей на FTP-сервере

Сертификаты пользователей используют в целом ту же схему хранения, что и сертификаты издателей. Отличия в следующем:

- 1 Сертификат пользователя хранится в файле с именем user.crt.

- 2 Для успешной публикации сертификат пользователя должен иметь расширение Subject Key Identifier. Фактически это означает, что имя папки с сертификатом пользователя всегда имеет следующий вид: kid131890B2951899E62159569AE7D542AA3766ED3B.

При размещении CRL сетей ViPNet на FTP-сервере, имя папки формируется следующим образом:

Имя папки = номер сети в десятичном формате + дефис + kid + Шестнадцатеричное представление идентификатора.

Пример: 4342-kidBE5FB4BC7096CC236CBFD60909851345CCA43B39

При размещении CRL сторонних сетей на FTP-сервере, имя папки формируется следующим образом:

Имя каталога = IssuerDisplayName + дефис + "kid" + Шестнадцатеричное представление идентификатора.

IssuerDisplayName строится на основе одного из предопределенных атрибутов имени издателя по следующему правилу: если в имени задан CN, то IssuerDisplayName = CN. Если в имени задан Pseudonym, то IssuerDisplayName = Pseudonym. Далее, аналогично для атрибутов: OU и O.

Пример: AtlasNW-App CA-kidBE5FB4BC7096CC236CBFD60909851345CCA43B39

Независимо от типа CRL внутри папки размещаются файлы с именами:

- 1 issuer – бинарный файл. Хранит имя издателя в формате ASN.1
- 2 revokedCerts.crl – бинарный файл. Хранит CRL в кодировке DER.

6

Настройка взаимодействия программ ViPNet Удостоверяющий и ключевой центр и ViPNet Publication Service

Настройка папок обмена	59
Подготовка публикуемых данных в УКЦ	61

Настройка папок обмена

Обмен данными между программами ViPNet Publication Service и [ViPNet Удостоверяющий и ключевой центр](#) (см. глоссарий, стр. 132) осуществляется через папки обмена, которые должны быть заданы в этих программах. Программа ViPNet Удостоверяющий и ключевой центр помещает в заданную папку обмена данные, которые требуется опубликовать. Программа ViPNet Publication Service помещает в папку обмена отчеты о публикации данных.



Примечание. Для обмена файлами между программами ViPNet Удостоверяющий и ключевой центр и ViPNet Publication Service рекомендуется отдавать предпочтение локальным, а не сетевым папкам, так как уведомления об изменениях содержимого папки, находящейся в общем доступе, не всегда работают корректно. Поэтому возможны ситуации, когда программа ViPNet Publication Service не может получить информацию о появлении новых файлов в такой папке.

Кроме того, при выборе сетевых папок могут возникнуть проблемы при настройке прав доступа к папкам и их содержимому.

Также необходимо обеспечить доступность папок обмена, а также обеспечить возможность изменения содержимого папок. Если при запуске программы папки обмена данными будут недоступны, будет выведено соответствующее предупреждение.

Если программы ViPNet Удостоверяющий и ключевой центр и ViPNet Publication Service установлены на разных компьютерах, необходимо обеспечить сетевой доступ к заданным папкам обмена для компьютера, на котором установлена программа ViPNet Publication Service.

Схема обмена файлами между УКЦ и Сервисом публикации представлена ниже.



Рисунок 27. Схема обмена данными между программами ViPNet УКЦ и ViPNet Publication Service

Чтобы в программе ViPNet Publication Service указать папки для обмена данными с УКЦ, выполните следующие действия:

- 1 В окне программы на панели навигации выберите раздел **Настройки**.

- 2 В поле **Папка приема файлов из Удостоверяющего и Ключевого центра** с помощью кнопки **Обзор** укажите папку для приема данных из УКЦ.

Файлы, попадающие в папку приёма файлов от УКЦ, могут оставаться необработанными в следующих случаях:

- публикация подходящего типа не создана;
- публикация подходящего типа создана, но не включена(неактивна).

Диагностировать указанные ситуации можно по сообщениям в журнале публикации на вкладке **Прочее** (см. [Просмотр журнала публикаций](#) на стр. 80).

- 3 В поле **Папка отправки файлов в Удостоверяющий и Ключевой центр** с помощью кнопки **Обзор** укажите папку для передачи отчетов о публикации в УКЦ.

В указанной папке отправки файлов будет автоматически создана папка `\unpublished` для передачи в УКЦ сертификатов и CRL, при публикации которых возникли ошибки.

Внимание! Заданные папки обмена должны совпадать с папками, указанными в настройках программы ViPNet Удостоверяющий и ключевой центр. Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».



Кроме того, в случае использования сетевых папок обмена данными с УКЦ мы рекомендуем выполнить сопоставление локальных папок программы ViPNet Publication Service с сетевыми папками обмена данных с УКЦ. Затем в разделе **Общие** укажите локальные пути к сопоставленным папкам программы ViPNet Publication Service. В противном случае папка `\unpublished` не будет создана, и сертификаты и CRL, при публикации которых возникли ошибки, не будут переданы в УКЦ.

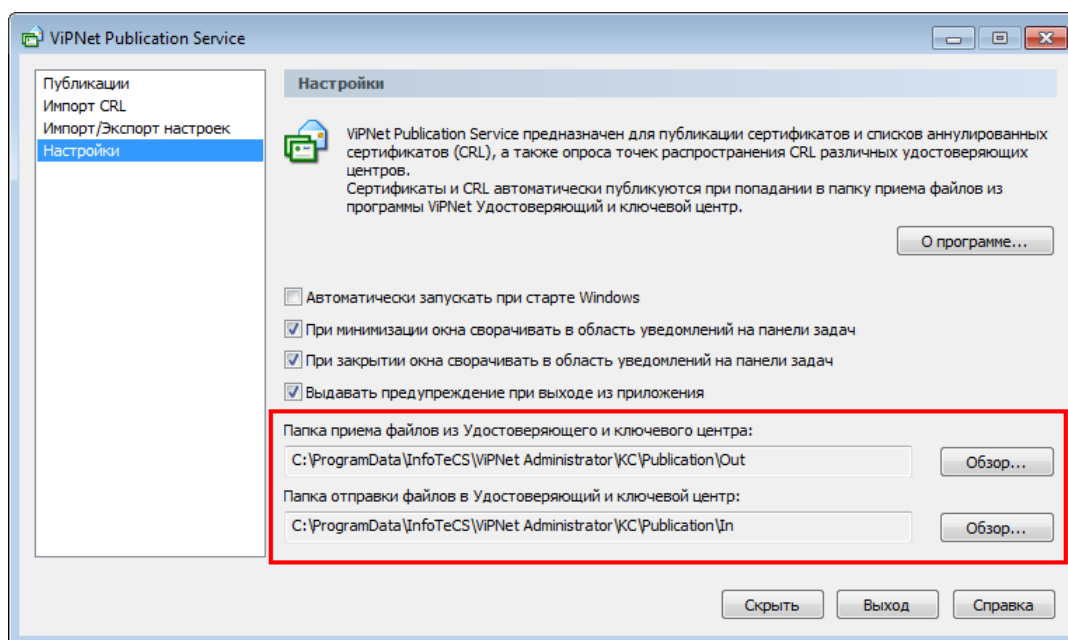


Рисунок 28. Задание папок обмена файлами между УКЦ и Сервисом публикаций

Подготовка публикуемых данных в УКЦ

В программе ViPNet Удостоверяющий и ключевой центр необходимо указать, какие данные подлежат публикации, чтобы эти данные были помещены в папку обмена с ViPNet Publication Service.

Отправку данных из УКЦ в папку обмена можно производить в двух режимах:

- автоматически;
- вручную.

В автоматическом режиме на публикацию можно передать только новые изданные сертификаты пользователей и обновленные CRL сети ViPNet. В ручном режиме на публикацию можно передать сертификаты издателей, кросс-сертификаты, сертификаты пользователей и CRL сети ViPNet.

Для настройки автоматического режима выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка**.
- 2 Чтобы настроить переход в автоматический режим при бездействии администратора (в том случае, если не будут производиться никакие действия в программе в течение заданного времени), в окне **Настройка** перейдите в раздел **Автоматический режим**, установите соответствующий флажок и в поле ниже укажите время бездействия в программе.

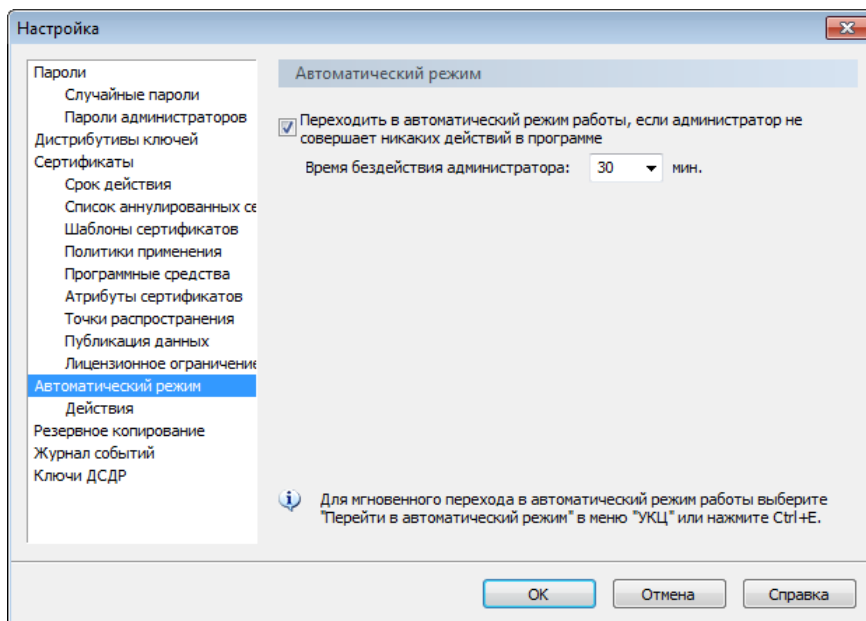


Рисунок 29. Настройка параметров перехода в автоматический режим работы в случае бездействия администратора

- 3 Чтобы передавать на публикацию сертификаты пользователей после издания, в окне **Настройка** перейдите в раздел **Сертификаты** и установите флажок **Публиковать сертификат пользователя после издания**.
- 4 Чтобы передавать на публикацию CRL после обновления, в окне **Настройка** перейдите в раздел **Сертификаты** > **Список аннулированных сертификатов**. В группе **Действия после обновления списка аннулированных сертификатов** установите флажок **Публиковать список аннулированных сертификатов**.
- 5 В окне **Настройка** нажмите кнопку **ОК**, чтобы сохранить настройки.

В результате при после издания сертификатов пользователей или обновлений CRL они будут автоматически помещаться в папку приема файлов из Удостоверяющего и ключевого центра.

Чтобы отправить данные для публикации в папку обмена в ручном режиме:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр выберите объекты, которые требуется передать для публикации: изданные сертификаты пользователей, администраторов, кросс-сертификаты или CRL сети ViPNet.



Примечание. Публикация сертификатов сторонних УЦ, сертификатов пользователей сторонних УЦ и CRL сторонних УЦ из программы ViPNet УКЦ не предусмотрен. Для этого необходимо вручную скопировать файлы сертификатов и CRL в **Папку приема файлов из Удостоверяющего и ключевого центра** (см. [Настройка папок обмена](#) на стр. 59).

- 2 В контекстном меню выбранных объектов выберите пункт **Опубликовать**.

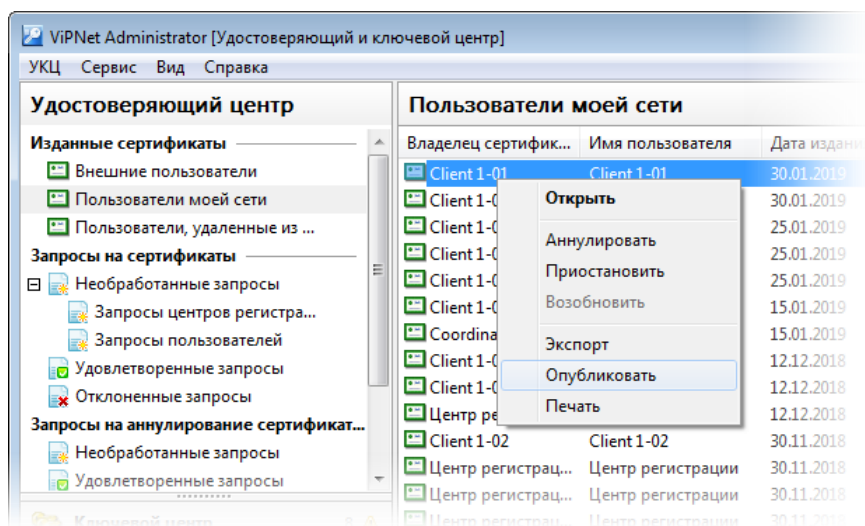


Рисунок 30. Отправка данных для публикации из УКЦ в папку обмена

В результате файлы выбранных объектов будут помещены в папку приема файлов из Удостоверяющего и ключевого центра.

7

Добавление публикаций

Публикация в AD LDS	64
Публикация в AD DS	67
Публикация на FTP-сервер	71
Изменение параметров публикации	73
Отключение и удаление публикации	74

Публикация в AD LDS



Примечание. В AD LDS могут публиковаться сертификаты пользователей, сертификаты издателей (корневые и кросс-сертификаты), CRL сетей ViPNet и сторонних УЦ.

Для добавления публикации в AD LDS выполните следующие действия:

- 1 В главном окне программы перейдите в раздел **Публикации** и нажмите кнопку **Добавить**.

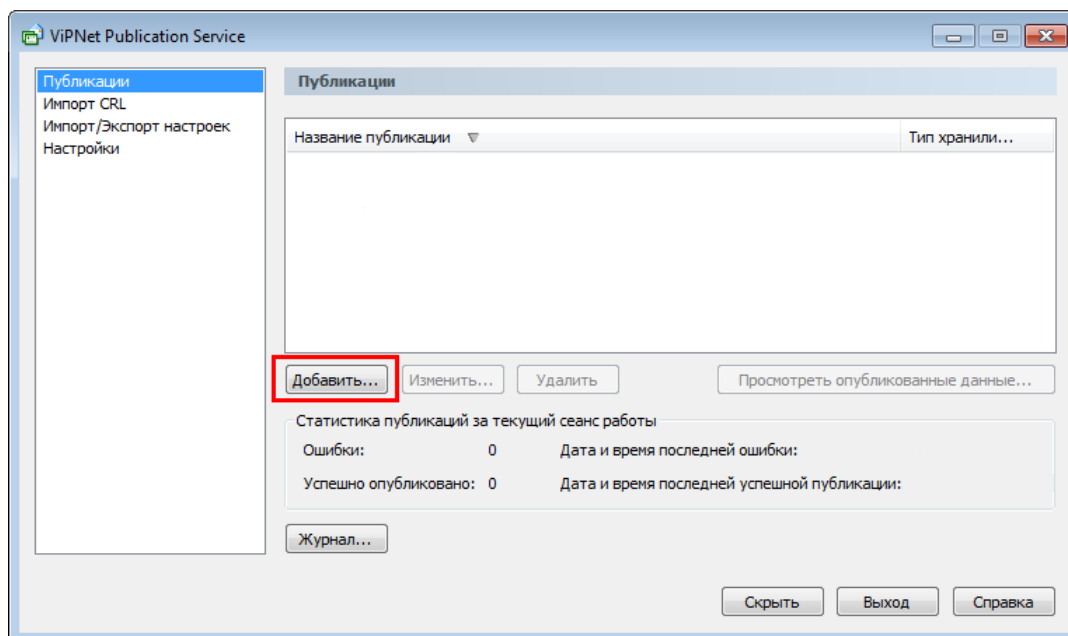


Рисунок 31. Добавление новой публикации

- 2 В окне **Мастер создания публикации** поочередно, на каждой странице укажите ряд параметров. Для перемещения между страницами используйте кнопки **Далее** и **Назад**.
 - **Тип публикуемых данных:** выберите нужное значение.
 - **Тип хранилища:** выберите **AD LDS**.
 - **Параметры подключения:** укажите IP-адрес или DNS-имя и номер порта для подключения к экземпляру AD LDS.
 - **Учетная запись:** введите имя пользователя и пароль учетной записи Windows или учетной записи AD LDS.
 - **Состояние схемы:** нажмите кнопку **Проверить состояние схемы**, чтобы убедиться в возможности взаимодействия схемы AD LDS с ViPNet Publication Service.
 - **Параметры публикации:** если вы хотите публиковать сертификаты, у которых в имени владельца содержатся неизвестные атрибуты, установите соответствующий флажок.



Примечание. При добавлении публикации CRL страница **Параметры публикации** не отображается.

- **Контейнер:** укажите имя контейнера в формате X.500.

Например:

- В случае публикации сертификатов пользователей: CN=userCerts, cn=storage.
- В случае публикации сертификатов издателей: CN=issuerCerts, cn=storage.
- В случае публикации CRL сетей ViPNet: CN=vipnetCRL, cn=storage.
- В случае публикации CRL сторонних сетей: CN=nonVipnetCRL, cn=storage.

- **Название публикации:** введите название, которое будет отображаться в списке публикаций. По умолчанию название складывается из типа публикуемых данных и адреса сервера, например: «Сертификаты пользователей на 192.168.77.20».



Примечание. При изменении параметров публикации (например, тип публикуемых данных) рекомендуется также менять название публикации, чтобы избежать расхождения названия с назначением публикации.

- **Сводка:** проверьте все параметры создаваемой публикации, проведите тест публикации, нажав кнопку **Проверить указанные параметры**.

Нажмите кнопку **Готово** для окончания процесса создания публикации.

Чтобы вернуться к редактированию параметров публикации, нажмите кнопку **Назад**. Для отмены процесса создания публикации нажмите кнопку **Отмена**.

В результате в списке публикаций появится созданная публикация.

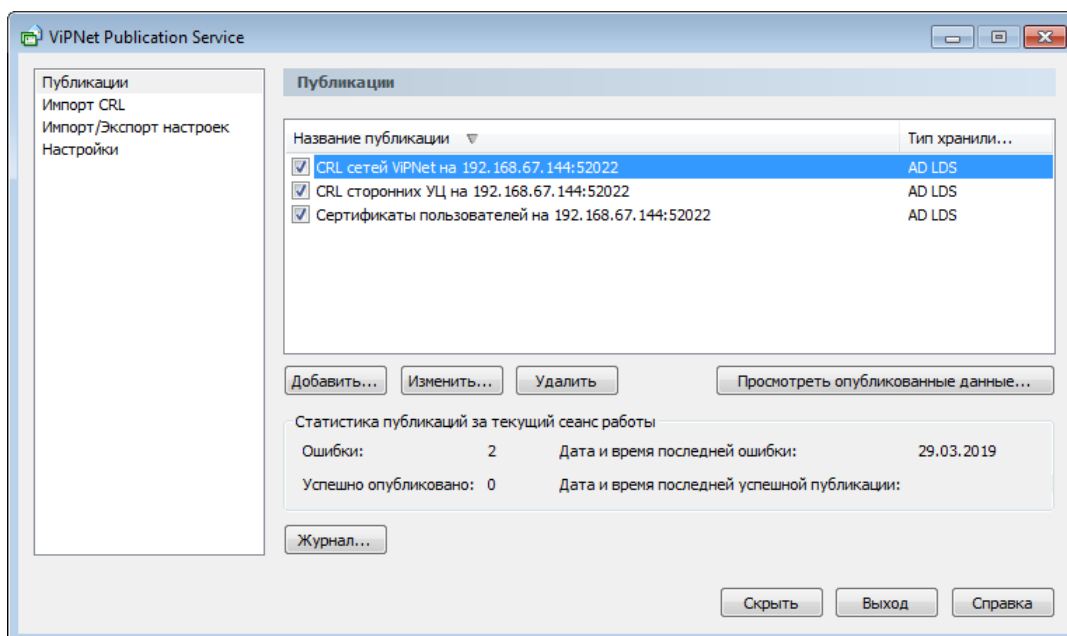


Рисунок 32. Завершение добавления публикации

Теперь при появлении в папке обмена новых данных программа автоматически опубликует их в соответствии с правилами созданной публикации.



Примечание. Если вам требуется публиковать данные в несколько экземпляров AD LDS, для каждого экземпляра необходимо создать свою публикацию.

При публикации в AD LDS сертификатов пользователей, содержащих в поле **Субъект** атрибуты **ИНН**, **СНИЛС** и **ОГРН**, дополнительно будут опубликованы данные, содержащие значения указанных атрибутов.

Публикация в AD DS

В AD DS могут публиковаться только:

- сертификаты пользователей этого домена (см. [Публикация сертификатов](#) на стр. 67);
- CRL сетей ViPNet и CRL сторонних УЦ (см. [Публикация CRL](#) на стр. 69).

Публикация сертификатов

Чтобы настроить публикацию сертификатов пользователей в Active Directory:

- 1 В главном окне на панели навигации перейдите в раздел **Публикации** и нажмите кнопку **Добавить**.
- 2 В окне **Мастер создания публикации** поочередно, на каждой странице укажите ряд параметров. Для перемещения между страницами используйте кнопки **Далее** и **Назад**.
 - **Тип публикуемых данных:** установите переключатель в положение **Сертификаты пользователей**.
 - **Тип хранилища:** установите переключатель в положение **AD DS**.
 - **Параметры подключения:** выполните одно из действий:
 - Если вы хотите публиковать данные на одном из контроллеров домена, в который выполнен вход, установите переключатель в положение **Домен, в который выполнен вход**. В силу специфики публикации эту опцию нежелательно выбирать в случае, если тип публикуемых данных — CRL, а в домене более одного контроллера. При невыполнении этой рекомендации возможно появление дубликатов опубликованных данных.
 - Если вы хотите публиковать данные в другой домен, установите переключатель в положение **Другой домен или контроллер домена** и в поле ниже укажите адрес контроллера домена. При настройке публикации CRL желательно выбрать этот вариант и указать конкретный контроллер домена.
 - **Учетная запись:** выполните одно из действий:
 - Если подключение к контроллеру домена будет выполняться с учетными данными пользователя, от имени которого выполнен вход в систему на момент публикации, установите переключатель в положение **Учетные данные текущего пользователя**.
 - Если авторизация в домене будет выполняться с помощью другой учетной записи, установите переключатель в положение **Другие учетные данные** и в соответствующих полях укажите данные учетной записи для публикации.



Примечание. Для получения учетной записи, при помощи которой будет выполняться публикация в AD DS, необходимо обратиться к администратору домена. Данная учетная запись должна входить в группу Certificate Publishers.

Для запуска программы ViPNet Publication Service рекомендуется использовать учетную запись, полученную от администратора домена, это позволит упростить настройку публикации и уменьшить вероятность ошибок при настройке.

- **Сопоставление сертификатов пользователям:** настройте соответствие сертификатов пользователям домена Active Directory.

По умолчанию используются только те атрибуты, совокупность которых с высокой вероятностью обеспечивает уникальность объекта, а именно: E, CN и SerialNumber.

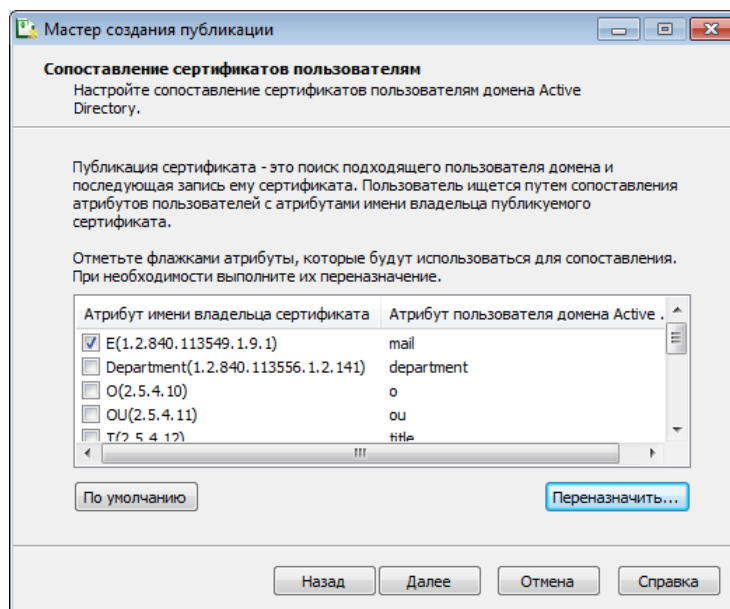


Рисунок 33. Сопоставление сертификатов пользователям Active Directory

При необходимости вы также можете отметить флажками другие атрибуты и выполнить их переназначение.

Чтобы переназначить атрибут, выберите его в списке и нажмите кнопку **Переназначить**. В окне **Переназначение атрибута** укажите новое значение атрибута пользователя Active Directory.

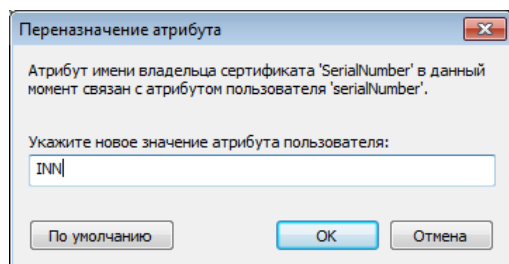


Рисунок 34. Переназначение атрибута сопоставления: атрибут имени владельца сертификата SerialNumber связан с атрибутом пользователя INN

- **Параметры публикации:** выполните следующие действия:

- Если вы хотите публиковать сертификаты, у которых в имени владельца содержатся атрибуты не представленные в таблице сопоставления атрибутов (см. предыдущий шаг), установите соответствующий флажок. При включении данной опции следует учесть, что вы не сможете искать опубликованные сертификаты по тем атрибутам поля **Subject** сертификата, которые отсутствуют в таблице сопоставления. Например, включив данную опцию, вы сможете публиковать сертификаты, у которых в поле **Subject** используется атрибут OGRN, однако вы не сможете искать опубликованные сертификаты по этому атрибуту.
- Чтобы при публикации новых сертификатов пользователей не удалялись старые, в группе **Поведение при записи сертификата пользователю** установите переключатель в положение **Добавлять к ранее опубликованным сертификатам**. По умолчанию старые сертификаты пользователей заменяются новыми.



Внимание! Для публикации квалифицированных сертификатов флажок **Разрешить публикацию сертификатов, у которых имя владельца содержит атрибуты, не представленные в таблице сопоставления атрибутов** должен быть установлен.

- **Название публикации:** укажите имя публикации, которое будет отображаться в списке публикаций.
- **Сводка:** ознакомьтесь с настроенными параметрами публикации и нажмите кнопку **Проверить указанные параметры**.

В случае успешной проверки появится соответствующее сообщение. Нажмите **ОК**, а затем кнопку **Готово**.

Если при проверке параметров возникли ошибки, выполните рекомендации, предложенные программой или перейдите к разделу [Часто задаваемые вопросы по настройке публикации в AD DS](#) (на стр. 93).

Публикация CRL

Чтобы настроить публикацию CRL в AD DS:

- 1 В главном окне на панели навигации перейдите в раздел **Публикации** и нажмите кнопку **Добавить**.
- 2 В окне **Мастер создания публикации** поочередно, на каждой странице укажите ряд параметров. Для перемещения между страницами используйте кнопки **Далее** и **Назад**.
 - **Тип публикуемых данных:** установите переключатель в положение **Списки аннулированных сертификатов сетей ViPNet** или **Списки аннулированных сертификатов, выпущенные сторонними УЦ**.
 - **Тип хранилища:** установите переключатель в положение **AD DS**.
 - **Параметры подключения:** выполните одно из действий:

- Если вы хотите публиковать данные на одном из контроллеров домена, в который выполнен вход, установите переключатель в положение **Домен, в который выполнен вход**. В силу специфики публикации эту опцию нежелательно выбирать в случае, если тип публикуемых данных — CRL, а в домене более одного контроллера. При невыполнении этой рекомендации возможно появление дубликатов опубликованных данных.
- Если вы хотите публиковать данные в другой домен, установите переключатель в положение **Другой домен или контроллер домена** и в поле ниже укажите адрес контроллера домена. При настройке публикации CRL желательно выбрать этот вариант и указать конкретный контроллер домена.
- **Учетная запись:** выполните одно из действий:
 - Если подключение к контроллеру домена будет выполняться с учетными данными пользователя, от имени которого выполнен вход в систему на момент публикации, установите переключатель в положение **Учетные данные текущего пользователя**.
 - Если авторизация в домене будет выполняться с помощью другой учетной записи, установите переключатель в положение **Другие учетные данные** и в соответствующих полях укажите данные учетной записи для публикации.



Примечание. Для получения учетной записи, при помощи которой будет выполняться публикация в AD DS, необходимо обратиться к администратору домена. Данная учетная запись должна входить в группу Certificate Publishers.

Для запуска программы ViPNet Publication Service рекомендуется использовать учетную запись, полученную от администратора домена, это позволит упростить настройку публикации и уменьшить вероятность ошибок при настройке.

- **Контейнер:** укажите различающееся [имя контейнера для размещения CRL](#) (см. [AD DS](#) на стр. 51).

Например:

- В случае публикации CRL сетей ViPNet: CN=vipnetCRL, DC=domain, DC=com.
- В случае публикации CRL сторонних сетей: CN=nonVipnetCRL, DC=domain, DC=com.

- **Название публикации:** укажите имя публикации, которое будет отображаться в списке публикаций.
- **Сводка:** ознакомьтесь с настроенными параметрами публикации и нажмите кнопку **Проверить указанные параметры**.

В случае успешной проверки появится соответствующее сообщение. Нажмите **ОК**, а затем кнопку **Готово**.

Если при проверке параметров возникли ошибки, выполните рекомендации, предложенные программой или перейдите к разделу [Часто задаваемые вопросы по настройке публикации в AD DS](#) (на стр. 93).

Публикация на FTP-сервер



Примечание. На FTP могут быть опубликованы сертификаты пользователей, издателей, CRL сетей ViPNet и сторонних УЦ.

Для добавления публикации на FTP-сервер, выполните следующие действия:

- 1 В главном окне на панели навигации перейдите в раздел **Публикации** и нажмите кнопку **Добавить**.
- 2 В появившемся окне **Мастер создания публикации** поочередно, на каждой странице мастера укажите ряд параметров. Для перемещения между страницами используйте кнопки **Далее** и **Назад**.

- **Тип публикуемых данных:** выберите необходимый тип данных.
- **Тип хранилища:** FTP-сервер.
- **Параметры подключения:**
 - укажите IP-адрес или DNS-имя FTP-сервера,
 - номер порта для подключения к FTP-серверу (по умолчанию – 21),
 - если подключение к FTP-серверу происходит не в пассивном режиме, снимите соответствующий флажок (подробнее см. RFC 959 <http://www.ietf.org/rfc/rfc959.txt>).
- **Учетная запись:** введите имя пользователя и пароль учетной записи для доступа к FTP-серверу.
- **Каталог:** укажите путь к каталогу, в котором будут размещаться публикуемые данные. Предварительно данный каталог должен быть создан на FTP-сервере (см. [Настройка FTP-сервера](#) на стр. 54).

Например, если планируется размещать сертификаты издателей в папке [Issuers] в корне домашнего каталога, то путь будет выглядеть так: /Issuers.

- **Название публикации:** введите уникальное название публикации, которое будет отображаться в списке публикаций. По умолчанию название складывается из типа публикуемых данных и адреса сервера, например:
«Сертификаты издателей на 192.168.77.20».
- На странице **Сводка** нажмите кнопку **Проверить указанные параметры**. Если проверка прошла успешно, для завершения создания публикации нажмите **Готово**.

Если при соединении с сервером возникли ошибки, проверьте правильность указанных параметров. Чтобы вернуться к редактированию параметров публикации, нажмите кнопку **Назад**.

Для отмены процесса создания публикации, нажмите **Отмена**.

После создания публикации, при появлении в папке обмена новых данных программа автоматически опубликует их в соответствии с правилами созданной публикации.



Примечание. При необходимости публикации данных на нескольких FTP-серверах — для каждого нужно создать свою публикацию.

Опубликованный сертификат хранится на сервере в отдельной папке, имя которой формируется на основе имени владельца сертификата. Внутри каждой папки помимо сертификата хранится служебная информация.

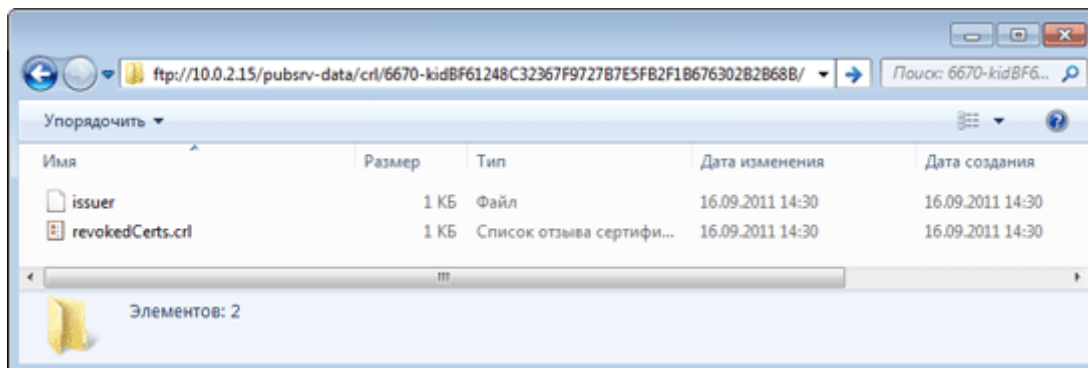


Рисунок 35: Структура хранения CRL семей ViPNet на FTP-сервере

Изменение параметров публикации

Вы можете изменить параметры публикации, например, если изменились данные учетной записи службы AD LDS.

Чтобы изменить параметры публикации, выполните следующие действия:

- 1 В главном окне программы на панели навигации перейдите в раздел **Публикации**.
- 2 В списке публикаций выберите нужную и нажмите кнопку **Изменить**.
- 3 В мастере создания публикации измените параметры публикации таким же образом, как и при добавлении публикации (см. [Добавление публикаций](#) на стр. 63).

В результате публикация будет осуществляться в соответствии с новыми параметрами.

Отключение и удаление публикации

Если какая-то из созданных ранее публикаций стала неактуальной, ее можно временно отключить или удалить. Для этого выполните следующие действия:

- 1 В главном окне на панели навигации перейдите в раздел **Публикации**.
- 2 Выполните одно из действий:
 - Чтобы временно отключить публикацию, снимите флажок слева от нужной публикации в списке. Публикация будет отключена.
 - Чтобы удалить публикацию, в списке выберите нужную публикацию, нажмите кнопку **Удалить** и подтвердите свое действие. Публикация будет удалена.

8

Контроль опубликованных данных

Поиск и просмотр опубликованных данных	76
Просмотр статистики публикаций	79
Просмотр журнала публикаций	80
Экспорт опубликованных сертификатов	83

Поиск и просмотр опубликованных данных

При необходимости вы можете выполнить поиск и просмотр сертификатов (см. [Поиск опубликованных сертификатов пользователей и сертификатов издателей](#) на стр. 76) или CRL (см. [Поиск и просмотр опубликованных CRL](#) на стр. 77), опубликованных в рамках одной публикации.

Поиск опубликованных сертификатов пользователей и сертификатов издателей

Для поиска сертификатов пользователей или издателей по заданным критериям:

- 1 В главном окне на панели навигации перейдите в раздел **Публикации**.
- 2 В списке публикаций выберите запись, соответствующую нужному хранилищу и нажмите кнопку **Просмотреть опубликованные данные**.
- 3 В окне **Поиск опубликованных сертификатов**:
 - В списке **Атрибут** выберите название атрибута сертификата.



Примечание. Если публикация сертификатов пользователей производится в AD LDS и сертификаты пользователей в поле **Субъект** содержат атрибуты ИНН, СНИЛС или ОГРН, то опубликованные сертификаты можно найти в данных хранилищах по указанным атрибутам.

- В поле **Значение** введите желаемое значение атрибута.
- Нажмите кнопку **Добавить**. Фильтр поиска появится в таблице ниже. Если необходимо, добавьте в таблицу другие критерии поиска.
- Чтобы удалить фильтр из таблицы, выберите нужную запись и нажмите кнопку **Удалить**.

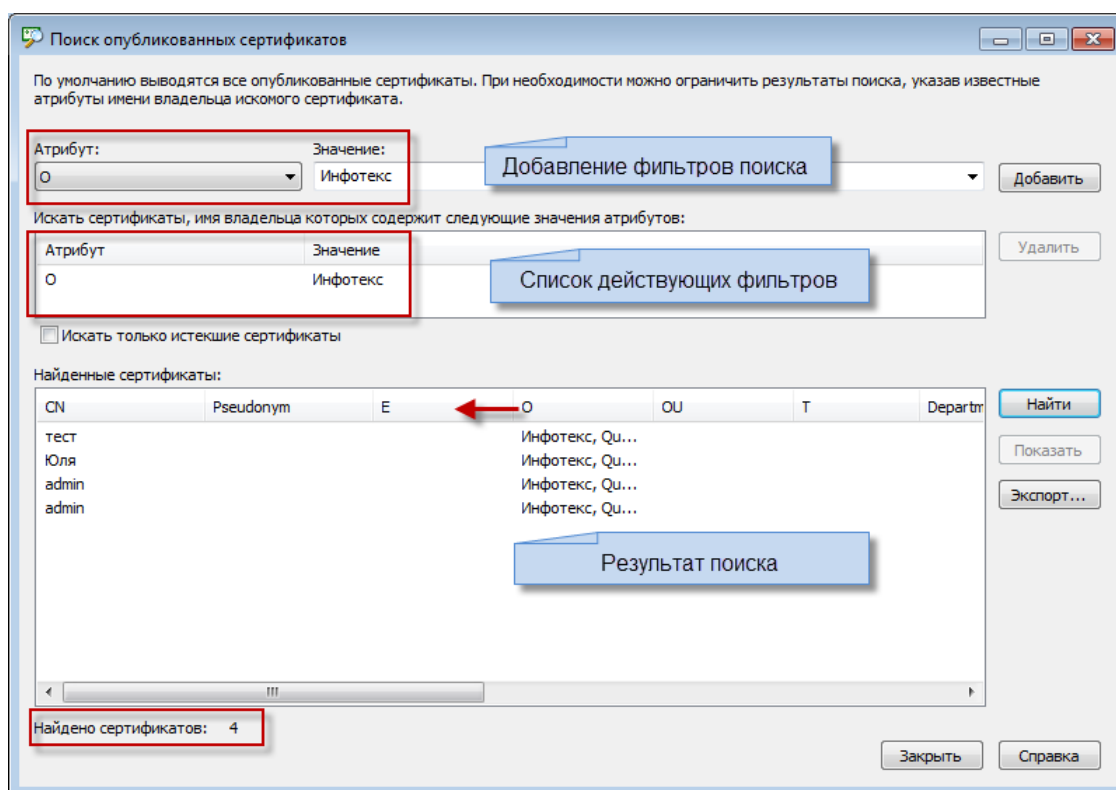


Рисунок 36. Поиск опубликованных сертификатов

4 После добавления фильтров нажмите кнопку **Найти**. Дождитесь окончания поиска.

В таблице **Найденные сертификаты** будут отображены сертификаты, опубликованные в данном хранилище и удовлетворяющие заданным критериям. Для просмотра сертификата выберите его в списке и нажмите кнопку **Показать**.

Поиск и просмотр опубликованных CRL

Для поиска опубликованных CRL, выполните следующие действия:

- 1 В главном окне на панели навигации перейдите в раздел **Публикации**.
- 2 В списке публикаций выберите запись, соответствующую нужному хранилищу, и нажмите кнопку **Просмотреть опубликованные данные**.
- 3 В окне **Поиск опубликованных CRL сетей ViPNet** или **Поиск опубликованных CRL сторонних сетей**:
 - В поле **Значение атрибута имени издателя** введите один из атрибутов издателя или несколько первых символов.
 - В поле **Номер сети** (для сетей ViPNet) введите значение фильтра по номеру сети.

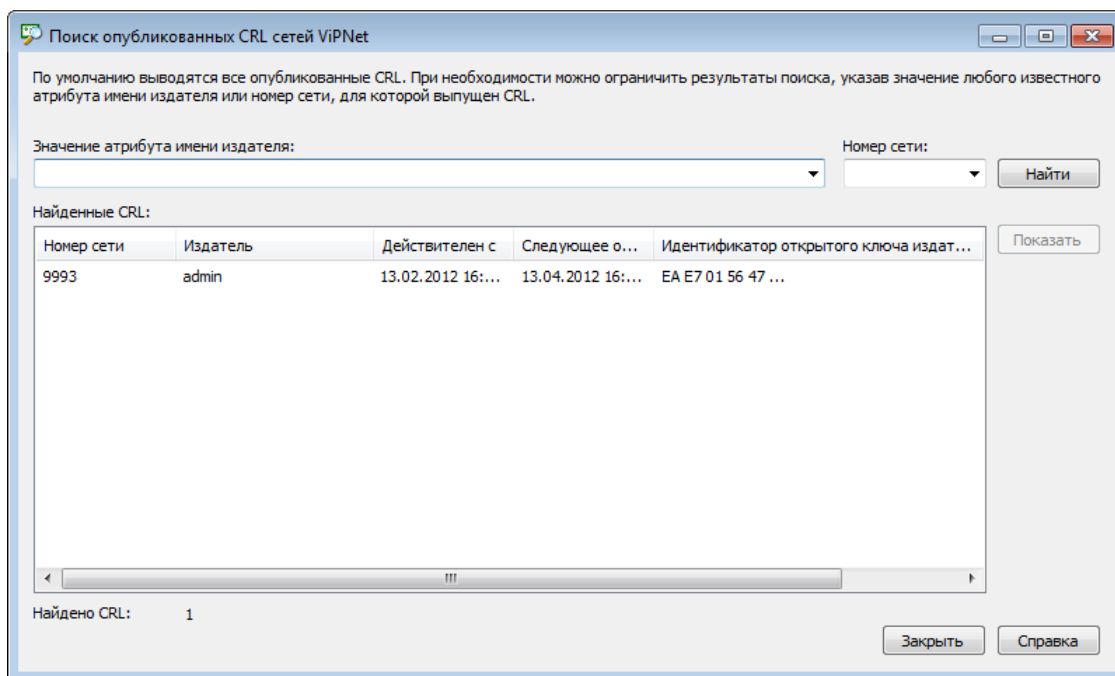


Рисунок 37. Поиск CRL по заданным критериям

4 После указания фильтров нажмите кнопку **Найти**. Дождитесь окончания поиска.

В таблице **Найденные CRL** будут отображены CRL, опубликованные в данном хранилище и удовлетворяющие заданным критериям. Для просмотра CRL выберите его в списке и нажмите кнопку **Показать**.

Просмотр статистики публикаций



Примечание. В программе ViPNet Publication Service хранится статистика только за текущий сеанс работы. После выхода из программы статистика сеанса удаляется.

Чтобы посмотреть общую статистику по текущему сеансу публикаций, выполните следующие действия:

- 1 В главном окне на панели навигации перейдите в раздел **Публикации**.
- 2 На панели **Статистика публикаций за текущий сеанс работы** будут отображены:
 - о количество ошибок при публикациях и время последней ошибки;
 - о количество успешных публикаций и время последней.

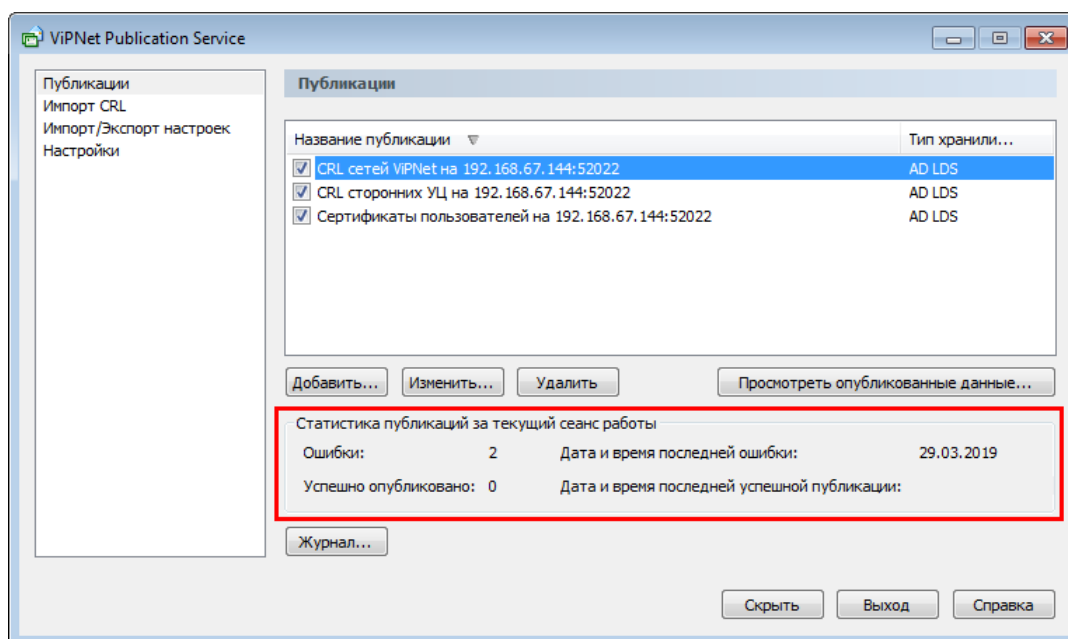


Рисунок 38. Общая статистика публикаций

Если в ходе публикации возникла ошибка, вы можете посмотреть ее описание в журнале публикаций (см. [Просмотр журнала публикаций](#) на стр. 80).

Просмотр журнала публикаций



Примечание. В программе ViPNet Publication Service хранится статистика только за текущий сеанс работы. После закрытия программы статистика сеанса удаляется.

Журнал публикаций может быть полезен для контроля публикуемых данных и для отслеживания ошибочных публикаций. В журнале содержится следующая информация:

- Время публикации.
- Сообщение о результатах публикации.
- Название публикуемого файла и его атрибуты.

Чтобы посмотреть детальную статистику по публикуемым данным, выполните следующие действия:

- 1 В главном окне на панели навигации перейдите в раздел **Публикации**.
- 2 На панели просмотра нажмите кнопку **Журнал**.
- 3 В окне **Журнал публикации за текущий сеанс работы** на панели навигации выберите тип публикуемых данных, журнал публикаций которых необходимо просмотреть:
 - **Сертификаты**.
 - **Списки аннулированных сертификатов**.
 - **Прочее** — информация о неопубликованных файлах.
- 4 Чтобы отобразить в журналах последние данные по публикациям, нажмите кнопку **Обновить**.

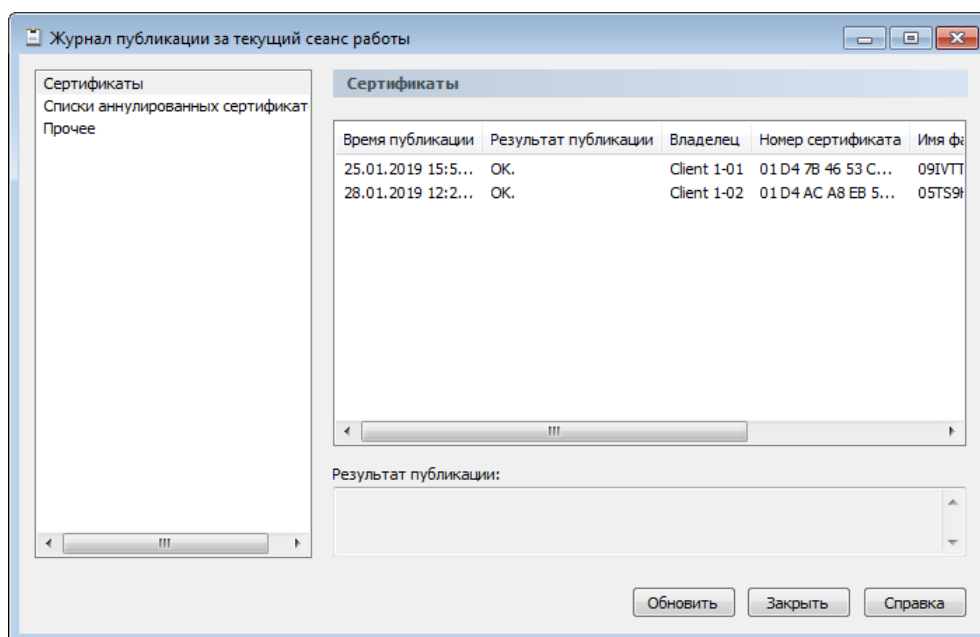


Рисунок 39. Окно журнала публикации

- 5 На панели навигации выберите название публикации, детальную информацию о которой необходимо просмотреть. В поле **Результат публикации** отобразится детальная информация о выбранной публикации.

Если в разделе **Прочее** в поле **Описание события** выводится сообщение об отложенной обработке файла из папки приема файлов от УКЦ — это значит, что активные (включенные) публикации, соответствующие типу данного файла не найдены.

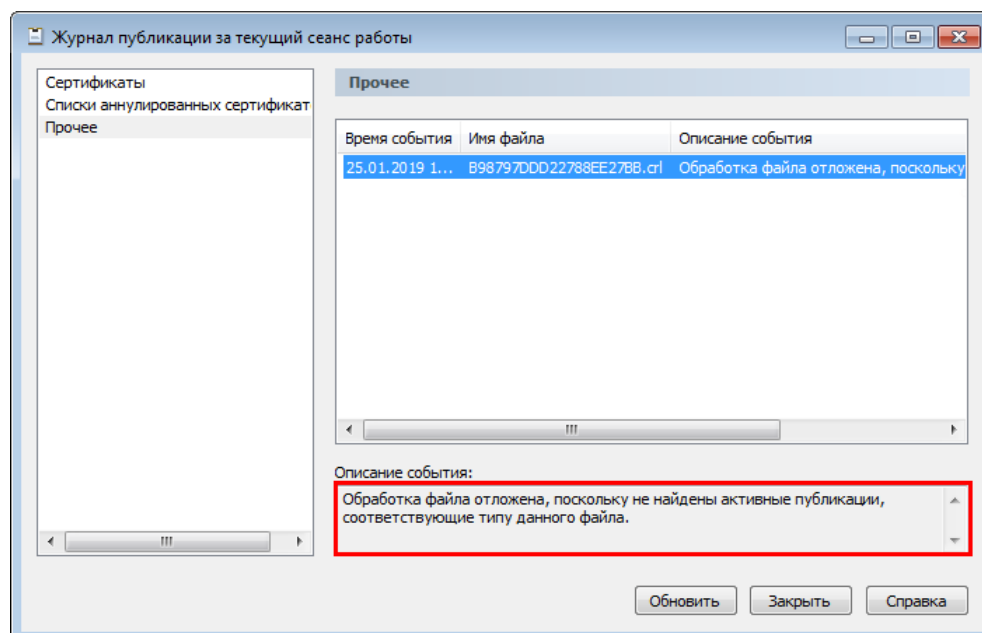


Рисунок 40. Сообщение об отложенной обработке файла

Чтобы опубликовать отложенные файлы из УКЦ, необходимо включить публикацию соответствующего типа или, если она еще не создана, создать ее. После добавления или включения публикации файл будет опубликован и в журнал публикации будет добавлено соответствующее сообщение.

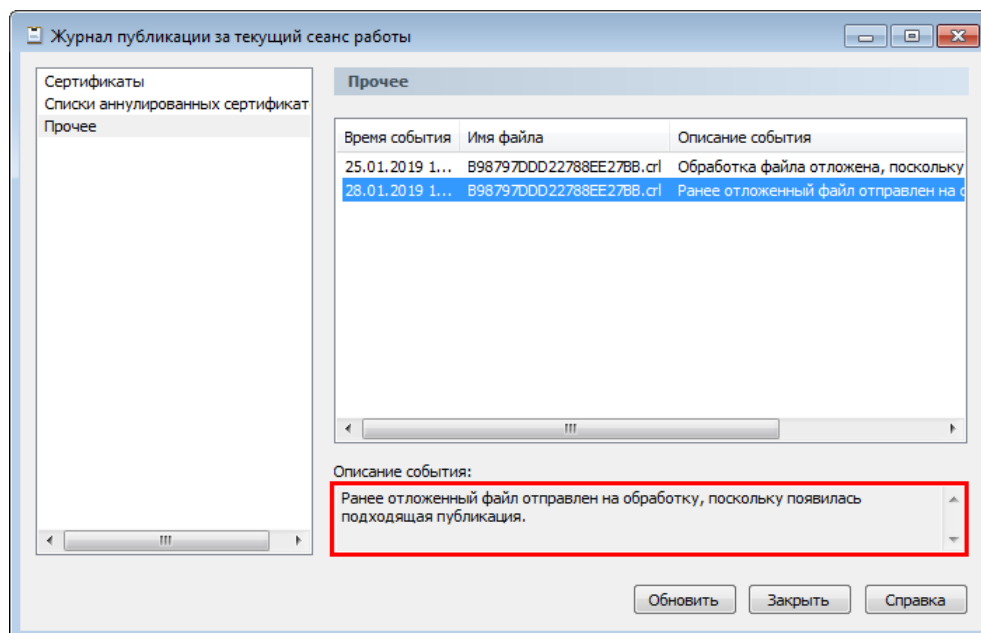


Рисунок 41. Сообщение об обработке отложенного файла

Экспорт опубликованных сертификатов

Программа ViPNet Publication Service позволяет экспортировать опубликованные сертификаты и при необходимости удалять успешно экспортированные сертификаты из хранилищ. Функция экспорта может быть полезна для создания архивного хранилища. С помощью функции экспорта устаревшие опубликованные сертификаты могут быть перенесены из сетевых хранилищ в папку на жестком диске, заданную администратором, или внешние устройства хранения данных.

Чтобы экспортировать опубликованные сертификаты, выполните следующие действия:

- 1 В главном окне на панели навигации перейдите в раздел **Публикации**.
- 2 На панели просмотра выберите нужную публикацию сертификатов и нажмите кнопку **Просмотреть опубликованные данные**.
- 3 Выполните поиск по опубликованным сертификатам (см. [Поиск опубликованных сертификатов пользователей и сертификатов издателей](#) на стр. 76).
- 4 В группе **Найденные сертификаты** нажмите кнопку **Экспорт**.
- 5 В окне **Экспорт найденных сертификатов** в группе **Параметры сохранения** выполните одно из действий:
 - Если вы хотите экспортировать каждый сертификат в отдельный файл со случайным уникальным именем, установите переключатель в соответствующее положение и с помощью кнопки **Обзор** укажите папку для сохранения экспортируемых данных. Данные параметры сохранения удобно использовать, если вам необходимо экспортировать один или несколько сертификатов, например, для их последующей передачи пользователям.
 - Если вы хотите экспортировать все найденные сертификаты в один файл формата PKCS#7, установите переключатель в соответствующее положение. С помощью кнопки **Сохранить как** укажите папку и задайте имя файла для сохранения экспортируемых сертификатов. Данные параметры сохранения удобно использовать, если вам необходимо экспортировать большое количество сертификатов, например, для переноса их в архивное хранилище.

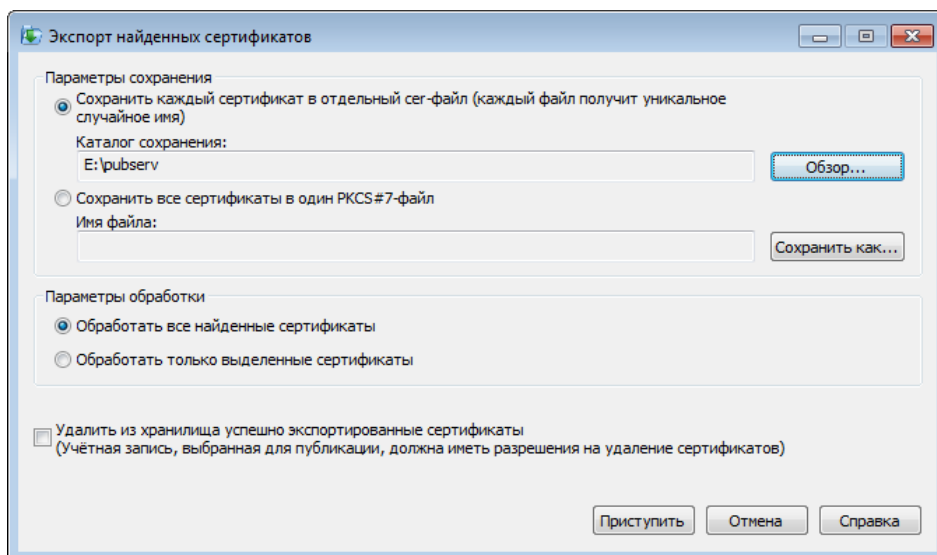


Рисунок 42. Задание параметров экспорта опубликованных данных

6 В группе **Параметры обработки** выполните одно из действий:

- Если вы хотите экспортировать все найденные сертификаты, установите флажок **Обработать все найденные сертификаты**, .
- Если вы хотите экспортировать только сертификаты, выбранные в списке **Найденные сертификаты**, установите флажок **Обработать только выделенные сертификаты**.

7 Чтобы после экспорта сертификаты были удалены из хранилища, установите соответствующий флажок.



Примечание. Для удаления экспортированных сертификатов из хранилища учетная запись, выбранная для публикации, должна обладать правами на удаление из этого хранилища.

8 Нажмите кнопку **Прислупить**.

В результате опубликованные данные будут экспортированы в указанном формате в выбранную папку на диске.

9

Настройка автоматической загрузки CRL

Добавление точки распространения	86
Опрос точек распространения	88

Добавление точки распространения

Импорт CRL (см. [Импорт CRL из доверенных сетей ViPNet и сторонних УЦ](#) на стр. 40) происходит через специальные точки распространения CRL, которые доступны по протоколам HTTP, FTP, LDAP. Для автоматической загрузки CRL необходимо указать URL-адреса в настройках программы ViPNet Publication Service и настроить расписание проверки обновленных CRL.

Чтобы добавить точку распространения CRL, выполните следующие действия:

- 1 В главном окне на панели навигации перейдите в раздел **Импорт CRL**.
- 2 Нажмите кнопку **Добавить**.
- 3 В появившемся окне **Точка распространения** укажите:
 - В поле **Имя** — произвольное уникальное имя, которое будет отображаться в таблице точек распространения (по умолчанию это «Точка распространения N»).
 - В поле **Сетевой путь** — URL-адрес точки распространения. Для получения CRL можно использовать протоколы HTTP, FTP, LDAP.



Примечание. Вы можете найти необходимую информацию об URL-адресах точек распространения CRL в поле сертификата **Точки распространения списков отзыва (CRL)** или узнать ее в удостоверяющем центре.

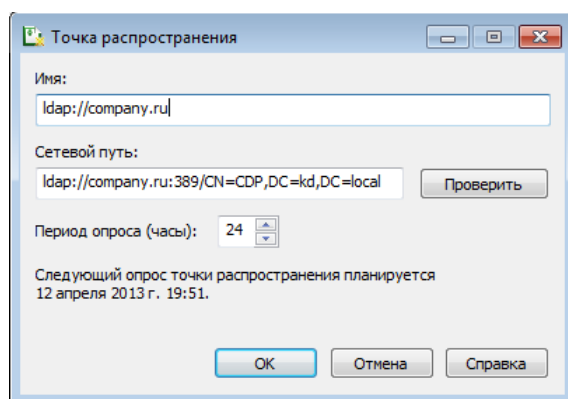


Рисунок 43. Пример указания сетевого пути для точки распространения, доступной по протоколу LDAP

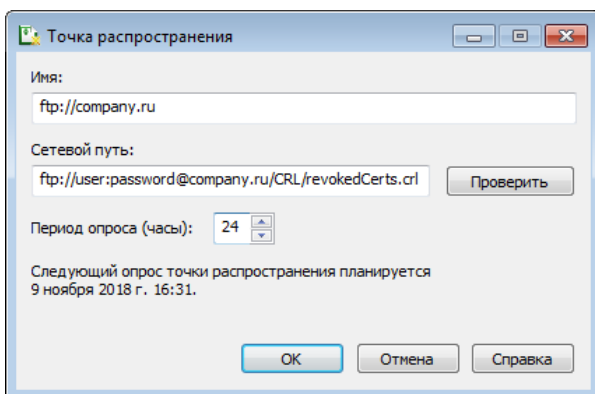


Рисунок 44. Пример указания сетевого пути точки распространения, доступной по протоколу FTP

- Нажмите кнопку **Проверить**, чтобы удостовериться в корректности введенного адреса.
- В поле **Период опроса (часы)** — частоту обращения к точке распространения CRL.

После задания периода опроса в нижней части окна произойдет изменение информационной записи **Следующий опрос точки распространения планируется** <Дата> <Время> .

После создания новой точки распространения произойдет ее немедленный опрос. Следующий опрос будет произведен через время, указанное в поле **Период опроса**.

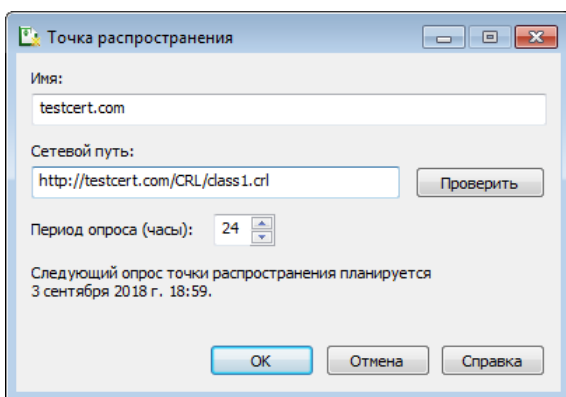


Рисунок 45. Окно добавления точки распространения CRL

- Для завершения процесса создания точки нажмите кнопку **OK**.

В результате из добавленной точки распространения будут загружаться обновленные CRL.

Опрос точек распространения

Плановый (автоматический) опрос точек распространения происходит согласно периодам опроса точек, указанным при их добавлении или редактировании.



Примечание. Как правило, автоматического опроса точек распространения бывает достаточно, для поддержания базы CRL в актуальном состоянии. Внеплановый опрос может понадобиться в тестовых целях или для форсированного обновления CRL.

Чтобы провести внеплановый опрос точек распространения, выполните следующие действия:

- 1 В главном окне на панели навигации перейдите в раздел **Импорт CRL**.
- 2 В списке **Точки распространения CRL** выберите нужные точки распространения и нажмите кнопку **Опросить сейчас**.

Чтобы остановить опрос точек распространения, нажмите кнопку **Прервать опрос** (появляется на месте кнопки **Опросить сейчас**).

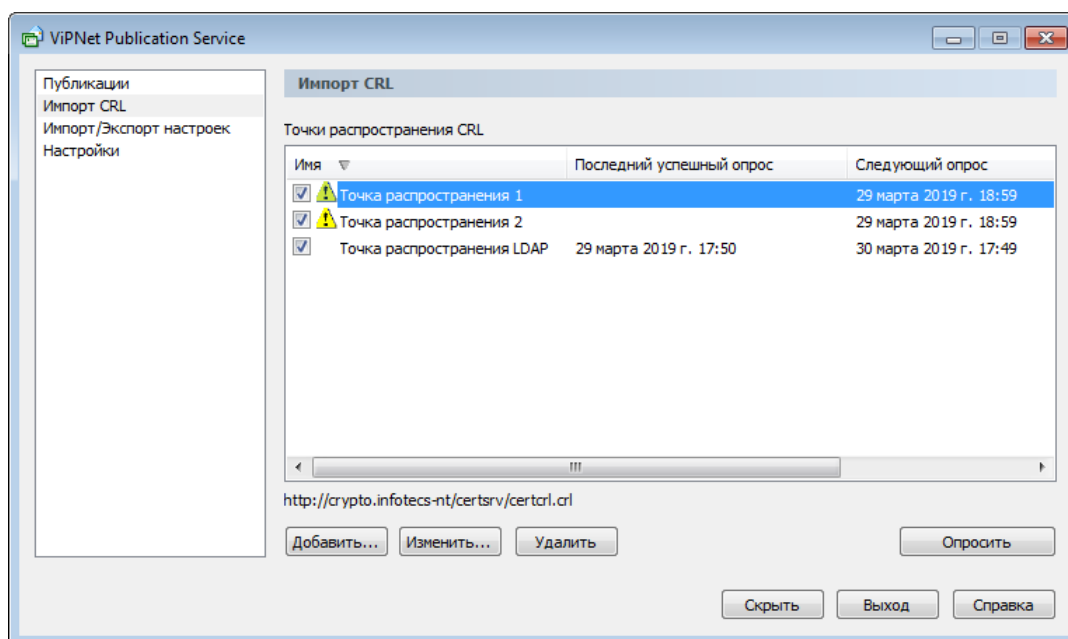


Рисунок 46. Внеплановый опрос точек распространения CRL

- 3 По окончании опроса появится сообщение с результатами.

Точки распространения, последний (успешный) опрос которых был проведен более срока «период опроса + 3 дня» помечаются в списке значком ⚠.

10

Экспорт и импорт настроек программы ViPNet Publication Service

Зачем нужны экспорт и импорт настроек программы	90
Экспорт настроек	91
Импорт настроек	92

Зачем нужны экспорт и импорт настроек программы

Программа ViPNet Publication Service позволяет экспортировать настройки в файлы и при необходимости импортировать в программу нужные настройки из файлов экспорта. С помощью функции экспорта вы можете создать резервные копии настроек, а с помощью функции импорта — восстановить эти настройки в случае сбоев либо перенести настройки из одной копии программы ViPNet Publication Service в другую.

Вы можете экспортировать и импортировать следующие настройки:

- настройки публикаций;
- настройки опроса точек распространения CRL;
- общие настройки программы ViPNet Publication Service.

Экспорт настроек

Чтобы экспортировать настройки программы ViPNet Publication Service, выполните следующие действия:

- 1 В главном окне на панели навигации перейдите в раздел **Импорт/Экспорт настроек**.
- 2 На панели просмотра в группе **Экспорт настроек** выберите настройки, которые необходимо экспортировать.
- 3 Чтобы сразу после экспорта открыть папку с файлами экспорта, установите флажок **Показать результаты экспорта**.
- 4 Нажмите кнопку **Экспортировать**.

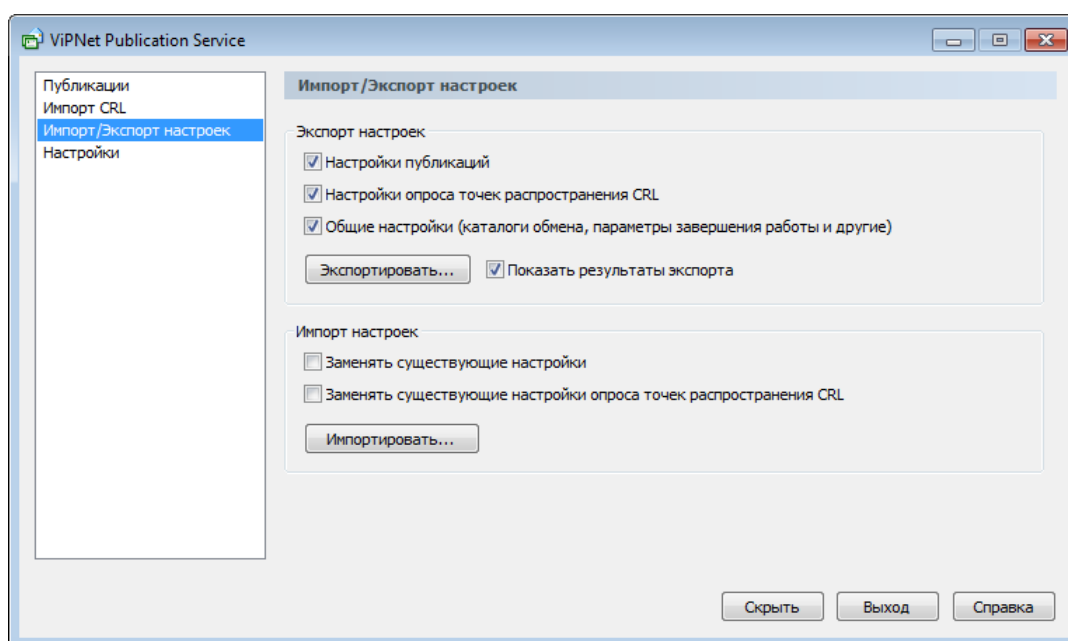


Рисунок 47. Экспорт и импорт настроек программы

- 5 В появившемся окне укажите папку, в которой будут сохранены файлы экспорта, и нажмите кнопку **ОК**.

В результате в указанной папке будет создана вложенная папка с именем «Настройки ViPNet Publication Service гggг.мм.дд-чч.мм.сс», где гggг.мм.дд — дата экспорта, чч.мм.сс — время экспорта. В зависимости от того, какие настройки были выбраны для экспорта, папка будет содержать один или несколько файлов экспорта:

- o ViPNet Publication Service.publist — настройки публикаций.
- o ViPNet Publication Service.cdplist — настройки опроса точек распространения CRL.
- o ViPNet Publication Service.ini — общие настройки программы ViPNet Publication Service.

Импорт настроек

Чтобы импортировать настройки программы ViPNet Publication Service, выполните следующие действия:

- 1 В главном окне на панели навигации перейдите в раздел **Импорт/Экспорт настроек**.
- 2 На панели просмотра в группе **Импорт настроек** (см. рисунок на стр. 91) выберите, какие из существующих настроек программы необходимо заменить аналогичными настройками из файлов, выбранных для импорта:

- **Заменять существующие настройки публикаций.**
- **Заменять существующие настройки опроса точек распространения CRL.**

Общие настройки программы ViPNet Publication Service заменяются всегда (если для импорта будет выбран файл `ViPNet Publication Service.ini`).

- 3 Нажмите кнопку **Импортировать**.
- 4 В появившемся окне выберите нужные файлы и нажмите кнопку **Открыть**.



Примечание. В ViPNet Publication Service 3.2 не реализованы импорт и экспорт настроек. Если вы хотите применить настройки программы после обновления до версии 4.x, сохраните содержимое папки
`\%ProfileName%\AppData\Local\InfoTeCS\ViPNet Publication Service\1.0\`.
Где `%ProfileName%` — имя учетной записи Windows, под которой запускалась программа ViPNet Publication Service. После обновления программы вы сможете восстановить настройки с помощью этих данных.

В результате в программе ViPNet Publication Service будут установлены настройки, содержащиеся в выбранных файлах. При этом, в зависимости от настроек самого импорта, существующие настройки программы будут сохранены либо заменены соответствующими настройками из файлов.



А

Часто задаваемые вопросы
по настройке публикации в
AD DS

Использование контейнеров для разных версий ViPNet Publication Service

При переходе с ViPNet Publication Service версий 3.1 (и ниже) на версию 3.2.x и выше следует помнить, что для публикации CRL недопустимо указывать тот же контейнер, который использовался ViPNet Publication Service версий 3.1 и ниже, поскольку в версии 3.2.x и выше формат размещения изменился.

При добавлении и настройке публикации необходимо указать имя того контейнера, который не содержит данных, созданных старой версией программы ViPNet Publication Service 3.1.

Общие вопросы и проблемы

Как с помощью стороннего приложения, установленного на компьютере не входящем в домен, получить доступ к опубликованным данным?

Для предоставления доступа к опубликованным данным пользователям приложений, которые установлены на компьютеры не входящие в домен, необходимо предоставить всем анонимным пользователям доступ к контейнерам с опубликованными данными.

Анонимный доступ дает стороннему ПО возможность читать опубликованные данные из хранилища без необходимости проходить аутентификацию. Если учесть особенности лицензионной политики компании Microsoft по отношению к продуктам семейства Windows Server, это позволит радикально уменьшить количество необходимых для работы лицензий клиентского доступа.

Анонимный доступ подразумевает анонимную привязку к объектам каталога, которая по умолчанию запрещена. Чтобы разрешить анонимный доступ, выполните следующие действия:

- 1 Запустите оснастку **Редактирование ADSI**.
- 2 Подключитесь к разделу конфигурации контроллера домена.
- 3 Найдите объект с именем **CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=YourDomainName** и откройте его свойства.
- 4 Найдите атрибут **dsHeuristics** и измените его значение таким образом, чтобы седьмой символ слева был 2. Если значение атрибута не задано, можно написать 0000002.

Теперь необходимо назначить разрешения на доступ анонимных пользователей к опубликованным данным. Для этого выполните следующие действия:

- 1 Подключитесь к разделу домена (domain partition) каталога и выберите контейнер с опубликованными данными, к которым необходимо разрешить доступ (например, к контейнеру со списками аннулированных сертификатов).
- 2 Вызовите контекстное меню на выбранном контейнере и на вкладке **Безопасность** нажмите кнопку **Дополнительно**.
- 3 Откроется окно **Дополнительные параметры безопасности для ИмяВыбранногоКонтейнера**. Нажмите кнопку **Добавить**.
- 4 В открывшемся окне в поле для ввода имен объектов вручную введите **АНОНИМНЫЙ ВХОД** или воспользуйтесь поиском данного объекта. Нажмите кнопку **ОК**. Появится окно **Элемент разрешения для <Имя Выбранного Контейнера>**.

- 5 В окне **Элемент разрешения для <Имя Выбранного Контейнера>** перейдите на вкладку **Объект** и в списке **Применить:** выберите **Этот элемент и все дочерние элементы**. В списке разрешений установите **Разрешить** для элементов **Список содержимого**, **Прочитать все свойства** и **Чтение разрешений**. Нажмите **ОК**.
- 6 В окне **Дополнительные параметры безопасности для <Имя Выбранного Контейнера>** нажмите **ОК**.
- 7 Закройте окно свойств контейнера, нажав **ОК**.

В результате пользователи приложений, установленных на компьютеры не входящие в домен, будут иметь доступ к контейнеру с опубликованными данными.

Где находится журнал событий (лог) для ViPNet Publication Service?

Файл журнала событий ViPNet Publication Service.log находится в папке

C:\Users\%ProfileName%\AppData\Local\InfoTeCS\ViPNet Publication Service\1.0

Ошибка: Не удалось подключиться

Если при проверке параметров публикации появляется окно с ошибкой подключения, рекомендуется выполнить действия, описанные в окне ошибки.

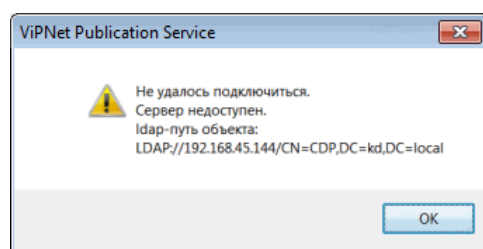


Рисунок 48: Не удалось подключиться

Если проверка указанных параметров не помогла решить проблему, проанализируйте журнал событий ViPNet Publication Service. Для этого откройте файл журнала событий ViPNet Publication Service.log (см. [Где находится журнал событий \(лог\) для ViPNet Publication Service?](#) на стр. 96) и найдите строку, содержащую текст `ADsOpenObject() failed` и датированную временем появления ошибки.

В данной строке содержится код ошибки и ее текстовая расшифровка. Ниже описаны возможные ошибки и причины их появления.

ErrorCode: 0x8007203A. The server is not operational

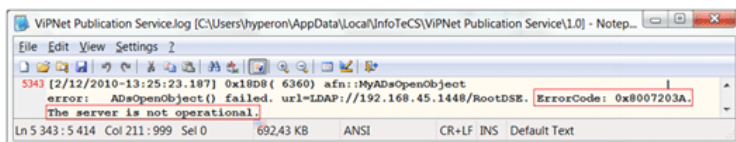


Рисунок 49. Не удалось подключиться

Ошибка соединения с сервером в большинстве случаев происходит по следующим причинам:

- неверно указан адрес контроллера домена;
- указанное имя не соответствует IP-адресу работающего контроллера домена;
- межсетевой экран блокирует LDAP-трафик через порт 389.

ErrorCode: 0x8007054B

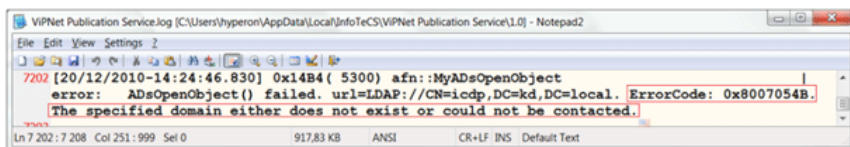


Рисунок 50. Не удалось подключиться

Данная ошибка, как правило, возникает по тем же причинам что и ошибка ErrorCode: 0x8007203A, описанная выше.

ErrorCode: 0x8007052E

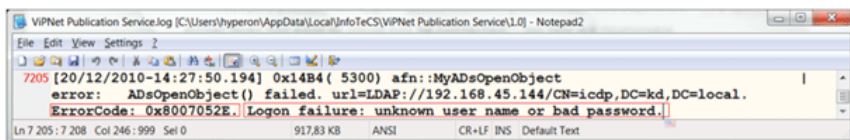


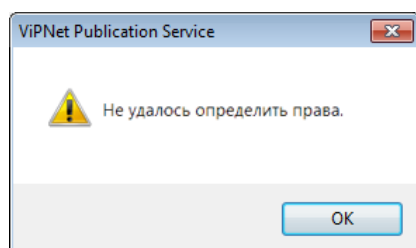
Рисунок 51. Не удалось подключиться

Ошибка авторизации — неверно указано имя пользователя или пароль для доступа к домену.



Примечание. Если в журнале событий присутствуют ошибки, не рассмотренные здесь, воспользуйтесь поиском кода или номера ошибки в Интернете или обратитесь в службу поддержки (см. [Обращение в службу поддержки «ИнфоТекС»](#) на стр. 98).

Ошибка: Не удалось определить права



В подавляющем большинстве случаев данное сообщение означает, что у используемой для публикации учетной записи недостаточно прав для публикации. Чтобы получить более подробное сообщение об этой ошибке, обновите программу ViPNet Publication Service до версии 3.2 или выше с номером сборки больше 7000. Указанная версия программы позволяет получить более информативные сообщения об ошибках.

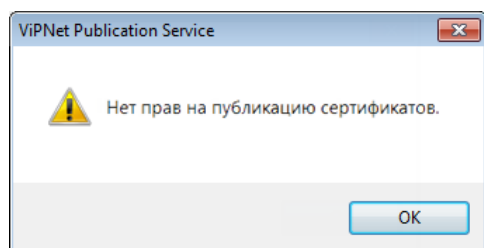
Обращение в службу поддержки «ИнфоТеКС»

Если представленные в данном документе сведения не помогли решить вашу проблему, обратитесь в службу поддержки «ИнфоТеКС» (см. [Обратная связь](#) на стр. 13), приложив к письму:

- файл журнала событий (лог) ViPNet Publication Service;
- по возможности подробное описание ваших действий по настройке программы;
- снимки экрана, иллюстрирующие параметры настройки программы;
- версии ОС и программного обеспечения, установленного на компьютере.

Проблемы публикации сертификатов

Ошибка: Нет прав на публикацию сертификата



При появлении данной ошибки добавьте учетную запись, выбранную для публикации, в группу **Certificate Publishers**.

Ошибок нет, но сертификаты не публикуются

Иногда может возникнуть ситуация, когда проверка параметров в программе ViPNet Publication Service прошла успешно, но публикации сертификатов в AD не происходит. Причины данной проблемы могут быть различны, например, это может происходить, если в AD не найдена учетная запись пользователя, указанная в публикуемом сертификате. Об этой ошибке свидетельствует следующая строка в файле `ViPNet Publication Service.log` (см. [Где находится журнал событий \(лог\) для ViPNet Publication Service?](#) на стр. 96).

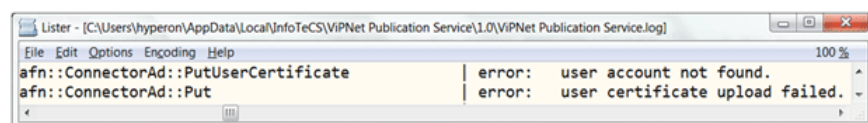


Рисунок 52. Не найдена учетная запись пользователя, соответствующая сертификату

Для решения данной проблемы выполните следующие действия:

- 1 В Мастере создания публикации на странице **Параметры публикации** установите флажок **Разрешить публикацию сертификатов, у которых имя владельца содержит атрибуты, не представленные в таблице сопоставления атрибутов**.

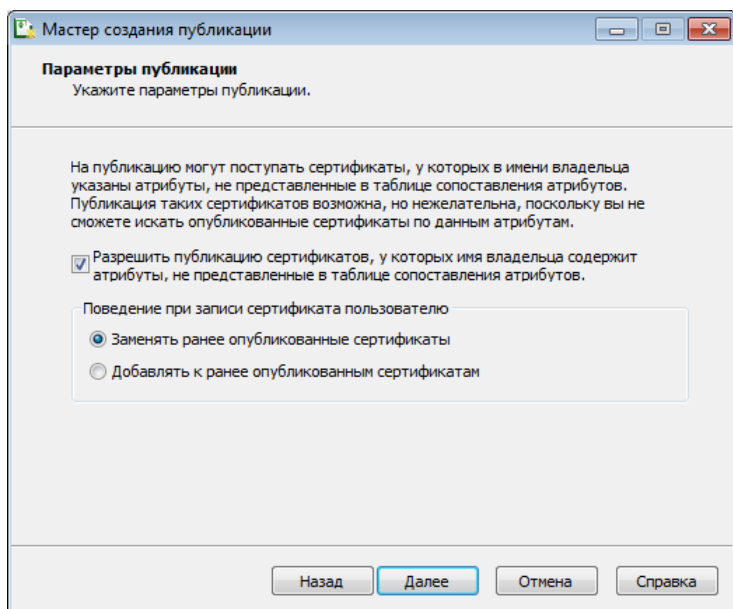


Рисунок 53. Задание дополнительных параметров публикации

- 2 Если проблема сохранилась, то возможной ее причиной может быть изменение атрибутов имени пользователя в Active Directory с момента его регистрации в программе ViPNet Registration Point. В этом случае следует обновить изменившиеся атрибуты пользователя в ViPNet Registration Point, следуя приведенным ниже рекомендациям:
 - В программе ViPNet Registration Point повторите процесс регистрации пользователя, сертификат которого не удастся опубликовать.
 - Если при регистрации появится окно **Регистрация**, выберите **Заменить регистрационные данные пользователя** и в списке ниже выберите пользователя, для которого требуется обновить атрибуты.

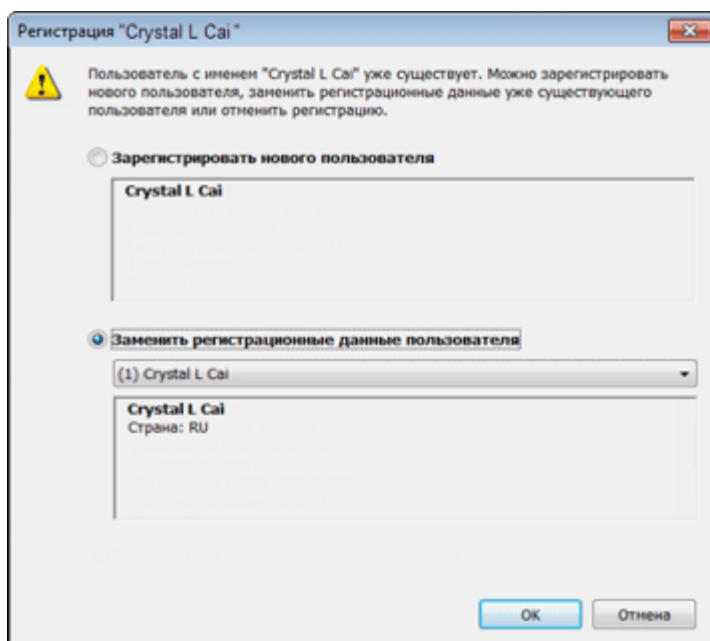


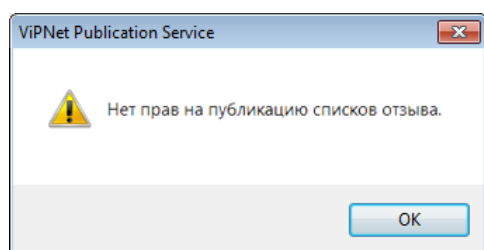
Рисунок 54. Повторная регистрация пользователя в ViPNet Registration Point

В примере, приведенном на рисунке выше, после обновления у пользователя будет удалено поле с идентификатором страны. Также изменится значение поля **Владелец** у сертификатов, которые будут изданы после смены регистрационных данных. В данном случае значение поля **Владелец** в издаваемых сертификатах изменится с `cn=Crystal L Cai, c=ru` на `cn=Crystal L Cai`.

- Если при регистрации пользователя появится сообщение об ошибке, это означает, что ключевые атрибуты пользователя не изменились, и, возможно, имел место программный сбой. Для решения проблемы рекомендуем обратиться в службу поддержки.

Проблемы публикации CRL

Ошибка: Нет прав на публикацию списков отзыва



Указанная для публикации учетная запись не имеет прав на создание и изменение объектов следующих классов (данные объекты используются для хранения CRL):

- cRLDistributionPoint;
- container.



Примечание. Требования к учетной записи, необходимые для успешной публикации CRL, описаны на странице **Контейнер в Мастере создания публикации**.

Для устранения ошибки следует назначить соответствующие права учетной записи, указанной для публикации. Для этого:

- 1 На контроллере домена запустите оснастку **Редактирование ADSI**.
- 2 В меню **Действие** выберите пункт **Подключение к**.
- 3 В открывшемся окне укажите параметры для подключения к AD DS и нажмите кнопку **ОК**.
- 4 Откройте свойства контейнера, предназначенного для хранения CRL.
- 5 Перейдите на вкладку **Безопасность** и удостоверьтесь, что в списке пользователей и групп присутствует учетная запись, предназначенная для публикации. Проверьте список разрешений для данной учетной записи. Он должен включать в себя разрешения на создание и изменение объектов классов cRLDistributionPoint и container внутри данного контейнера. В отдельных случаях данной учетной записи можно разрешить полный доступ.

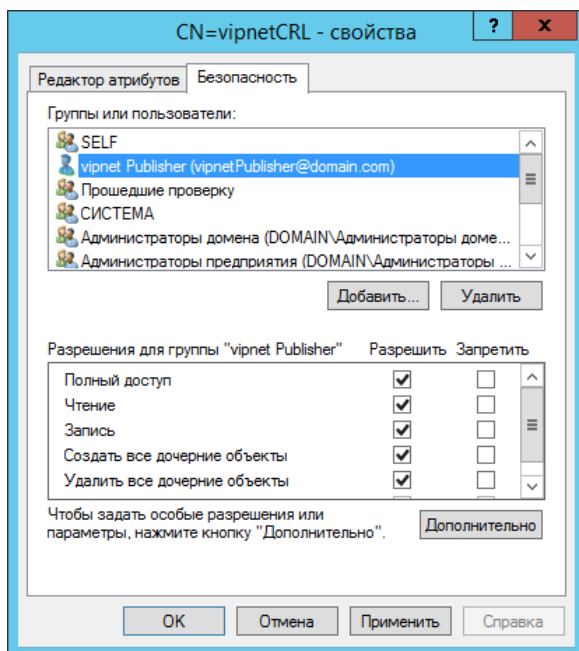


Рисунок 55. Параметры безопасности в окне свойств контейнера

Ошибка: Не удалось подключиться, ErrorCode: 0x80072030. There is no such object on the server

Имя контейнера указано некорректно, проверьте правильность написания имени контейнера.

Ошибка: Не удалось подключиться. ErrorCode: 0x8007202B. A referral was returned from the server

Вероятнее всего имя контейнера указано некорректно. Проверьте часть имени контейнера, которая является названием раздела.

Ошибка: Не удалось подключиться. ErrorCode: 0x80005000(E_ADS_BAD_PATHNAME) или E_ADS_BAD_PATHNAME

Имя контейнера синтаксически некорректно. Возможно, в имени допущена опечатка, например, из-за лишней запятой в конце имени, или другого символа, добавленного случайно. Чтобы избежать подобных ошибок имя контейнера рекомендуется копировать из его атрибута distinguishedName.

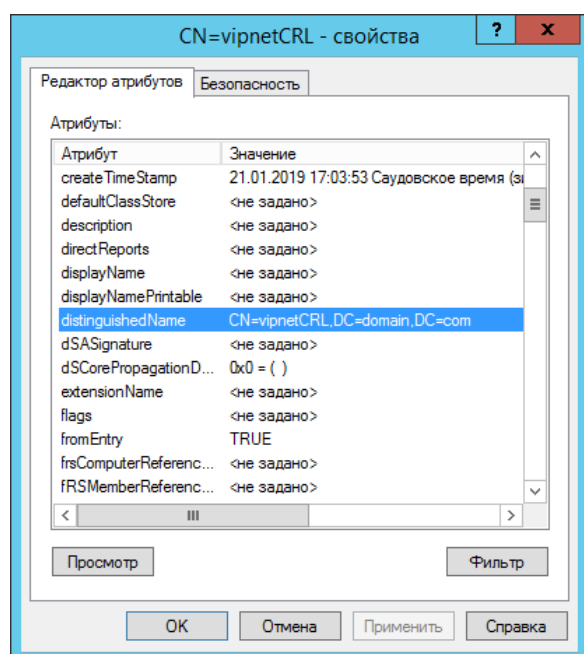


Рисунок 56. Редактор атрибутов в окне свойств контейнера

В

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 ОС Windows 7, Windows Server 2008 R2

Для установки поддержки кириллицы на ОС Windows 7, Windows Server 2008 R2 выполните следующие действия:

- 1 Откройте панель управления (Control Panel) и в категории **Часы, язык и регион (Clock, Language, and Region)** выберите параметр **Язык и региональные стандарты (Region and Language)**.
- 2 В окне **Язык и региональные стандарты (Region and Language)** перейдите на вкладку **Дополнительно (Administrative)**.

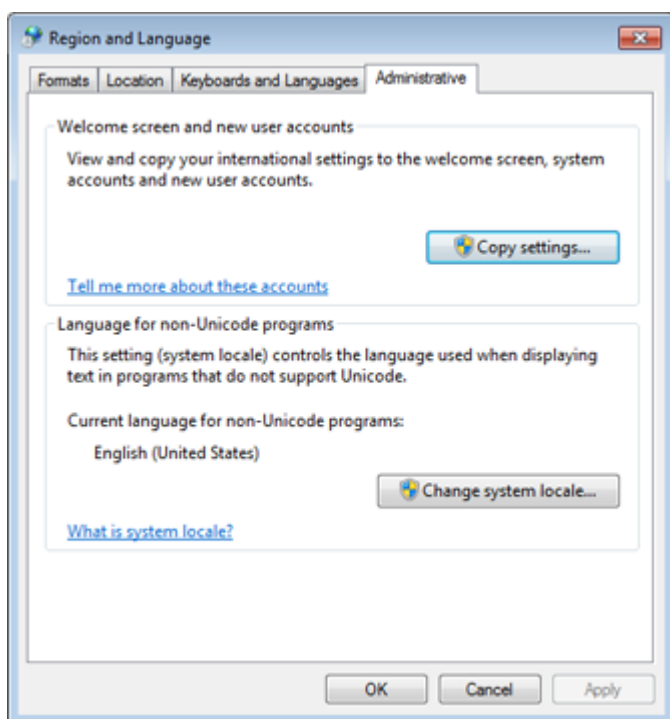


Рисунок 57. Дополнительные языковые параметры

- 3 На вкладке **Дополнительно (Administrative)** нажмите кнопку **Изменить язык системы (Change system locale)**.
- 4 В появившемся окне в списке **Current system locale** выберите **Русский (Россия) (Russian (Russia))**.

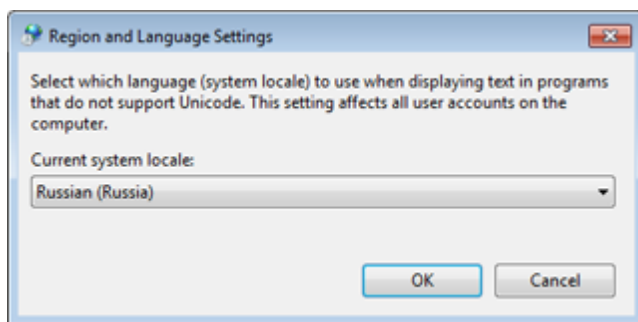


Рисунок 58. Выбор языка системы

- 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 **Язык и региональные стандарты (Region and Language)**.
- 7 В окне **Язык и региональные стандарты (Region and Language)** перейдите на вкладку **Дополнительно (Administrative)** (см. рисунок на стр. 106).
- 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**.

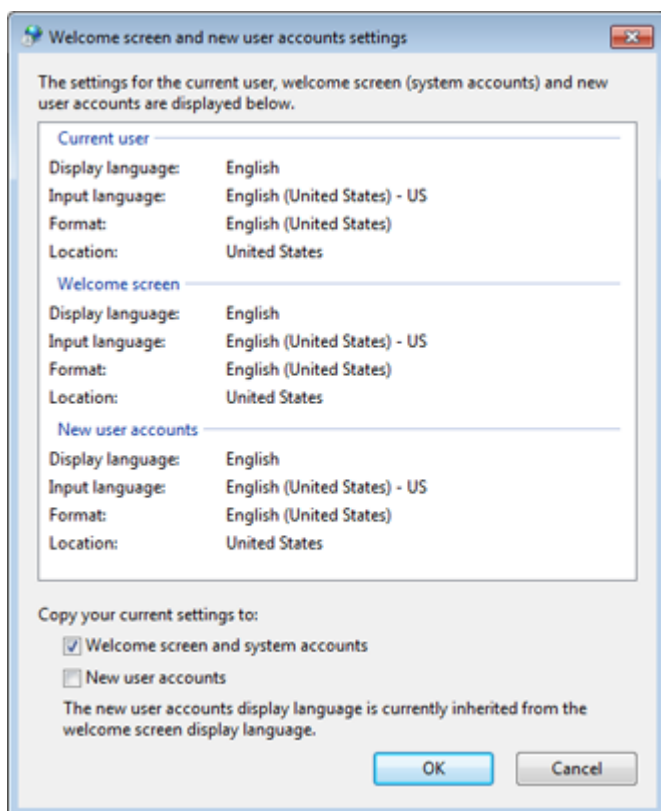


Рисунок 59. Копирование параметров

Также для исключения проблем с кодировкой в некоторых системах мы рекомендуем выполнить следующие действия:

- 1 В окне **Язык и региональные стандарты (Region and Language)** на вкладке **Форматы (Formats)** в списке **Формат (Format)** выберите **Русский (Россия) (Russian (Russia))**.

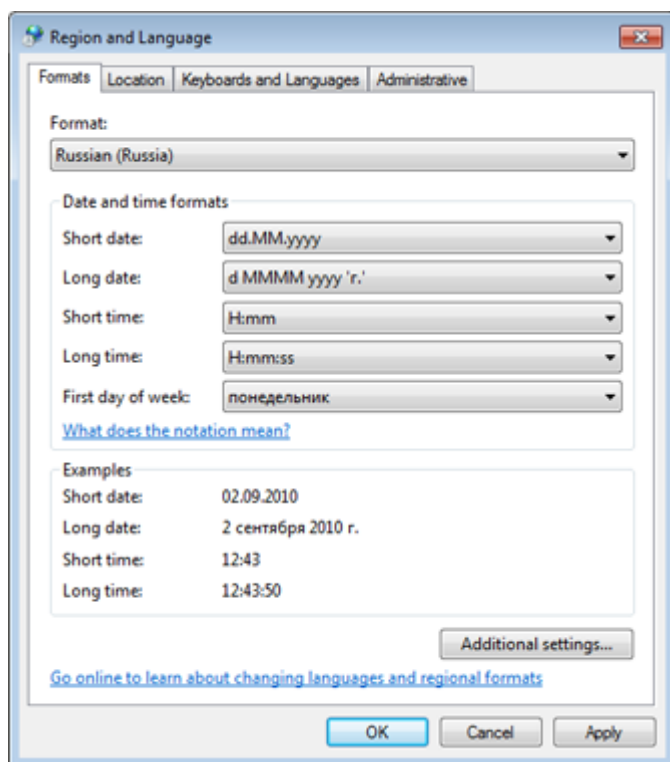


Рисунок 60. Настройка форматов

- 2 В окне **Язык и региональные стандарты (Region and Language)** на вкладке **Расположение (Location)** в списке **Текущее расположение (Current location)** выберите **Россия (Russia)**.

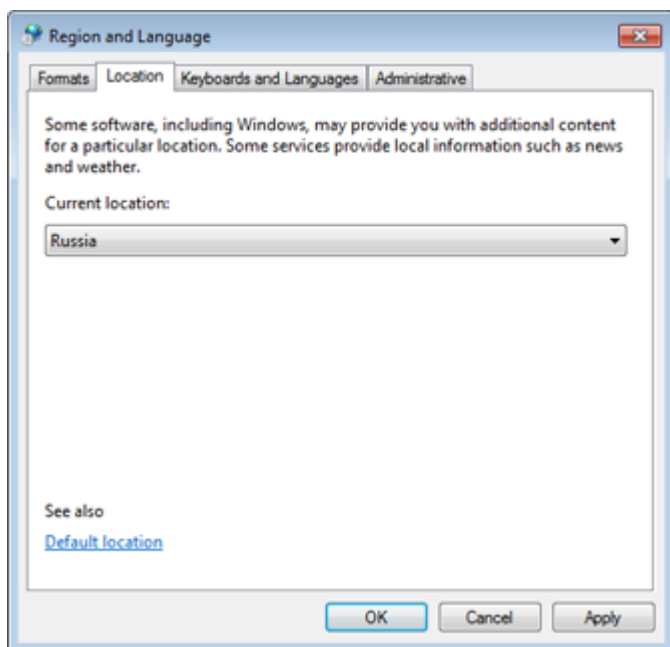


Рисунок 61. Выбор текущего расположения

Региональные настройки в ОС Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10

Для установки поддержки кириллицы на ОС Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10 выполните следующие действия:

- 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)**.

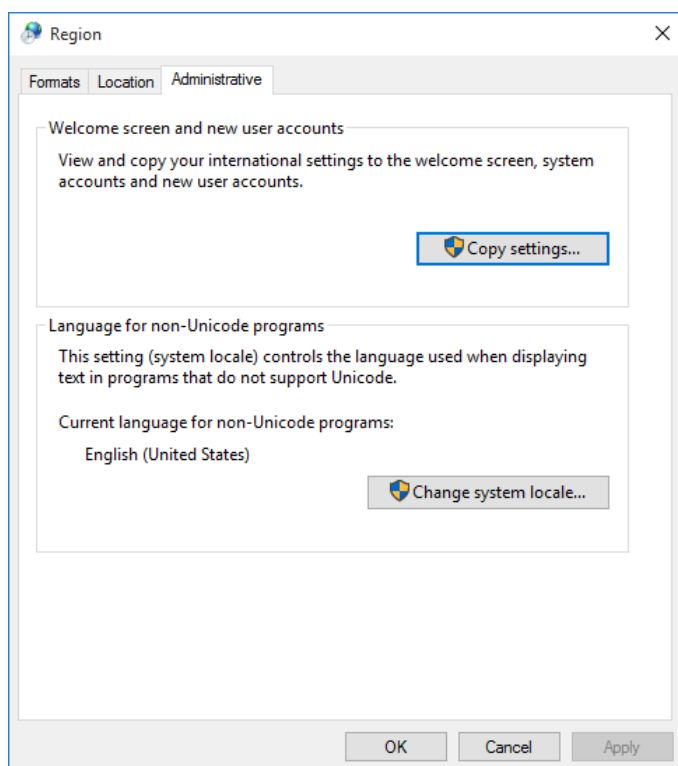


Рисунок 62. Дополнительные языковые параметры

- 3 На вкладке **Дополнительно (Administrative)** нажмите кнопку **Изменить язык системы (Change system locale)**.
- 4 В появившемся окне в списке выберите **Русский (Россия) (Russian (Russia))**.

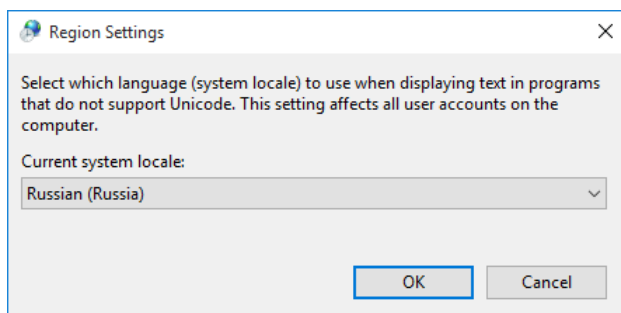


Рисунок 63. Выбор языка системы

- 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)** (см. рисунок на стр. 110).
- 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**.

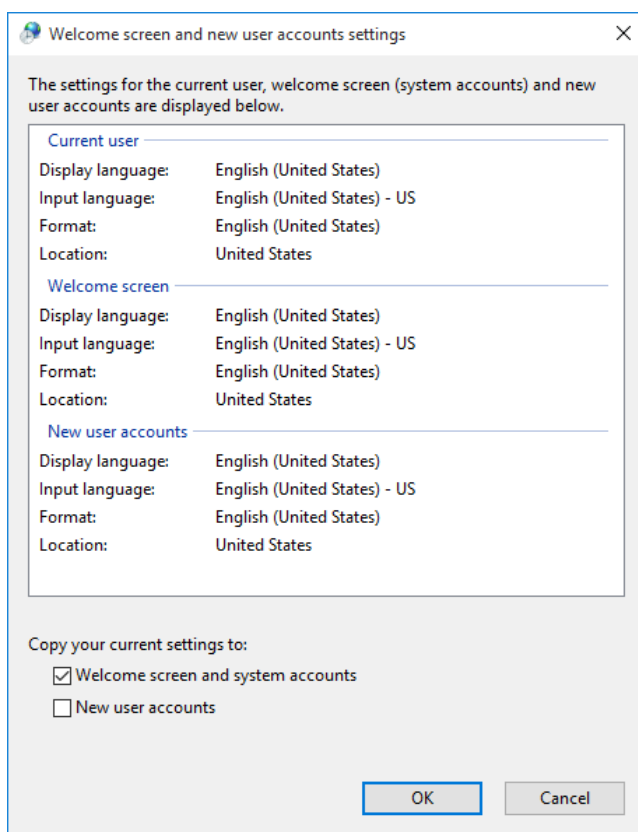


Рисунок 64. Копирование параметров

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))**.

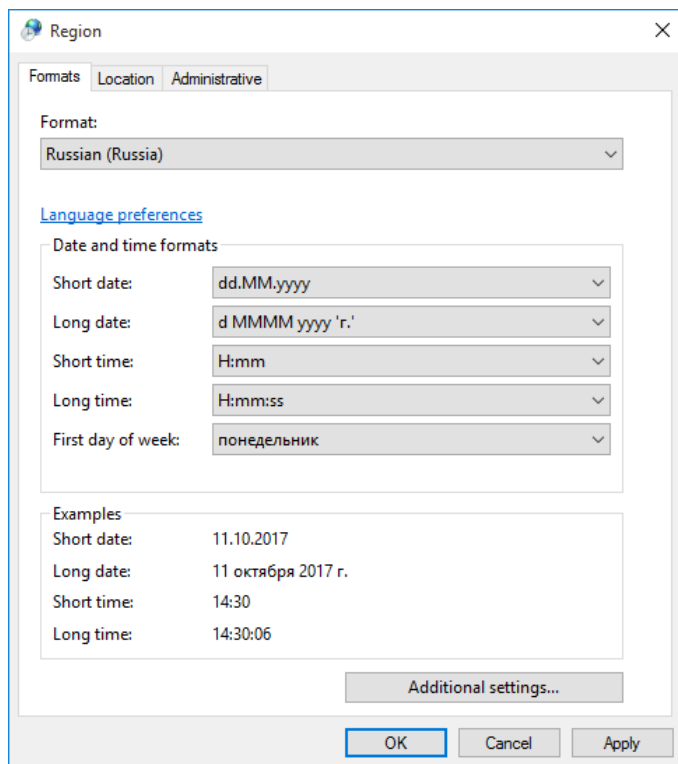


Рисунок 65. Настройка форматов

- 2 В окне **Регион (Region)** на вкладке **Местоположение (Location)** в списке **Основное расположение (Home location)** выберите **Россия (Russia)**.

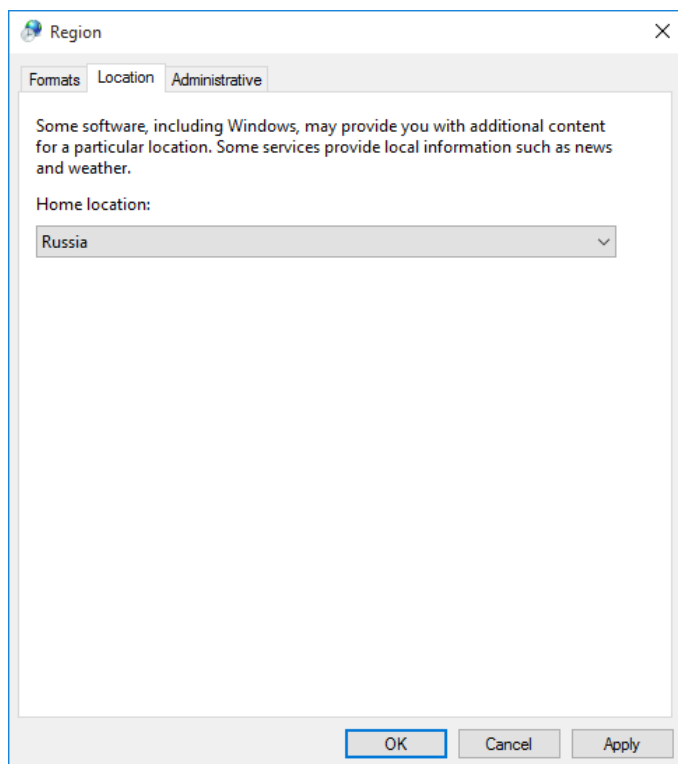


Рисунок 66. Выбор текущего расположения



История версий

В данном приложении описаны основные изменения в предыдущих версиях программы ViPNet Publication Service.

Что нового в версии 4.6

В версии 4.6 улучшена внутренняя функциональность программы, исправлены незначительные ошибки, выявленные в процессе эксплуатации версии 4.4.

Информация об изменениях в предыдущих версиях программы приведена в приложении [История версий](#) (на стр. 114).

Что нового в версии 4.4

В версии 4.4 улучшена внутренняя функциональность программы, исправлены незначительные ошибки, выявленные в процессе эксплуатации версии 4.3.

Что нового в версии 4.3

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Publication Service версии 4.3:

- **Поддержка атрибутов `surname` и `givenName` поля Субъект**

Реализована поддержка атрибутов `givenName` и `surname` поля Субъект. Теперь указанные атрибуты отображаются при просмотре списка опубликованных сертификатов под именами **G**

и SN соответственно. Также возможен поиск опубликованных сертификатов по этим атрибутам.

Сертификаты с заполненными атрибутами givenName и surname, которые были опубликованы с помощью более ранних версий ViPNet Publication Service, необходимо опубликовать заново, чтобы значения этих атрибутов появились в сертификатах, размещенных в хранилищах.

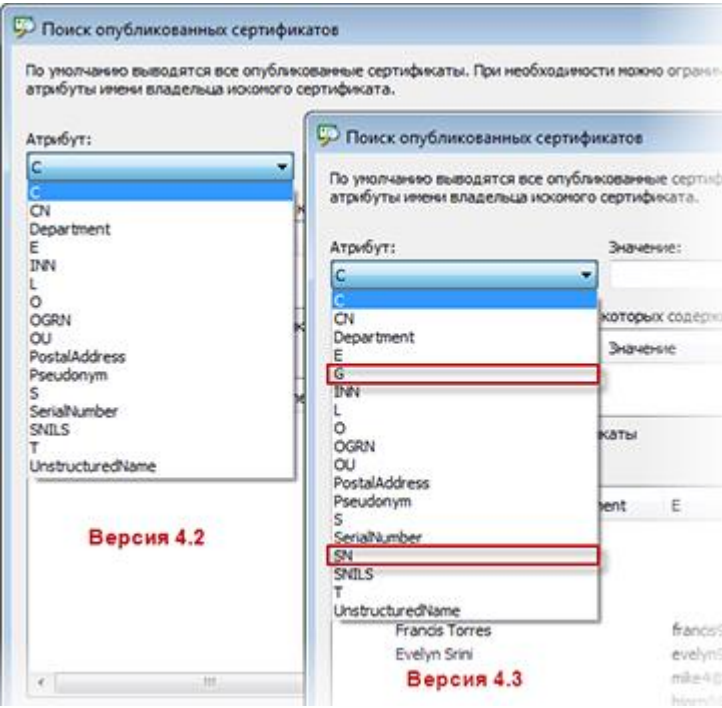


Рисунок 67. Поддержка атрибутов G (givenName) и SN (surname) поля Субъект

- **Изменения в файлах расширения схемы ADAM/AD LDS**

В связи с поддержкой атрибутов surname и givenName поля Субъект изменены файлы расширения схемы ADAM/AD LDS.

- **Возможность экспорта и импорта настроек программы**

Реализована возможность экспорта и импорта следующих настроек программы: настройки публикаций, настройки опроса точек распространения CRL, общие настройки программы ViPNet Publication Service. Эти функции позволяют создавать резервные копии настроек для их восстановления в случае сбоев, а также переносить настройки из одной копии программы ViPNet Publication Service в другую.

- **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 (COC)	Список аннулированных сертификатов (CRL)	CRL
Отзыв сертификата	Аннулирование сертификата	—

В связи с изменениями переработан интерфейс программы.

- **Возможность работы как с зарегистрированной версией, так и с незарегистрированной**
Теперь ViPNet Publication Service является коробочным продуктом, который может работать как в демо-режиме, не требующем регистрации, так и в полнофункциональном режиме, который требует регистрации (см. [Регистрация ViPNet Publication Service](#) на стр. 22).

Что нового в версии 4.2

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Publication Service версии 4.2:

- **Мастер установки ключей ViPNet**

В версии 4.2 мастер первичной инициализации больше не используется. Мастер установки ключей ViPNet позволяет выполнять все сценарии, связанные с установкой и обновлением ключей на сетевом узле ViPNet.

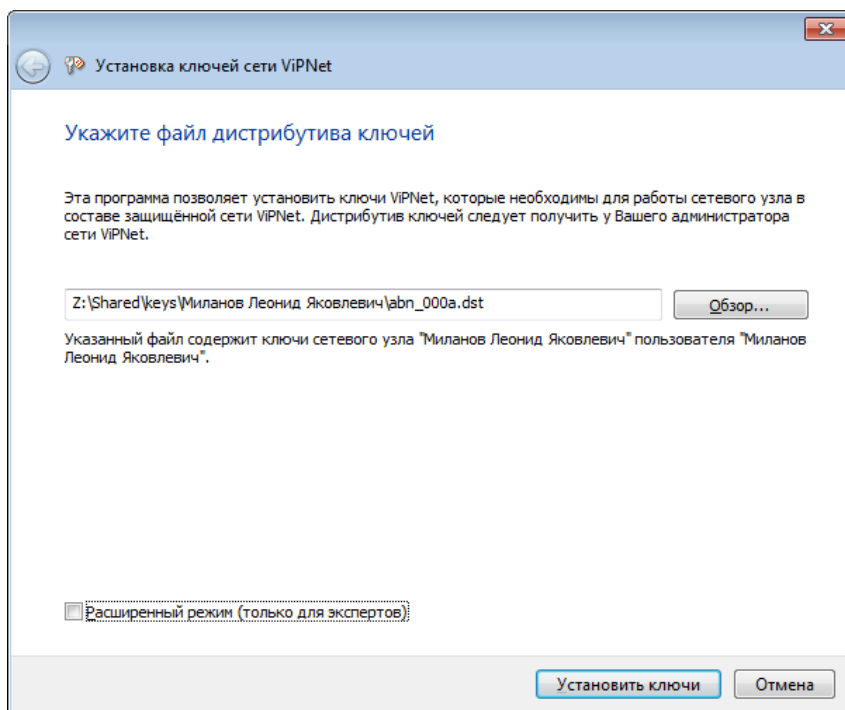


Рисунок 68. Выбор файла дистрибутива ключей

- Способы аутентификации пользователя

В версии 4.2 при использовании устройства аутентификации (способ **Устройство**) для входа в программу реализована возможность выполнять аутентификацию пользователя не только с помощью персонального ключа (как в версии 3.2.x), но и с помощью сертификата.

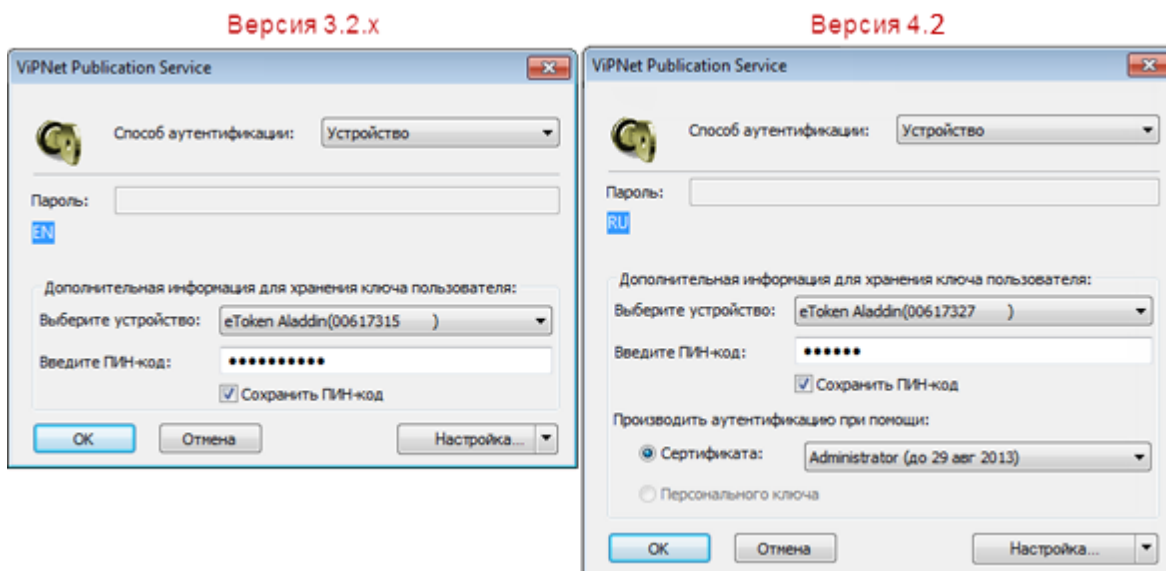


Рисунок 69. Изменение способа аутентификации пользователя

Способ аутентификации **Пароль на устройстве** в дальнейшем поддерживаться не будет, поэтому в версии 4.2 рекомендуется перейти на другие способы аутентификации.

- Выбор пользователя, от имени которого требуется войти в программу

Если для входа в программу используется пароль, то при входе в программу или смене пользователя достаточно выбрать в соответствующем списке учетную запись. При этом не требуется указывать папку ключей пользователя.

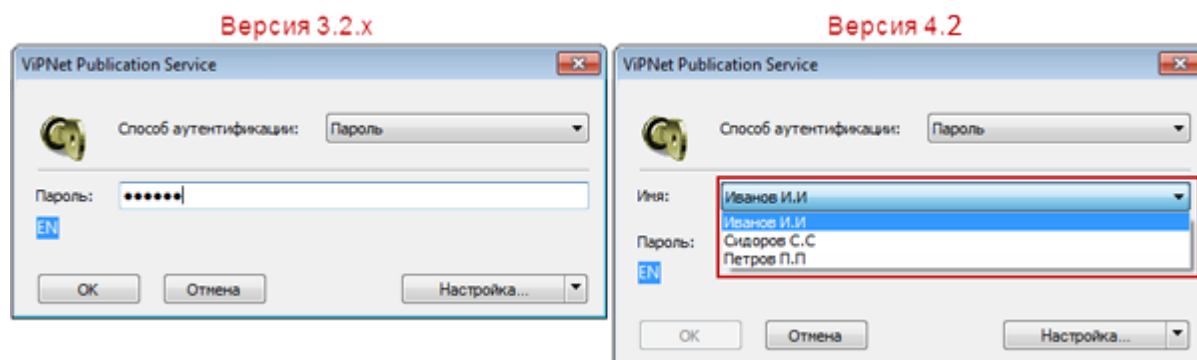


Рисунок 70. Выбор пользователя при входе в программу

- **Новая программа установки ViPNet Publication Service**

Для ViPNet Publication Service версии 4.2 разработана новая программа установки, в которой используется технология MSI.

- **Обновление документации и справки**

Документация и справка, поставляемые вместе с программным обеспечением ViPNet Publication Service, были обновлены.

Что нового в версии 3.2.10

В версии 3.2.10 улучшена внутренняя функциональность программы, исправлены незначительные ошибки, выявленные в процессе эксплуатации предыдущих версий.

Что нового в версии 3.2.9

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Publication Service версии 3.2.9.

- **Обеспечена поддержка квалифицированных сертификатов, требования к которым описаны в федеральном законе от 06.04.2011 №63-ФЗ «Об электронной подписи» и приказе ФСБ РФ от 27.12.2011 №795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»**

Обеспечена возможность публикации квалифицированных сертификатов на FTP-сервере и LDAP-сервере ADAM/AD LDS.

Обеспечена возможность поиска опубликованных сертификатов по полям ИНН, СНИЛС и ОГРН на LDAP-сервере ADAM/AD LDS.

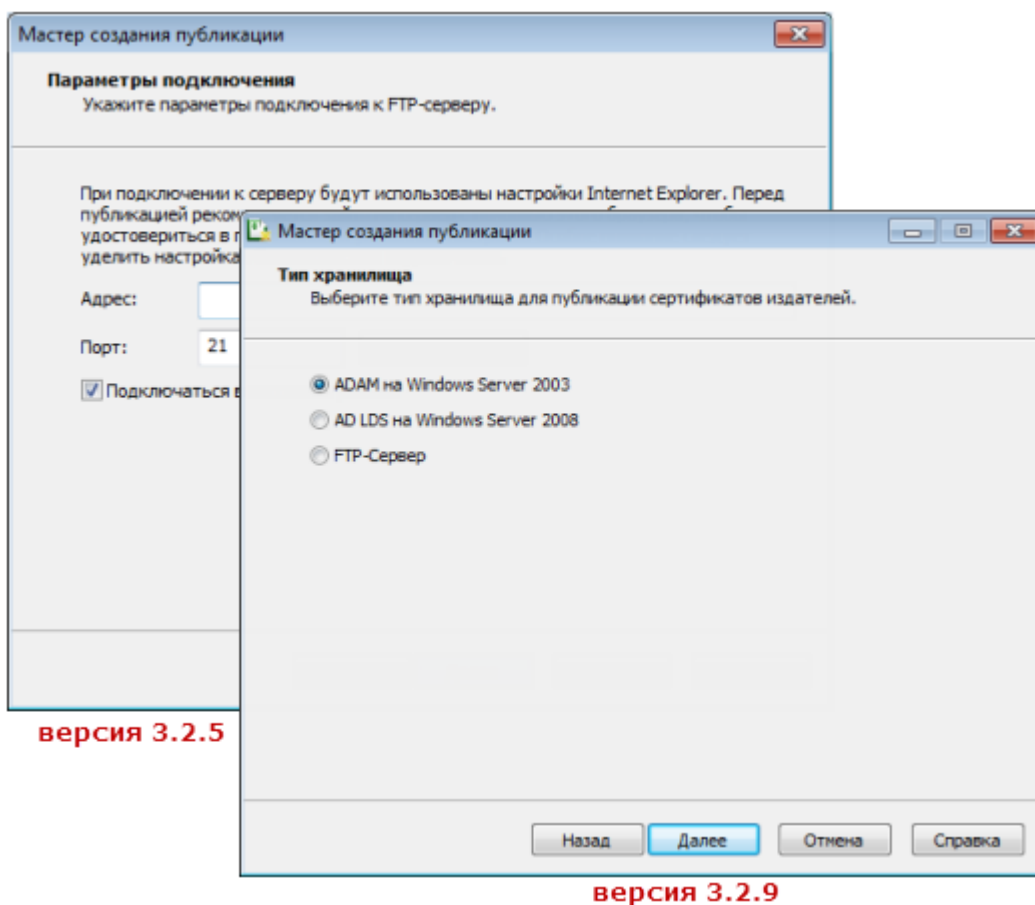


Рисунок 72. Добавление возможности публикации сертификатов издателей на LDAP-серверы

- Добавлена возможность публикации обновлений, выпущенных в УЦ «Верба-сертификат МВ» (pse-файлы)

Ранее программа ViPNet Publication Service не поддерживала публикацию обновлений, выпущенных в УЦ «Верба-сертификат МВ» (см. глоссарий, стр. 133). Теперь с помощью ViPNet Publication Service при необходимости можно настроить публикацию этого типа данных в сетевые хранилища ADAM/AD LDS.

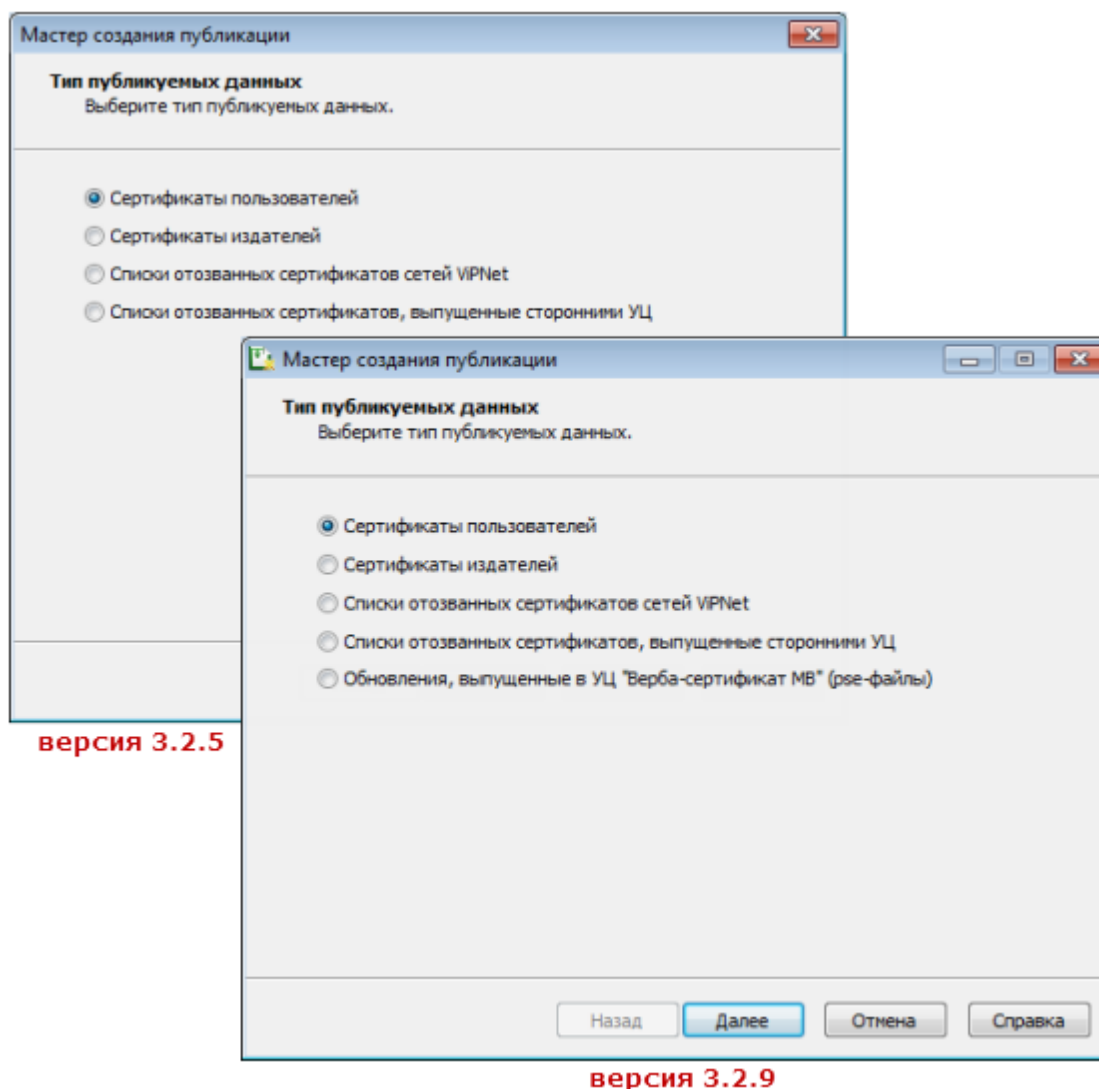


Рисунок 73. Добавление Публикации обновлений, выпущенных в УЦ «Верба-сертификат МВ»

- **Добавлена возможность публикации сертификатов пользователей на FTP-сервер**

Ранее программа ViPNet Publication Service не поддерживала публикацию сертификатов пользователей на FTP-сервер. Теперь с помощью ViPNet Publication Service при необходимости можно настроить публикацию этого типа данных на FTP-сервер.

- **Добавлена функция экспорта опубликованных сертификатов и сохранения pse-файлов**

Появилась возможность производить экспорт опубликованных сертификатов и сохранение pse-файлов из хранилищ в папку, заданную администратором. Данная функция позволяет перемещать устаревшие опубликованные данные в резервные хранилища и при необходимости удалять устаревшие данные из сетевых хранилищ (Active Directory, ADAM/AD LDS, FTP-серверов). Данная функция позволяет хранить в сетевых хранилищах только актуальные данные.

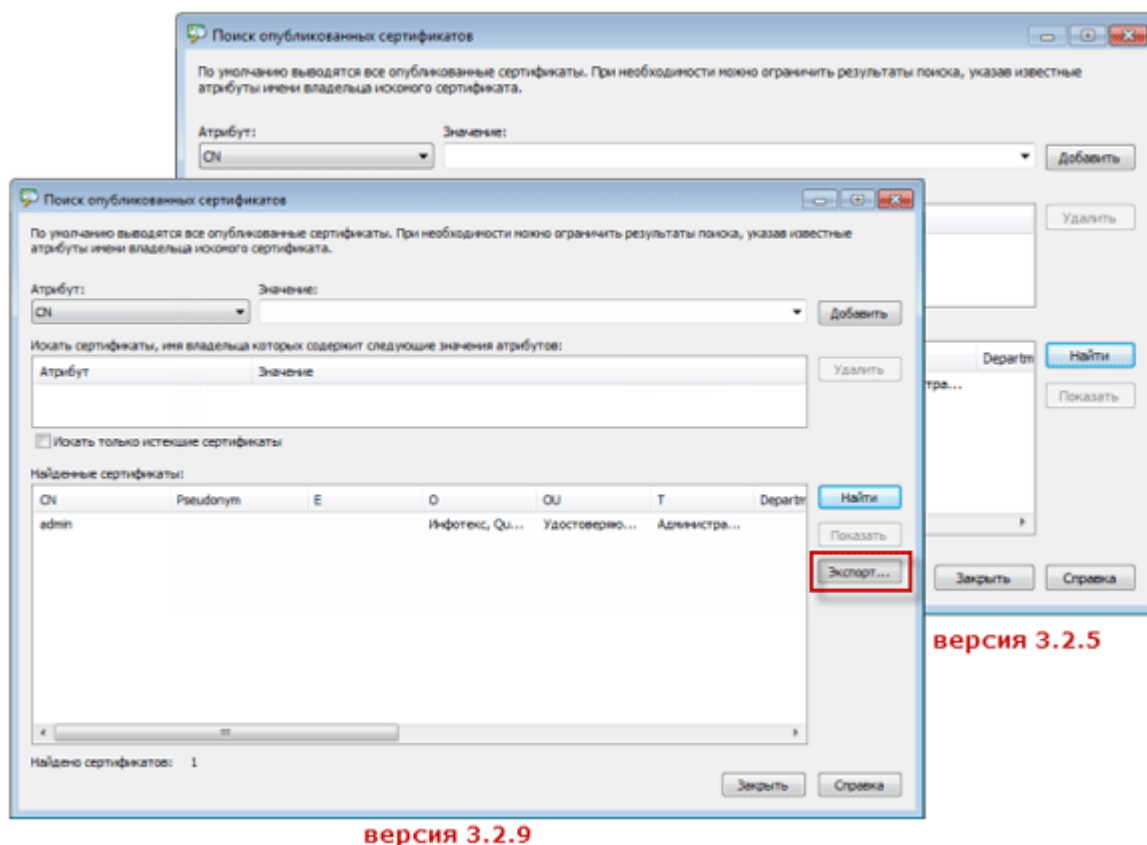


Рисунок 74. Добавление функции экспорта

- Добавлена возможность настройки сопоставления сертификатов пользователям домена Active Directory. Ранее при публикации сертификатов пользователям домена Active Directory использовалась жестко заданная таблица сопоставления атрибутов.

Теперь появилась возможность редактировать эту таблицу, указывая те атрибуты, по которым будет выполняться поиск подходящего пользователя домена при публикации сертификата.

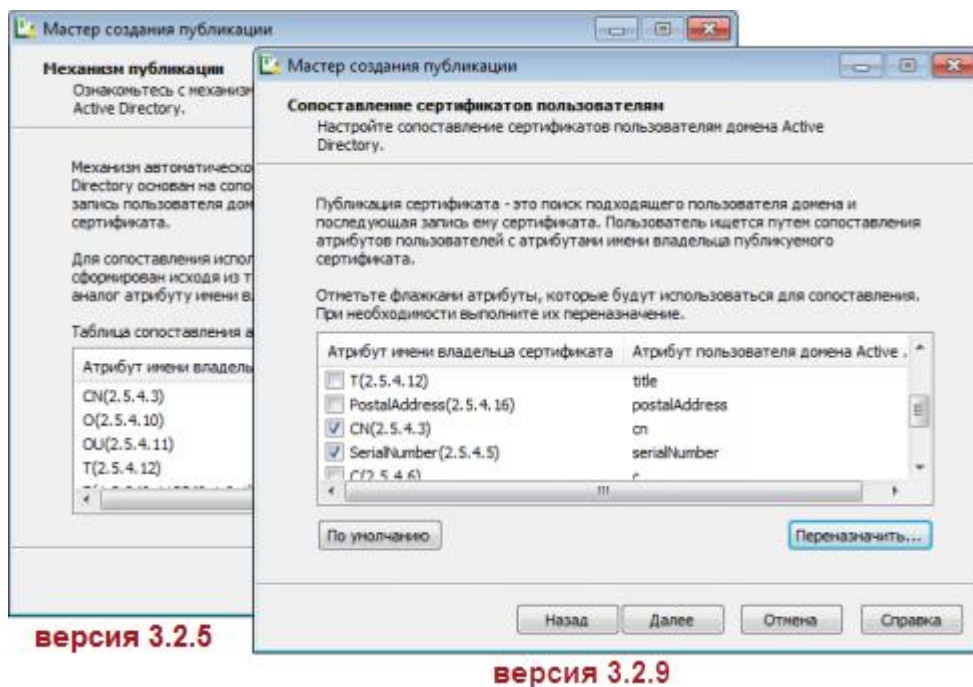


Рисунок 75. Изменение механизма сопоставления сертификатов пользователям Active Directory

- Изменен журнал публикации

В связи с появлением возможности публикации обновлений, выпущенных в удостоверяющем центре «Верба-сертификат МВ», переработан интерфейс журнала публикации. Новый интерфейс позволяет ускорить поиск возможных ошибок публикаций по типам публикуемых данных.

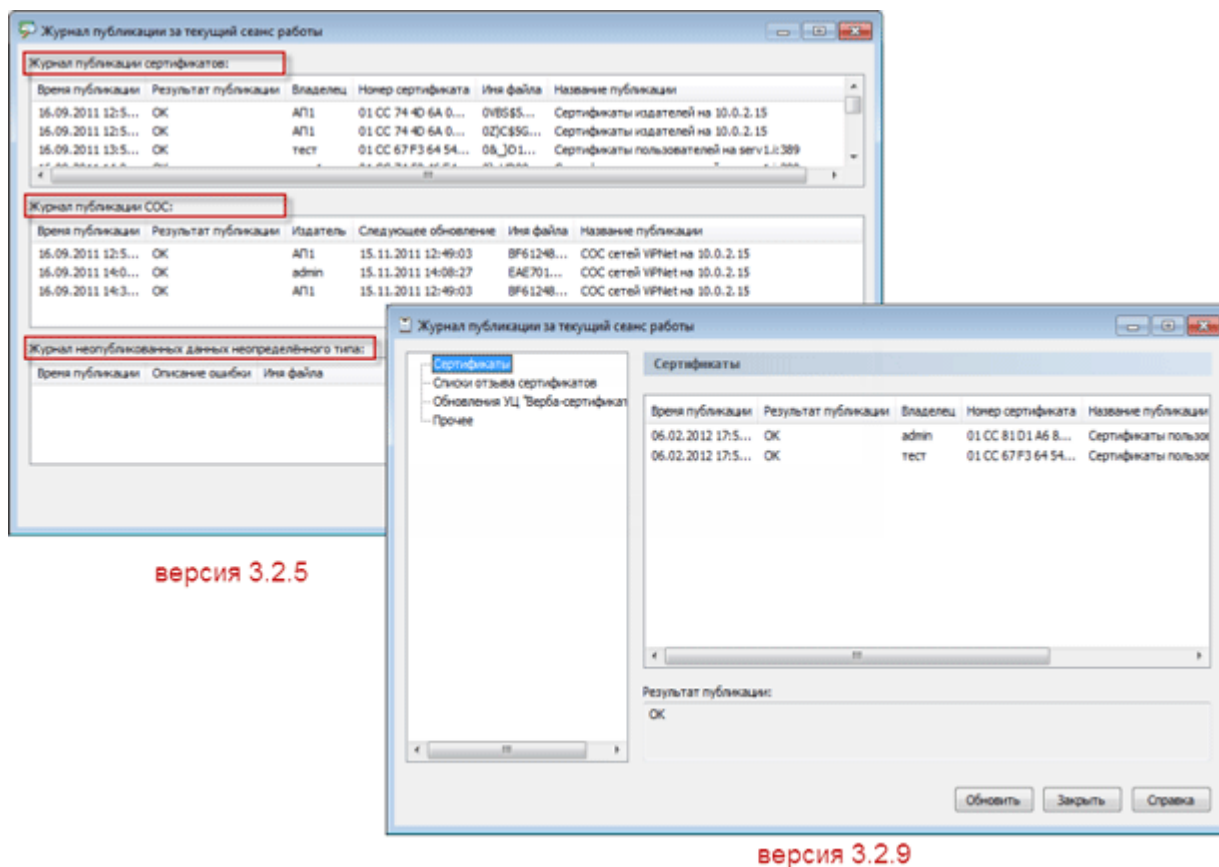


Рисунок 76. Измененный интерфейс журнала публикации

- Улучшена детализация диагностических сообщений об ошибках

Ранее сообщения об ошибках журнала публикации не содержали подробного описания проблем при публикации. Теперь для удобства решения возникающих проблем при публикации сообщения содержат подробную информацию, которая конкретизирует ошибки публикации и содержит рекомендации по их устранению.

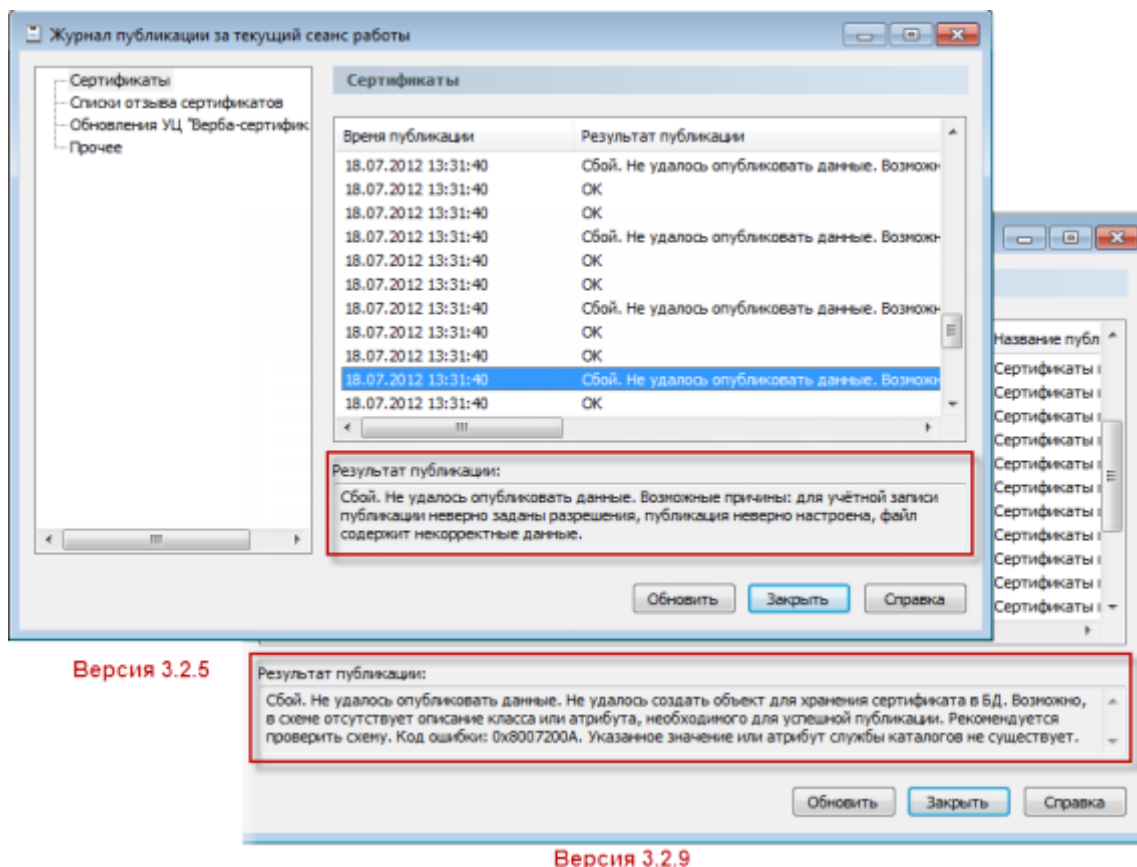


Рисунок 77. Улучшение детализации сообщений об ошибках

- **Расширенный список поддерживаемых устройств аутентификации**

Реализована поддержка следующих устройств аутентификации: JaCarta, устройства компании Gemalto с апплетом «Аладдин Р.Д.», устройство Kaztoken с поддержкой казахстанского стандарта электронной подписи. Теперь эти устройства можно применять для хранения персональных ключей и ключей электронной подписи.

- **В интерфейсе программы и документации изменен термин «электронная цифровая подпись»**

Для соответствия Федеральному закону 06.04.2011 N 63-ФЗ «Об электронной подписи» (текст закона <http://www.rg.ru/2011/04/08/podpis-dok.html>) термин «электронная цифровая подпись» («цифровая подпись») в интерфейсе программы изменен на термин «электронная подпись».

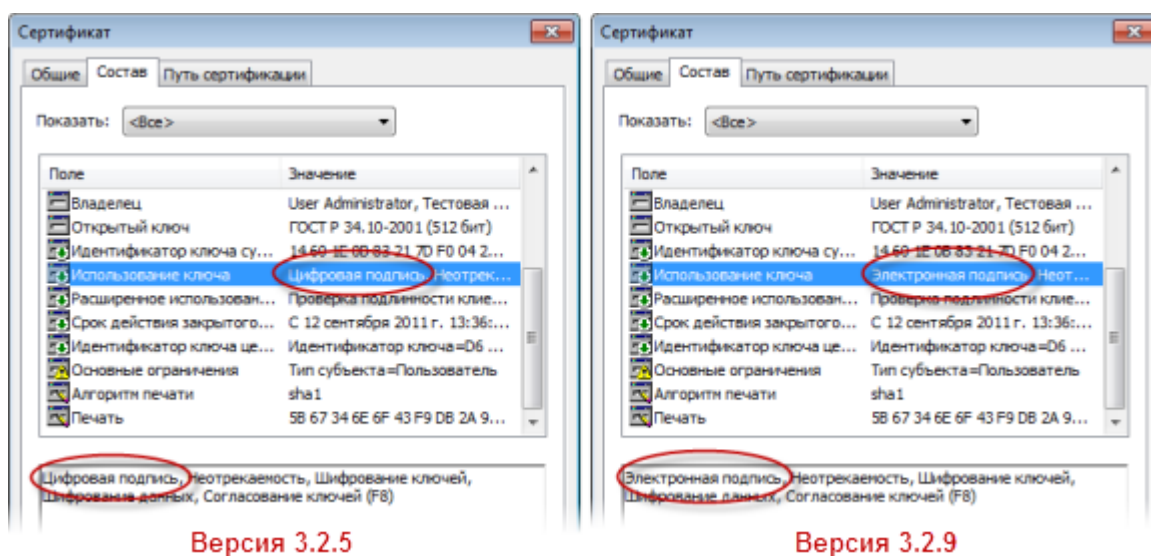


Рисунок 78. Изменение термина «цифровая подпись» на примере окна «Сертификат»

- Усовершенствованы документация и справка

Переработаны документация и справка. Добавлено описание новых функций программы, обновлена информация в разделах, касающаяся изменений в интерфейсе. Обновлено документы:

- «Сетевые хранилища сертификатов 3.0. Руководство администратора»;
- «ViPNet Publication Service. Форматы хранения опубликованных данных».

Что нового в версии 3.2.5

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Publication Service версии 3.2.5.

- Изменен термин «Режим авторизации» и названия элементов интерфейса, содержащие этот термин

Произведена замена термина «Режим авторизации» на «Способ аутентификации». В связи с изменением переработан интерфейс программы.

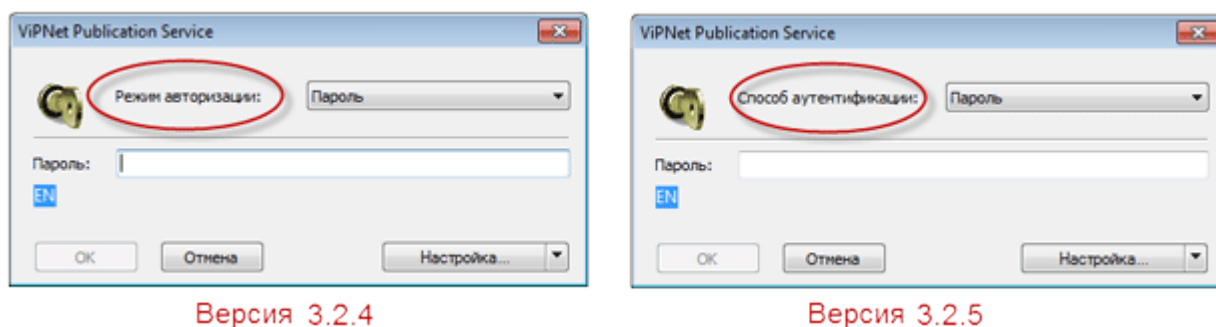


Рисунок 79. Измененный интерфейс окна ввода пароля

- Усовершенствованы документация и справка

Переработаны документация и справка, улучшено их качество.

Что нового в версии 3.2.3

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Publication Service версии 3.2.3.

- **Усовершенствованы документация и справка**

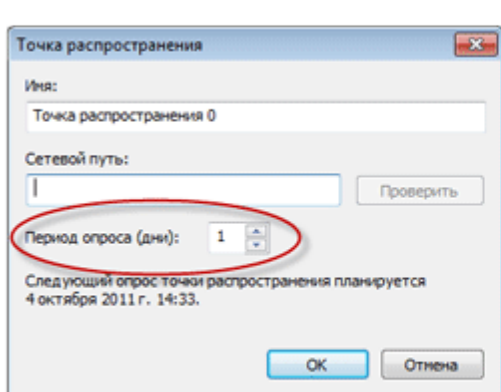
Переработаны документация и справка, улучшено их качество. Обновлен документ «Сетевые хранилища сертификатов. Руководство администратора».

Что нового в версии 3.2.2

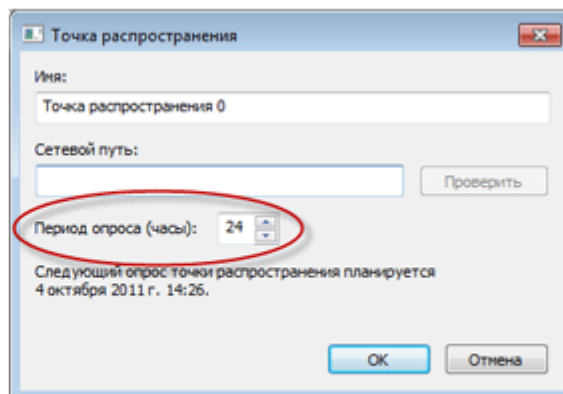
В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Publication Service версии 3.2.2.

- **Изменен период автоматического опроса точек распространения СОС**

Ранее опрос точек распространения задавался в днях, в настоящей версии — в часах. В связи с изменениями переработан интерфейс программы.



Версия 3.2.0



Версия 3.2.2

Рисунок 80. Измененный интерфейс окна "Точка распространения"

- **Усовершенствованы документация и справка**

Переработаны документация и справка, улучшено их качество. Обновлен документ «Форматы хранения опубликованных данных». В документ «ViPNet Publication Service 3.2. Руководство администратора» добавлено описание условий совместимости программ ViPNet Publication Service и FTP-сервер Serv-U.

Что нового в версии 3.2.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Publication Service версии 3.2.0.

- **Расширена возможность публикации сертификатов пользователя**

Появилась возможность публиковать в сетевые хранилища ADAM/AD LDS несколько сертификатов для одного пользователя.

- **Добавлен новый тип публикации**

Реализована возможность публикации списков отозванных сертификатов, выпущенных сторонними УЦ.

- **Изменены файлы расширения схемы ADAM/AD LDS**

В связи с добавлением новых типов публикаций были изменены файлы расширения схемы ADAM/AD LDS.

- **Изменена концепция добавления публикаций**

Ранее определение публикации базировалось на типе сервера, в версии 3.2.0 — на типе публикуемых данных и типе хранилища.

- **Переработан интерфейс управления публикациями**

Ранее публикации настраивались в окне **Серверы публикации** и параметры публикации задавались на различных вкладках. Теперь для настройки публикаций создан **Мастер создания публикаций**.

В связи с изменениями переработан интерфейс программы.

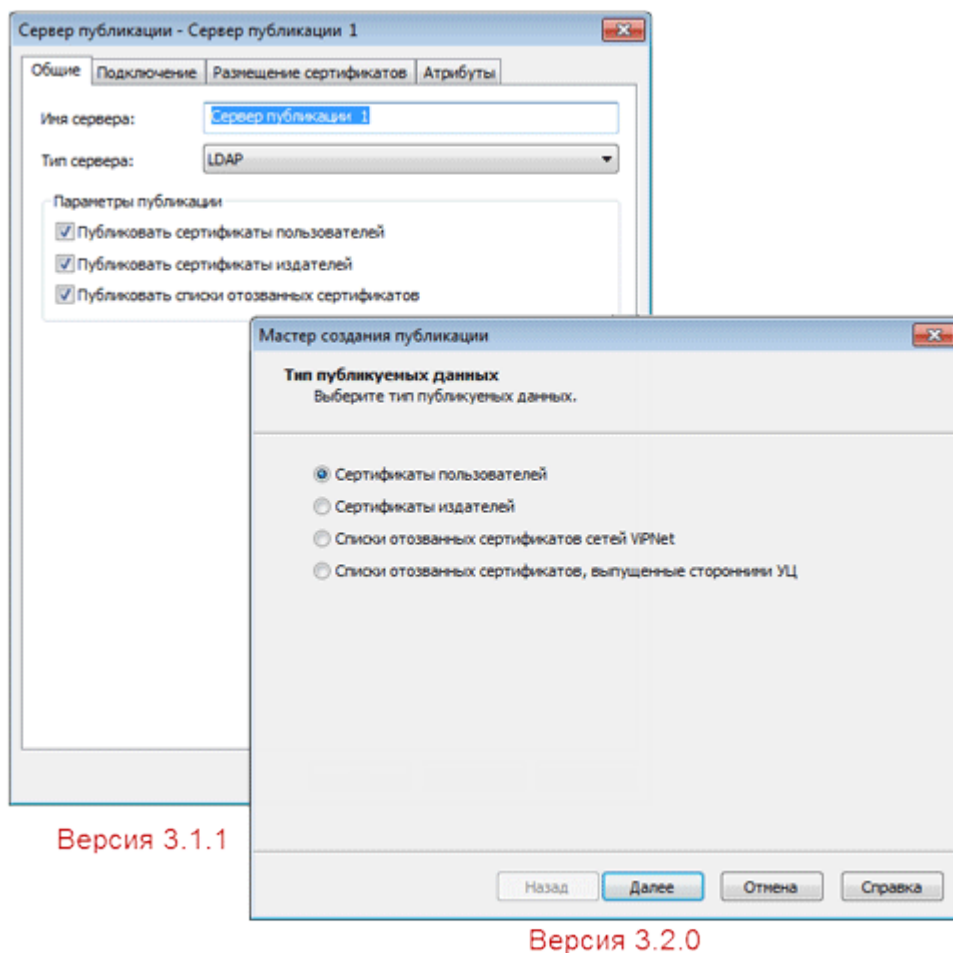


Рисунок 81. Измененный интерфейс окна создания и настройки публикации

- Добавлен журнал публикации за текущий сеанс работы

Ранее информация о публикации отображалась в общем окне журнала событий. Теперь для информации о публикации создано отдельное окно **Журнал публикации за текущий сеанс работы**.

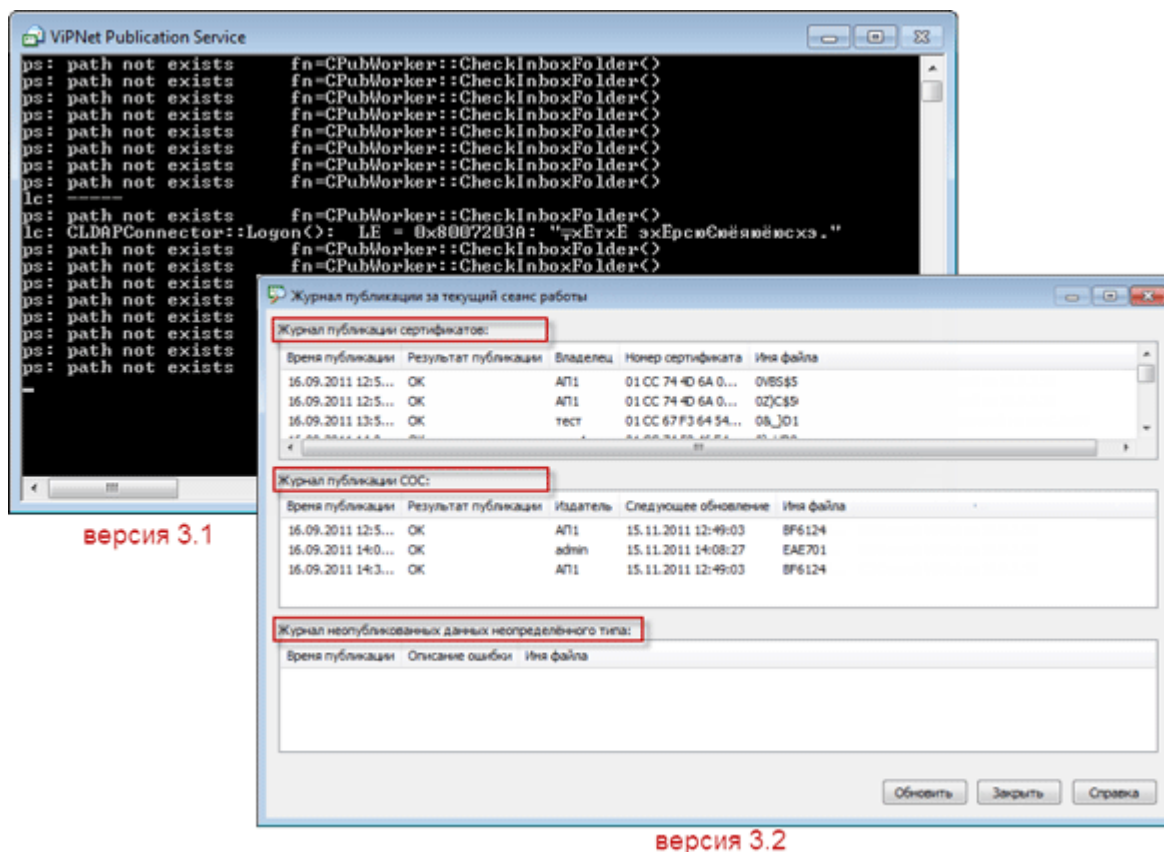


Рисунок 82. Измененный интерфейс журнала публикации

- Усовершенствованы документация и справка

Полностью переработаны документация и справка, улучшено их качество. При переработке документации акцент сделан на сценарный подход.



Глоссарий

Active Directory (AD)

Служба каталогов, разработанная Microsoft для доменных сетей Windows. Эта служба интегрирована в большинство операционных систем Windows Server.

Active Directory является центром администрирования и обеспечения безопасности сети. Она служит для аутентификации и авторизации всех пользователей и компьютеров внутри сети доменного типа Windows. При помощи Active Directory задаются и применяются политики безопасности для всех компьютеров в сети, а также устанавливается или обновляется программное обеспечение на компьютерах сети. Active Directory хранит данные и настройки среды в централизованной базе данных.

AD LDS (Active Directory Lightweight Directory Services)

Служба Active Directory облегченного доступа к каталогам, работающая под управлением операционной системы Microsoft Windows Server 2008, Windows Server 2012.

Authority Key Identifier (идентификатор ключа центра сертификатов)

Данный параметр является информационным дополнением сертификата и его указание необязательно. Может принимать одно из значений:

- идентификатор ключа проверки электронной подписи издателя;
- серийный номер сертификата издателя плюс имя издателя.

Выбранный способ формирования этого параметра не рекомендуется изменять, пока действителен сертификат издателя, выпускающего списки аннулированных сертификатов (CRL) с данным параметром. Это обусловлено тем, что значение расширения отчасти определяет URL, по которому будет доступен опубликованный CRL.

FTP (File Transfer Protocol)

Стандартный протокол прикладного уровня для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер.

LDAP (Lightweight Directory Access Protocol)

Упрощённая версия протокола доступа к каталогу стандарта X.500. LDAP является основным протоколом, используемым для доступа к Active Directory и AD LDS.

ViPNet Administrator

Набор программного обеспечения для администрирования сети ViPNet, включающий в себя серверное и клиентское приложения ViPNet Центр управления сетью, а также программу ViPNet Удостоверяющий и ключевой центр.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Администратор УКЦ формирует и обновляет ключи для сетевых узлов ViPNet, а также управляет сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

ViPNet Центр управления сетью — это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

Администратор 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.

Доверенное лицо (администратор) удостоверяющего центра

Лицо, обладающее правом издавать сертификаты от имени удостоверяющего центра.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. Клиент должен быть зарегистрирован на координаторе. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Контейнер

Объект службы каталогов (Active Directory, AD LDS) который может содержать в себе другие объекты.

Кросс-сертификат

Сертификат уполномоченного лица одного удостоверяющего центра, изданный уполномоченным лицом другого удостоверяющего центра.

Обновления, выпущенные в удостоверяющем центре «Верба-сертификат МВ»

Представляют собой файл в формате *.pse, который содержит сертификат издателя и актуальный список аннулированных сертификатов (CRL). Также pse-файл может содержать только сертификат издателя или только CRL.

Папка ключей пользователя

Папка, в которой находятся ключи пользователя ViPNet.

Публикация

Размещение сформированной в удостоверяющем центре информации на источниках данных, доступных по общеизвестным протоколам (например, FTP, LDAP).

Сервис публикации

ViPNet Publication Service. Программа, которая описывается в данном документе.

Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

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.

Электронная подпись

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