ViPNet CSP 4.2

Руководство пользователя

infotecs

ФРКЕ.00106-04 34 01, версия 4.2.8

ОАО «ИнфоТеКС»

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

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

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

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

Для кого предназначен документ

Данное руководство предназначено для пользователей программы ViPNet CSP. В нем содержится информация о назначении криптопровайдера, описываются основные сценарии работы с ним: шифрование документов и сообщений электронной почты, подписание и проверка подлинности электронной подписи, организация удаленного доступа к ресурсам по протоколам TLS и другие.

Предполагается, что читатель данного руководства имеет общее представление о сетевых технологиях, IP-протоколах, межсетевых экранах и информационной безопасности.

Соглашения документа

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

Таблица 1. Обозначения, используемые в примечаниях

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

Таблица 2. Обозначения, используемые для выделения информации в тексте

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

О программе

Программа ViPNet CSP представляет собой криптопровайдер (см. «Назначение криптопровайдера» на стр. 20), обеспечивающий вызов криптографических функций из различных приложений Microsoft и другого ПО, использующего интерфейс CryptoAPI 2.0.

С помощью ViPNet CSP вы можете выполнять следующие действия:

- Создание ключей электронной подписи (см. глоссарий, стр. 232) в соответствии с алгоритмами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.
- Формирование и проверка электронной подписи в соответствии с алгоритмами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.
- Хэширование данных в соответствии с алгоритмами ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012.
- Шифрование и имитозащита данных в соответствии с алгоритмом ГОСТ 28147-89.
- Создание последовательностей случайных и псевдослучайных чисел, сессионных ключей шифрования.
- Аутентификация и выработка сессионного ключа при передаче данных по протоколу TLS.
- Хранение сертификатов открытых ключей непосредственно в контейнерах ключей.
- Работа с электронными ключами на различных внешних устройствах: eToken, Рутокен, УЭК и других (см. «Внешние устройства» на стр. 214).

Совместимость ViPNet CSP с криптопровайдерами других производителей обеспечивается при условии реализации ими требований, содержащихся в документах: RFC 4357 (https://tools.ietf.org/html/rfc4357), RFC 4490 (https://tools.ietf.org/html/rfc4490), RFC 4491 (https://tools.ietf.org/html/rfc4491), RFC 7836 (http://tools.ietf.org/html/rfc7836), «Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89» (http://www.tc26.ru/methods/recommendation/ТК26УЗ.pdf), «Задание параметров эллиптических кривых в соответствии с ГОСТ Р 34.10-2012» (http://www.tc26.ru/methods/recommendation/ТК26ЭК.pdf), «Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012» (http://www.tc26.ru/methods/recommendation/ТК26АЛГ.pdf), «Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)» (http://www.tc26.ru/methods/recommendation/TK26TLS.pdf).

Системные требования

Требования к компьютеру для установки программы ViPNet CSP:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 512 Мбайт.
- Свободное место на жестком диске — не менее 100 Мбайт.
- Операционная система:
  - Windows 7 — 32/64-разрядная, сборка 6.1.7601;
  - Windows Server 2008 R2 — 64-разрядная, сборка 6.1.7601;
  - Windows 8 — 32/64-разрядная, сборка 6.2.9200;
  - Windows Server 2012 — 64-разрядная, сборка 6.2.9200;
  - Windows 8.1 — 32/64-разрядная, сборка 6.3.9600;
  - Windows Server 2012 R2 — 64-разрядная, сборка 6.3.9600;
  - Windows 10 — 32/64-разрядная следующих версий и сборок:
    - версия 1507, сборка 10240,
    - версия 1511, сборка 10586,
    - версия 1607, сборка 14393,
    - версия 1703, сборка 15063,
    - версия 1709, сборка 16299,
    - версия 1803, сборка 17134.

  Для каждой из указанных сборок должны быть установлены последние пакеты обновлений. Работа ViPNet CSP на компьютерах, работающих под управлением операционных систем других сборок, не гарантируется.

Примечание. В ОС Windows 10 поддерживаются все заявленные криптографические операции, кроме организации защищенных подключений по протоколу TLS в веб-браузере Microsoft Edge.

- Internet Explorer — версия 10 или более поздняя.
- При использовании программ Microsoft Office — версия 2010 или 2013.

ViPNet CSP поддерживает работу с несколькими типами устройств хранения электронных ключей. Подробную информацию о поддерживаемых электронных ключах см. в приложении Внешние устройства (на стр. 214).

Комплект поставки

В комплект поставки программы ViPNet CSP входят следующие компоненты:

- Установочный файл ViPNet CSP.
- Документы в формате PDF:
  - «ViPNet CSP. Руководство пользователя».
  - «ViPNet CSP. Быстрый старт».
  - «ViPNet CSP. Лицензионные соглашения на компоненты сторонних производителей».
  - «Криптографический интерфейс ViPNet CSP. Руководство разработчика».
  - «Криптографический интерфейс ViPNet CNG. Руководство разработчика».
  - «Криптографический интерфейс ViPNet PKCS#11 VT. Руководство разработчика».
  - «ViPNet SysLocker. Руководство администратора».

Новые возможности версии 4.2.8

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet CSP версии 4.2.8 по сравнению с программой версии 4.2.2. Информация об изменениях в предыдущих версиях программы приведена в приложении История версий (на стр. 201).

- **Изменения в списке поддерживаемых операционных систем**

  В криптопровайдере ViPNet CSP частично реализована поддержка операционной системы Windows 10 (32-разрядная и 64-разрядная). Поддерживаются все заявленные криптографические операции, кроме организации защищенных подключений по протоколу TLS в веб-браузере Microsoft Edge.

  В связи с тем, что компания Microsoft прекратила общую поддержку операционных систем Windows 2003 (32-разрядная) и Windows Vista (32/64-разрядная), работа ViPNet CSP на компьютерах с этими операционными системами также более не поддерживается ОАО «ИнфоТеКС». Кроме того, работа ViPNet CSP более не поддерживается на компьютерах с операционной системой Windows Server 2008 (32/64-разрядная).

- **Контроль версии операционной системы Windows при установке ViPNet CSP**

  Во избежание появления ошибок ViPNet CSP из-за возможных конфликтов с версиями операционных систем, работа с которыми не была протестирована, установка ViPNet CSP 4.2.8 возможна только на компьютеры под управлением определенных версий (сборок) операционных систем Windows (см. «Системные требования» на стр. 11). При попытке установки ViPNet CSP на компьютер под управлением неподдерживаемой версии операционной системы появляется окно с предупреждением и процесс установки прекращается.

- **Создание точки восстановления Windows при установке ViPNet CSP**

  Чтобы обеспечить возможность восстановления состояния операционной системы Windows, предшествовавшего установке ViPNet CSP, при установке новой версии ViPNet CSP автоматически создается точка восстановления Windows. Если в настройках Windows отключена функция создания точек восстановления, программа установки ViPNet CSP автоматически включит эту функцию. При этом, в зависимости от настроек восстановления системы, Windows может отменить создание точки восстановления (например, если такая точка в этот день уже создавалась). Использование точек восстановления не поддерживается в серверных версиях Windows (см. «Восстановление системных файлов и параметров ОС Windows после неудачной установки ViPNet CSP» на стр. 196).

- **Совместимость ViPNet CSP с системой Microsoft Device Guard**

  Драйверы ViPNet CSP были подписаны электронной подписью доверенного издателя WHQL (Windows Hardware Quality Lab). Теперь при проверке программного обеспечения система Microsoft Device Guard, входящая в некоторые версии операционной системы Windows, считает программу ViPNet CSP доверенным приложением и при включенном компоненте Secure Boot не препятствует запуску драйверов ViPNet CSP.

- **Добавление комплекта средств разработки (SDK)**

  Вместе с новой версией ViPNet CSP распространяется архив SDK, включающий в себя набор заголовочных файлов и примеры программ.

- **Работа с ключами, находящимися на удаленном сервере ViPNet HSM**

  В новой версии программы ViPNet CSP появилась возможность использовать закрытые и открытые ключи, находящиеся на удаленном сервере ViPNet HSM (см. глоссарий, стр. 229), как если бы эти ключи находились на токене, подключенном к вашему компьютеру. Для этого в списке подключаемых устройств необходимо выбрать пункт **ViPNet HSM** и в специальном окне задать параметры подключения к серверу ViPNet HSM. Подробнее см. в разделе Взаимодействие с сервером ViPNet HSM (на стр. 155).

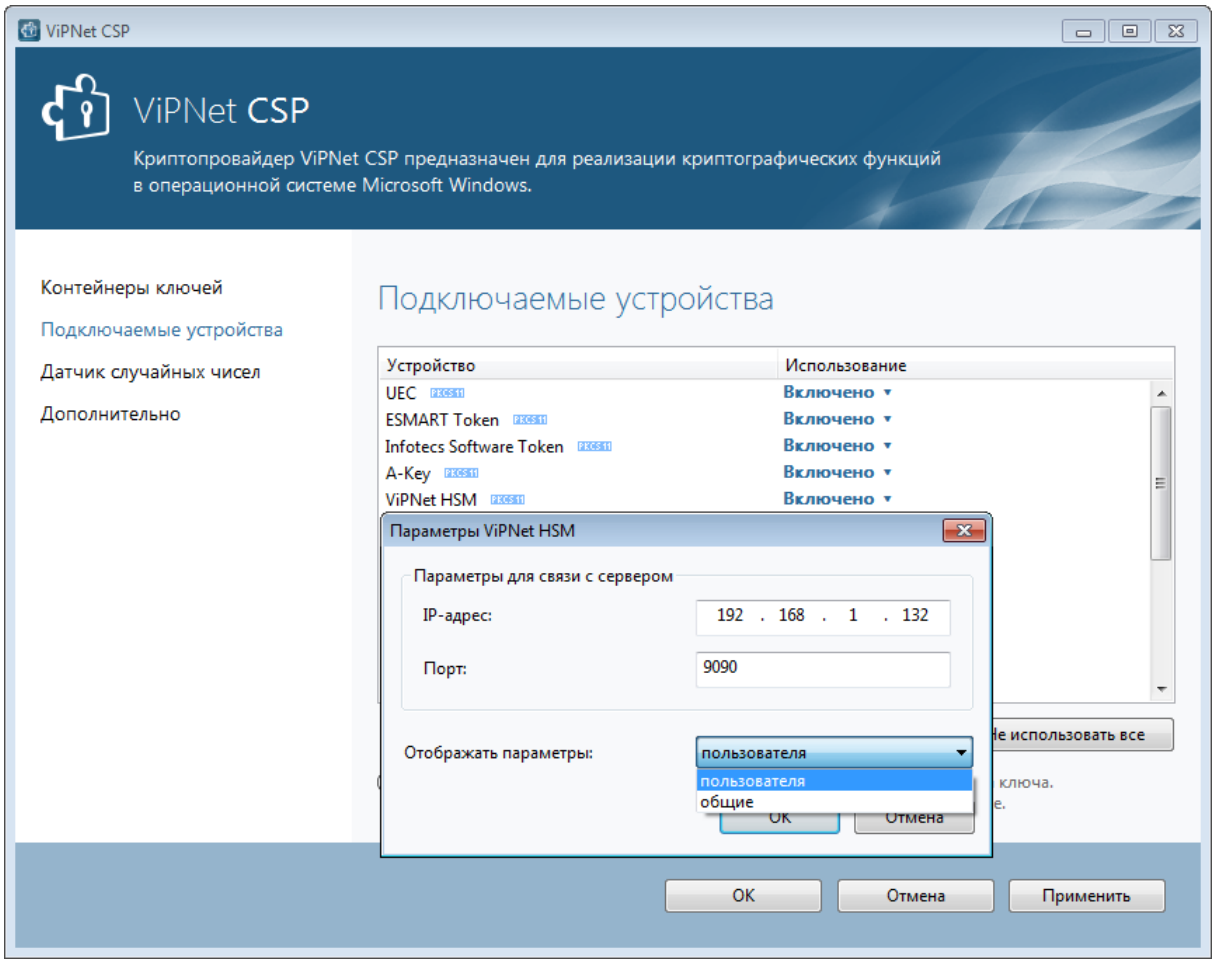


Рисунок 1. Задание параметров подключения к серверу ViPNet HSM

Функции, необходимые для взаимодействия с сервером ViPNet HSM, объединены в отдельный компонент программы ViPNet CSP. При необходимости в процессе установки или после установки ViPNet CSP вы можете отключить этот компонент (см. «Добавление, удаление и восстановление компонентов программы» на стр. 34).

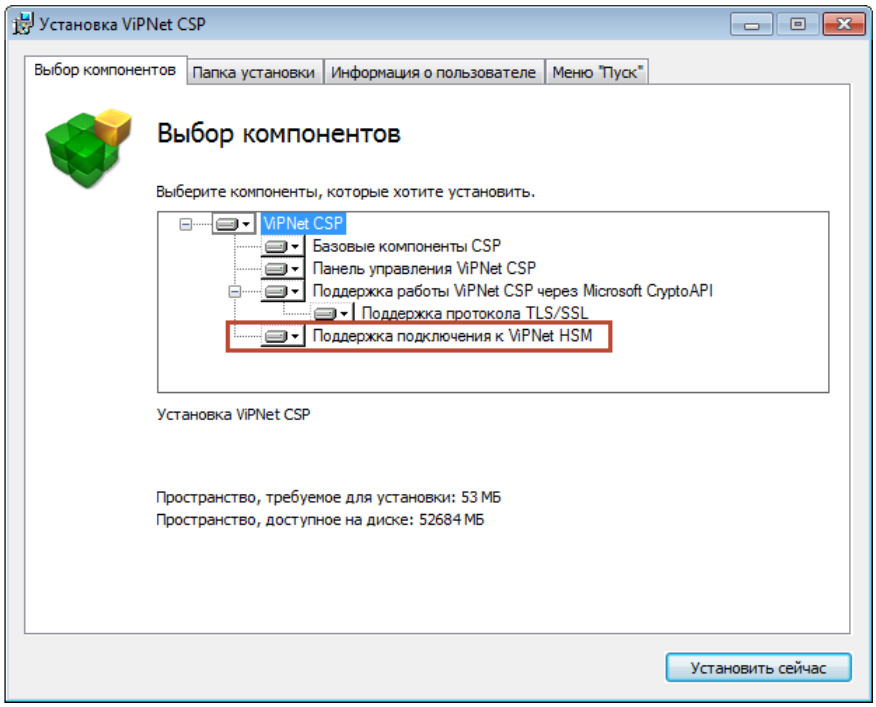


Рисунок 2. Компонент программы ViPNet CSP, предназначенный для взаимодействия с сервером ViPNet HSM

- **Изменение списка компонентов ViPNet CSP, устанавливаемых по умолчанию на компьютер под управлением Windows 10**

  При установке новой версии ViPNet CSP на компьютер под управлением Windows 10 компонент **Поддержка протокола TLS/SSL** по умолчанию теперь отключен.

- **Поддержка новых внешних устройств хранения данных**

  Реализована поддержка новых устройств хранения данных:

  - Персональные электронные ключи Gemalto SafeNet eToken 5100, 5105, 5200, 5205, 5110, 7300, а также смарт-карта Gemalto SafeNet eToken 4100 производства компании Gemalto (SafeNet).

    Так как для работы с указанными устройствами на компьютер необходимо установить то же программное обеспечение, что и для работы с устройствами семейства **eToken Aladdin**, это семейство устройств было переименовано в **SafeNet eToken (eToken Aladdin)**.

  - Электронный идентификатор Рутокен ЭЦП 2.0 производства компании «Актив».

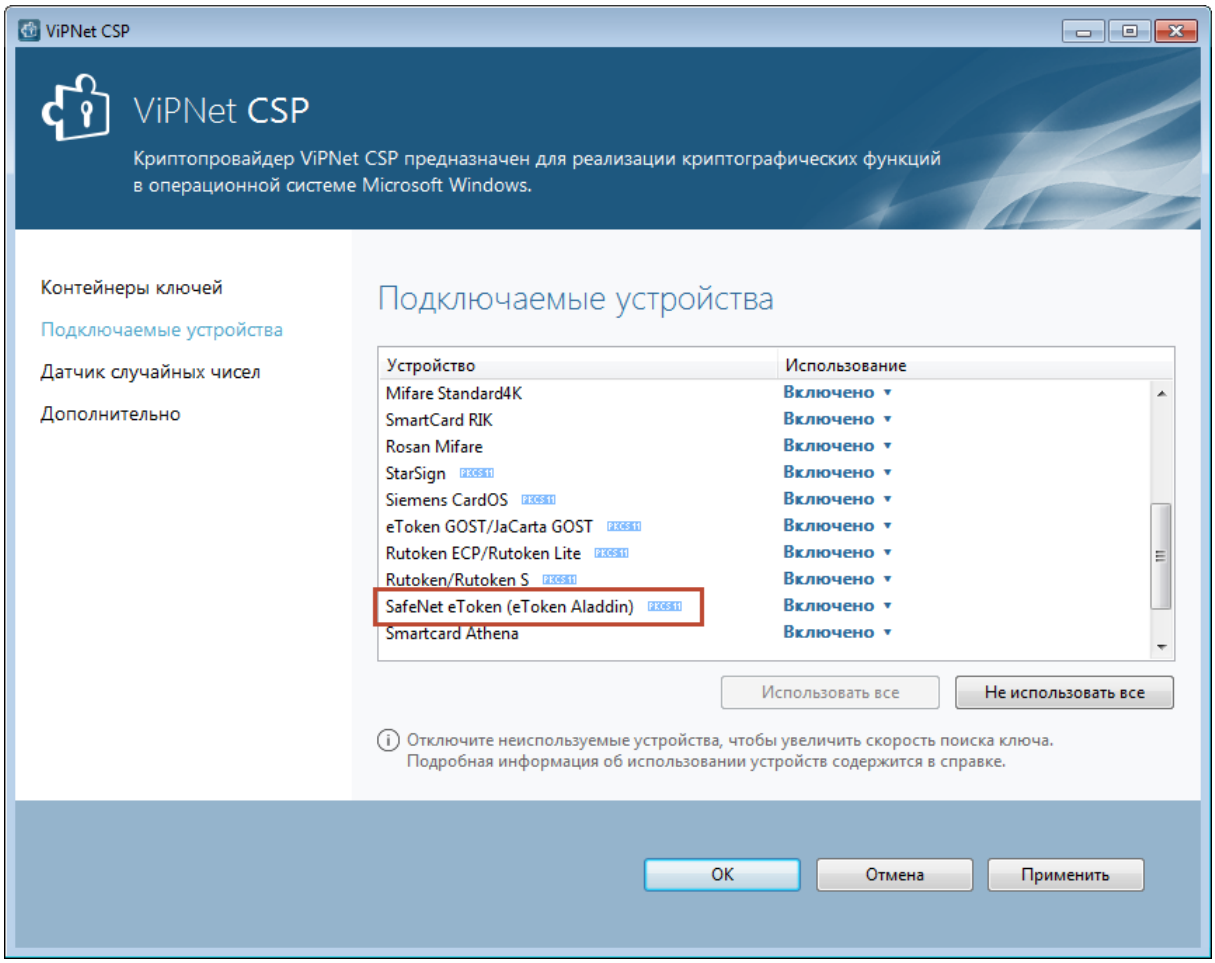


Рисунок 3. Поддержка устройств SafeNet eToken

- **Изменение в списке поддерживаемых пакетов программ Microsoft Office**

  В связи с тем, что компания Microsoft в 2017 году прекращает поддержку пакета программ Microsoft Office 2007, работа ViPNet CSP в этих программах также более не поддерживается ОАО «ИнфоТеКС».

- **Изменение в списке поддерживаемых почтовых программ Microsoft**

  В связи с тем, что компания Microsoft прекратила поддержку программы Почта Windows Live, взаимодействие ViPNet CSP с этой программой также более не поддерживается ОАО «ИнфоТеКС».

- **Исправление ошибок**

  В версии 4.2.8 исправлены ошибки, выявленные в процессе эксплуатации версии 4.2.2.

Обратная связь

Дополнительная информация

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

- Веб-портал документации ViPNet http://docs.infotecs.ru.
- Описание продуктов ViPNet http://www.infotecs.ru/products/line/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/.
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet http://www.infotecs.ru/forum/.

Контактная информация

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

- Техническая поддержка для пользователей продуктов ViPNet: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки http://www.infotecs.ru/support/request/.
- Консультации по телефону для клиентов, имеющих расширенный уровень технического сопровождения:

  8 (495) 737-6192,

  8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

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

1

Использование криптографических функций в системах защиты данных

Назначение криптопровайдера

Если существует необходимость защищать электронные документы средствами криптографии, а также подписывать документы электронной подписью, обеспечивая их подлинность и целостность, необходимо установить специализированный программный модуль — криптопровайдер.

Все версии операционной системы Windows, начиная с Windows 2000, имеют встроенный криптопровайдер Microsoft Base Cryptographic Provider. Алгоритмы, используемые этим криптопровайдером, не сертифицированы по требованиям ФСБ. Закон РФ «Об электронной подписи» (http://www.rg.ru/2011/04/08/podpis-dok.html) требует применения сертифицированных криптографических средств.

Криптопровайдер ViPNet CSP выполняет следующие задачи:

- Авторизация и обеспечение подлинности документов в процессе защищенного документооборота. Для этого используются средства формирования и проверки электронной подписи в соответствии со стандартами ГОСТ Р 34.11–94, ГОСТ Р 34.11-2012, ГОСТ Р 34.10–2001 и ГОСТ Р 34.10–2012.
- Обеспечение конфиденциальности и контроля целостности информации путем ее шифрования и имитозащиты в соответствии с ГОСТ 28147–89.
- Обеспечение аутентичности и конфиденциальности соединений TLS.

Электронная подпись

Электронная подпись — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием ключа электронной подписи.

Электронная подпись позволяет подтвердить следующее:

- Подлинность: электронная подпись удостоверяет личность поставившего подпись.
- Целостность: электронная подпись подтверждает, что документ не был изменен после подписания.
- Неотрекаемость: электронная подпись защищает от отказа субъекта от авторства документа.

Таким образом, электронная подпись может использоваться физическими и юридическими лицами в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе, подписанного собственноручной подписью правомочного лица и скрепленного печатью. Условия использования электронной подписи, особенности ее использования в сферах государственного управления и в корпоративной информационной системе регламентируются Законом РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи» (http://www.rg.ru/2011/04/08/podpis-dok.html).

Контейнер ключей

Пара ключей — закрытый и открытый (входящий в состав сертификата пользователя) — позволяет выполнять операции шифрования и подписи документов.

Закрытый ключ создается в удостоверяющем центре или самим пользователем и хранится в контейнере ключей на диске или внешнем устройстве.

Сертификат пользователя издается в удостоверяющем центре по запросу пользователя (см. «Создание запроса на сертификат и формирование закрытого ключа» на стр. 57) или, в некоторых случаях, по инициативе администратора удостоверяющего центра. Запрос на выдачу или обновление сертификата пользователя вы можете сделать с помощью клиентского программного обеспечения ViPNet Client, ViPNet CryptoService или программы «Создание запроса на сертификат» (см. «Порядок получения и ввода в действие закрытого ключа и сертификата» на стр. 56), входящей в пакет установки ViPNet CSP.

Кроме того, для проверки подлинности и актуальности сертификата пользователя необходимы цепочка сертификатов издателя (см. глоссарий, стр. 231) и список аннулированных сертификатов (CRL) (см. глоссарий, стр. 231).

При организации защищенного документооборота приложение (например, программа из состава Microsoft Office, служба сервера IIS) обращается к криптопровайдеру, передавая ему параметры сертификатов и местоположение закрытого ключа. Чтобы обеспечить приложениям доступ к сертификатам, их необходимо установить в хранилище операционной системы:

- Сертификат пользователя и закрытый ключ пользователя устанавливаются с помощью программы ViPNet CSP (см. «Установка контейнеров ключей и сертификатов» на стр. 64).
- Сертификат издателя и списки аннулированных сертификатов (CRL) (см. глоссарий, стр. 231) устанавливаются стандартными средствами операционной системы (см. «Установка сертификата издателя и списка аннулированных сертификатов» на стр. 78).

Программа ViPNet CSP позволяет устанавливать закрытые ключи и сертификаты открытого ключа следующими способами:

- Путем добавления контейнера, содержащего закрытый ключ и сертификат. При этом контейнер может находиться в папке на диске (см. «Установка контейнера ключей из папки» на стр. 66) или на внешнем устройстве (см. «Установка контейнера ключей с внешнего устройства» на стр. 69).
- Путем установки сертификата и сопоставления ему закрытого ключа из контейнера ключей в папке на диске или внешнем устройстве (см. «Установка сертификата в системное хранилище Windows» на стр. 72).

Сертификат может находиться отдельно от закрытого ключа в тех случаях, когда сертификат создается по запросу пользователя. Сертификат и закрытый ключ находятся в одном контейнере, когда их выдача выполняется администратором удостоверяющего центра.

Формат файла контейнера ключей зависит от разработчика конкретного криптопровайдера.

Внимание! Программа ViPNet CSP не может работать с контейнерами ключей, созданными с помощью другого криптопровайдера.

Контейнеры ключей ViPNet CSP могут храниться на компьютере в одной из двух папок:

- Папка хранения ключей текущего пользователя — папка, к содержимому которой имеют доступ только текущий пользователь и администратор операционной системы. Эта папка находится по адресу:

  `C:\Users\<Имя пользователя>\AppData\Local\Infotecs\Containers`.

- Папка хранения ключей компьютера — папка, к содержимому которой имеет доступ только администратор операционной системы. Эта папка находится по адресу:

  `C:\ProgramData\Infotecs\Containers`.

Примечание. С целью обеспечения соответствия рекомендациям Технического комитета по стандартизации (ТК 26) «Криптографическая защита информации» (http://www.tc26.ru/) изменен формат контейнеров ключей, созданных по алгоритму ГОСТ 34.10-2012.

Контейнеры ключей, созданные в программе ViPNet CSP 4.1 с помощью ГОСТ 34.10-2012, более не поддерживаются.

Файлы сертификатов всегда создаются только в определенных стандартных форматах:

- Файл формата X.509, содержащий только сертификат (файлы с расширениями `.cer`, `.crt`).
- Файл формата PKCS#7. Этот формат предназначен для хранения зашифрованных и подписанных сообщений вместе с соответствующими сертификатами. Файл также может использоваться для передачи наборов сертификатов и списков CRL (файлы с расширениями `.spc`, `.p7b`, `.p7s`).
- Файл формата PKCS#12. Этот формат предназначен для передачи зашифрованных на пароле закрытых ключей и сертификатов (файлы с расширениями `.pfx`, `.p12`). Файлы формата PKCS#12 формируются в соответствии с рекомендациями Технического комитета по стандартизации (ТК 26) «Криптографическая защита информации».

Примечание. Файлы формата PKCS#12, не соответствующие рекомендациям ТК 26 (например, файлы, созданные в ПО компании «Криптоком»), не поддерживаются.

В программе ViPNet CSP может использоваться неограниченное количество сертификатов и контейнеров ключей. В этом случае при подписании документа необходимо выбрать, каким именно ключом он будет подписан.

Шифрование и подписание документов

Для выполнения функций шифрования и проверки электронной подписи криптопровайдер ViPNet CSP использует открытый ключ, находящийся в сертификате (см. глоссарий, стр. 231) того пользователя, которому адресован зашифрованный документ или от которого поступил документ с электронной подписью.

Для расшифрования и формирования электронной подписи криптопровайдер применяет закрытый ключ пользователя, который расшифровывает или подписывает документ (тот ключ, который будет указан самим пользователем).

На рисунке ниже представлена схема защищенного обмена документами на примере передачи конфиденциального сообщения электронной почты.

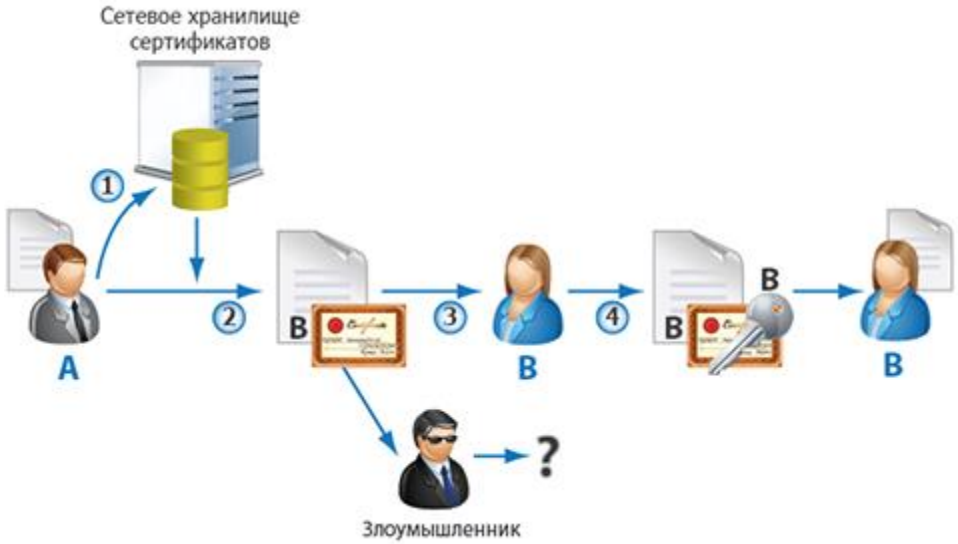


Рисунок 4. Схема обмена защищенными документами

Пользователю **A** необходимо передать пользователю **B** конфиденциальное сообщение электронной почты. Для этого пользователи выполняют следующие действия:

1. Пользователь **A** запрашивает из сетевого хранилища сертификат открытого ключа пользователя **B** и сопоставляет его с контактом **B** в своей почтовой программе.
2. Пользователь **A** зашифровывает документ с использованием открытого ключа из сертификата пользователя **B**.
3. Пользователь **A** отправляет пользователю **B** зашифрованное сообщение.
4. Пользователь **B** расшифровывает документ с помощью своего закрытого ключа.

Таким образом, пользователь **B** получает конфиденциальное сообщение от пользователя **A**.

Если сообщение перехватит злоумышленник, прочитать письмо ему не удастся, поскольку у него нет закрытого ключа пользователя **B**.

Если пользователь **B** не сможет расшифровать сообщение, пришедшее от пользователя **A**, это значит, что это сообщение было изменено сторонними лицами или повреждено в процессе пересылки. В этом случае пользователь **B** может запросить у пользователя **A** повторную отправку сообщения.

Процесс формирования и проверки электронной подписи представлен ниже.

Рисунок 5. Процесс формирования и проверки электронной подписи документа

Пользователю **A** необходимо заверить документ (например, сообщение электронной почты) электронной подписью, для того чтобы остальные пользователи не смогли внести в него изменения и каждый мог удостовериться, что автор данного документа — пользователь **A**. Для этого пользователи выполняют следующие действия:

1. Пользователь **A** подписывает документ своим закрытым ключом.
2. Пользователь **A** отправляет документ всем заинтересованным лицам (пользователи **B**, **C** и **D**) или выкладывает для общего доступа.
3. Пользователь **B** запрашивает сертификат открытого ключа пользователя **A** в сетевом хранилище, где хранятся сертификаты, изданные удостоверяющим центром.
4. Пользователь **B** проверяет электронную подпись документа с помощью открытого ключа пользователя **A**, который находится в сертификате пользователя **A**.

Если проверка прошла успешно, это означает, что автор документа — действительно пользователь **A** и документ не подвергался изменениям с момента подписания.

Если проверка показала несоответствие электронной подписи и открытого ключа в сертификате отправителя, это означает, что документ либо не принадлежит пользователю **A,** либо редактировался сторонними лицами, либо был поврежден в процессе пересылки. В этом случае пользователь **B** может запросить у пользователя **A** документ повторно.

Аутентичность и конфиденциальность соединений TLS

Протокол TLS используется для организации удаленного защищенного соединения, например доступа к ресурсам удаленного сервера. Протокол позволяет провести одностороннюю или взаимную аутентификацию взаимодействующих сторон, а также обеспечить конфиденциальную передачу информации. Необходимость защищенного доступа может возникнуть при реализации общего доступа к базам данных или хранилищам, при создании систем электронных платежей и в других случаях.

Взаимодействие двух узлов при защищенном соединении представлено на схеме ниже.

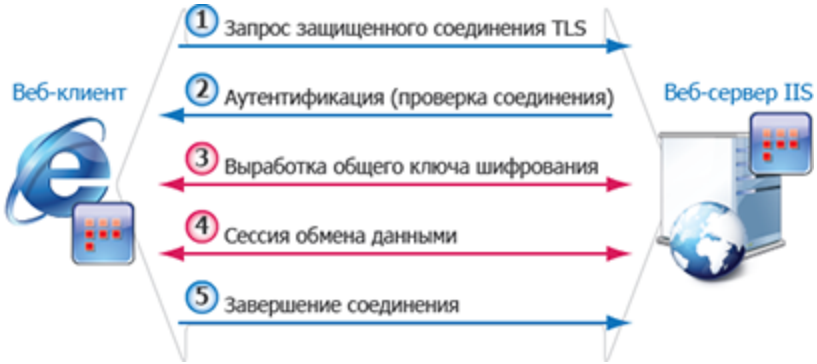


Рисунок 6. Схема взаимодействия узлов при TLS-соединении

Таким образом, использование протокола TLS, реализуемого средствами криптопровайдера ViPNet CSP, позволяет гарантировать надежное и санкционированное соединение с удаленными серверами и строго ограниченный доступ к защищенным данным.

Практическое применение ViPNet CSP

Внимание! Если вы установили программу ViPNet CSP в составе другого ПО ViPNet и хотите использовать криптопровайдер в сторонних приложениях, сначала запустите установочный файл ViPNet CSP и добавьте компонент **Поддержка работы ViPNet CSP через Microsoft CryptoAPI** (см. «Добавление, удаление и восстановление компонентов программы» на стр. 34). Убедитесь, что в разделе **Дополнительно** установлен флажок **Поддержка работы ViPNet CSP через Microsoft CryptoAPI**.

С помощью программы ViPNet CSP вы можете выполнять следующие операции:

- Подписывать сообщения Microsoft Outlook (см. «Электронная подпись и шифрование в Microsoft Outlook» на стр. 124).
- Зашифровывать сообщения Microsoft Outlook и вложенные файлы (см. «Шифрование сообщений электронной почты» на стр. 137).
- Формировать и проверять электронную подпись в приложениях Microsoft Office (см. «Электронная подпись в документах Microsoft Office» на стр. 113).
- Подписывать формы Microsoft Office InfoPath (см. «Электронная подпись в Microsoft Office InfoPath» на стр. 142).
- Подписывать макросы в программах Microsoft Word, Excel, Outlook, PowerPoint, Access, Publisher и Visio (см. «Электронная подпись макросов, форм и баз данных» на стр. 141).
- Устанавливать защищенные веб-соединения TLS, используя сервер IIS и браузер Microsoft Internet Explorer (см. «Организация защищенного соединения TLS» на стр. 149).
- Подписывать документы и выполнять авторизацию на Едином портале государственных и муниципальных услуг с помощью универсальной электронной карты (см. «Работа с универсальной электронной картой» на стр. 159).
- Выполнять криптографические функции в системах электронного документооборота Docsvision http://www.docsvision.com/ и ViPNet ЭДО http://www.iitrust.ru/products/.
- Выполнять криптографические операции, необходимые для работы службы сертификатов Active Directory (см. «Развертывание центра сертификации Microsoft CA» на стр. 111).

2

Установка и запуск программы

Установка программы

В случае если программа ViPNet CSP входит в состав ПО ViPNet, она устанавливается автоматически в процессе развертывания этого ПО.

В случае если необходимо установить программу ViPNet CSP отдельно, следуйте инструкциям, приведенным в этой главе.

Внимание! При установке ViPNet CSP на компьютер с операционной системой Windows, локализация которой отличается от русской, для правильного отображения кириллицы в интерфейсе программы измените региональные настройки Windows (см. «Региональные настройки» на стр. 220).

Для установки программы ViPNet CSP вы должны обладать правами администратора операционной системы.

Чтобы установить программу ViPNet CSP, выполните следующие действия:

1. Запустите установочный файл  .
2. На странице **Лицензионное соглашение** мастера установки ViPNet CSP ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку **Продолжить**.
3. Чтобы после завершения установки компьютер перезагрузился автоматически, на странице **Способ установки** установите флажок **Автоматически перезагрузить компьютер после завершения**.
4. Если вы хотите настроить параметры установки, на странице **Способ установки** нажмите кнопку **Настроить** и укажите следующее:
   - компоненты программы, которые хотите установить;
   - путь к папке установки программы на компьютере;
   - имя пользователя и название организации;
   - название папки программы в меню **Пуск**.

   Вы можете выбрать или отключить следующие компоненты для установки:
   - **Панель управления ViPNet CSP** — если отключить этот компонент, будут установлены лишь библиотеки криптопровайдера без исполняемого файла ViPNet CSP. Такой способ установки может быть использован разработчиками.
   - **Поддержка работы ViPNet CSP через Microsoft CryptoAPI** — добавляет функции, позволяющие использовать криптопровайдер ViPNet CSP в сторонних приложениях, например в приложениях Microsoft Office. Компонент включен по умолчанию при отдельной установке ViPNet CSP и отключен при установке ViPNet CSP в составе другого ПО ViPNet.

Примечание. Если вы установили программу ViPNet CSP в составе другого ПО ViPNet и хотите использовать криптопровайдер в сторонних приложениях, например в приложениях Microsoft Office, запустите установочный файл ViPNet CSP и добавьте необходимый компонент (см. «Добавление, удаление и восстановление компонентов программы» на стр. 34).

- **Поддержка протокола TLS/SSL** —добавляет функции, позволяющие организовать защищенное соединение по протоколу TLS (см. «Организация защищенного соединения TLS» на стр. 149). При установке ViPNet CSP на компьютер, работающий под управлением ОС Windows 10, компонент по умолчанию отключен.
- **Поддержка подключения к ViPNet HSM** — добавляет функции, позволяющие организовать подключение к серверу ViPNet HSM и работать с ключами, хранящимися на этом сервере (см. «Взаимодействие с сервером ViPNet HSM» на стр. 155).

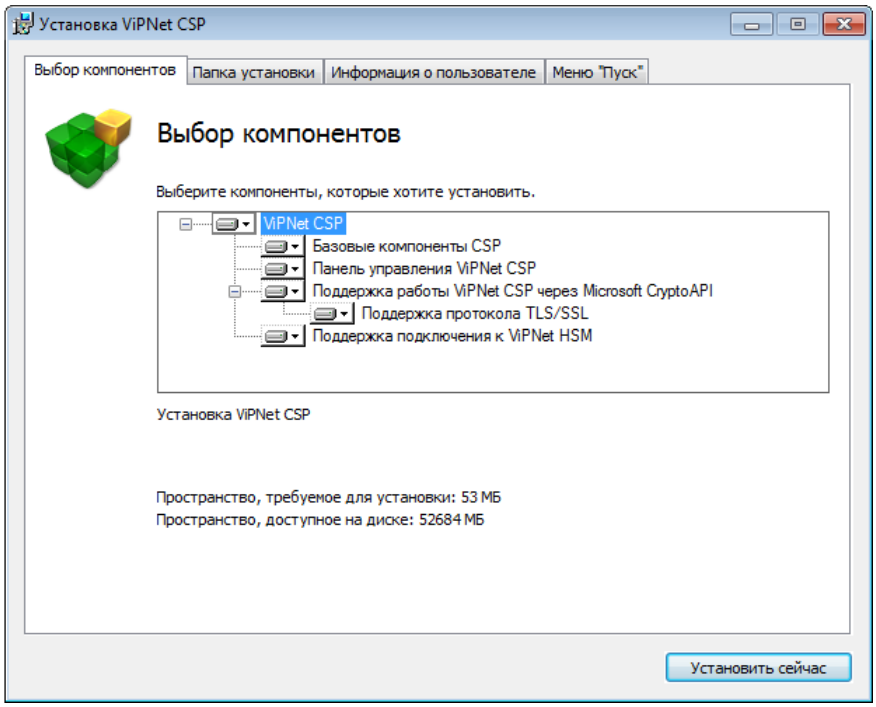


Рисунок 7. Настройка параметров установки ViPNet CSP

5 Чтобы начать установку, нажмите кнопку **Установить сейчас**.

6 Если ранее на странице **Способ установки** вы установили флажок **Автоматически перезагрузить компьютер после завершения**, по окончании установки компьютер перезагрузится автоматически. В противном случае по окончании установки программа предложит перезагрузить компьютер. В окне сообщения о перезагрузке нажмите кнопку **Да**.

В результате выбранные компоненты будут установлены. В процессе установки также будет создана точка восстановления системных файлов и параметров.

Примечание. Использование точек восстановления не поддерживается на серверных операционных системах Windows.

Если в настройках вашей операционной системы отключена функция создания точек восстановления, программа установки ViPNet CSP автоматически включит эту функцию.

В процессе установки ViPNet CSP обращается к системным функциям Windows, чтобы создать точку восстановления системных файлов и параметров. При этом, в зависимости от настроек восстановления системы, Windows может отменить создание точки восстановления (например, если такая точка в этот день уже создавалась).

Если на компьютере необходимо создать замкнутую программную среду для соответствия требованиям ФСБ России к средствам криптографической защиты информации класса КС3, дополнительно установите программу ViPNet SysLocker Подробнее о работе с ViPNet SysLocker см. документ «ViPNet SysLocker. Руководство администратора».

Обновление программы

Внимание! При обновлении с любой несертифицированной версии ViPNet CSP на текущую во избежание неработоспособности TLS-соединений мы рекомендуем удалить старую версию программы, а затем установить новую.

При необходимости вы можете обновить программу ViPNet CSP, для этого выполните следующие действия:

1 Запустите установочный файл  более новой версии программы ViPNet CSP. Дождитесь завершения подготовки к установке.

2 В окне **Обновление** нажмите кнопку **Начать обновление**.

Чтобы после завершения обновления компьютер перезагрузился автоматически, установите флажок **Автоматически перезагрузить компьютер после завершения**.

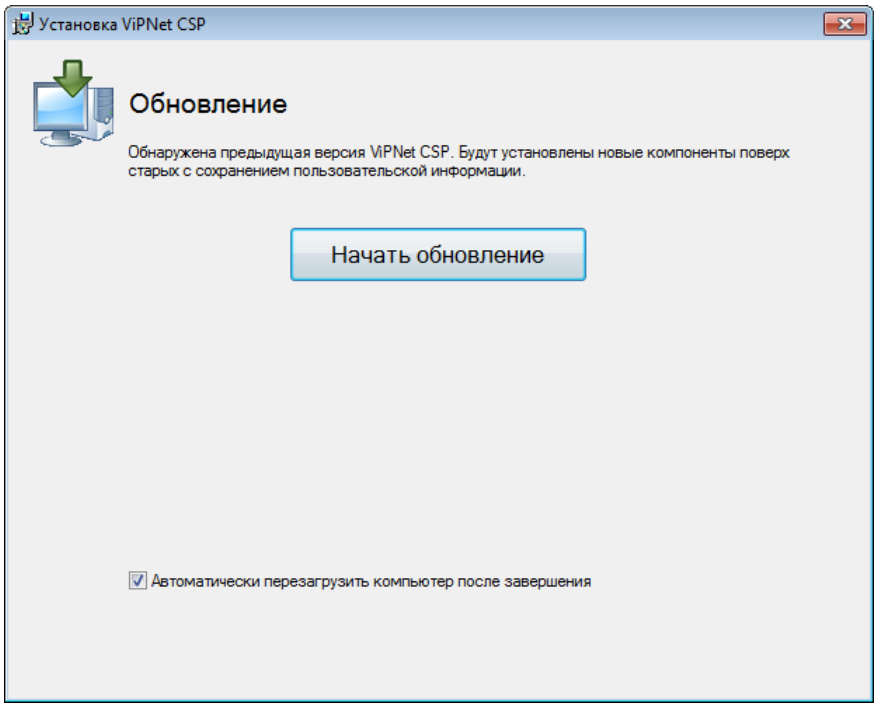


Рисунок 8. Обновление программы ViPNet CSP

3 Если появится окно с предупреждением о том, что права доступа к папке хранения ключей компьютера заданы неверно, нажмите кнопку **Да**.

4 Дождитесь завершения обновления программы.

5 Если ранее на странице **Обновление** вы установили флажок **Автоматически перезагрузить компьютер после завершения**, по окончании установки компьютер перезагрузится автоматически. В противном случае по окончании установки программа предложит перезагрузить компьютер. В окне сообщения о перезагрузке нажмите кнопку **Да**.

В результате программа будет обновлена. В процессе обновления также будет создана точка восстановления системных файлов и параметров.

Примечание. Использование точек восстановления не поддерживается на серверных операционных системах Windows.

Если в настройках вашей операционной системы отключена функция создания точек восстановления, программа установки ViPNet CSP автоматически включит эту функцию.

В процессе обновления ViPNet CSP обращается к системным функциям Windows, чтобы создать точку восстановления системных файлов и параметров. При этом, в зависимости от настроек восстановления системы, Windows может отменить создание точки восстановления (например, если такая точка в этот день уже создавалась).

Добавление, удаление и восстановление компонентов программы

При необходимости вы можете установить или удалить компоненты программы ViPNet CSP, а также восстановить программу при обнаружении повреждений. Для установки, удаления компонентов или для восстановления программы ViPNet CSP выполните следующие действия:

1. Запустите установочный файл  . Дождитесь завершения подготовки к установке компонентов ViPNet CSP.
2. В окне **Изменение установленных компонентов** выберите нужный пункт:
   - для установки или удаления компонентов выберите **Добавить или удалить компоненты**;
   - для восстановления установленных компонентов программы выберите **Восстановить**;
   - для удаления всех компонентов программы выберите **Удалить все компоненты**.

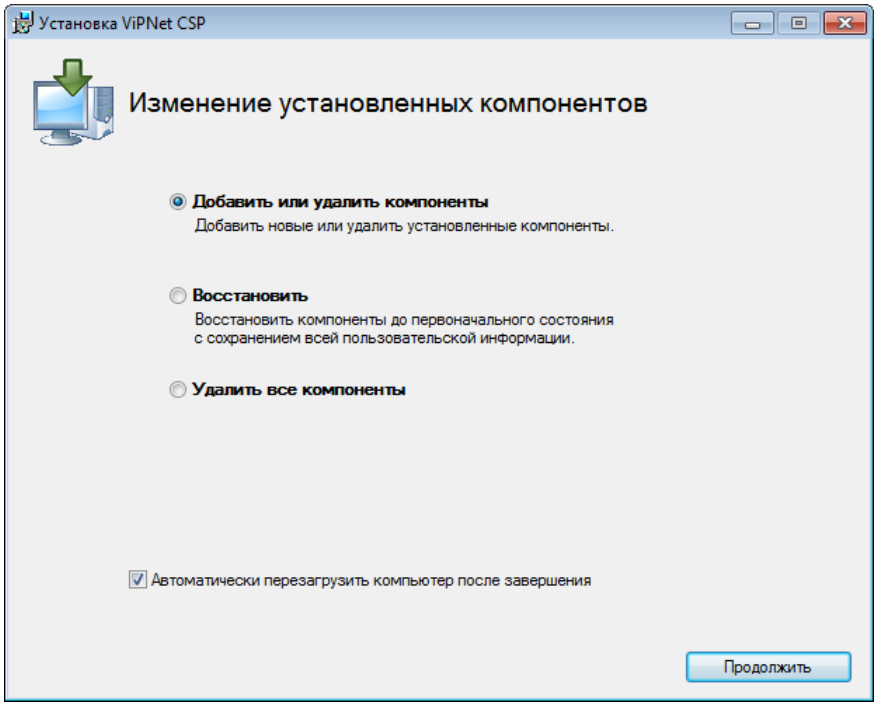


Рисунок 9. Изменение установленных компонентов

Чтобы после завершения установки компьютер перезагрузился автоматически, установите флажок **Автоматически перезагрузить компьютер после завершения**. Затем нажмите кнопку **Продолжить**.

3 Если вы устанавливаете или удаляете компоненты программы, на странице выбора компонентов укажите те, которые необходимо добавить или удалить. Затем нажмите кнопку **Продолжить**.

4 Дождитесь завершения установки (восстановления, удаления) компонентов программы.

5 Если ранее на странице **Изменение установленных компонентов** вы установили флажок **Автоматически перезагрузить компьютер после завершения**, по окончании установки компьютер перезагрузится автоматически. В противном случае по окончании установки программа предложит перезагрузить компьютер. В окне сообщения о перезагрузке нажмите кнопку **Да**.

Примечание. При добавлении или удалении компонентов, а также при восстановлении программы точка восстановления Windows не создается.

Совместимость с программным обеспечением КриптоПро CSP

Внимание! Сертификаты, сформированные в удостоверяющем центре КриптоПро по запросу из программы ViPNet CSP, могут использоваться криптопровайдером ViPNet CSP.

Сертификаты, сформированные с помощью программы ViPNet Удостоверяющий и ключевой центр по запросу из программного обеспечения КриптоПро CSP, могут использоваться криптопровайдером КриптоПро CSP.

Контейнеры ключей, сформированные с помощью криптопровайдера ViPNet CSP, невозможно использовать в ПО КриптоПро CSP.

Программа ViPNet CSP может быть установлена на одном компьютере с программным обеспечением КриптоПро CSP. Однако при этом необходимо соблюдать следующие условия:

- Если для выполнения криптографических операций в поддерживаемых приложениях (см. «Практическое применение ViPNet CSP» на стр. 27) требуется использовать криптопровайдер ViPNet CSP:
  - В программе ViPNet CSP в разделе **Дополнительно** должен быть установлен флажок **Поддержка работы ViPNet CSP через Microsoft CryptoAPI**.
  - Компонент ПО КриптоПро CSP «Совместимость с продуктами Microsoft» не должен быть установлен.

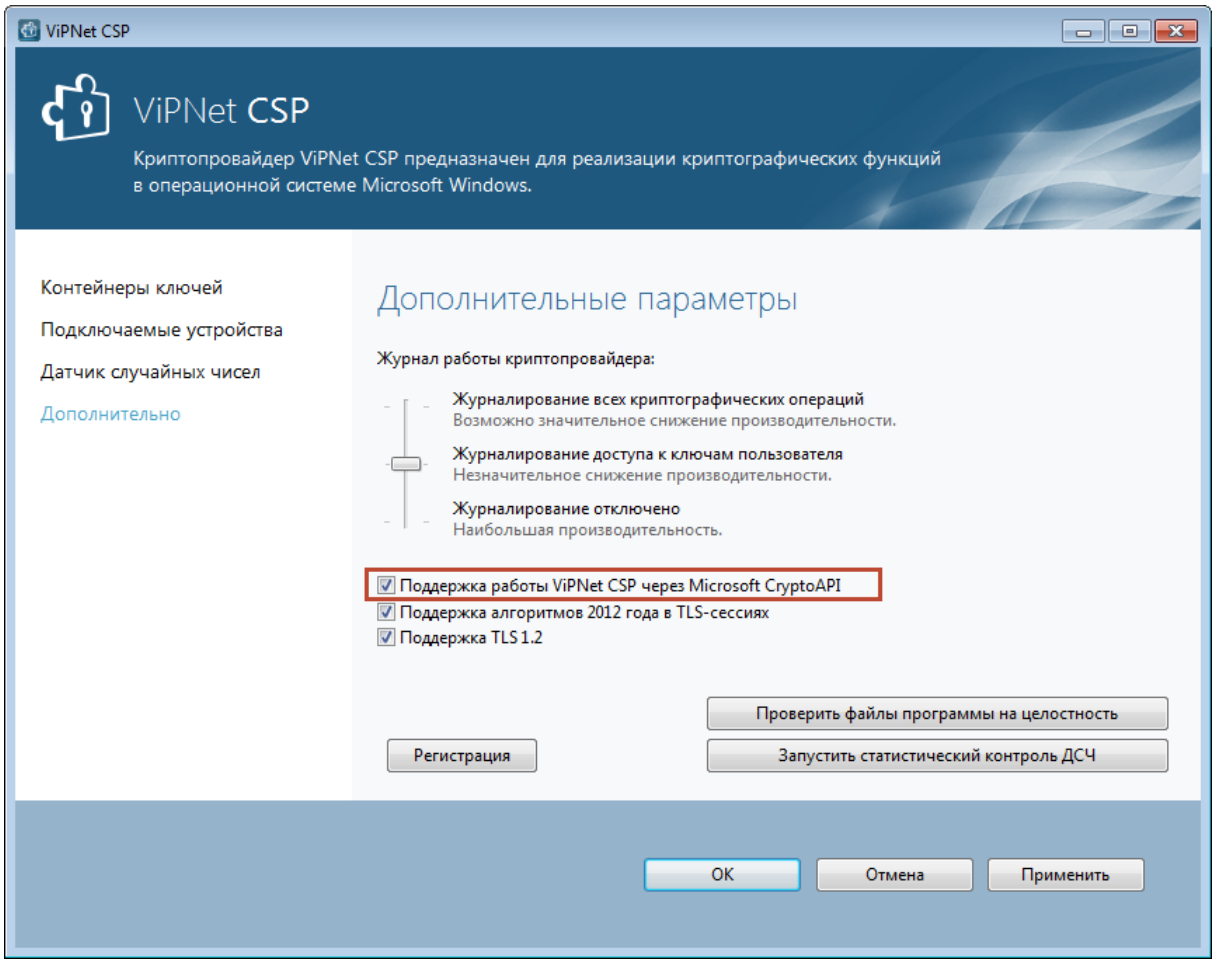


Рисунок 10. Использование ViPNet CSP при одновременной работе с криптопровайдером КриптоПро CSP

- Если для выполнения криптографических операций в поддерживаемых приложениях требуется использовать криптопровайдер КриптоПро CSP:
  - В программе ViPNet CSP в разделе **Дополнительно** должен быть снят флажок **Поддержка работы ViPNet CSP через Microsoft CryptoAPI**.
  - Компонент ПО КриптоПро CSP «Совместимость с продуктами Microsoft» должен быть установлен.
  - Для заверения электронной подписью документов Microsoft Office необходимо дополнительно установить программу КриптоПро Office Signature.

Внимание! Не следует одновременно устанавливать на компьютер компонент ПО КриптоПро CSP «Совместимость с продуктами Microsoft» и в программе ViPNet CSP устанавливать флажок **Поддержка работы ViPNet CSP через Microsoft CryptoAPI**.

По умолчанию после установки ViPNet CSP на компьютер с уже установленным ПО КриптоПро CSP флажок **Поддержка работы ViPNet CSP через Microsoft CryptoAPI** снят. В этом случае непосредственно после установки криптографические операции продолжают выполняться с помощью криптопровайдера КриптоПро CSP.

Если вы хотите, чтобы при установке ViPNet CSP на компьютер с уже установленным ПО КриптоПро CSP криптографические операции сразу начинали выполняться с помощью криптопровайдера ViPNet CSP, запустите установочный файл ViPNet CSP с дополнительным параметром `INJECT_HOOK_OFF=Yes`. В этом случае после установки флажок **Поддержка работы ViPNet CSP через Microsoft CryptoAPI** будет автоматически установлен.

Пример команды установки:

```
C:\ViPNet_CSP_RUS.exe INJECT_HOOK_OFF=Yes
```

Внимание! Если на вашем компьютере установлены программа ViPNet CSP и ПО КриптоПро CSP и вы хотите удалить программу ViPNet CSP, то во избежание потери работоспособности ОС выполните следующие действия:

1. Удалите ViPNet CSP и не перезагружайте компьютер.
2. Запустите установочный файл КриптоПро CSP и восстановите компоненты ПО.
3. Перезагрузите компьютер.

Установка с использованием командной строки

Программа ViPNet CSP может быть установлена из командной строки Windows с указанием ряда стандартных параметров установщика Windows.

Таблица 3. Параметры режима установки

Параметр	Описание
`/qn`	Установка без демонстрации интерфейса (Silent mode).
`/qb`	Установка с минимальным интерфейсом (на экране присутствует только стандартный индикатор прогресса и информационные сообщения).
`/qf`	Установка с полным интерфейсом (по умолчанию).

Таблица 4. Параметры перезагрузки

Параметр	Описание
`/norestart`	Отключение перезагрузки после завершения установки.
`/promptrestart`	Вывод диалогового окна с запросом на перезагрузку.
`/forcerestart`	Перезагрузка компьютера после установки и принудительное закрытие других приложений без сохранения открытых файлов. Данный параметр действует только в сочетании с параметром `/qn`.

Примечание. При установке ViPNet CSP с использованием командной строки точка восстановления Windows не создается.

Пример команды установки:

```
setup.exe /qn /norestart
```

Запуск программы

Для запуска программы ViPNet CSP выполните одно из действий:

- Если вы используете операционную систему Windows 7 или Windows Server 2008 R2, в меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet CSP** > **ViPNet CSP**.
- Если вы используете операционную систему Windows 8, Windows Server 2012 или более поздней версии, на начальном экране откройте список приложений и выберите **ViPNet** > **ViPNet CSP**.

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

Если вы установили ViPNet CSP в составе другого ПО ViPNet, отдельной регистрации программы не требуется. Если вы установили ViPNet CSP отдельно, при первом запуске откроется окно **ViPNet CSP** с предложением зарегистрировать программу (см. «Регистрация ViPNet CSP» на стр. 41). Вы можете перейти к регистрации программы либо начать работу с демо-версией программы (см. «Зачем нужно регистрировать ViPNet CSP» на стр. 42).

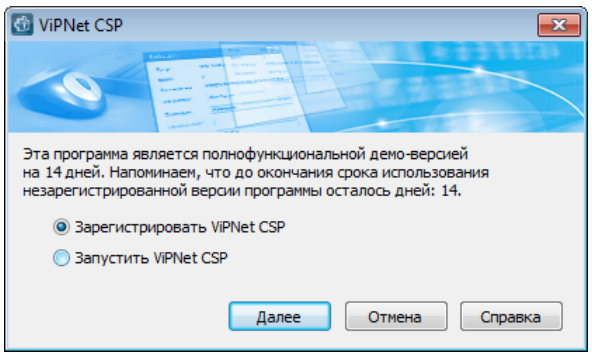


Рисунок 11. Запуск незарегистрированной версии программы

Внимание! При обновлении программы ViPNet CSP может потребоваться повторная регистрация.

После запуска программы откроется главное окно ViPNet CSP. Начните работу с программой с установки контейнера ключей и сертификата (см. глоссарий, стр. 64).

3

Регистрация ViPNet CSP

Прежде чем регистрировать ViPNet CSP

Зачем нужно регистрировать ViPNet CSP

После установки ViPNet CSP на компьютер программа работает в демо-режиме, то есть срок ее использования ограничен двумя неделями. Зарегистрировать программу ViPNet CSP вы можете в любой момент, и тогда программа будет доступна для использования неограниченное время.

Мы рекомендуем поступить следующим образом:

- установите ViPNet CSP и пользуйтесь незарегистрированной версией программы, чтобы оценить возможности и преимущества продукта;
- по истечении срока действия демо-версии зарегистрируйте вашу копию ViPNet CSP.

Примечание. Также существует возможность зарегистрировать программу в автоматическом режиме во время установки (см. «Автоматическая регистрация в процессе установки программы» на стр. 54).

Начало регистрации

Примечание. Если программа ViPNet CSP 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. 52).

Если вы провели обновление конфигурации компьютера, на котором будете использовать ViPNet CSP, ознакомьтесь с разделом Если конфигурация вашего компьютера изменилась (на стр. 53).

Чтобы зарегистрировать ViPNet CSP, используя серийный номер, полученный во время загрузки программы с веб-сайта ОАО «ИнфоТеКС», следуйте приведенным ниже указаниям.

1 Запустите незарегистрированную программу. Появится окно **ViPNet CSP**.

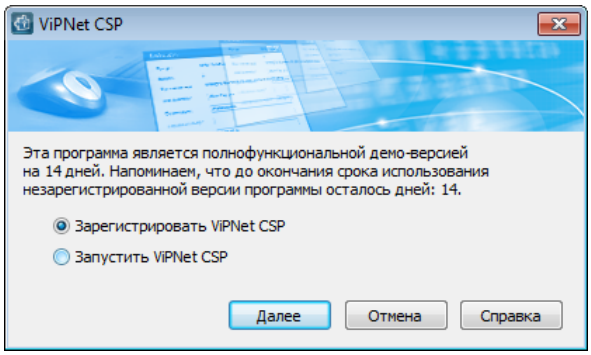


Рисунок 12. Вызов мастера регистрации

2 Выберите пункт **Зарегистрировать ViPNet CSP** и нажмите кнопку **Далее**. Будет запущен мастер **Регистрация ViPNet CSP**.

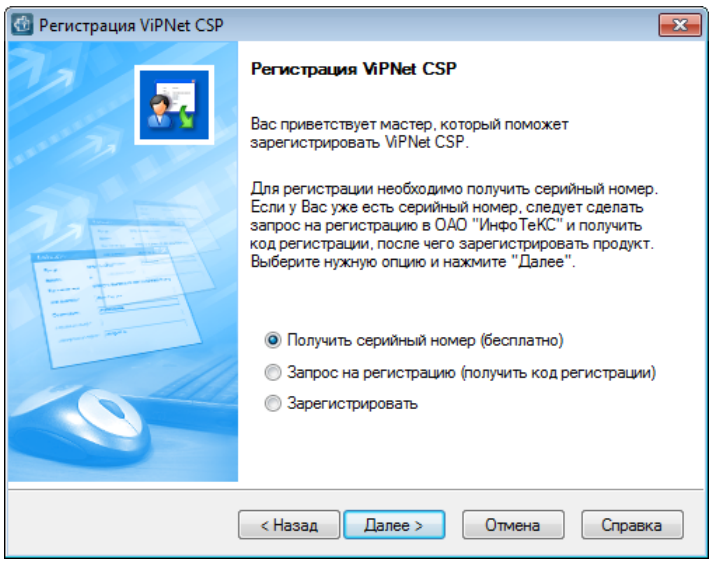


Рисунок 13. Первая страница регистрации

3 Выполните одно из следующих действий:

- Если перед этим вы получили серийный номер, выберите пункт **Запрос на регистрацию (получить код регистрации)** (см. «Получение кода регистрации» на стр. 44).

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

- Если перед этим вы получили серийный номер и код регистрации, выберите пункт **Зарегистрировать** (см. «Регистрация ViPNet CSP» на стр. 51).

Получение кода регистрации

Чтобы запросить код регистрации для ViPNet CSP, выполните следующие действия:

1 На странице **Регистрация ViPNet CSP** 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. 44).
- **По электронной почте** (см. «Получение кода регистрации по электронной почте» на стр. 47).
- **По телефону** (см. «Получение кода регистрации по телефону» на стр. 48).
- **Через файл** (см. «Регистрация через файл» на стр. 49).

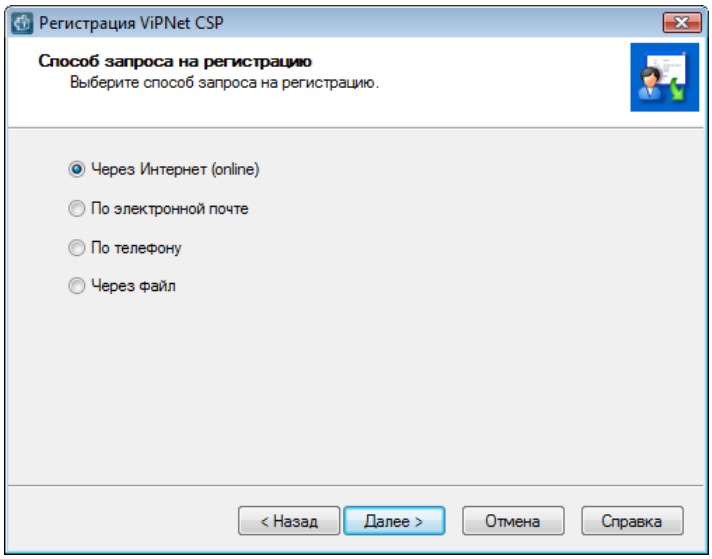


Рисунок 14. Выбор типа запроса на регистрацию

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**.

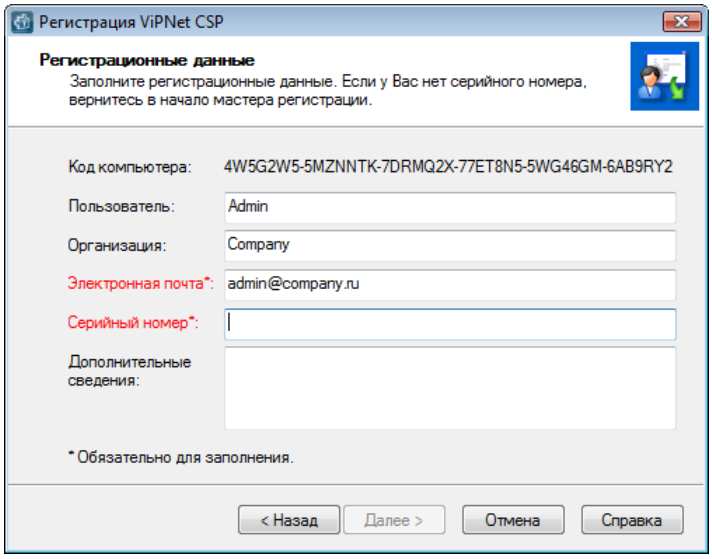


Рисунок 15. Ввод регистрационных данных

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

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

Примечание. Серийный номер выдается при загрузке ViPNet CSP с веб-страницы ОАО «ИнфоТеКС».

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 CSP.

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 CSP.

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.

6 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.

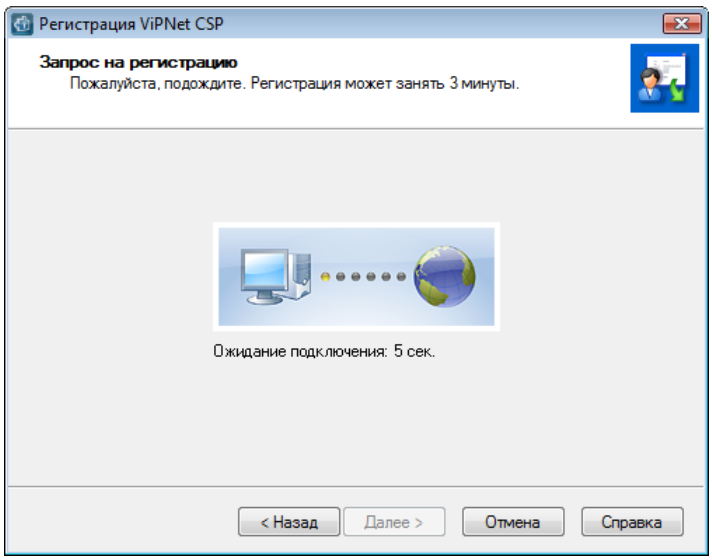


Рисунок 16. Запрос на регистрацию через Интернет

Если в течение 3 минут соединение с сервером системы регистрации ОАО «ИнфоТеКС» не было установлено, вы увидите соответствующее сообщение. Для устранения неполадки см. раздел Не удается получить код регистрации через Интернет (на стр. 165).

Если соединение с сервером установлено, попытка регистрации может оказаться неудачной в случае возникновения следующих ошибок:

- Предоставленные вами данные оказались неверными. В этом случае программа выдаст сообщение с предложением проверить введенную информацию.

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

- Введенный серийный номер уже зарегистрирован. В этом случае программа выдаст сообщение с предложением бесплатно получить другой серийный номер.

  Перейдите по ссылке, содержащейся в сообщении, и сделайте запрос на получение серийного номера.

Если регистрация прошла успешно, откроется страница **Регистрация ViPNet CSP успешно завершена**. На этой странице приведена рекомендация, как безопасно сохранить ваши регистрационные данные (см. «Сохранение регистрационных данных» на стр. 52).

7 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. 44).

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.

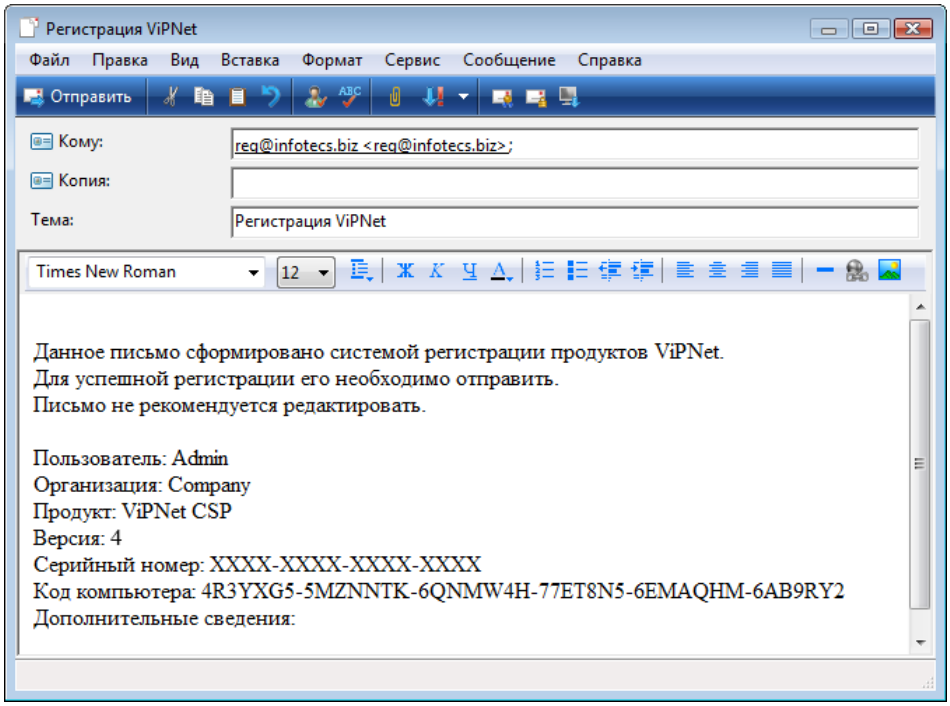


Рисунок 17. Запрос на регистрацию по электронной почте

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», попытайтесь снова отправить свое сообщение. Для этого повторите все шаги, описанные в данном разделе. Если после этого вам все же не удалось зарегистрировать ViPNet CSP, обратитесь в службу поддержки ОАО «ИнфоТеКС».

4 Получив сообщение с кодом регистрации, зарегистрируйте вашу копию ViPNet CSP (см. «Регистрация ViPNet CSP» на стр. 51).

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».

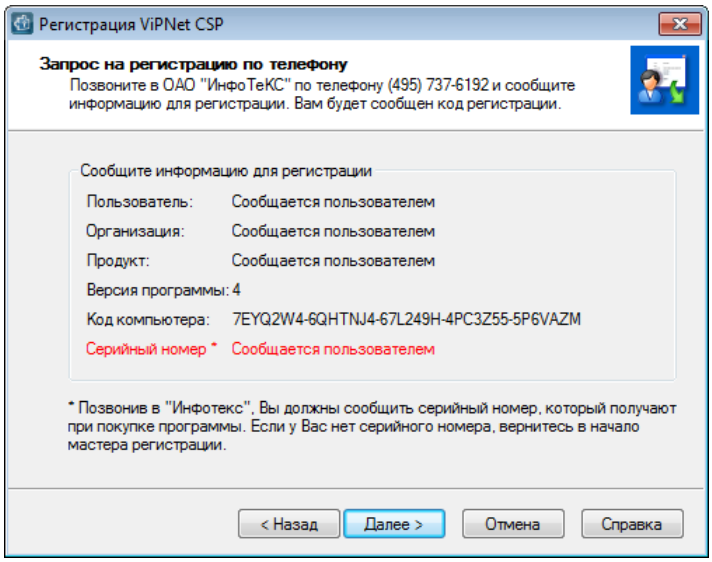


Рисунок 18. Запрос на регистрацию по телефону

Выполните следующие действия:

1 Позвоните в ОАО «ИнфоТеКС» по телефону, приведенному в верхней части страницы, и сообщите регистрационную информацию. В ответ вам будет сообщен код регистрации.

2 Получив код регистрации, нажмите кнопку **Далее**, откроется страница **Зарегистрировать**.

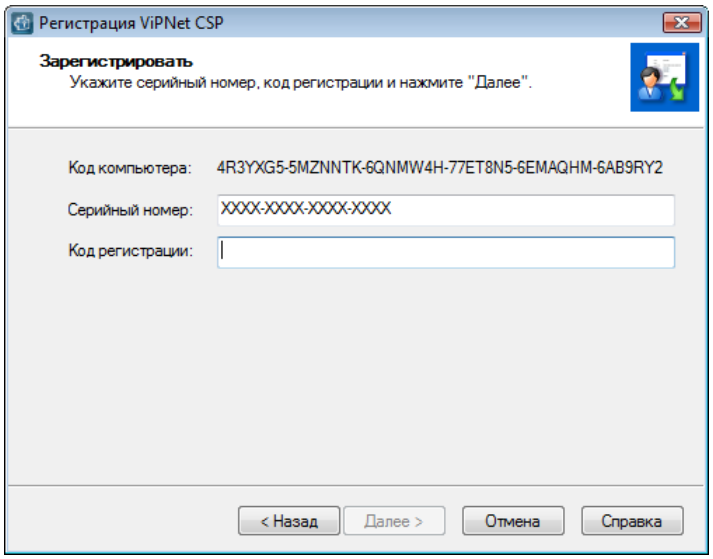


Рисунок 19. Ввод регистрационного кода

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

Если введенные данные верны, откроется страница **Регистрация ViPNet CSP успешно завершена**. На этой странице приведены рекомендации, как безопасно сохранить ваши регистрационные данные (см. «Сохранение регистрационных данных» на стр. 52).

4 Нажмите кнопку **Готово**.

Регистрация через файл

Для того чтобы зарегистрировать ViPNet CSP через файл, выполните следующие действия:

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. 44). Нажмите кнопку **Далее**.

3 На странице **Сохранение регистрационных данных** нажмите кнопку **Обзор** и укажите папку, в которой будет сохранен файл с вашими регистрационными данными.

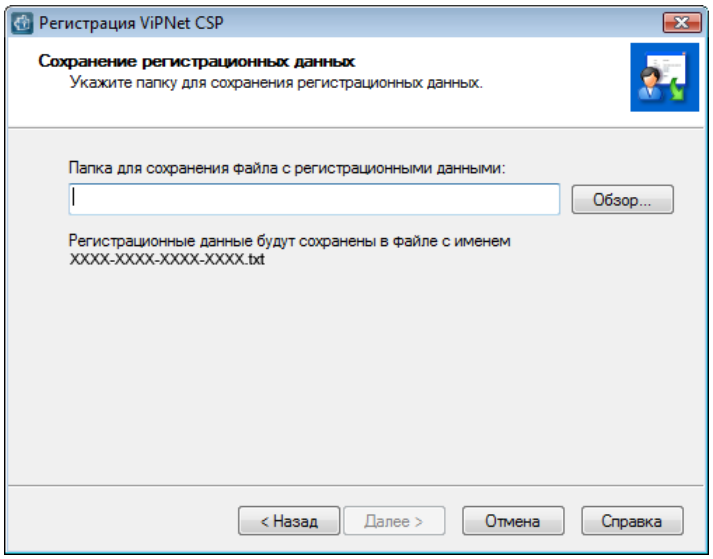


Рисунок 20. Сохранение регистрационных данных

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

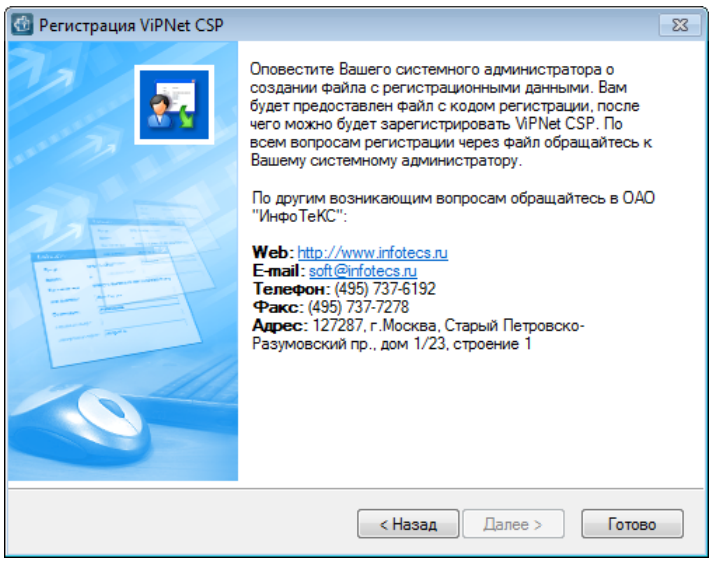


Рисунок 21. Данные для регистрации через файл сохранены

5 На следующей странице мастера нажмите кнопку **Готово**.

6 Отправьте файл, содержащий регистрационные данные, на адрес электронной почты reg@infotecs.biz. В теме сообщения укажите: ViPNet Registration Using File.

7 После обработки запроса ОАО «ИнфоТеКС» вы получите сообщение, в котором содержится код регистрации.

8 Получив код регистрации, зарегистрируйте свою копию ViPNet CSP (см. «Регистрация ViPNet CSP» на стр. 51).

Регистрация ViPNet CSP

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

1 Запустите мастер **Регистрация ViPNet CSP** (см. «Начало регистрации» на стр. 42).

2 На первой странице мастера выберите **Зарегистрировать** и нажмите кнопку **Далее**.

3 На странице **Серийный номер** введите ваш серийный номер и нажмите кнопку **Далее**.

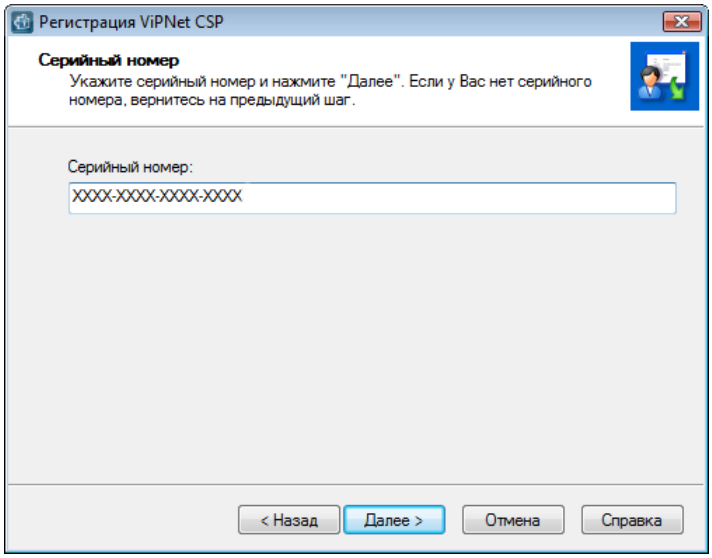


Рисунок 22. Ввод серийного номера

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

4 На странице **Код регистрации** выполните одно из следующих действий:

- Если вы запрашивали код регистрации через Интернет, по электронной почте или по телефону, выберите **Обычная регистрация** и введите код регистрации.
- Если вы запрашивали код регистрации через файл, выберите **Регистрация через файл**, затем нажмите кнопку **Обзор** и укажите путь к файлу, содержащему код регистрации.

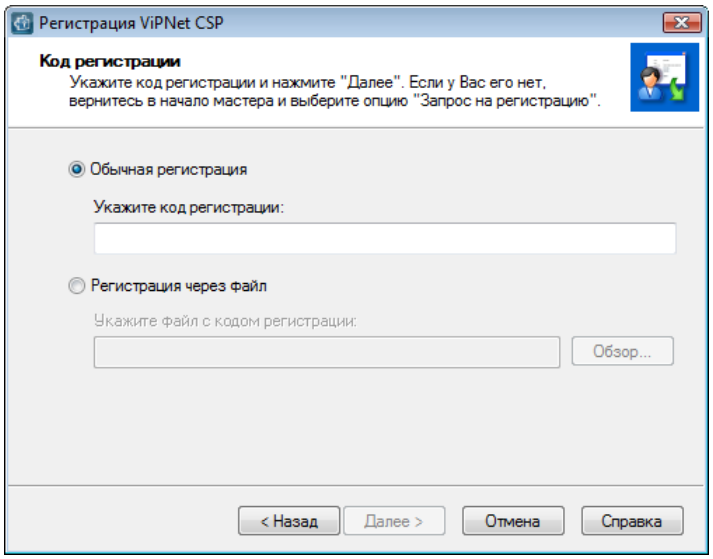


Рисунок 23. Ввод кода регистрации

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

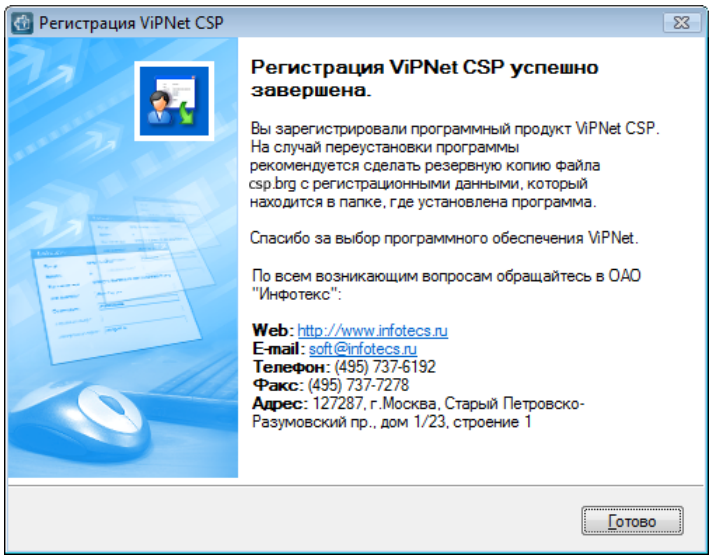


Рисунок 24. Завершение регистрации

6 Нажмите кнопку **Готово**.

7 Сохраните регистрационные данные (см. «Сохранение регистрационных данных» на стр. 52), скопировав в надежное место файл `*.brg`, находящийся в папке установки программы ViPNet CSP.

Сохранение регистрационных данных

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

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 CSP (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 CSP 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 CSP, может сказаться на ее работе. Если изменение конфигурации было значительным (вы заменили большую часть комплектующих), необходимо перерегистрировать вашу копию ViPNet CSP (см. «Получение кода регистрации» на стр. 44). Если изменения в конфигурации были небольшими, вам не нужно снова регистрировать ViPNet CSP.

При первом запуске ViPNet CSP 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 CSP, вам нужно будет скопировать этот файл в папку установки ViPNet CSP, и программа будет зарегистрирована.

Автоматическая регистрация в процессе установки программы

Если вы хотите автоматически зарегистрировать программу в процессе установки, перед началом установки подготовьте файл регистрации `cspreg.txt` с серийным номером, полученным при загрузке программы, и переместите его в папку с установочным файлом  . Файл `cspreg.txt` должен иметь вид:

```
Serial Number: XXXX-XXXX-XXXX-XXXX
E-mail: email@company.com
User name: <ФИО пользователя>
Company: <Название компании>
```

Примечание. Поля `User name` и `Company` не являются обязательными.

4

Получение сертификата и закрытого ключа

Порядок получения и ввода в действие закрытого ключа и сертификата

Чтобы иметь возможность подписывать электронные документы, необходим закрытый ключ пользователя, а для проверки подлинности подписи — сертификат открытого ключа.

Примечание. Порядок получения и ввода в действие сертификата и закрытого ключа определяется регламентом работы вашего удостоверяющего центра. Прежде чем формировать запрос на создание сертификата, уточните у администратора удостоверяющего центра, принимаются ли запросы, сформированные с помощью программы «Создание запроса на сертификат».

Для того чтобы получить и ввести в действие новый сертификат или обновить уже имеющийся, выполните следующие действия:

1. Сформируйте файл запроса на сертификат в программе «Создание запроса на сертификат» (см. «Создание запроса на сертификат и формирование закрытого ключа» на стр. 57).
2. Создайте закрытый ключ и сохраните контейнер с ним на диске или внешнем устройстве.
3. Передайте файл с запросом администратору удостоверяющего центра (по электронной почте или другим, принятым в вашей организации способом) и дождитесь получения сертификата.
4. Установите полученный сертификат в контейнер ключей (см. «Установка сертификата в контейнер ключей» на стр. 70).
5. Установите в системное хранилище полученный сертификат (см. «Установка сертификата в системное хранилище Windows» на стр. 72), а также сертификаты издателей и списки CRL (см. «Установка сертификата издателя и списка аннулированных сертификатов» на стр. 78).

Создание запроса на сертификат и формирование закрытого ключа

Для создания запроса на новый сертификат или для обновления уже существующего выполните следующие действия:

1. Запустите программу «Создание запроса на сертификат», для этого выполните одно из действий:
   - Если вы используете операционную систему Windows 7 или Windows Server 2008 R2, в меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet CSP** > **Создание запроса на сертификат**.
   - Если вы используете операционную систему Windows 8, Windows Server 2012 или более поздней версии, на начальном экране откройте список приложений и выберите **ViPNet** > **Создание запроса на сертификат**.
2. В окне **Служба сертификации** выберите одно из действий:
   - **Запросить новый сертификат** — для создания запроса на новый сертификат.
   - **Запросить обновление действующего сертификата** — для обновления уже имеющегося.

     При создании запроса на обновление сертификата выполните следующие действия:
     - В окне **Обновление сертификата** выберите сертификат, который требуется обновить, и нажмите кнопку **ОК**.
     - Если требуется выбрать другой сертификат или просмотреть выбранный сертификат, воспользуйтесь кнопками **Выбрать сертификат** и **Свойства сертификата**.
     - Если необходимо, укажите новые параметры сертификата и данные о владельце или оставьте реквизиты предыдущего сертификата.

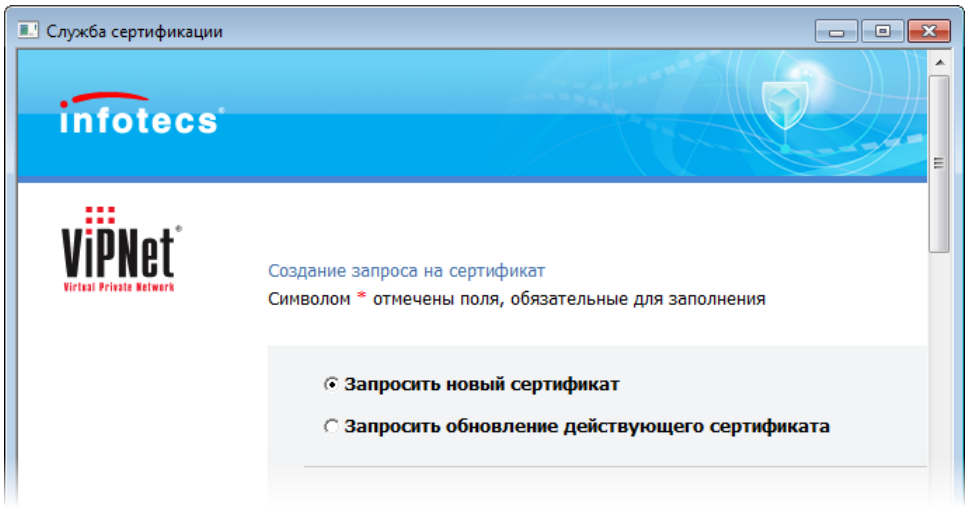


Рисунок 25. Выбор типа запроса на сертификат

3 В разделе **Параметры сертификата** укажите следующие параметры:

- В списке **Криптопровайдер** выберите криптопровайдер, с помощью которого вы хотите создать закрытый и открытый ключи. При этом ниже отобразится используемый алгоритм хэширования.
- В списке **Назначение** выберите действия, которые необходимо выполнять с помощью сертификата:
  - **Подпись и шифрование** (по умолчанию), если необходимо сформировать ключ и сертификат для шифрования сообщений и их защиты с помощью электронной подписи.
  - **Подпись**, если необходимо сформировать ключ и сертификат только для подписания сообщений и документов электронной подписью.
  - **Шифрование**, если необходимо сформировать ключ и сертификат только для шифрования сообщений электронной почты и документов.
- В списке **Шаблон сертификата** выберите один из вариантов:
  - **Веб-сервер** — чтобы создать запрос на сертификат для установки на веб-сервере IIS.
  - **Квалифицированный ViPNet CSP** (по умолчанию) — чтобы создать запрос на квалифицированный сертификат (см. глоссарий, стр. 230), в котором можно указать атрибуты ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя), СНИЛС (страховой номер индивидуального лицевого счета), ИНН (идентификационный номер налогоплательщика), ОГРН (основной государственный регистрационный номер).
  - **Отчетность** — чтобы создать запрос на сертификат, с помощью которого можно подписывать документы, формируемые для сдачи бухгалтерской отчетности.
  - **Стандартный** — для всех остальных случаев.

  Также вы можете использовать шаблоны сертификатов, созданные в программе ViPNet Registration Point. Для этого получите у администратора центра регистрации файлы с расширением `*.p10tmp` и сохраните их в папку `C:\ProgramData\InfoTeCS\Certificate Templates`. После этого в списке **Шаблоны сертификата** появятся имена новых шаблонов.
- Чтобы иметь возможность экспортировать вместе с полученным сертификатом также закрытый ключ в файл формата PKCS#12 (см. «Экспорт сертификата и закрытого ключа в файл» на стр. 88), установите флажок **Экспортируемый.**
- Чтобы контейнер ключей, необходимый для формирования запроса на сертификат, был создан в папке хранения ключей компьютера, установите флажок **Системный**, в противном случае контейнер ключей будет создан в папке хранения ключей текущего пользователя (см. «Контейнер ключей» на стр. 22).

4 В разделе **Данные о владельце сертификата** укажите необходимую информацию о лице, для которого формируется запрос на сертификат.

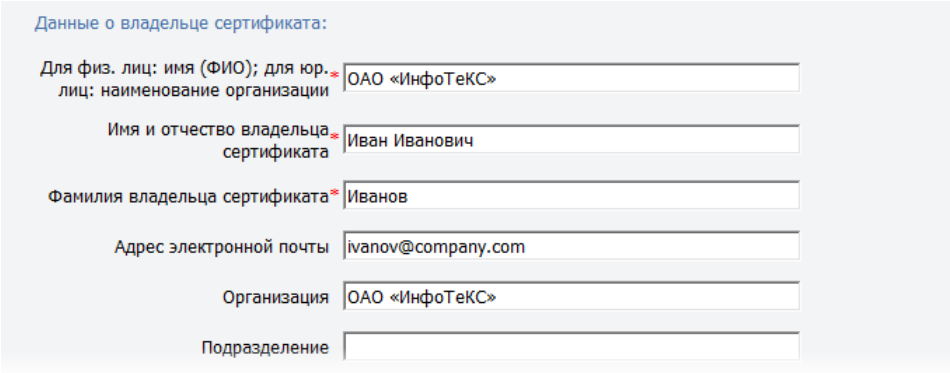


Рисунок 26. Указание данных о владельце сертификата

Внимание! Если сертификат планируется использовать для подписания сообщений электронной почты программы Microsoft Outlook, обязательно укажите адрес электронной почты. Сертификат, не содержащий адреса электронный почты, не может быть использован для подписания сообщений электронной почты.

---

5 В разделе **Сохранение запроса в файл** нажмите кнопку **Обзор** и укажите место на диске или съемном носителе, а также имя файла для сохранения файла запроса.

Примечание. Формат названия файла запроса определяется регламентом работы вашего удостоверяющего центра. Чтобы ваш запрос было легко идентифицировать, рекомендуется включить в название файла запроса ваши имя и фамилию.

---

6 Нажмите кнопку **Сформировать запрос**. Эта кнопка появляется после того, как будут заполнены все обязательные поля.

Внимание! Если после заполнения обязательных полей кнопка **Сформировать запрос** не появилась, убедитесь, что в разделе **Дополнительно** установлен флажок **Поддержка работы ViPNet CSP через Microsoft CryptoAPI** (см. Рисунок 10 на стр. 37). Если указанный флажок не активен, добавьте соответствующий компонент программы (см. «Добавление, удаление и восстановление компонентов программы» на стр. 34).

Далее выполните следующие шаги, необходимые для создания контейнера ключей.

7 В появившемся окне **ViPNet CSP - инициализация контейнера ключей** укажите:

- Имя контейнера ключей или оставьте значение по умолчанию в соответствующем поле.
- Место размещения контейнера ключей, установив переключатель в одно из значений: **Папка на диске** или **Выберите устройство**.

  В зависимости от места размещения контейнера ключей в запрос будет добавлено расширение со следующей информацией:

- При размещении контейнера ключей в папке на диске — с информацией о том, что желаемый срок действия закрытого ключа — 1 год.
- При размещении контейнера ключей на устройстве с аппаратной поддержкой алгоритмов ГОСТ (см. «Алгоритмы и функции, поддерживаемые внешними устройствами» на стр. 218) — с информацией о том, что желаемый срок действия закрытого ключа — 3 года.

Нажмите кнопку **OK**.

Примечание. В ряде случаев появление окна **ViPNet - инициализация контейнера ключей** может происходить с запозданием. Дождитесь появления этого окна.

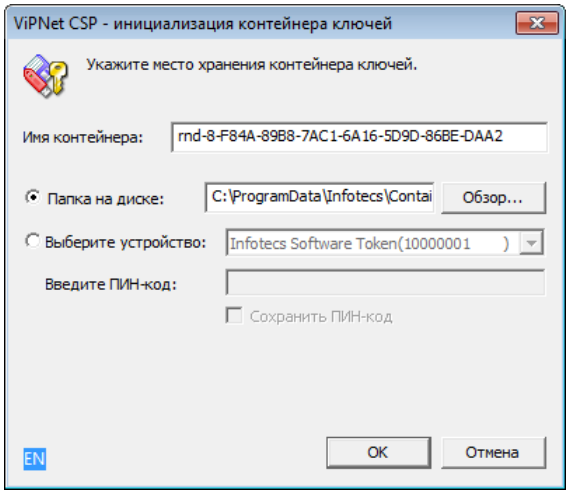


Рисунок 27. Создание контейнера ключей

8 В окне **ViPNet CSP - пароль контейнера ключей** задайте пароль доступа к контейнеру ключей и нажмите кнопку **OK**.

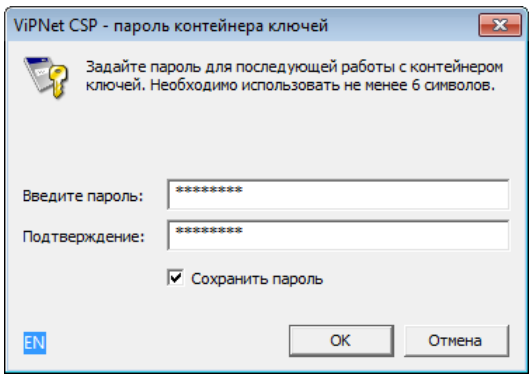


Рисунок 28. Задание пароля доступа к контейнеру ключей

9 Появится электронная рулетка (см. глоссарий, стр. 232), если она еще не запускалась в рамках текущего сеанса работы программы. Поводите указателем в пределах окна **Электронная рулетка**.

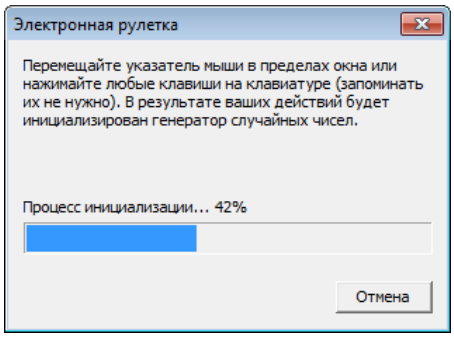


Рисунок 29. Электронная рулетка

Примечание. Если в программе ViPNet CSP был выбран датчик случайных чисел, отличный от биологического (см. «Использование датчика случайных чисел» на стр. 100), электронная рулетка не появится.

Если для сохранения контейнера выбрано устройство с аппаратной поддержкой алгоритмов ГОСТ, электронная рулетка также не появится, так как в этом случае формирование закрытого ключа происходит средствами этого устройства.

10 В окне сообщения об успешном создании файла запроса на сертификат нажмите кнопку **OK**.

11 После создания файла запроса окно **Служба сертификации** можно закрыть.

После создания запроса на сертификат передайте файл запроса администратору вашего удостоверяющего центра и получите у него изданный сертификат. Затем в программе **ViPNet CSP** установите полученный сертификат (см. «Установка сертификата в системное хранилище Windows» на стр. 72) и укажите для него соответствующий контейнер ключей.

Использование ключей подписи пользователя сетевого узла

Контейнер ключей, установленный на сетевом узле ViPNet с программным обеспечением ViPNet CryptoService, ViPNet Client или ViPNet Coordinator (версии 3.2.2 или выше), можно перенести на другой компьютер для использования в программе ViPNet CSP.

Чтобы использовать в программе ViPNet CSP ключи подписи пользователя сетевого узла ViPNet, выполните следующие действия:

1 В программе ViPNet CryptoService, ViPNet Client или ViPNet Coordinator откройте окно **Настройки параметров безопасности** и перейдите на вкладку **Ключи**.

2 В группе **Электронная подпись** нажмите кнопку **Перенести**.

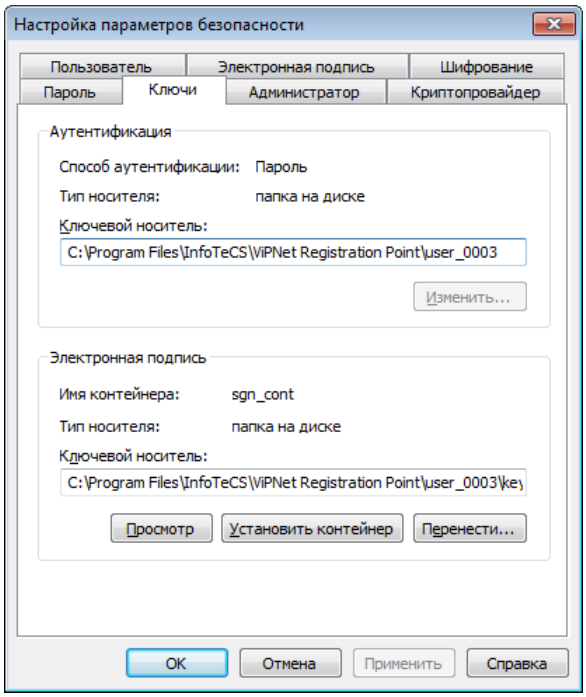


Рисунок 30. Работа с контейнером ключей

3 В окне **ViPNet CSP - инициализация контейнера ключей** нажмите кнопку **Обзор** и укажите папку или съемный носитель, на который требуется перенести контейнер ключей. Затем нажмите кнопку **OK**, контейнер будет перенесен в указанную папку.

4 Скопируйте контейнер ключей на компьютер, на котором установлена программа ViPNet CSP.

Внимание! При удалении контейнера ключей с сетевого узла ViPNet использование ключей подписи на этом сетевом узле будет невозможно.

---

5 В программе ViPNet CSP выполните установку контейнера ключей (см. «Установка контейнера ключей из папки» на стр. 66).

5

Установка контейнеров ключей и сертификатов

Способы установки закрытого ключа и сертификата

Для того чтобы начать работу с механизмами электронной подписи, выполните следующие действия:

1. Установите контейнер ключей:
   - Если закрытый ключ и сертификат находятся в одном контейнере, и этот контейнер размещен в папке на диске, см. раздел Установка контейнера ключей из папки (на стр. 66).
   - Если закрытый ключ и сертификат находятся в одном контейнере и размещены на внешнем устройстве, см. раздел Установка контейнера ключей с внешнего устройства (на стр. 69).
   - Если сертификат был издан в удостоверяющем центре по запросу, и в результате имеется контейнер ключей и отдельный файл сертификата, см. раздел Установка сертификата в контейнер ключей (на стр. 70).
2. Установите сертификат в системное хранилище (см. «Установка сертификата в системное хранилище Windows» на стр. 72).
3. Установите сертификаты издателей и список аннулированных сертификатов (CRL) в системное хранилище (см. «Установка сертификата издателя и списка аннулированных сертификатов» на стр. 78).

Установка контейнера ключей из папки

Для установки в программу контейнера ключей рекомендуется скопировать его в одну из папок хранения контейнеров ключей (см. «Контейнер ключей» на стр. 22). После этого в окне **ViPNet CSP** в разделе **Контейнеры ключей** этот контейнер ключей появится автоматически.

Если вы хотите хранить контейнер ключей в другой папке или на съемном флэш-диске, выполните следующие действия:

1 В окне **ViPNet CSP** в разделе **Контейнеры ключей** нажмите кнопку **Добавить контейнер**.

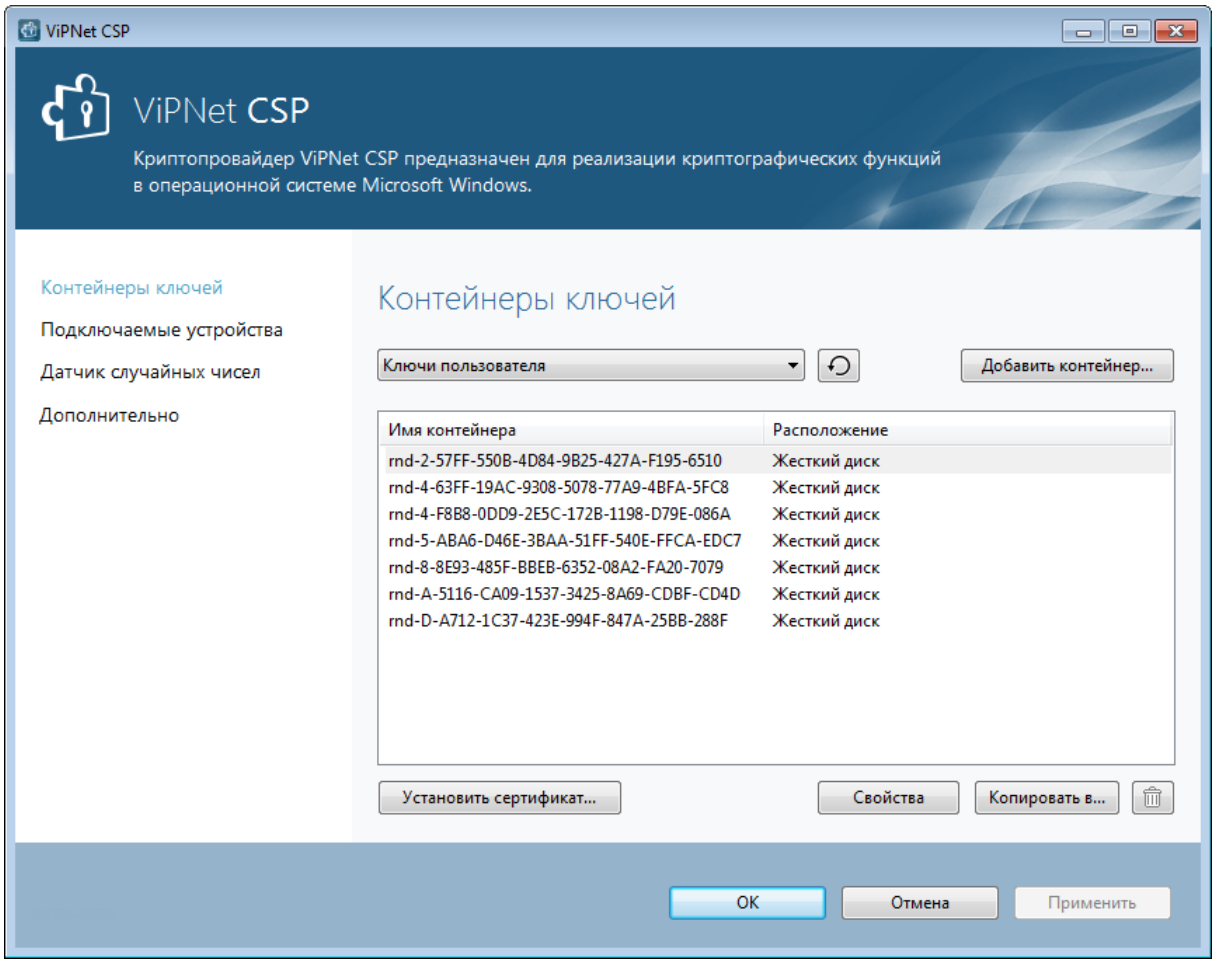


Рисунок 31. Управление контейнерами ключей

2 В окне **ViPNet CSP - инициализация контейнера ключей** нажмите кнопку **Обзор**.

- Если контейнер ключей хранится на жестком диске, в окне **Обзор папок** укажите путь к папке, содержащей контейнер.

Примечание. Полный путь к контейнеру ключей (например, `D:\Folder1\Container1`) не должен превышать 259 символов.

- Если контейнер ключей хранится на съемном флэш-диске, в окне **Обзор папок** укажите этот съемный диск. В поле **Папка на диске** автоматически будет подставлен путь, например `E:\Infotecs\Containers`.

Внимание! На съемном флэш-диске контейнер ключей обязательно должен находиться в папке `Infotecs\Containers`.

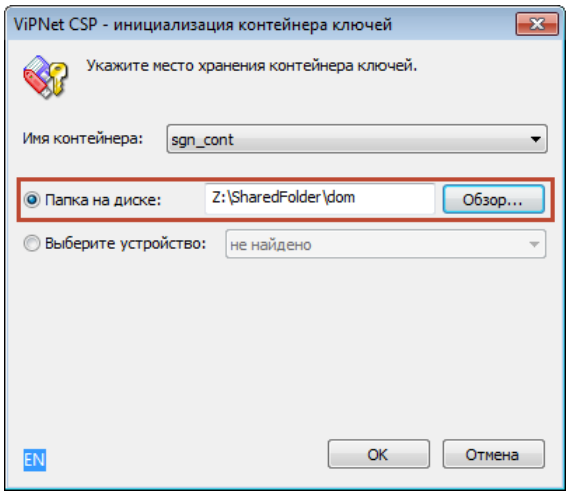


Рисунок 32. Установка контейнера ключей из папки

3 В списке **Имя контейнера** выберите файл контейнера ключей или оставьте значение по умолчанию.

4 Нажмите кнопку **OK**. В окне **Контейнер ключей** появится сообщение об успешном добавлении контейнера ключей и предложение установить сертификат в системное хранилище.

Для работы с сертификатами их необходимо установить в хранилище текущего пользователя.

Внимание! Если программа ViPNet CSP установлена на сервере и используется для организации защищенных соединений TLS, сертификат необходимо устанавливать в хранилище локального компьютера вручную (см. «Установка сертификата из контейнера ключей» на стр. 75).

В окне **Контейнер ключей** выполните одно из следующих действий:

- Чтобы автоматически установить сертификат в системное хранилище, нажмите кнопку **Да**.
- Если сертификаты устанавливать не требуется (или установка будет происходить вручную), нажмите кнопку **Нет**.
- Для просмотра списка сертификатов в контейнере ключей нажмите кнопку **Сертификаты**.

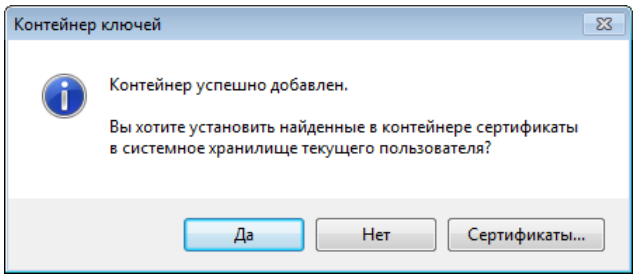


Рисунок 33. Установка сертификатов из контейнера ключей в системное хранилище

5 После установки (или отмены установки) сертификатов в хранилище в списке доступных контейнеров ключей (см. Рисунок 31 на стр. 66) появится добавленный контейнер ключей.

Примечание. Вы можете установить сертификаты из контейнера ключей вручную в окне настройки свойств контейнера (см. «Установка сертификата из контейнера ключей» на стр. 75).

После добавления контейнера ключей установите сертификат издателя и список CRL (см. «Установка сертификата издателя и списка аннулированных сертификатов» на стр. 78) и приступайте к выполнению криптографических операций (см. «Практическое применение ViPNet CSP» на стр. 27).

Установка контейнера ключей с внешнего устройства

Внимание! Для доступа к контейнерам ключей, хранящимся на внешнем устройстве, на компьютере с ViPNet CSP предварительно должно быть установлено необходимое программное обеспечение, а также выполнены другие условия для работы с устройством (см. «Список поддерживаемых внешних устройств» на стр. 214).

При подключении внешнего устройства к компьютеру с ViPNet CSP контейнеры ключей, записанные на это устройство, устанавливаются в программу автоматически. Чтобы просмотреть контейнеры ключей, хранящиеся на подключенном внешнем устройстве, выполните следующие действия:

1 В окне **ViPNet CSP** перейдите в раздел **Контейнеры ключей** (см. Рисунок 31 на стр. 66).

2 В раскрывающемся списке в верхней части окна выберите название подключенного внешнего устройства. В окне отобразятся контейнеры ключей, находящиеся на внешнем устройстве.

Совет. Если внешнее устройство было извлечено, а после вновь вставлено в компьютер, контейнер ключей, находящийся на данном устройстве, может не отобразиться разделе **Контейнеры ключей**. Чтобы отобразить данный контейнер, в разделе **Контейнеры ключей** нажмите кнопку  .

Далее выберите необходимый контейнер ключей из списка и установите сертификат из контейнера в системное хранилище (см. «Установка сертификата из контейнера ключей» на стр. 75).

Установка сертификата в контейнер ключей

При создании запроса на сертификат формируется контейнер, содержащий закрытый ключ. По запросу в удостоверяющем центре издается сертификат, соответствующий этому закрытому ключу.

Чтобы использовать сертификат, полученный из удостоверяющего центра, для формирования электронной подписи и других целей, этот сертификат нужно установить в контейнер с соответствующим закрытым ключом.

Чтобы установить сертификат в контейнер ключей, выполните следующие действия:

1 В окне **ViPNet CSP** в разделе **Контейнеры ключей** (см. Рисунок 31 на стр. 66) выберите контейнер ключей, в который требуется установить сертификат.

Примечание. Папку хранения контейнеров ключей (см. «Контейнер ключей» на стр. 22), отображаемых в списке, вы можете выбрать с помощью раскрывающегося списка в верхней части окна:

- чтобы отобразить в списке контейнеры ключей из папки хранения ключей текущего пользователя, выберите пункт **Ключи пользователя**;
- чтобы отобразить контейнеры ключей из папки хранения ключей компьютера, выберите пункт **Ключи компьютера**;
- чтобы отобразить контейнеры ключей на внешнем устройстве, выберите пункт с именем этого устройства.

Пункт **Ключи компьютера** появляется в списке только при наличии хотя бы одного контейнера ключей в папке хранения ключей компьютера (см. «Контейнер ключей» на стр. 22).

2 Нажмите кнопку **Свойства** либо дважды щелкните нужный контейнер ключей.

3 В окне **Свойства контейнера ключей** нажмите кнопку **Добавить сертификат из файла**.

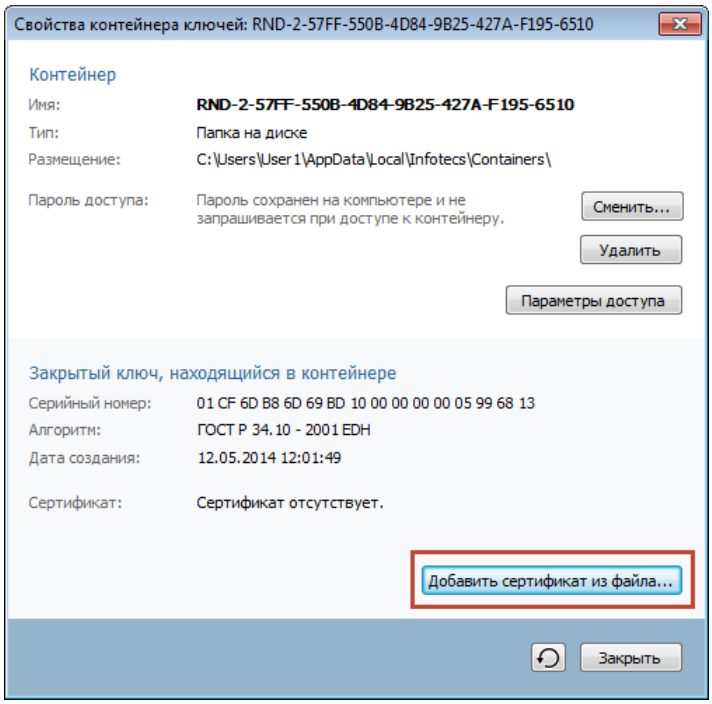


Рисунок 34. Добавление сертификата в контейнер ключей

4 В окне **Открыть** укажите файл сертификата, который соответствует закрытому ключу в контейнере, и нажмите кнопку **Открыть**. Если указан верный сертификат, он будет добавлен в контейнер, в противном случае появится сообщение «Сертификат не соответствует закрытому ключу в контейнере».

Установка сертификата в системное хранилище Windows

Чтобы использовать сертификат в различных приложениях, следует установить его в одно из следующих хранилищ сертификатов операционной системы Windows:

- Хранилище текущего пользователя (Current User), раздел **Личное** > **Сертификаты** — сертификат следует установить в это хранилище в целях шифрования, расшифрования, создания и проверки электронной подписи файлов, а также для доступа к защищенным ресурсам через веб-браузер.
- Хранилище компьютера (Local Machine), раздел **Личное** > **Сертификаты** — сертификат следует установить в это хранилище при использовании ViPNet CSP на веб-сервере для организации доступа к защищенным ресурсам. Также в хранилище компьютера следует устанавливать сертификаты, которые будут использоваться службами данного компьютера.

Вы можете установить сертификат в системное хранилище Windows одним из следующих способов:

- Если сертификат еще не установлен в контейнер ключей, содержащий соответствующий закрытый ключ, в окне **ViPNet CSP** перейдите в раздел **Контейнеры ключей** (см. Рисунок 31 на стр. 66) и нажмите кнопку **Установить сертификат** (см. «Установка сертификата, не добавленного в контейнер ключей» на стр. 72).
- Если сертификат уже установлен в контейнер ключей, установите сертификат в системное хранилище с помощью окна свойств контейнера ключей (см. «Установка сертификата из контейнера ключей» на стр. 75).

Установка сертификата, не добавленного в контейнер ключей

Если сертификат еще не добавлен в контейнер ключей, для установки сертификата в системное хранилище выполните следующие действия:

1. В окне **ViPNet CSP** в разделе **Контейнеры ключей** (см. Рисунок 31 на стр. 66) нажмите кнопку **Установить сертификат**.
2. В окне **Открыть** укажите путь к файлу сертификата на диске (см. «Контейнер ключей» на стр. 22).
3. На странице приветствия мастера установки сертификатов нажмите кнопку **Далее**.
4. На странице **Выбор хранилища сертификатов** укажите, в какое хранилище будет установлен ваш сертификат (см. «Установка сертификата в системное хранилище Windows» на стр. 72).

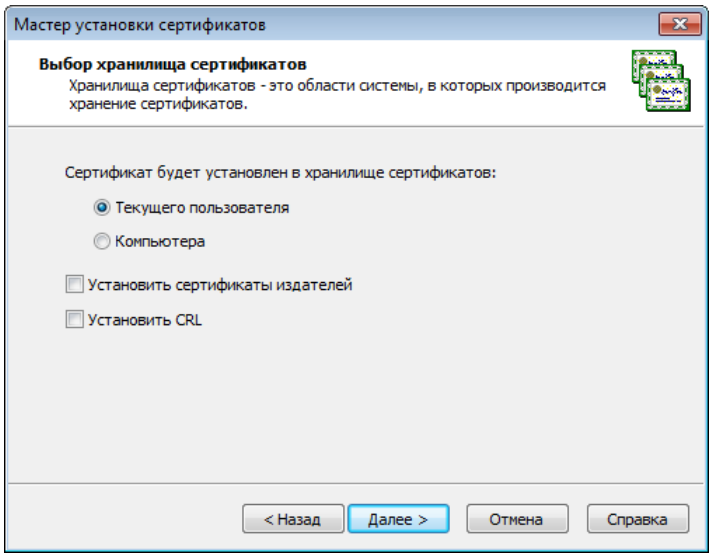


Рисунок 35. Выбор хранилища сертификатов

Если возможность установки сертификата в хранилище компьютера недоступна, войдите в систему с правами администратора.

Примечание. Если вы устанавливаете сертификат из файла с расширением `*.p7b`, `*.p7s`, `*.p12` или `*.pfx`, в котором также содержатся сертификаты издателей или списки CRL, с помощью соответствующих флажков укажите, следует ли устанавливать эти сертификаты издателей или CRL.

Нажмите кнопку **Далее**.

5 На странице **Готовность к установке сертификата** выполните следующие действия:

- Проверьте правильность выбранных параметров. При необходимости вернитесь на предыдущую страницу мастера с помощью кнопки **Назад** и выберите другие параметры.

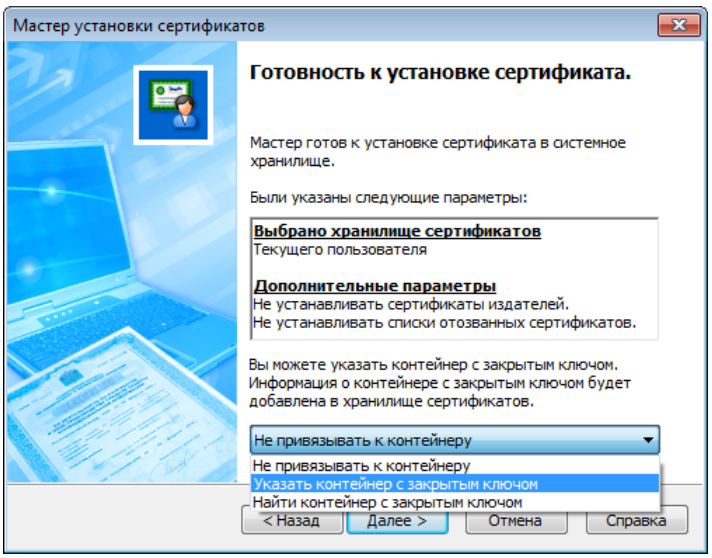


Рисунок 36. Сертификат готов к установке

- В списке в нижней части окна выберите одно из действий:

- Если вы хотите указать расположение контейнера ключей, соответствующего сертификату, позже, выберите действие **Не привязывать к контейнеру**. Работа мастера установки сертификата при этом завершается.
- Если вы хотите указать расположение контейнера ключей, соответствующего сертификату, вручную, выберите действие **Указать контейнер с закрытым ключом**.
- Если вы хотите, чтобы программа автоматически выполнила поиск подходящего контейнера ключей среди контейнеров, установленных в ViPNet CSP, выберите действие **Найти контейнер с закрытым ключом**.

○ Нажмите кнопку **Далее**.

6 Если вы выбрали действие **Указать контейнер с закрытым ключом**, в появившемся окне **ViPNet CSP – инициализация контейнера ключей** укажите расположение контейнера ключей: папку на диске (см. «Установка контейнера ключей из папки» на стр. 66) либо устройство с указанием его параметров и ПИН-кода (см. «Установка контейнера ключей с внешнего устройства» на стр. 69).

Примечание. Для использования какого-либо внешнего устройства необходимо подключить это устройство и установить для него драйверы. Перечень поддерживаемых устройств хранения данных и полезная информация об их использовании содержится в приложении Внешние устройства (на стр. 214).

После этого нажмите кнопку **OK**.

7 Если вы выбрали действие **Найти контейнер с закрытым ключом** и программа нашла подходящий контейнер ключей, в окне **ViPNet CSP – инициализация контейнера ключей** нажмите кнопку **OK**.

8 В окне подтверждения нажмите кнопку **Да**, чтобы добавить сертификат в контейнер ключей, или кнопку **Нет**, чтобы оставить сертификат в виде отдельного файла.

Совет. Сохранение сертификата в одном контейнере с закрытым ключом удобно, если контейнер планируется переносить и устанавливать на другом компьютере.

9 Если на предыдущем шаге вы согласились добавить сертификат в контейнер ключей и нажали кнопку **Да**, в появившемся окне **ViPNet CSP – пароль контейнера ключей** в поле **Пароль** введите пароль доступа к контейнеру ключей, после чего нажмите кнопку **OK**.

Примечание. Окно **ViPNet CSP – пароль контейнера ключей** не отображается в том случае, если ранее был сохранен пароль и установлен флажок **Не показывать больше это окно**.

10 На странице **Завершение работы мастера установки сертификата** нажмите кнопку **Готово**.

Сертификат установлен в выбранное хранилище сертификатов. Если в процессе установки сертификата ему не был сопоставлен закрытый ключ, необходимо установить контейнер с

закрытым ключом, соответствующий сертификату (см. «Установка контейнера ключей из папки» на стр. 66), а затем установить в него этот сертификат (см. «Установка сертификата в контейнер ключей» на стр. 70).

Если в процессе установки сертификату был сопоставлен закрытый ключ, контейнер с которым ранее не был установлен в ViPNet CSP, этот контейнер появится в списке контейнеров (см. Рисунок 31 на стр. 66).

Кроме сертификата пользователя, для работы с защищенными файлами и организации соединений TLS необходимо установить сертификат издателя и список CRL (см. «Установка сертификата издателя и списка аннулированных сертификатов» на стр. 78).

Установка сертификата из контейнера ключей

Внимание! Сертификаты из контейнеров ключей в папке хранения ключей текущего пользователя следует устанавливать в хранилище ключей текущего пользователя.

Сертификаты из контейнеров ключей в папке хранения ключей компьютера следует устанавливать в хранилище ключей компьютера.

Для установки сертификата в системное хранилище из контейнера ключей выполните следующие действия:

1 В окне **ViPNet CSP** в разделе **Контейнеры ключей** (см. Рисунок 31 на стр. 66) выберите контейнер ключей, сертификат из которого требуется установить.

Примечание. Папку хранения контейнеров ключей (см. «Контейнер ключей» на стр. 22), отображаемых в списке, вы можете выбрать с помощью раскрывающегося списка в верхней части окна:

- чтобы отобразить в списке контейнеры ключей из папки хранения ключей текущего пользователя, выберите пункт **Ключи пользователя**;
- чтобы отобразить контейнеры ключей из папки хранения ключей компьютера, выберите пункт **Ключи компьютера**;
- чтобы отобразить контейнеры ключей на внешнем устройстве, выберите пункт с именем этого устройства.

Пункт **Ключи компьютера** появляется в списке только при наличии хотя бы одного контейнера ключей в папке хранения ключей компьютера (см. «Контейнер ключей» на стр. 22).

2 Нажмите кнопку **Свойства** либо дважды щелкните нужный контейнер ключей.

3 Если вы хотите установить сертификат в хранилище ключей текущего пользователя (см. «Установка сертификата в системное хранилище Windows» на стр. 72), выполните следующие действия:

3.1 В окне **Свойства контейнера ключей** нажмите кнопку **Открыть**.

3.2 В окне **Сертификат** на вкладке **Общие** нажмите кнопку **Установить сертификат**. Будет запущен мастер импорта сертификатов.

3.3 На странице приветствия мастера импорта сертификатов нажмите кнопку **Далее**.

3.4 На странице **Хранилище сертификатов** выберите вариант **Поместить все сертификаты в следующее хранилище** и нажмите кнопку **Обзор**.

3.5 В окне **Выбор хранилища сертификатов** выберите хранилище **Личное**.

3.6 На странице **Завершение мастера импорта сертификатов** нажмите кнопку **Готово**.

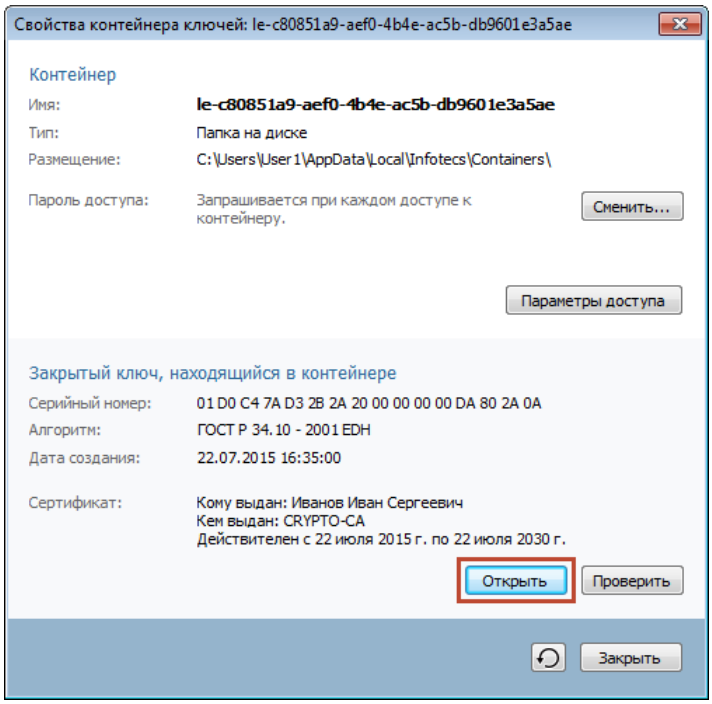


Рисунок 37. Установка сертификата в хранилище ключей текущего пользователя

4 Если вы хотите установить сертификат в хранилище ключей компьютера (см. «Установка сертификата в системное хранилище Windows» на стр. 72), в окне **Свойства контейнера ключей** нажмите кнопку **Установить в личное хранилище**.

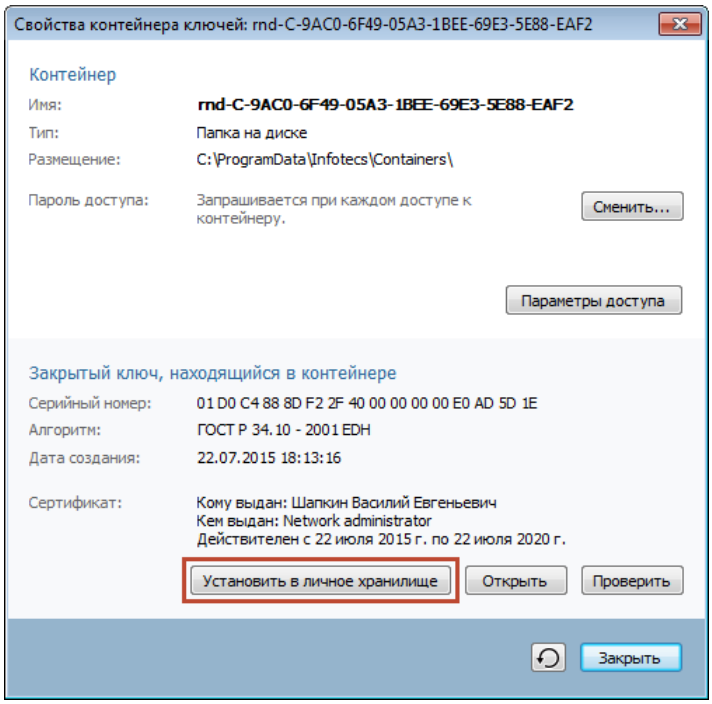


Рисунок 38. Установка сертификата в хранилище ключей компьютера

Примечание. Кнопка **Установить в личное хранилище** отображается только в окне свойств контейнера ключей, находящегося в папке хранения ключей компьютера (см. «Контейнер ключей» на стр. 22).

В результате сертификат будет установлен в выбранное системное хранилище.

Кроме сертификата пользователя для работы с защищенными файлами и организации соединений TLS необходимо установить сертификат издателя и список CRL (см. «Установка сертификата издателя и списка аннулированных сертификатов» на стр. 78).

Установка сертификата издателя и списка аннулированных сертификатов

Для выполнения операций с защищенными файлами и организации соединений TLS требуется установить в системное хранилище:

- Сертификат пользователя (см. «Установка сертификата в системное хранилище Windows» на стр. 72).
- Сертификат издателя или цепочку сертификатов издателей.
- Список аннулированных сертификатов (CRL).

Примечание. Если в вашем сертификате указан URL-адрес точки распространения списков аннулированных сертификатов и если ваш компьютер подключен к Интернету, список CRL устанавливается и обновляется автоматически при просмотре свойств сертификата (см. «Установка и обновление CRL через Интернет» на стр. 80).

Установка сертификата издателя и списка CRL выполняется средствами операционной системы. Такой способ установки сертификата также необходим, если ПО ViPNet установлено на веб-сервере и используется для организации защищенных соединений TLS.

Для установки сертификата издателя и CRL выполните следующие действия:

1 Нажмите сочетание клавиш **Win**+**R**.

В меню **Пуск** также можно выбрать пункт **Выполнить**.

2 В появившемся окне в поле **Открыть** введите команду `mmc` и нажмите кнопку **OK**.

3 В окне консоли управления Microsoft в меню **Файл** выберите пункт **Добавить или удалить оснастку**.

4 В окне **Добавление и удаление оснасток** в списке **Доступные оснастки** выберите оснастку **Сертификаты** и нажмите кнопку **Добавить**.

5 В окне **Оснастка диспетчера сертификатов** выберите один из следующих вариантов:

- Чтобы установить сертификат издателя или список CRL в хранилище компьютера (см. «Установка сертификата в системное хранилище Windows» на стр. 72), выберите вариант **учетной записи компьютера**, нажмите кнопку **Далее**, а затем кнопку **Готово**.
- Чтобы установить сертификат издателя или список CRL в хранилище текущего пользователя (см. «Установка сертификата в системное хранилище Windows» на стр. 72), выберите вариант **моей четной записи пользователя** и нажмите кнопку **Готово**.

Нажмите кнопку **OK**.

6 На панели навигации консоли управления Microsoft щелкните правой кнопкой мыши следующее хранилище:

- **Доверенные корневые центры сертификации**, если вы устанавливаете сертификат издателя, являющийся корневым в цепочке сертификации (см. глоссарий, стр. 230).

Примечание. Если сертификат издателя является единственным в цепочке сертификации (см. глоссарий, стр. 232), он также считается корневым.

- **Промежуточные центры сертификации**, если вы устанавливаете:
  - список CRL;
  - сертификат издателя, который является промежуточным в цепочке сертификации (см. глоссарий, стр. 232).

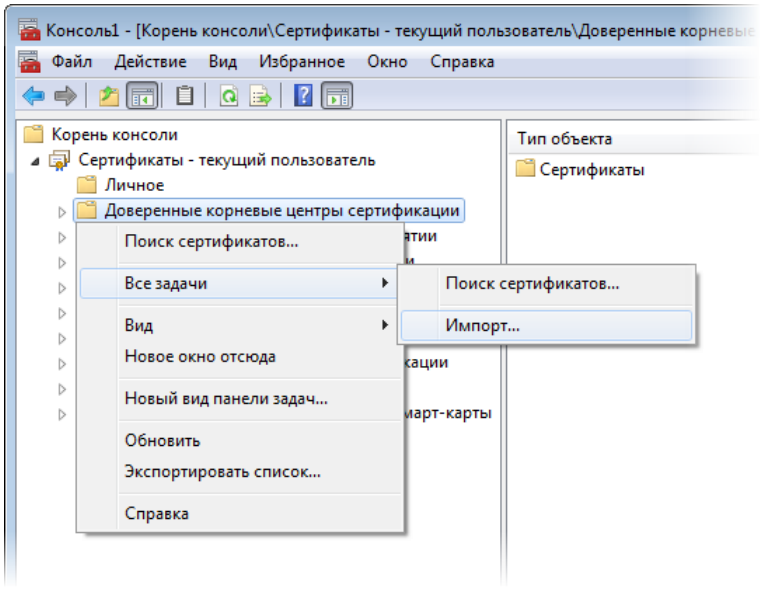


Рисунок 39. Выбор хранилища для сертификата издателя

7 В контекстном меню выберите пункт **Все задачи** > **Импорт**.

8 На первой странице мастера импорта сертификатов нажмите кнопку **Далее**.

9 На странице **Мастер импорта сертификатов** выберите файл с сертификатом издателя или списком CRL.

10 На странице **Хранилище сертификатов** отобразится выбранное ранее хранилище сертификатов.

11 На странице **Завершение мастера импорта сертификатов** нажмите кнопку **Готово**.

Внимание! Если система не сможет проверить подлинность сертификата (например, отсутствует подключение к Интернету или узел проверки недоступен), появится окно **Предупреждение системы безопасности**. Чтобы установить сертификат, нажмите кнопку **Да**.

Устанавливайте только те сертификаты, в подлинности которых вы уверены.

---

12 В появившемся окне с сообщением об успешном импорте сертификата нажмите кнопку **OK**. Установка будет завершена.

После этого, если вы уже выполнили установку сертификата пользователя, можно приступать к выполнению криптографических операций (см. «Практическое применение ViPNet CSP» на стр. 27).

Установка и обновление CRL через Интернет

Если в вашем сертификате указан URL-адрес точки распространения списков аннулированных сертификатов и если ваш компьютер подключен к Интернету, вы можете установить или обновить список CRL автоматически. Для этого выполните следующие действия:

1 В окне **ViPNet CSP** в разделе **Контейнеры ключей** (см. Рисунок 31 на стр. 66) выберите контейнер ключей, которому соответствует сертификат, список CRL для которого требуется установить или обновить.

Примечание. Папку хранения контейнеров ключей (см. «Контейнер ключей» на стр. 22), отображаемых в списке, вы можете выбрать с помощью раскрывающегося списка в верхней части окна:

- чтобы отобразить в списке контейнеры ключей из папки хранения ключей текущего пользователя, выберите пункт **Ключи пользователя**;
- чтобы отобразить контейнеры ключей из папки хранения ключей компьютера, выберите пункт **Ключи компьютера**;
- чтобы отобразить контейнеры ключей на внешнем устройстве, выберите пункт с именем этого устройства.

Пункт **Ключи компьютера** появляется в списке только при наличии хотя бы одного контейнера ключей в папке хранения ключей компьютера (см. «Контейнер ключей» на стр. 22).

---

2 Нажмите кнопку **Свойства** либо дважды щелкните нужный контейнер ключей.

3 В окне **Свойства контейнера ключей** (см. Рисунок 34 на стр. 71) нажмите кнопку **Открыть**.

Откроется окно со свойствами сертификата. При этом будет выполнено подключение к точке распространения списков CRL:

- Если список CRL не был установлен ранее, он будет загружен и автоматически установлен.
- Если список CRL уже установлен, будет проверена его актуальность, при необходимости он будет автоматически обновлен.

6

Операции с контейнерами ключей

Просмотр и настройка свойств контейнера ключей

Чтобы просмотреть свойства контейнера ключей или изменить его настройки, в окне **Свойства контейнера ключей** (см. Рисунок 34 на стр. 71) выполните следующие действия:

1 В окне **ViPNet CSP** в разделе **Контейнеры ключей** (см. Рисунок 31 на стр. 66) выберите контейнер, свойства которого вы хотите просмотреть.

Примечание. Папку хранения контейнеров ключей (см. «Контейнер ключей» на стр. 22), отображаемых в списке, вы можете выбрать с помощью раскрывающегося списка в верхней части окна:

- чтобы отобразить в списке контейнеры ключей из папки хранения ключей текущего пользователя, выберите пункт **Ключи пользователя**;
- чтобы отобразить контейнеры ключей из папки хранения ключей компьютера, выберите пункт **Ключи компьютера**;
- чтобы отобразить контейнеры ключей на внешнем устройстве, выберите пункт с именем этого устройства.

Пункт **Ключи компьютера** появляется в списке только при наличии хотя бы одного контейнера ключей в папке хранения ключей компьютера (см. «Контейнер ключей» на стр. 22).

---

2 Нажмите кнопку **Свойства** либо дважды щелкните нужный контейнер ключей.

Далее вы можете выполнить следующие операции:

- Просмотреть информацию о закрытом ключе и сертификате, которые находятся в контейнере ключей.
- Сменить пароль доступа к контейнеру ключей (см. «Смена пароля к контейнеру ключей» на стр. 83).
- Удалить сохраненный пароль доступа к контейнеру ключей (см. «Удаление сохраненного пароля» на стр. 84).
- Произвести установку сертификата пользователя (см. «Установка сертификата в контейнер ключей» на стр. 70).
- Настроить права доступа к контейнеру ключей (см. «Настройка прав доступа к контейнеру ключей» на стр. 85).

Смена пароля к контейнеру ключей

Для смены пароля к контейнеру ключей в папке на диске выполните следующие действия:

1 В окне **Свойства контейнера ключей** нажмите кнопку **Сменить**.

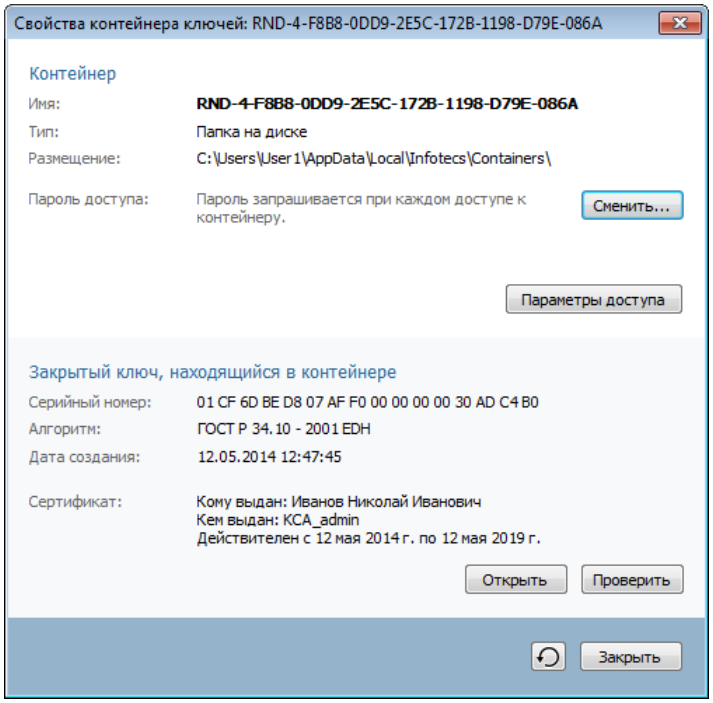


Рисунок 40. Информация о контейнере ключей

2 В окне **Пароль** введите текущий пароль доступа к контейнеру ключей и нажмите кнопку **OK**.

Примечание. Если ранее был установлен режим **Сохранить пароль**, то окно **Пароль** не появится.

---

3 В окне **ViPNet CSP - смена пароля контейнера ключей** укажите текущий пароль, задайте и подтвердите новый пароль. Нажмите кнопку **OK**.

Чтобы сохранить пароль для последующих обращений к контейнеру ключей, установите флажок **Сохранить пароль**.

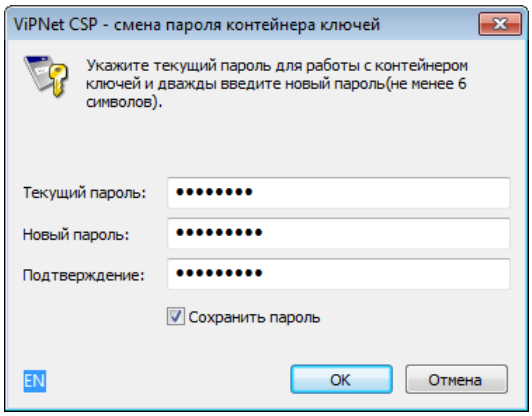


Рисунок 41. Смена пароля доступа к контейнеру ключей

Внимание! Не создавайте пароль длиной в 32 символа. Пароли с такой длиной не могут использоваться в текущих версиях приложений ViPNet. Данное ограничение связано с существующим алгоритмом передачи пароля в криптопровайдер. В соответствии с этим алгоритмом длина пароля не должна превышать 31 символ.

Пароль доступа к контейнеру ключей изменен.

Удаление сохраненного пароля

Удалять сохраненный пароль к контейнеру ключей может потребоваться в том случае, если изменились условия эксплуатации пароля или регламент вашей организации, вследствие чего хранение пароля на компьютере стало недопустимым.

Для удаления ранее сохраненного в системе пароля к контейнеру ключей в окне **Свойства контейнера ключей** (см. Рисунок 34 на стр. 71) нажмите кнопку **Удалить**.

Сохраненный пароль удален. Теперь пароль необходимо вводить всякий раз при обращении к контейнеру ключей.

Проверка контейнера ключей

Проверка контейнера ключей позволяет убедиться, что файл контейнера не поврежден, хранящиеся в контейнере сертификат и ключ электронной подписи соответствуют друг другу и могут быть использованы для работы с защищенными документами.

Чтобы проверить контейнер ключей, выполните следующие действия:

1. В окне **Свойства контейнера ключей** нажмите кнопку **Проверить**.
2. В окне **ViPNet CSP - пароль контейнера ключей** введите пароль доступа к контейнеру и нажмите кнопку **OK**.

Чтобы сохранить пароль для последующих обращений к контейнеру ключей, установите флажок **Сохранить пароль**.

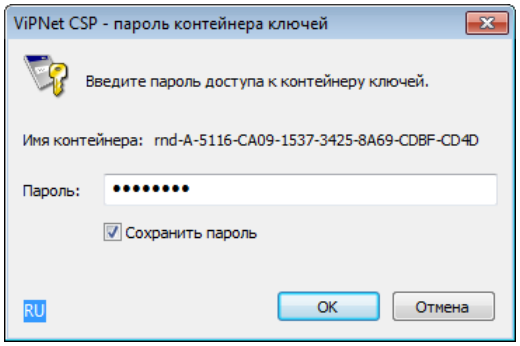


Рисунок 42. Ввод пароля доступа к контейнеру ключей

В результате будет сформирован фрагмент данных, который будет подписан с помощью ключа электронной подписи, после чего будет выполнена проверка электронной подписи с помощью ключа проверки электронной подписи. Таким образом, будет проверена пригодность ключа электронной подписи и его соответствие сертификату ключа проверки электронной подписи, хранящемуся в контейнере.

Примечание. Проверка возможна только в том случае, если в контейнере ключей есть сертификат, соответствующий ключу электронной подписи. Сертификат может отсутствовать в контейнере ключей, если он размещен отдельно. Сертификат размещается отдельно от контейнера ключей, если запрос на обновление сертификата сформирован в ПО ViPNet CSP. Если запрос сформирован в другой программе, сертификат автоматически помещается в контейнер ключей.

При проверке ключа электронной подписи проверка действительности сертификата (срок его действия, отсутствие в списках аннулированных сертификатов и прочее) не выполняется.

Настройка прав доступа к контейнеру ключей

С помощью прав доступа вы можете разрешать или запрещать доступ к контейнеру ключей для субъектов безопасности операционной системы Microsoft Windows (например, учетных записей и групп пользователей). Например, разрешение на доступ к контейнеру ключей для встроенной учетной записи NETWORK SERVICE может потребоваться при настройке сервера IIS (см. «Настройка серверной части» на стр. 150).

Для настройки прав доступа к контейнеру ключей выполните следующие действия:

1. В окне **Свойства контейнера ключей** (см. Рисунок 40 на стр. 83) нажмите кнопку **Параметры доступа**.
2. В окне **Разрешения для группы** выполните следующие действия:

2.1 В области **Группы и пользователи** выберите учетную запись или группу учетных записей Windows, для которых необходимо задать разрешения.

2.2 В области **Разрешения для группы** задайте разрешения для выбранных учетных записей.

2.3 Нажмите кнопку **OK**.

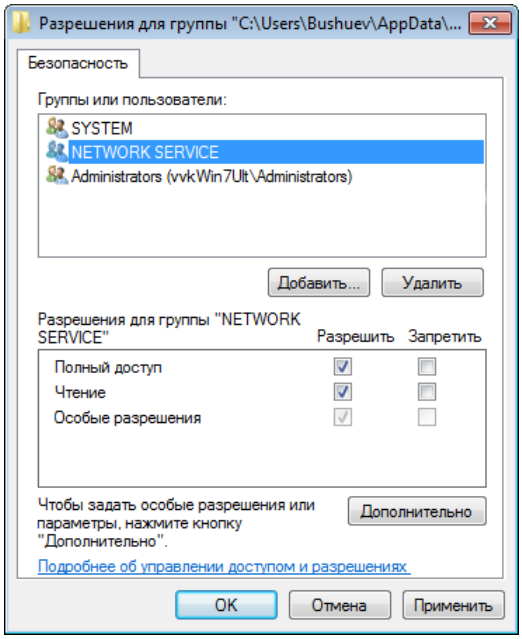


Рисунок 43. Настройка прав доступа к контейнеру ключей

Права доступа для выбранных учетных записей изменены.

Создание резервной копии контейнера ключей

Вы можете скопировать контейнер ключей в папку на диске или на внешнее устройство. Эта функция может быть использована для создания резервной копии контейнера ключей.

Примечание. Копирование контейнера ключей подписи с внешних устройств с аппаратной поддержкой алгоритмов ГОСТ невозможно.

Для копирования контейнера выполните следующие действия:

1 В окне **ViPNet CSP** в разделе **Контейнеры ключей** (см. Рисунок 31 на стр. 66) выберите контейнер ключей, который вы хотите скопировать.

Примечание. Папку хранения контейнеров ключей (см. «Контейнер ключей» на стр. 22), отображаемых в списке, вы можете выбрать с помощью раскрывающегося списка в верхней части окна.

2 Нажмите кнопку **Копировать в**.

3 В окне **ViPNet CSP - инициализация контейнера ключей** (см. Рисунок 32 на стр. 67) укажите новое имя для контейнера и место его расположения. Вы можете скопировать контейнер ключей в папку на диске или на внешнее устройство. Нажмите кнопку **OK**.

4 В окне **ViPNet CSP - пароль контейнера ключей** (см. Рисунок 42 на стр. 85) введите пароль (или ПИН-код, если контейнер ключей находится на внешнем устройстве) доступа к контейнеру ключей, копию которого требуется создать.

Чтобы сохранить пароль для последующих обращений к контейнеру ключей, установите флажок **Сохранить пароль**.

Затем нажмите кнопку **OK**.

5 В окне **ViPNet CSP - пароль контейнера ключей** (см. Рисунок 28 на стр. 60) задайте и подтвердите пароль, который будет использоваться для доступа к создаваемой копии контейнера.

Примечание. Сохранение пароля к контейнеру ключей в системе ведет к снижению уровня безопасности.

6 Копия контейнера ключей появится в списке контейнеров ключей (в папке хранения ключей текущего пользователя) и в указанной папке (либо на устройстве).

Перенос сертификатов и закрытых ключей между компьютерами

Если вы хотите перенести сертификаты и закрытые ключи с компьютера, на котором установлена программа ViPNet CSP, на другой компьютер с ViPNet CSP либо на компьютер с криптопровайдером другого производителя, выполните следующие действия:

1. На компьютере с ViPNet CSP экспортируйте сертификат отдельно или вместе с закрытым ключом в файл одного из универсальных форматов (см. «Экспорт сертификата и закрытого ключа в файл» на стр. 88).
2. На компьютере, где вы хотите использовать экспортированный сертификат или сертификат с закрытым ключом, выполните одно из следующих действий:
   - Если на компьютере установлена программа ViPNet CSP, импортируйте сертификат или сертификат с закрытым ключом (см. «Импорт сертификата и закрытого ключа из файла» на стр. 90).
   - Если на компьютере используется криптопровайдер другого производителя, импортируйте сертификат или сертификат с закрытым ключом, следуя руководству для данного криптопровайдера.

Экспорт сертификата и закрытого ключа в файл

Для переноса сертификатов и закрытых ключей между компьютерами вы можете экспортировать установленные сертификаты и закрытые ключи из контейнера в файлы различных форматов. Для этого выполните следующие действия:

1. В окне **ViPNet CSP** в разделе **Контейнеры ключей** (см. Рисунок 31 на стр. 66) выберите контейнер ключей, содержащий сертификат или сертификат и закрытый ключ, которые вы хотите экспортировать.

Примечание. Папку хранения контейнеров ключей (см. «Контейнер ключей» на стр. 22), отображаемых в списке, вы можете выбрать с помощью раскрывающегося списка в верхней части окна:

- чтобы отобразить в списке контейнеры ключей из папки хранения ключей текущего пользователя, выберите пункт **Ключи пользователя**;
- чтобы отобразить контейнеры ключей из папки хранения ключей компьютера, выберите пункт **Ключи компьютера**;
- чтобы отобразить контейнеры ключей на внешнем устройстве, выберите пункт с именем этого устройства.

Пункт **Ключи компьютера** появляется в списке только при наличии хотя бы одного контейнера ключей в папке хранения ключей компьютера (см. «Контейнер ключей» на стр. 22).

Нажмите кнопку **Свойства** либо дважды щелкните нужный контейнер ключей.

2 В окне **Свойства контейнера ключей** (см. Рисунок 34 на стр. 71) нажмите кнопку **Открыть**.

3 В окне **Сертификат** перейдите на вкладку **Состав** и нажмите кнопку **Копировать в файл**.

4 На странице приветствия мастера экспорта сертификатов нажмите кнопку **Далее**.

5 На странице **Экспортирование закрытого ключа** укажите, хотите ли вы вместе с сертификатом экспортировать закрытый ключ.

Примечание. Вы можете экспортировать вместе с сертификатом закрытый ключ, только если при формировании запроса на этот сертификат был установлен флажок **Экспортируемый** (см. «Создание запроса на сертификат и формирование закрытого ключа» на стр. 57).

6 На странице **Формат экспортируемого файла** выберите необходимый формат. Если вы экспортируете закрытый ключ вместе с сертификатом, при необходимости выберите дополнительные опции экспорта.

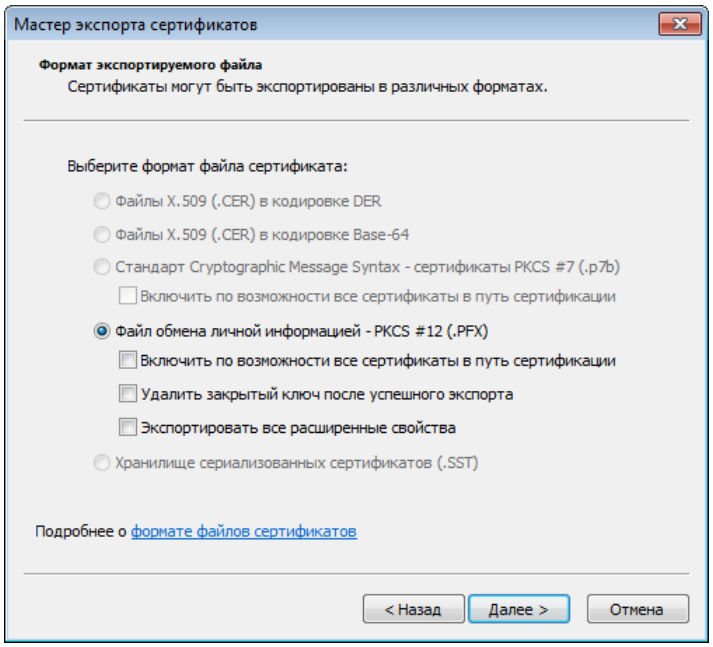


Рисунок 44. Выбор формата экспортируемого файла

7 Если вы экспортируете закрытый ключ вместе с сертификатом, на странице **Пароль** задайте и подтвердите пароль доступа к экспортируемому закрытому ключу.

8 На странице **Имя файла экспорта** укажите папку, в которой вы хотите создать файл с экспортируемыми ключами, и задайте имя этого файла.

9 На странице завершения работы мастера экспорта сертификатов нажмите кнопку **Готово.**

В результате сертификат или сертификат с закрытым ключом будут сохранены в файл, который вы можете перенести на другой компьютер.

Внимание! Несмотря на то что файл формата PFX, содержащий закрытый ключ, защищен паролем, по требованиям безопасности он должен передаваться на другой компьютер только защищенным способом.

Импорт сертификата и закрытого ключа из файла

Для того чтобы на компьютере с установленной программой ViPNet CSP импортировать сертификат отдельно или вместе с закрытым ключом из файла, выполните следующие действия:

- Если файл содержит только сертификат, для установки сертификата см. раздел Установка сертификата, не добавленного в контейнер ключей (на стр. 72).
- Если файл содержит помимо сертификата закрытый ключ, выполните следующие действия:
  - В окне **ViPNet CSP** в разделе **Контейнеры ключей** (см. Рисунок 31 на стр. 66) нажмите кнопку **Установить сертификат**.

- В окне **Открыть** укажите путь к файлу, содержащему сертификат вместе с закрытым ключом (см. «Контейнер ключей» на стр. 22).
- В окне **ViPNet CSP - пароль контейнера ключей** введите пароль доступа к контейнеру и нажмите кнопку **OK**.
- В окне **ViPNet CSP - инициализация контейнера ключей** (см. Рисунок 32 на стр. 67) нажмите кнопку **OK**.

В результате закрытый ключ и сертификат из файла будут установлены в контейнер ключей, и этот контейнер появится в списке раздела **Контейнеры ключей**.

Удаление контейнера ключей

Если вы хотите отказаться от использования какого-либо сертификата и закрытого ключа, вы можете удалить соответствующий контейнер. Для этого выполните следующие действия:

1 В окне **ViPNet CSP** в разделе **Контейнеры ключей** (см. Рисунок 31 на стр. 66) выберите контейнер ключей, который требуется удалить.

Примечание. Папку хранения контейнеров ключей (см. «Контейнер ключей» на стр. 22), отображаемых в списке, вы можете выбрать с помощью раскрывающегося списка в верхней части окна:

- чтобы отобразить в списке контейнеры ключей из папки хранения ключей текущего пользователя, выберите пункт **Ключи пользователя**;
- чтобы отобразить контейнеры ключей из папки хранения ключей компьютера, выберите пункт **Ключи компьютера**;
- чтобы отобразить контейнеры ключей на внешнем устройстве, выберите пункт с именем этого устройства.

Пункт **Ключи компьютера** появляется в списке только при наличии хотя бы одного контейнера ключей в папке хранения ключей компьютера (см. «Контейнер ключей» на стр. 22).

---

2 Нажмите кнопку  .

Внимание! Удаленный контейнер ключей невозможно будет более использовать. Перед удалением рекомендуется создать резервную копию контейнера (см. «Создание резервной копии контейнера ключей» на стр. 87).

---

3 Чтобы подтвердить удаление контейнера ключей, в появившемся окне нажмите кнопку **OK**.

Контейнер будет удален из списка контейнеров, а также из папки или с внешнего устройства, где он хранится.

7

Работа с внешними устройствами

Доступ к контейнерам ключей на внешнем устройстве

ViPNet CSP позволяет работать с контейнерами ключей, которые хранятся на внешних устройствах (см. «Внешние устройства» на стр. 214).

Для просмотра подключенных устройств и хранящихся на них контейнеров ключей выполните следующие действия:

1 В окне **ViPNet CSP** перейдите в раздел **Контейнеры ключей**.

2 В раскрывающемся списке в верхней части окна выберите название подключенного устройства.

Примечание. В раскрывающемся списке помимо папок хранения контейнеров ключей (см. «Контейнер ключей» на стр. 22) отображаются только те устройства, которые в данный момент подключены к разъему USB или считывателю смарт-карт.

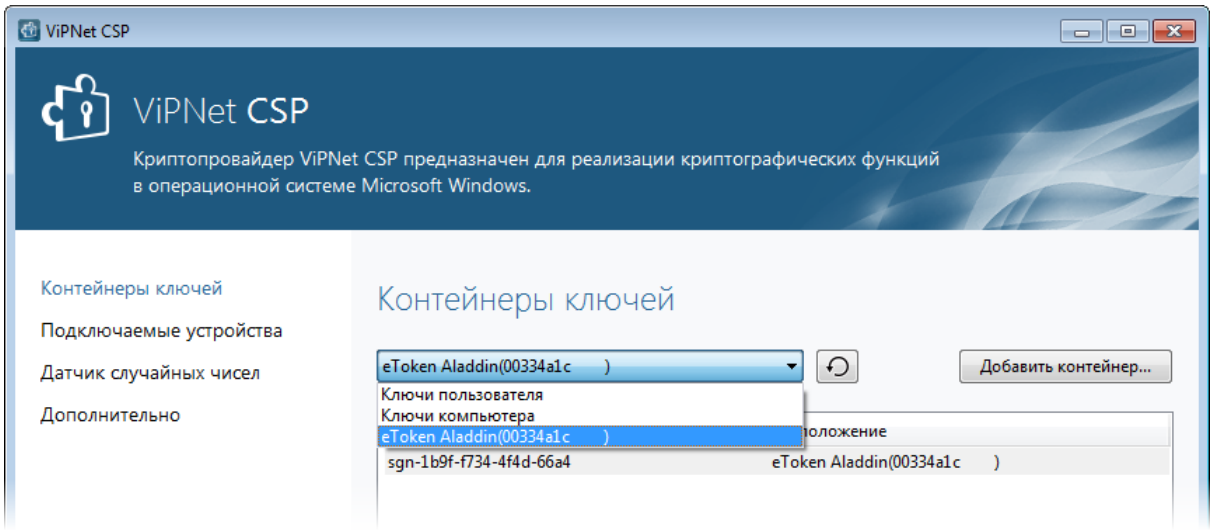


Рисунок 45. Выбор внешнего устройства

3 В списке появятся контейнеры ключей, сохраненные на выбранном устройстве.

Примечание. Если после выбора подключенного устройства список контейнеров ключей пуст, это значит, что на выбранном устройстве нет контейнеров ключей.

С контейнером ключей на внешнем устройстве вы можете работать так же, как и с контейнером ключей, хранящемся на вашем компьютере.

Настройка списка опрашиваемых устройств

В программе ViPNet CSP вы можете указать типы устройств, которыми будете пользоваться, в разделе **Подключаемые устройства**.

По умолчанию ViPNet CSP проводит поиск устройств всех поддерживаемых типов, кроме **Infotecs Software Token** и **ViPNet HSM** (см. «Внешние устройства» на стр. 214). Чтобы сократить время поиска нужного ключа, отключите неиспользуемые устройства. Для этого выполните следующие действия:

1 В окне **ViPNet CSP** перейдите в раздел **Подключаемые устройства**.

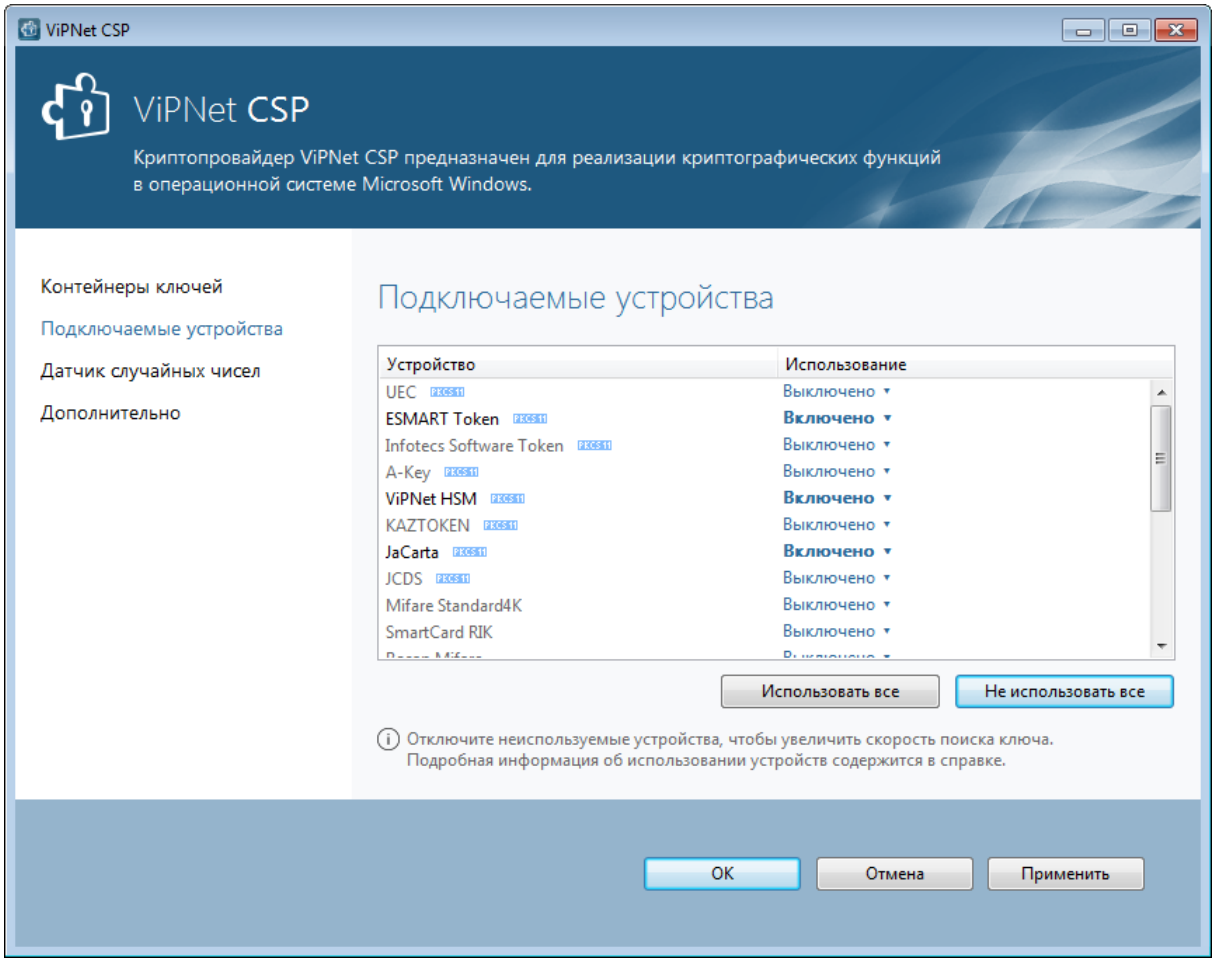


Рисунок 46. Настройка списка опрашиваемых устройств

2 Напротив типов устройств, которые не требуется использовать, щелкните ссылку **Включено** и в контекстном меню выберите пункт **Выключить**. После этого работа таких устройств с программой будет невозможна.

Примечание. Чтобы разрешить использование всех типов устройств, нажмите кнопку **Использовать все**.
Чтобы отменить использование всех типов устройств с целью последующего указания нескольких разрешенных, нажмите кнопку **Не использовать все**.

3 Чтобы сохранить настройки, нажмите кнопку **Применить**.

Инициализация устройства

Инициализацией называется форматирование памяти устройства. В процессе инициализации все данные, хранящиеся на устройстве, удаляются. Пароль и другие настройки устройства сбрасываются.

Если производитель устройства предоставляет специализированное ПО для администрирования, используйте для инициализации это ПО. Для остальных устройств доступна функция инициализации в программе ViPNet CSP.

Для инициализации подключенного устройства выполните следующие действия:

1. Убедитесь в том, что устройство, которое необходимо инициализировать, не содержит ценной информации. При необходимости перенесите все данные, хранящиеся на устройстве, на другой съемный носитель или жесткий диск компьютера.
2. В окне **ViPNet CSP** перейдите в раздел **Подключаемые устройства** (см. Рисунок 46 на стр. 95).
3. В списке **Подключаемые устройства** рядом с названием подключенного устройства нажмите кнопку ▾.
4. В появившемся меню выберите пункт **Инициализировать**.

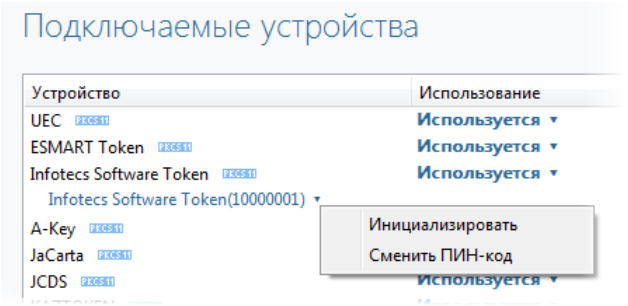


Рисунок 47. Выбор внешнего устройства для инициализации

5. В окне **Инициализация устройства** выполните следующие действия:
   - Введите ПИН-код администратора.
   - В двух других полях окна введите новый ПИН-код пользователя.
   - Установите флажок, подтверждающий согласие на инициализацию устройства.
   - Нажмите кнопку **OK**.

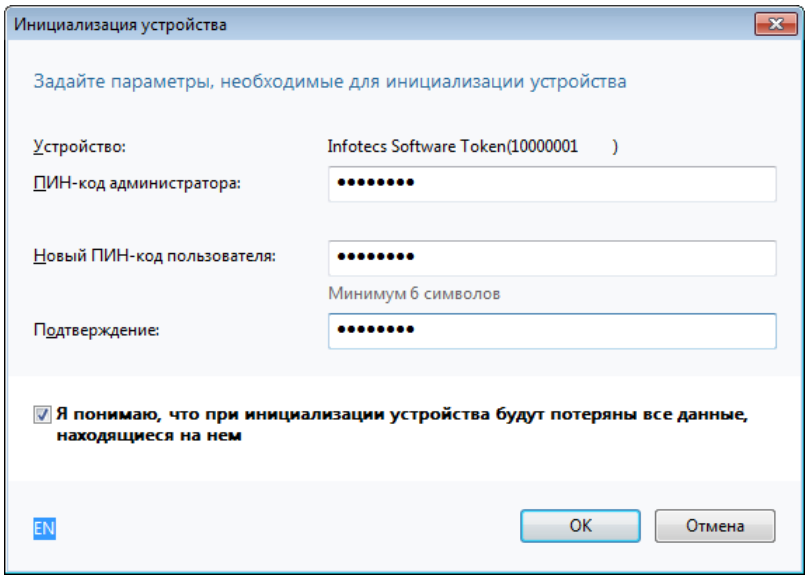


Рисунок 48. Инициализация внешнего устройства

Устройство будет инициализировано. При этом все хранившиеся на нем данные будут удалены. Для доступа к устройству будет использоваться заданный ПИН-код пользователя.

Смена ПИН-кода

Смена ПИН-кода устройства может потребоваться в связи с истечением срока действия пароля или по другим причинам, утвержденным регламентом организации.

Если производитель устройства предоставляет специализированное ПО для администрирования, используйте для смены ПИН-кода это ПО. Для остальных устройств доступна функция смены ПИН-кода в программе ViPNet CSP.

Чтобы сменить ПИН-код устройства, выполните следующие действия:

1 В окне **ViPNet CSP** перейдите в раздел **Подключаемые устройства** (см. Рисунок 46 на стр. 95).

2 В списке **Подключаемые устройства** (см. Рисунок 47 на стр. 97) рядом с названием подключенного устройства нажмите кнопку ▾.

3 В появившемся меню выберите пункт **Сменить ПИН-код**.

4 В окне **Смена ПИН-кода** выполните следующие действия:

4.1 В списке **Сменить** выберите тип изменяемого ПИН-кода.

4.2 В поле **Текущий ПИН-код** укажите прежний ПИН-код, а в оставшихся двух полях — новый ПИН-код.

4.3 Нажмите кнопку **OK**.

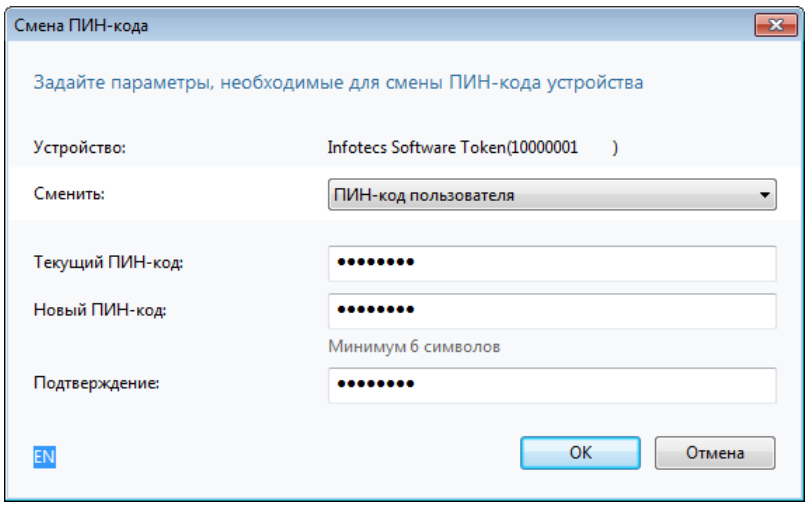


Рисунок 49. Смена ПИН-кода внешнего устройства

В результате ПИН-код устройства будет изменен.

Использование датчика случайных чисел

Датчик случайных чисел создает случайные последовательности чисел, на основе которых формируются закрытые ключи.

В качестве датчика случайных чисел в программе ViPNet CSP можно использовать встроенный датчик — «биологический» (электронная рулетка (см. глоссарий, стр. 232)), аппаратный датчик случайных чисел или предварительно созданную последовательность случайных чисел.

Чтобы выбрать используемый датчик случайных чисел, выполните следующие действия:

1 В окне **ViPNet CSP** перейдите в раздел **Датчик случайных чисел**.

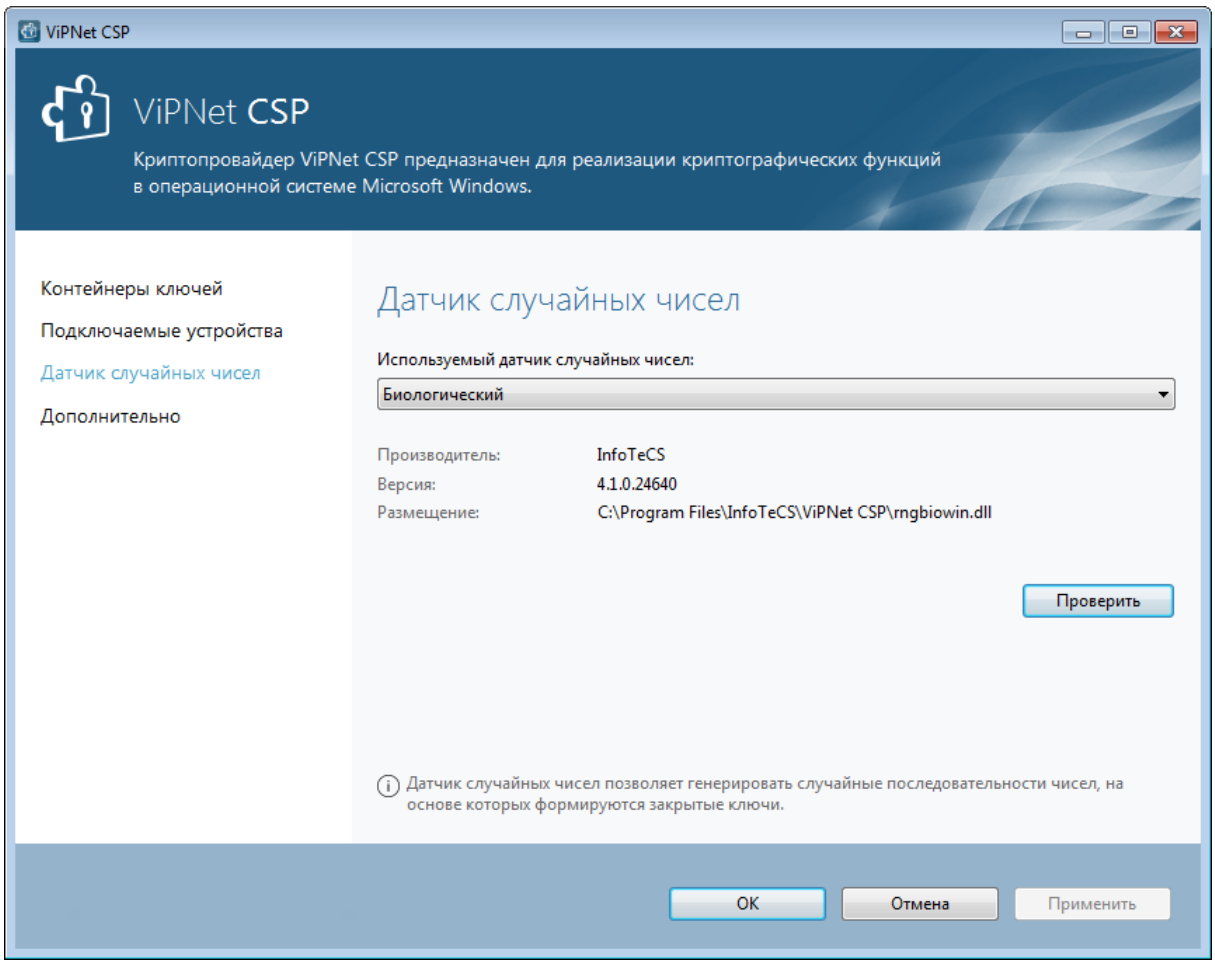


Рисунок 50. Выбор датчика случайных чисел

2 В списке **Используемый датчик случайных чисел** выберите один из вариантов:

- **Биологический** — чтобы использовать для создания последовательности случайных чисел «электронную рулетку».

- **Внешнее устройство (Token) PKCS#11** — чтобы использовать для создания последовательности случайных чисел поддерживаемое внешнее устройство (см. «Алгоритмы и функции, поддерживаемые внешними устройствами» на стр. 218).

Примечание. Если в качестве датчика случайных чисел выбрано внешнее устройство, перед созданием запроса на сертификат и перед проверкой работоспособности датчика случайных чисел подключите к компьютеру это внешнее устройство.

При использовании устройств с аппаратной поддержкой алгоритмов ГОСТ создание последовательностей случайных чисел всегда осуществляется средствами этих устройств вне зависимости от выбранного датчика случайных чисел.

- **ДСДР** — чтобы использовать предварительно созданную последовательность случайных чисел (гамму). После выбора этого варианта выполните следующие действия:
  - Нажмите кнопку **Добавить гамму**.
  - В окне **Обзор папок** укажите папку, в которой находятся файлы, содержащие последовательность случайных чисел.

Примечание. Последовательности случайных чисел (гаммы) поставляются на дисках ДСДР в составе ключевых блокнотов, которые вы можете получить в Федеральной службе безопасности России (ФСБ).

- Аппаратный датчик случайных чисел, установленный на компьютере.

Примечание. Аппаратные датчики случайных чисел, не установленные на компьютере, не отображаются в списке **Используемый датчик случайных чисел**.

При использовании датчика случайных чисел аппаратного модуля доверенной загрузки «Аккорд-АМДЗ» помимо установки стандартного программного обеспечения скопируйте файл `tmdrv32.dll` из комплекта поставки в папку `C:\Windows\System32` (для 32-разрядной версии Windows) или в папку `C:\Windows\SysWOW64` (для 64-разрядной версии Windows).

---

3 Для сохранения параметров нажмите кнопку **Применить**.

Свойства выбранного устройства отображаются под списком **Используемый датчик случайных чисел**.

Чтобы проверить работоспособность биологического или аппаратного датчика случайных чисел, нажмите кнопку **Проверить**. После проведения проверки программа выдаст сообщение о ее результате.

8

Регистрация событий криптопровайдера

Настройка регистрации событий криптопровайдера

В программе ViPNet CSP организовано ведение журнала событий, с помощью которого можно осуществлять мониторинг работы криптопровайдера. События записываются в системный журнал Windows.

Вы можете задать один из двух режимов ведения журнала либо отключить запись событий. Для этого выполните следующие действия:

1 В главном окне ViPNet CSP перейдите в раздел **Дополнительно**.

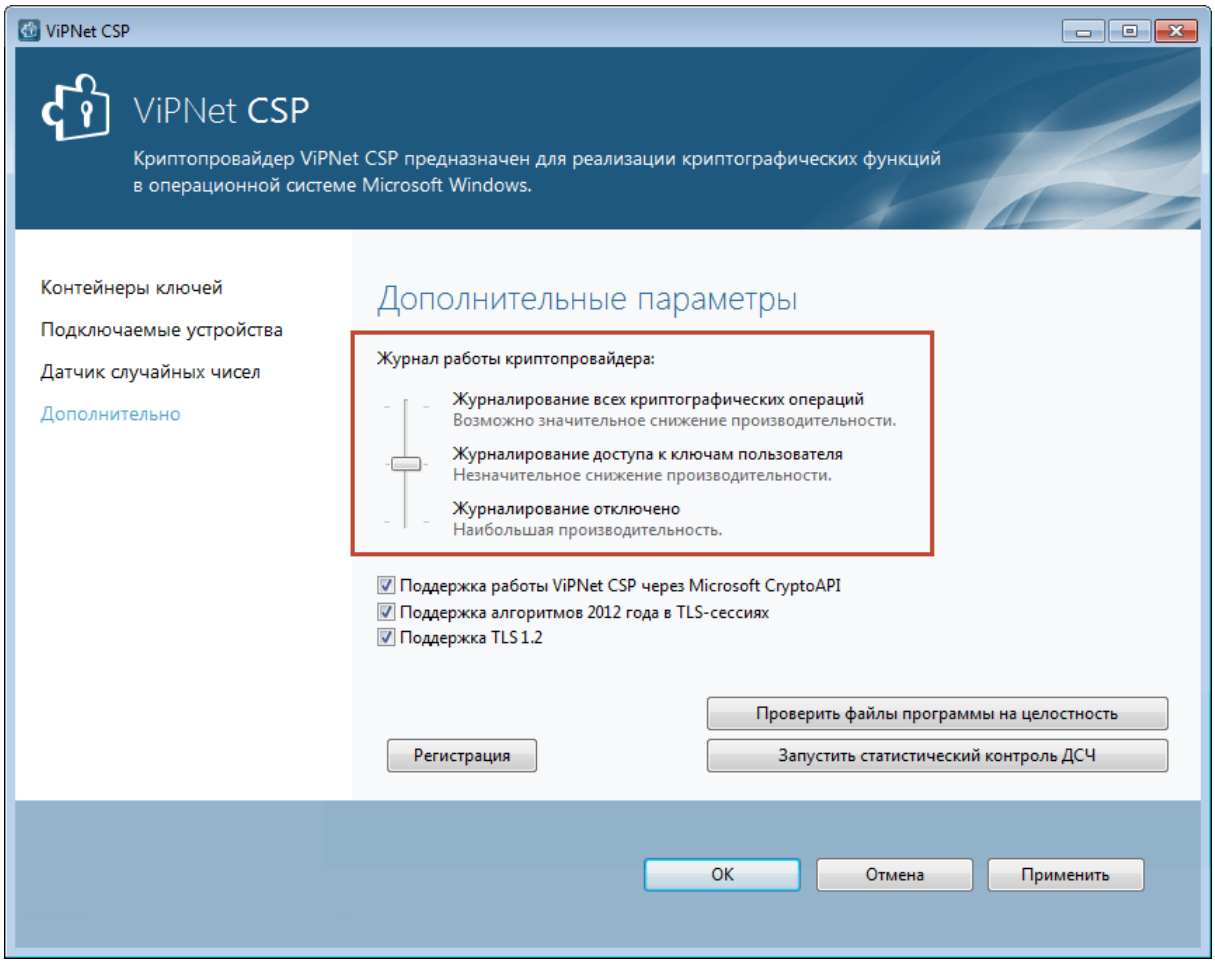


Рисунок 51. Задание режима ведения журнала

2 В области **Журнал работы криптопровайдера** переместите ползунок в одно из следующих положений:

- **Журналирование отключено** — регистрация событий в журнале отключена.

- **Журналирование доступа к ключам пользователя** — в журнал записываются только события, не связанные с долговременными операциями: обращения к ключам пользователя, подпись или проверка подписи хэш-сумм.
- **Журналирование всех криптографических операций** — в журнал также записываются события, связанные с долговременными операциями: хэшированием, шифрованием, расшифрованием, контролем целостности файлов. При выборе этого режима возможно значительное снижение производительности криптопровайдера из-за большого количества регистрируемых событий.

Регистрируемые события криптопровайдера вы можете просматривать в системном журнале Windows (см. «Просмотр событий криптопровайдера в системном журнале» на стр. 105).

Просмотр событий криптопровайдера в системном журнале

Если в программе ViPNet CSP включена регистрация событий криптопровайдера (см. «Настройка регистрации событий криптопровайдера» на стр. 103), вы можете осуществлять мониторинг этих событий с помощью системного журнала Windows. Чтобы просмотреть события, источником которых является криптопровайдер ViPNet CSP, выполните следующие действия:

1. На **Панели управления** в категории **Администрирование** дважды щелкните значок **Просмотр событий**.
2. В окне **Просмотр событий** на левой панели выберите **Журналы приложений и служб** > **ViPNet CSP**.

В результате на правой панели отобразится список зарегистрированных событий.

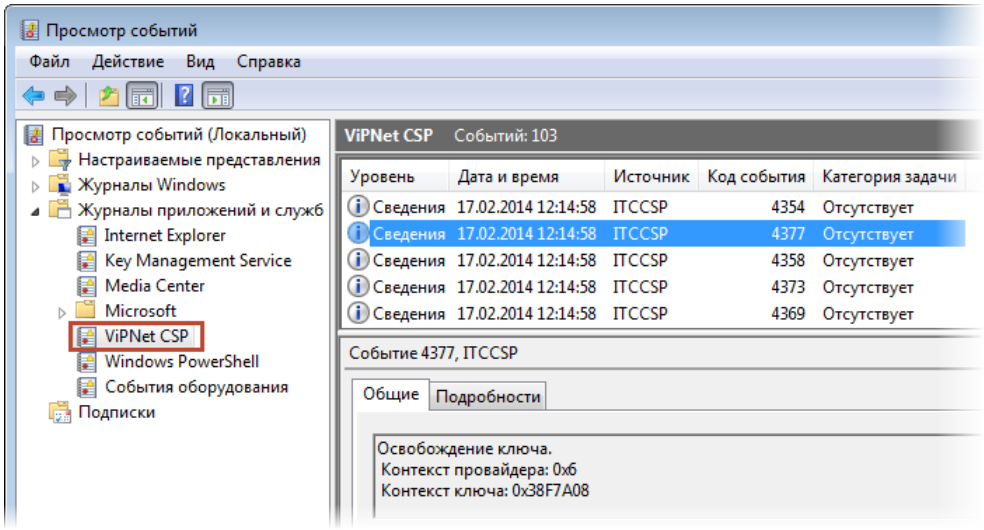


Рисунок 52. Просмотр событий ViPNet CSP

9

Использование функций криптопровайдера при разработке программ

Настройка проекта для использования функций ViPNet CSP

Внимание! Для сборки проектов, использующих библиотеки ViPNet CSP, вам понадобится компилятор Microsoft Visual Studio 2015 или более поздней версии.

Вместе с ViPNet CSP распространяется комплект средств разработки (SDK), который представляет собой архив с заголовочными файлами ViPNet CSP и примерами программ.

Для использования функций ViPNet CSP в своем проекте выполните следующие действия:

1 Извлеките файлы из архива SDK в папку на вашем жестком диске.

Примечание. Далее путь к папке, в которую вы разархивировали файлы, будет обозначаться `C:\\CSP_SDK`.

2 В настройках проекта укажите следующие папки:

- `C:\\CSP_SDK\headers\cspsdk` — для поиска заголовочных файлов криптоинтерфейса ViPNet CSP;
- `C:\\CSP_SDK\headers\pkcs11` — для поиска заголовочных файлов криптоинтерфейса PKCS#11 (работа с внешними устройствами);
- `C:\\CSP_SDK\headers\soft_token` — для поиска заголовочных файлов криптоинтерфейса ViPNet PKCS#11 VT (работа с программными токенами);
- рабочая папка Microsoft Windows SDK — для системных заголовочных файлов.

3 В исходный код проекта включите заголовочный файл `wincrypt.h`:

```
#include <wincrypt.h>
```

4 Чтобы использовать параметры, специфичные для ViPNet CSP, также включите заголовочный файл `importitccsp.h`:

```
#include <importitccsp.h>
```

В результате вы сможете использовать в своем проекте функции, описанные в руководстве «ViPNet CSP. Руководство разработчика».

Криптографические библиотеки, входящие в состав ViPNet CSP

После установки ViPNet CSP криптографические библиотеки будут размещены в папке:

- `C:\Program Files\InfoTeCS\ViPNet CSP` — для 32-разрядных версий ОС Windows.
- `C:\Program Files (x86)\InfoTeCS\ViPNet CSP` — для 64-разрядных версий ОС Windows.

Описание используемых криптографических библиотек приведено в документе «ViPNet CSP. Руководство разработчика».

10

Интеграция ViPNet CSP с центром сертификации на базе Microsoft CA

Порядок действий

Вы можете использовать удостоверяющий центр Microsoft (центр сертификации Microsoft CA) для выполнения криптографических функций в соответствии с алгоритмами ГОСТ. Для этого необходимо при развертывании центра сертификации задать в качестве поставщика криптографических функций ViPNet CSP.

Вы можете развернуть центр сертификации Microsoft CA на любом сервере, работающем под управлением одной из следующих операционных систем: Microsoft Windows Server 2008 R2, 2012, 2012 R2. В приведенном ниже примере предполагается, что для развертывания выделен сервер с операционной системой Microsoft Windows Server 2012, который подключен к локальной сети.

Для интеграции ViPNet CSP с центром сертификации Microsoft CA выполните следующие действия:

1. Установите и зарегистрируйте программу ViPNet CSP (см. «Установка и запуск программы» на стр. 28).
2. Разверните центр сертификации, добавив на сервер центра соответствующую роль (см. «Развертывание центра сертификации Microsoft CA» на стр. 111).

Развертывание центра сертификации Microsoft CA

Чтобы развернуть на сервере с ОС Windows Server 2012 центр сертификации, взаимодействующий с криптопровайдером ViPNet CSP, на сервер требуется установить специальную роль «Службы сертификации Active Directory». В процессе установки роли будет сформирована пара ключей и издан сертификат центра сертификации.

Для развертывания и настройки центра сертификации Microsoft CA выполните следующие действия:

1. На панели управления Windows в категории **Администрирование** запустите консоль **Диспетчер серверов**.
2. В меню **Управление** консоли **Диспетчер серверов** выберите пункт **Добавить роли и компоненты**. Откроется мастер добавления ролей и компонентов.
3. Следуйте указаниям мастера, при этом на странице **Выбор ролей сервера** установите флажок напротив роли **Службы сертификатов Active Directory**, и в окне **Мастер добавления ролей и компонентов** нажмите кнопку **Добавить компоненты**.
4. В меню **Уведомления** консоли **Диспетчер серверов** в пункте **Конфигурация после развертывания** щелкните ссылку **Настроить службы сертификатов Active Directory**. Откроется мастер конфигурации службы сертификатов Active Directory.

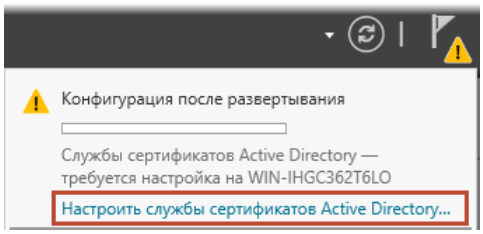


Рисунок 53. Настройка службы сертификатов Active Directory

5. Следуйте указаниям мастера, при этом:

   5.1 На странице **Службы ролей** установите флажок напротив службы **Центр сертификации**.

   5.2 На странице **Вариант установки** выберите один из следующий вариантов: **Автономный ЦС** или **ЦС предприятия**.

   5.3 На странице **Тип ЦС** задайте нужный тип центра сертификации и нажмите кнопку **Далее**.

   5.4 На странице **Закрытый ключ** выберите вариант **Создать новый закрытый ключ** и нажмите кнопку **Далее**.

   5.5 На странице **Шифрование для ЦС** выполните следующие действия:

   - В качестве поставщика служб шифрования в соответствующем списке выберите поставщика **GOST R 34.10#Infotecs Primitive Provider** или **Infotecs Cryptographic Service Provider**.

- Установите флажок **Разрешить взаимодействие с администратором, если ЦС обращается к закрытому ключу**.

Нажмите кнопку **Далее**.

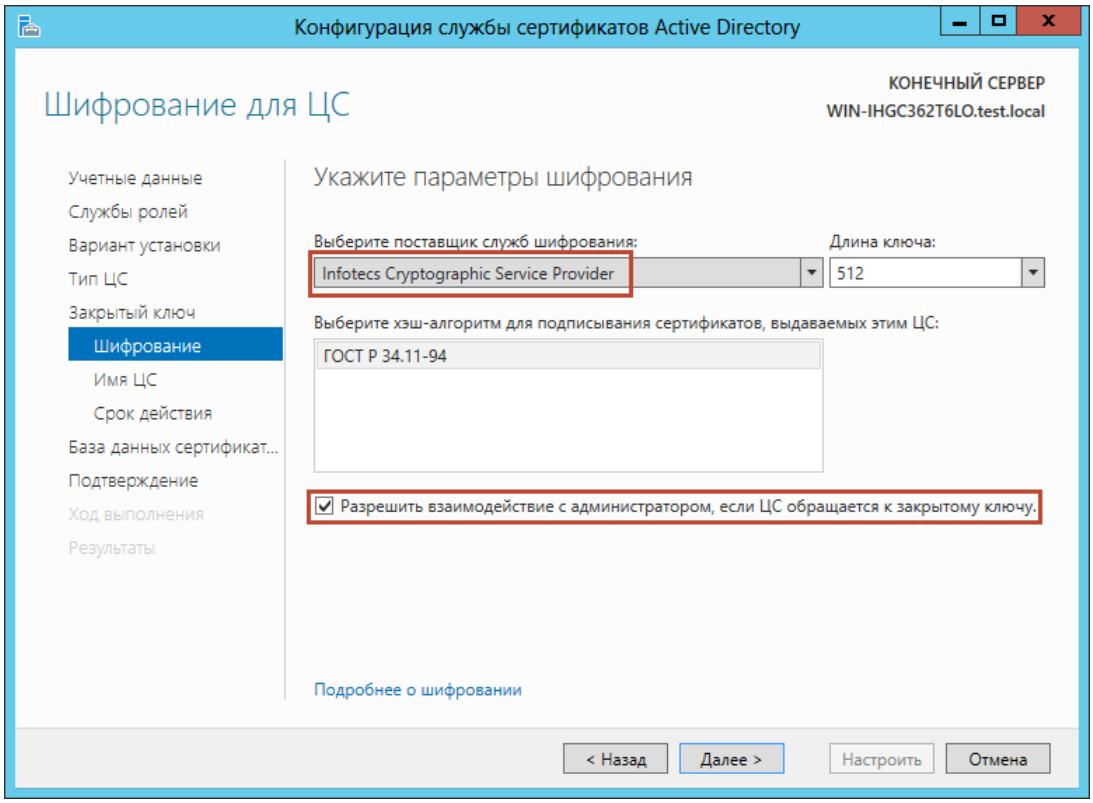


Рисунок 54. Выбор криптопровайдера при настройке удостоверяющего центра

6 На странице **Подтверждение** нажмите кнопку **Настроить**. При этом криптопровайдер ViPNet CSP начнет создание контейнера ключей с корневым сертификатом центра сертификации.

7 В окне **ViPNet CSP - инициализация контейнера ключей** (см. Рисунок 27 на стр. 60) выполните следующие действия:

- Укажите имя контейнера или оставьте значение по умолчанию в соответствующем поле.
- Укажите место размещения, установив переключатель в одно из значений: **Папка на диске** или **Выберите устройство**.

8 В окне **ViPNet CSP - пароль контейнера ключей** (см. Рисунок 28 на стр. 60) введите и подтвердите пароль доступа к контейнеру ключей.

Чтобы сохранить пароль для последующих обращений к контейнеру ключей, установите флажок **Сохранить пароль**.

9 Появится электронная рулетка (см. глоссарий, стр. 232), если она еще не запускалась в рамках текущего сеанса работы программы. Поводите указателем в пределах окна **Электронная рулетка** (см. Рисунок 29 на стр. 61).

10 На странице **Результаты** нажмите кнопку **Закрыть**.

В результате центр сертификации может начинать свою работу.

11

Электронная подпись в документах Microsoft Office

Подписание документов Microsoft Word, Excel и PowerPoint

При работе с документами в программах пакета Microsoft Office вы можете использовать электронную подпись.

В данном разделе содержится информация о том, как добавить электронную подпись в документы Microsoft Word, Excel и PowerPoint в случаях использования различных версий Microsoft Office.

Microsoft Office 2010

Чтобы добавить электронную подпись в документ Microsoft Word, Excel и PowerPoint, выполните следующие действия:

1 Сохраните документ.

2 Откройте вкладку **Файл** и выберите раздел **Сведения**.

3 В группе **Разрешения** нажмите кнопку **Защитить документ**, **Защитить книгу** или **Защитить презентацию**, затем выберите команду **Добавить цифровую подпись**. Откроется окно **Подписание**.

Примечание. Если документ не был предварительно сохранен, появится сообщение с предложением сохранить его перед добавлением подписи. В окне сообщения нажмите кнопку **Да**.

---

4 В окне **Подписание** вы можете заполнить поле **Цель подписания документа**. Ниже в этом же окне приведены краткие сведения о сертификате, которым предполагается подписать документ. При необходимости нажмите кнопку **Изменить** и выберите другой сертификат.

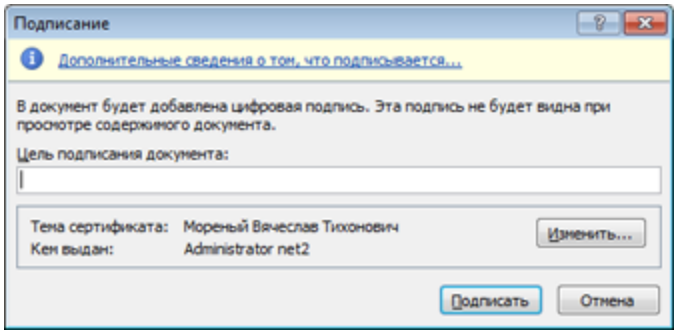


Рисунок 55. Добавление электронной подписи

5 Выбрав сертификат, нажмите кнопку **Подписать**. Откроется окно **ViPNet CSP – пароль контейнера ключей** (см. Рисунок 42 на стр. 85).

6 Введите пароль и нажмите кнопку **OK**. Появится сообщение об успешном добавлении электронной подписи.

В разделе **Сведения** будет отображена информация о том, что документ помечен как окончательный.

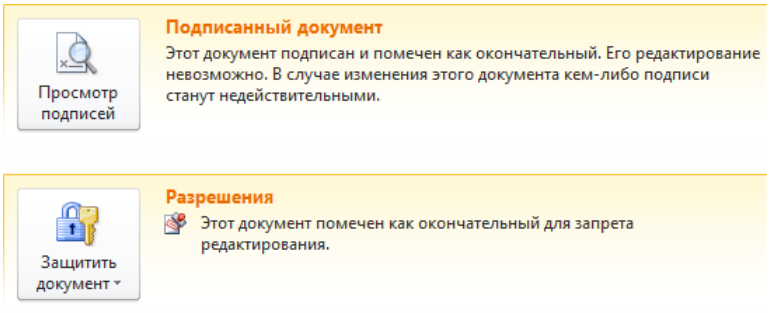


Рисунок 56. Информация о том, что документ помечен как окончательный

В строке состояния документа появится значок  , обозначающий, что документ содержит электронную подпись.

Совет. Возможность внесения правок в подписанный документ заблокирована. Если необходимо внести правки, сначала удалите электронную подпись (см. «Удаление электронной подписи в Microsoft Word, Excel и PowerPoint» на стр. 120).

Microsoft Office 2013

Чтобы добавить электронную подпись в документ Microsoft Word, Excel и PowerPoint, выполните следующие действия:

1 Сохраните документ.

2 Откройте вкладку **Файл** и выберите раздел **Сведения**.

3 Нажмите кнопку **Защита документа**, **Защита книги** или **Защита презентации** в одноименной группе и выберите команду **Добавить цифровую подпись**.

Примечание. Если документ не был предварительно сохранен, появится сообщение с предложением сохранить его перед добавлением подписи. В окне сообщения нажмите кнопку **Да**.

---

4 В окне **Подписание** вы можете выполнить следующие действия:

- В поле **Тип подтверждения** выбрать одну из заданных причин подписания документа.
- В поле **Цель подписания документа** указать цель подписания документа.

Ниже в этом же окне приведены краткие сведения о сертификате, которым предполагается подписать документ. При необходимости добавьте дополнительные сведения или нажмите кнопку **Изменить**, чтобы выбрать другой сертификат.

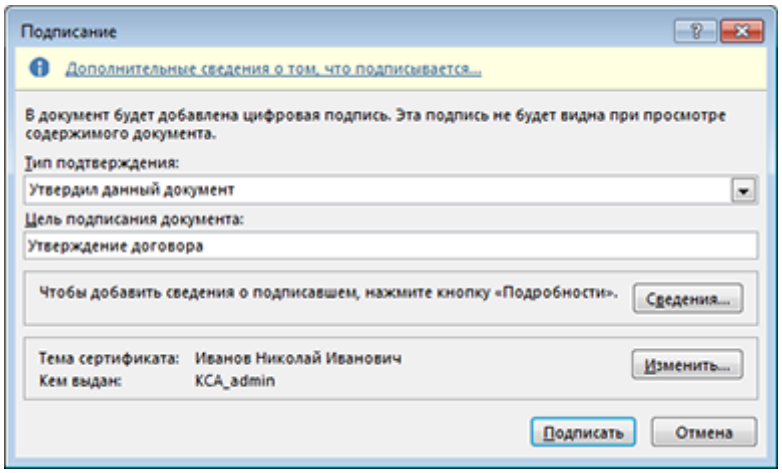


Рисунок 57. Добавление электронной подписи

5 Выбрав сертификат, нажмите кнопку **Подписать**. Откроется окно **ViPNet CSP – пароль контейнера ключей** (см. Рисунок 42 на стр. 85).

6 Введите пароль и нажмите кнопку **OK**. Появится сообщение об успешном добавлении электронной подписи.

В разделе **Сведения** будет отображена информация о том, что документ помечен как окончательный.

Рисунок 58. Информация о том, что документ помечен как окончательный

В строке состояния документа появится значок , обозначающий, что документ содержит электронную подпись.

Совет. Возможность внесения правок в подписанный документ заблокирована. Если необходимо внести правки, сначала удалите электронную подпись (см. «Удаление электронной подписи в Microsoft Word, Excel и PowerPoint» на стр. 120).

Просмотр электронной подписи в Microsoft Word, Excel и PowerPoint

Microsoft Office 2010

Для просмотра электронной подписи в документе Microsoft Word, Excel или PowerPoint выполните следующие действия:

1 Откройте вкладку **Файл** и в разделе **Сведения** нажмите кнопку **Просмотр подписей**. Откроется панель **Подписи**.

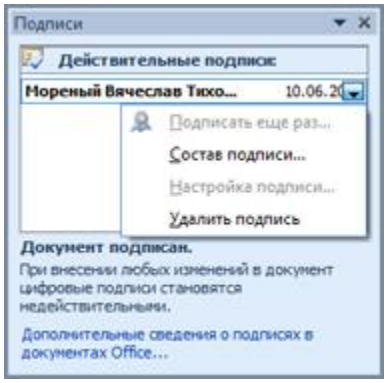


Рисунок 59. Панель «Подписи»

Примечание. Вы также можете вызвать панель **Подписи**, щелкнув в строке состояния значок электронной подписи .

---

2 На панели **Подписи** щелкните правой кнопкой мыши строку подписи (либо нажмите кнопку вызова меню справа). В меню выберите пункт **Состав подписи**.

3 В окне **Состав подписи** содержатся краткие сведения о подписи и сертификате. В нем вы можете выполнить следующие действия:

- Чтобы открыть сертификат, нажмите кнопку **Просмотр**.
- Чтобы просмотреть дополнительные сведения о подписи, щелкните ссылку **Дополнительные сведения, которые будут включены в подпись**.

Если при проверке сертификата возникли ошибки, сообщение об этом будет выведено под заголовком окна.

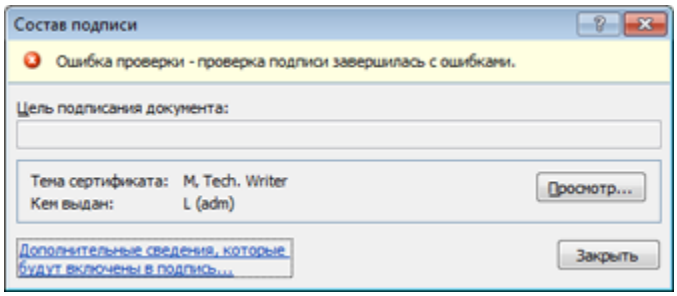


Рисунок 60. Состав подписи

Microsoft Office 2013

Для просмотра электронной подписи в документе Microsoft Word, Excel или PowerPoint выполните следующие действия:

1 Сохраните документ.

2 Откройте вкладку **Файл** и в разделе **Сведения** нажмите кнопку **Просмотр подписей**. Откроется панель **Подписи**.

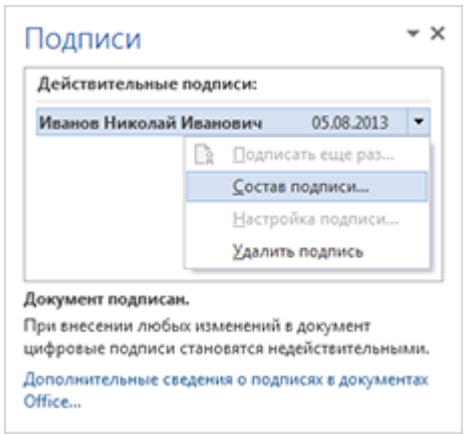


Рисунок 61. Панель «Подписи»

Примечание. Вы также можете вызвать панель **Подписи**, щелкнув в строке состояния значок электронной подписи .

---

3 На панели **Подписи** щелкните правой кнопкой мыши строку подписи (или нажмите кнопку вызова меню справа). В меню выберите пункт **Состав подписи**.

4 В окне **Состав подписи** содержатся краткие сведения о подписи и сертификате. В нем вы можете выполнить следующие действия:

- Чтобы открыть сертификат, нажмите кнопку **Просмотр**.
- Чтобы просмотреть дополнительные сведения о подписи, щелкните ссылку **Дополнительные сведения, которые будут включены в подпись**.

- Чтобы получить информацию о владельце сертификата, щелкните ссылку **Просмотр сведений о подписавшем**.

Примечание. Если при проверке сертификата возникли ошибки, сообщение об этом будет выведено под заголовком окна.

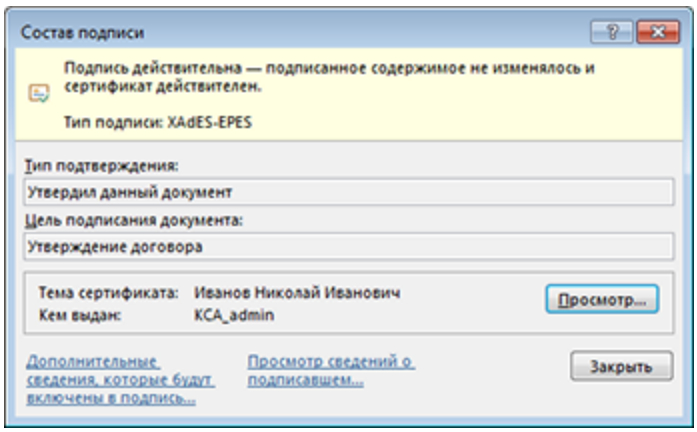


Рисунок 62. Состав подписи

Удаление электронной подписи в Microsoft Word, Excel и PowerPoint

Microsoft Office 2010

Чтобы удалить электронную подпись из документа Microsoft Word, Excel или PowerPoint, выполните следующие действия:

1 Откройте панель **Подписи**. Для этого откройте вкладку **Файл** и в разделе **Сведения** нажмите кнопку **Просмотр подписей**.

Примечание. Вы можете также вызвать панель **Подписи**, щелкнув в строке состояния документа значок электронной подписи  .

---

2 На панели **Подписи** (см. Рисунок 59 на стр. 117) щелкните правой кнопкой мыши строку подписи (либо нажмите кнопку вызова меню справа), в меню выберите пункт **Удалить подпись**.

3 В окне подтверждения нажмите кнопку **Да**. Электронная подпись будет удалена из документа.

Microsoft Office 2013

Чтобы удалить электронную подпись из документа Microsoft Word, Excel или PowerPoint, выполните следующие действия:

1 Откройте панель **Подписи**. Для этого откройте вкладку **Файл** и в разделе **Сведения** нажмите кнопку **Просмотр подписей**.

Примечание. Вы можете также вызвать панель **Подписи**, щелкнув в строке состояния документа значок электронной подписи  .

---

2 На панели **Подписи** (см. Рисунок 61 на стр. 118) щелкните правой кнопкой мыши строку подписи (либо нажмите кнопку вызова меню справа), в меню выберите пункт **Удалить подпись**.

3 В окне подтверждения нажмите кнопку **Да**. Электронная подпись будет удалена из документа.

Видимая строка подписи в документах Microsoft Word и Excel

Приложения Microsoft Word и Microsoft Excel позволяют вставить в документ одну или несколько видимых строк подписи. Такая строка выглядит как место для подписи в бумажном документе и одновременно с видимым представлением подписи в документе добавляет электронную подпись для удостоверения личности подписавшего.

Вставка видимой строки подписи

Чтобы добавить в документ видимую строку для подписи, выполните следующие действия:

1. Поместите курсор в то место документа, куда требуется вставить строку подписи.
2. На вкладке **Вставка** в группе **Текст** нажмите кнопку **Строка подписи**. Откроется окно **Настройка подписи**.

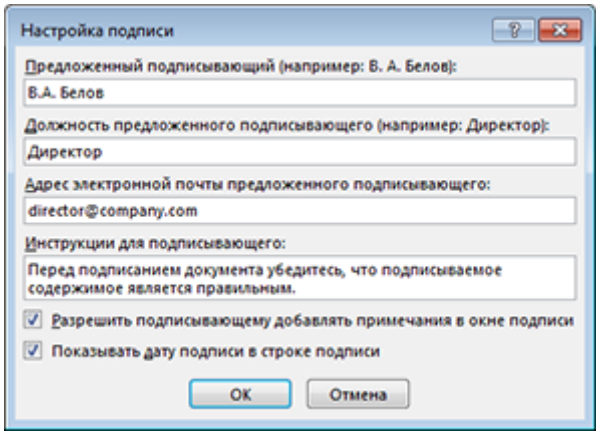


Рисунок 63. Окно «Настройка подписи»

3. Заполните поля **Предложенный подписывающий**, **Должность предложенного подписывающего**, **Адрес электронной почты предложенного подписывающего**. Вы можете ввести краткие инструкции для подписывающего, а также разрешить подписывающему добавлять примечания в окне подписи и включить отображение даты подписи (установив соответствующие флажки).
4. Выполнив настройку подписи, нажмите кнопку **OK**. В документ будет вставлена пустая строка для подписи, которая также будет отображаться на панели **Подписи**.

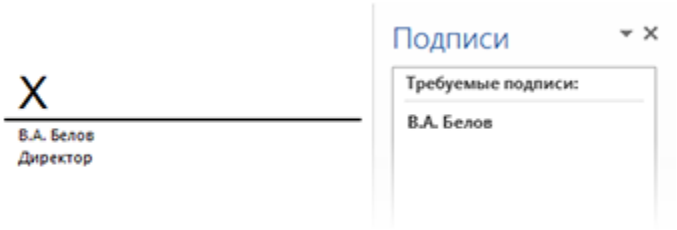


Рисунок 64. Видимая строка подписи и ее представление на панели «Подписи» в Microsoft Word 2013

До того как в строку подписи будет добавлена электронная подпись, вы можете изменить ее настройки. Для этого выполните следующие действия:

1 Щелкните правой кнопкой мыши строку подписи и в контекстном меню выберите пункт **Настройка подписи**.

2 В окне **Настройка подписи** (см. Рисунок 63 на стр. 121) внесите необходимые изменения и нажмите кнопку **ОК**.

Примечание. После подписания документа вы сможете просмотреть свойства подписи в окне **Настройки подписи**, но внесение изменений будет невозможно.

Добавление электронной подписи в строку подписи

В приложениях Microsoft Word и Excel вы можете подписать документ, используя видимую строку подписи.

Чтобы добавить электронную подпись в строку подписи, выполните следующие действия:

1 Щелкните правой кнопкой мыши строку подписи и в контекстном меню выберите пункт **Подписать**.

2 В окне **Подписание** введите свое имя либо щелкните ссылку **Выбрать рисунок**, чтобы вставить графическое изображение подписи. Ниже дано краткое описание сертификата, которым предполагается подписать документ. Чтобы подписать документ другим сертификатом, нажмите кнопку **Изменить** и выберите сертификат.

   В программе Microsoft Word или Excel версии 2013 в данном окне вы можете также выполнить следующие действия:

   - В поле **Тип подтверждения** выбрать одну из заданных причин подписания документа.
   - В поле **Цель подписания документа** указать цель подписания документа.
   - При необходимости нажать кнопку **Сведения** и добавить дополнительные сведения о подписавшем.

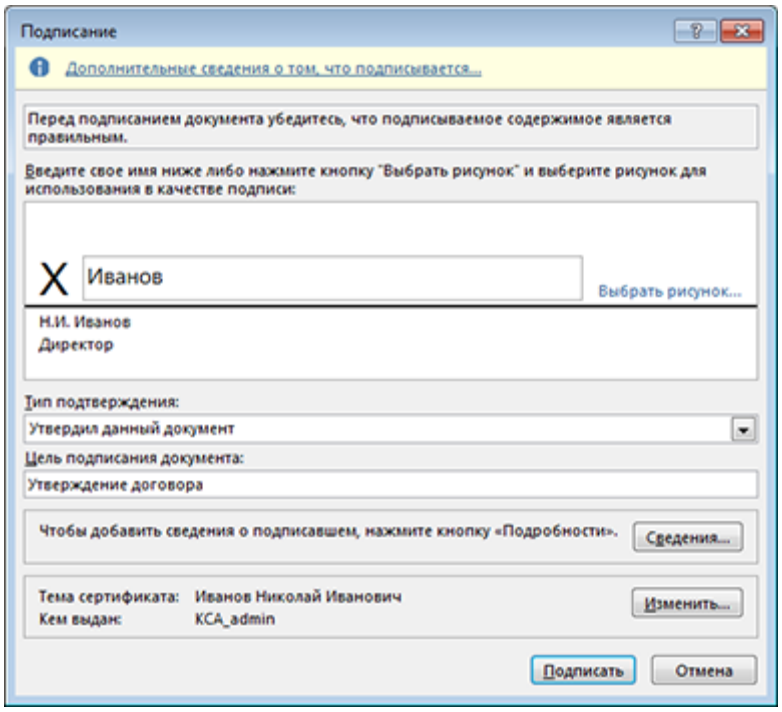


Рисунок 65. Подписание строки подписи в приложениях Microsoft Office 2013

3 После ввода имени и выбора сертификата нажмите кнопку **Подписать**. Откроется диалоговое окно **ViPNet CSP – пароль контейнера ключей** (см. Рисунок 42 на стр. 85).

4 Введите пароль и нажмите кнопку **OK**. В строке подписи появится имя подписавшего или графическое изображение его подписи.

Если по каким-либо причинам не удалось проверить надежность сертификата подписи, над строкой подписи будет стоять пометка **Недействительная подпись**.

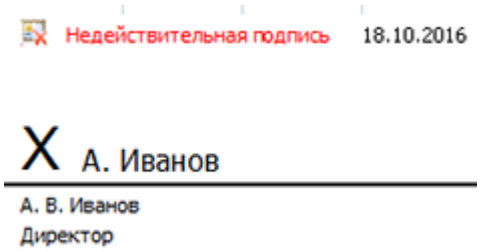


Рисунок 66. Недействительная подпись

Примечание. Строку с недействительной подписью можно подписать еще раз. Для этого щелкните правой кнопкой мыши строку подписи (или название подписи на панели **Подписи**) и выберите пункт **Подписать еще раз**.

Просмотреть состав подписи (см. «Просмотр электронной подписи в Microsoft Word, Excel и PowerPoint» на стр. 117) или удалить подпись (см. «Удаление электронной подписи в Microsoft Word, Excel и PowerPoint» на стр. 120) из видимой строки подписи можно так же, как в случае невидимой подписи.

12

Электронная подпись и шифрование в Microsoft Outlook

Порядок организации обмена защищенными сообщениями

В данном разделе описывается взаимодействие ViPNet CSP с почтовой программой Microsoft Office Outlook (2010 или 2013). Для того чтобы организовать обмен защищенными сообщениями с помощью ViPNet CSP в этой программе, выполните следующие действия:

1. Установите (см. «Способы установки закрытого ключа и сертификата» на стр. 65) контейнер ключей и сертификат в программе ViPNet CSP, а также сертификат издателя и список аннулированных сертификатов (см. «Установка сертификата издателя и списка аннулированных сертификатов» на стр. 78).
2. Обменяйтесь сертификатами с получателем (отправителем) сообщения (см. «Обмен сертификатами с получателем сообщения» на стр. 126).
3. При необходимости настройте почтовую программу для работы с цифровой подписью и зашифрованными сообщениями (см. «Настройка дополнительных параметров электронной подписи и шифрования» на стр. 128).
4. В зависимости от того, являетесь ли вы отправителем или получателем зашифрованного сообщения, выполните следующие действия:
   - Подпишите сообщение электронной подписью (см. «Добавление электронной подписи ко всем сообщениям» на стр. 130, «Добавление электронной подписи к отдельному сообщению» на стр. 133).
   - Создайте и отправьте зашифрованное сообщение (см. «Шифрование сообщений электронной почты» на стр. 137).
   - Расшифруйте полученное сообщение (см. «Просмотр зашифрованных сообщений» на стр. 139).

Внимание! Чтобы подписывать сообщения электронной почты, необходимо иметь сертификат электронной подписи, в котором указан адрес электронной почты владельца сертификата и присутствует расширение «Защищенная электронная почта» в поле «Расширенное использование ключа» («Улучшенный ключ»). Если такого сертификата нет, добавление электронной подписи к сообщению будет невозможно.

Чтобы получить возможность подписания сообщений электронной почты, создайте запрос на новый сертификат, укажите в нем адрес электронной почты и передайте запрос администратору вашего удостоверяющего центра.

Кроме обмена зашифрованными сообщениями электронной почты, с помощью программы Microsoft Outlook можно шифровать документы и файлы (см. «Шифрование документов и файлов» на стр. 140).

Обмен сертификатами с получателем сообщения

Чтобы зашифровать сообщение электронной почты для определенного получателя, вам необходим сертификат этого получателя. Обмен сертификатами может быть произведен одним из следующих способов:

- Путем отправки сообщения с электронной подписью (см. «Добавление электронной подписи к отдельному сообщению» на стр. 133). Добавляя имя отправителя в контакты, получатель тем самым добавляет сертификат отправителя.
- Путем отправки файла сертификата (с расширением `.cer`) получателю в сообщении электронной почты, на внешнем носителе или размещения его в общедоступном сетевом хранилище. Это дает возможность получателю импортировать CER-файл в контакт.
- Путем создания контакта с CER-файлом и его отправка.

Внимание! Сертификат получателя и ваш сертификат должны содержать адреса электронной почты владельцев (см. «Адрес электронной почты из сертификата не найден в списке адресов контакта» на стр. 171).

Чтобы импортировать сертификат в карточку контактов, в программе Microsoft Outlook выполните следующие действия:

1. Откройте представление **Контакты** (в Microsoft Outlook 2013 — представление **Люди**).
2. Двойным щелчком откройте нужный контакт.
3. Откройте окно управления сертификатами пользователя, для этого выполните следующие действия:
   - В программе Microsoft Outlook 2010 на вкладке **Контакт** в группе **Показать** нажмите кнопку **Сертификаты**  .
   - В программе Microsoft Outlook 2013 на вкладке **Контакт** в группе **Показ** нажмите кнопку **Сертификаты**  .
4. Нажмите кнопку **Импорт**.
5. В окне **Поиск сертификата** укажите путь к файлу сертификата и нажмите кнопку **Открыть**.

   Выбранный сертификат будет добавлен к данному контакту.

Внимание! Если после импорта сертификата появилось сообщение о том, что адрес электронной почты из сертификата не найден в списке (см. «Адрес электронной почты из сертификата не найден в списке адресов контакта» на стр. 171), то зашифровать письмо с помощью данного сертификата не удастся.

6 Чтобы убедиться, что добавленный сертификат является доверенным, выберите его и нажмите кнопку **Свойства**.

   Если в окне **Свойства сертификата** на вкладке **Общие** отображается значок  или , то сертификат не является доверенным.

7 Если сертификат не является доверенным, в окне **Свойства сертификата** откройте вкладку **Доверие** и в группе **Изменение правил доверия** выберите вариант **Явно доверять этому сертификату**. Затем нажмите кнопку **OK**.

Чтобы отправить карточку контакта с сертификатом, выполните следующие действия:

1 В программе Microsoft Outlook создайте новый контакт и заполните карточку своими данными.

2 Импортируйте в контакт ваш сертификат.

3 В контекстном меню контакта выберите пункт **Переслать контакт** и затем **Как контакт Outlook**.

4 В окне письма укажите адрес получателя, добавьте сопроводительный текст и нажмите **Отправить**.

После того как вы обменялись сертификатами с получателем, можно приступать к отправке зашифрованных сообщений.

Настройка дополнительных параметров электронной подписи и шифрования

В программе Microsoft Outlook для выбора сертификатов подписи и шифрования, формата криптографии и настройки других параметров выполните следующие действия:

1 Вызовите окно **Изменения настройки безопасности**, для этого откройте вкладку **Файл** и выберите пункт **Параметры**. В окне **Параметры Outlook** выберите раздел **Центр управления безопасностью** и нажмите кнопку **Параметры центра управления безопасностью**. В окне **Центр управления безопасностью** выберите раздел **Защита электронной почты** и нажмите кнопку **Параметры**.

2 В списке **Формат криптографии** выберите значение **S/MIME** (см. глоссарий, стр. 229).

3 Нажмите **Выбрать** напротив поля **Сертификат подписи** и укажите нужный сертификат.

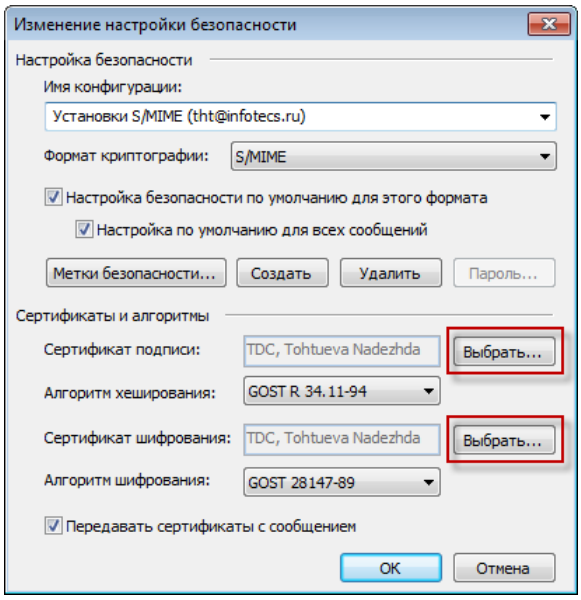


Рисунок 67. Выбор сертификатов для подписи и шифрования

4 Нажмите кнопку **Выбрать** напротив поля **Сертификат шифрования** и укажите нужный сертификат.

Внимание! Если выбранный для создания электронной подписи сертификат не содержит адреса электронной почты или адрес не совпадает с адресом отправки сообщения электронной почты, Microsoft Outlook не позволит выбрать данный сертификат в качестве сертификата электронной подписи.

Если выбранный сертификат не содержит электронного адреса отправки сообщения, возможны следующие сценарии:

- В хранилище операционной системы имеется другой сертификат с адресом электронной почты, который совпадает с адресом отправки сообщения электронной почты. При подписании сообщения электронной почты электронная подпись будет создана с помощью этого сертификата, а не указанного ранее.
- В хранилище операционной системы нет других сертификатов с адресом электронной почты, который бы совпадал с адресом отправки сообщения. При попытке подписания сообщения электронная подпись добавлена не будет.

Чтобы получить возможность подписания сообщений электронной почты сертификатом, создайте запрос на новый сертификат, укажите в нем корректный адрес электронной почты и передайте запрос администратору вашего удостоверяющего центра.

5 Если требуется, настройте остальные параметры и нажмите кнопку **OK**.

Добавление электронной подписи ко всем сообщениям

Программа Microsoft Outlook позволяет добавлять в сообщения электронной почты электронную подпись, чтобы гарантировать подлинность и целостность сообщения, а также обеспечить неотрекаемость. Чтобы обеспечить конфиденциальность сообщения, его нужно зашифровать (см. «Шифрование сообщений электронной почты» на стр. 137).

Примечание. Более подробные сведения о защите электронной почты средствами криптографии можно получить на веб-узле Office Online (http://office.microsoft.com/ru-ru/outlook-help/HA102748945.aspx?CTT=1).

Ниже описано, как настроить добавление электронной подписи к исходящим сообщениям в программе Microsoft Outlook.

Внимание! Чтобы подписывать сообщения электронной почты, необходимо иметь сертификат электронной подписи, в котором указан адрес электронной почты владельца сертификата и присутствует расширение «Защищенная электронная почта» в поле «Расширенное использование ключа» («Улучшенный ключ»). Если такого сертификата нет, добавление электронной подписи к сообщению будет невозможно.

Чтобы получить возможность подписания сообщений электронной почты, создайте запрос на новый сертификат, укажите в нем адрес электронной почты и передайте запрос администратору вашего удостоверяющего центра.

Чтобы добавлять электронную подпись ко всем сообщениям, выполните следующие действия:

1. Откройте окно управления безопасностью электронной почты:
   - Откройте вкладку **Файл** и выберите пункт **Параметры**. В окне **Параметры Outlook** выберите раздел **Центр управления безопасностью** и нажмите кнопку **Параметры центра управления безопасностью**.
   - В окне **Центр управления безопасностью** перейдите в раздел **Защита электронной почты**.
2. В группе **Шифрованная электронная почта** установите флажок **Добавлять цифровую подпись к исходящим сообщениям**.

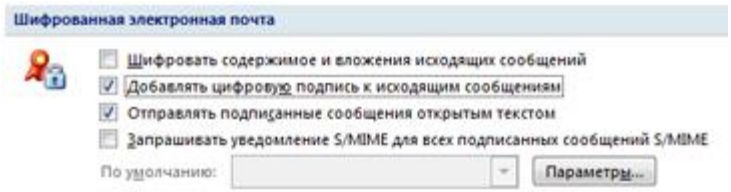


Рисунок 68. Группа «Шифрованная электронная почта» в окне управления безопасностью

3 Убедитесь, что установлен флажок **Отправлять подписанные сообщения открытым текстом** (иначе получатели, не использующие протокол S/MIME, не смогут прочесть сообщение).

4 Нажмите кнопку **Параметры**. Откроется окно **Изменение настройки безопасности**.

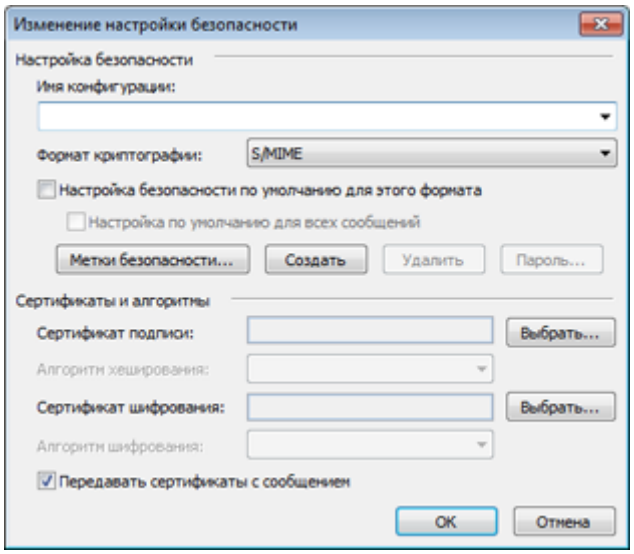


Рисунок 69. Окно «Изменение настройки безопасности»

5 Заполните поле **Имя конфигурации**.

6 Нажмите кнопку **Выбрать** напротив поля **Сертификат подписи**.

7 В окне **Выбор сертификата** выберите сертификат из списка. Чтобы просмотреть выбранный сертификат, щелкните ссылку **Просмотреть свойства сертификата**.

Выбрав сертификат подписи, нажмите кнопку **OK**. Тот же сертификат автоматически будет задан для шифрования сообщений.

Внимание! Если выбранный для создания электронной подписи сертификат не содержит адреса электронной почты или адрес не совпадает с адресом отправки сообщения электронной почты, Microsoft Outlook не позволит выбрать данный сертификат в качестве сертификата электронной подписи.

Если выбранный сертификат не содержит электронного адреса отправки сообщения, возможны следующие сценарии:

- В хранилище операционной системы имеется другой сертификат с адресом электронной почты, который совпадает с адресом отправки сообщения электронной почты. При

подписании сообщения электронной почты электронная подпись будет создана с помощью этого сертификата, а не указанного ранее.

- В хранилище операционной системы нет других сертификатов с адресом электронной почты, который бы совпадал с адресом отправки сообщения. При попытке подписания сообщения электронная подпись добавлена не будет.

Чтобы получить возможность подписания сообщений электронной почты сертификатом, создайте запрос на новый сертификат, укажите в нем корректный адрес электронной почты и передайте запрос администратору вашего удостоверяющего центра.

8 Чтобы сохранить настройки, дважды нажмите кнопку **OK**.

Добавление электронной подписи к отдельному сообщению

Чтобы добавить электронную подпись к отдельному сообщению, выполните действия, описанные ниже.

Внимание! Чтобы подписывать сообщения электронной почты, необходимо иметь сертификат электронной подписи, в котором указан адрес электронной почты владельца сертификата и присутствует расширение «Защищенная электронная почта» в поле «Расширенное использование ключа» («Улучшенный ключ»). Если такого сертификата нет, добавление электронной подписи к сообщению будет невозможно.

Чтобы получить возможность подписания сообщений электронной почты, создайте запрос на новый сертификат, укажите в нем адрес электронной почты и передайте запрос администратору вашего удостоверяющего центра.

Чтобы подписать сообщение электронной подписью, выполните следующие действия:

1 Создайте новое сообщение и в зависимости от версии программы Microsoft Outlook выполните одно из действий:

- в программе Microsoft Outlook 2010 откройте вкладку **Параметры** и в группе **Разрешение** нажмите кнопку **Подписать** ;
- в программе Microsoft Outlook 2013 откройте вкладку **Параметры** и в группе **Разрешение** нажмите кнопку **Подписать** .

Примечание. Кнопка **Сообщение с цифровой подписью** или **Подписать** ( ) может отсутствовать на панели инструментов, если предварительно в окне **Изменение настроек безопасности** не был выбран сертификат электронной подписи, используемый по умолчанию (см. «Добавление электронной подписи ко всем сообщениям» на стр. 130).

---

2 Если на панели инструментов нет кнопки **Сообщение с цифровой подписью** (или кнопки **Подписать** (**Подписать**)), выполните следующие действия:

2.1 Откройте окно **Свойства безопасности**. Для этого в программе Microsoft Outlook откройте вкладку **Параметры** и в группе **Дополнительные параметры** нажмите кнопку вызова диалогового окна **Свойства** . В окне **Свойства** нажмите кнопку **Параметры безопасности**.

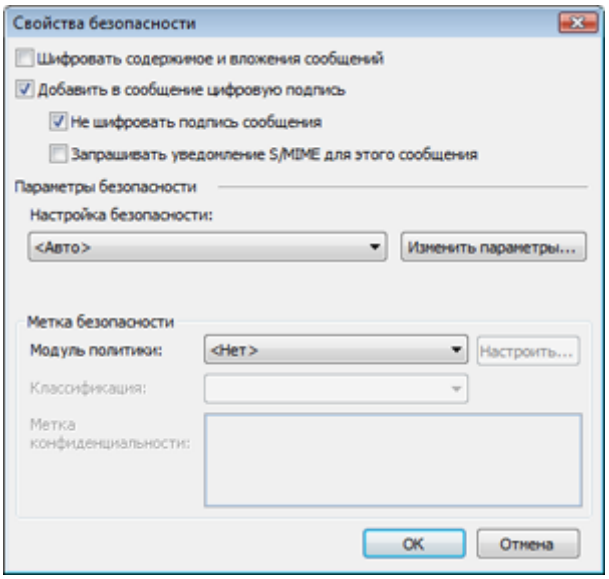


Рисунок 70. Окно «Свойства безопасности»

2.2 Установите флажок **Добавить в сообщение цифровую подпись**.

2.3 При необходимости в списке **Настройка безопасности** выберите предустановленные параметры электронной подписи и шифрования.

2.4 По умолчанию в списке **Настройка безопасности** установлено значение **<Авто>**. Это значит, что сертификат электронной подписи будет выбран автоматически. Чтобы выбрать сертификат самостоятельно, нажмите кнопку **Изменить параметры** (см. «Настройка дополнительных параметров электронной подписи и шифрования» на стр. 128).

2.5 Чтобы сохранить настройки, нажмите кнопку **OK**.

3 Введите текст сообщения, укажите тему и адресата. Если требуется, добавьте вложения.

4 Нажмите кнопку **Отправить**. Откроется окно **ViPNet CSP – пароль контейнера ключей** (см. Рисунок 42 на стр. 85).

5 Введите пароль и нажмите кнопку **OK**.

Примечание. В некоторых случаях может потребоваться ввести пароль несколько раз.

Просмотр электронной подписи сообщения

Для проверки электронной подписи сообщения в программе Microsoft Outlook выполните следующие действия:

1 Откройте сообщение с электронной подписью.

2 В строке **Подписано** проверьте адрес электронной почты лица, подписавшего сообщение.

Рисунок 71. Проверка электронной подписи в сообщении

Внимание! Если адрес электронной почты в строке **Подписано** не совпадает с адресом отправителя в строке **От**, то истинным отправителем сообщения следует считать подписавшее его лицо.

Если при проверке электронной подписи возникли какие-либо проблемы, строка **Подписано** подчеркнута красной линией.

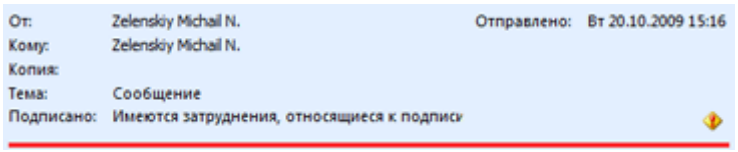


Рисунок 72. Сообщение с недействительной электронной подписью

3 Чтобы получить более подробную информацию об электронной подписи, нажмите кнопку **Цифровая подпись** . Откроется окно **Цифровая подпись: правильная**. Если электронная подпись, содержащаяся в сообщении, недействительна, откроется окно **Цифровая подпись: неправильная**.

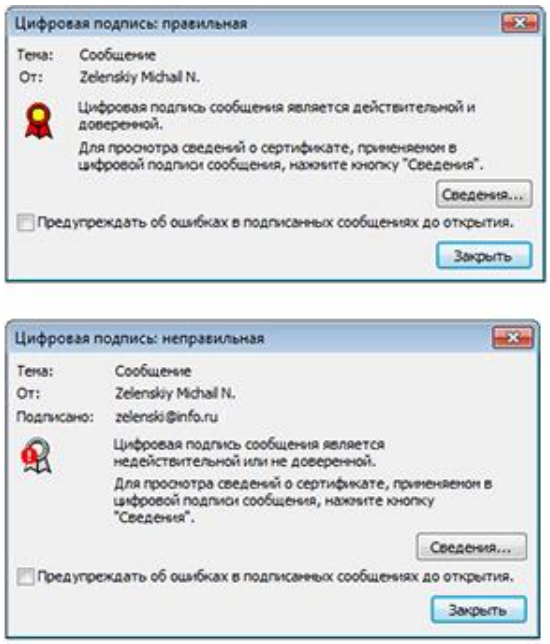


Рисунок 73. Сведения о действительности электронной подписи

4 Чтобы получить информацию о сертификате подписи, нажмите кнопку **Сведения**.

Шифрование сообщений электронной почты

Для шифрования отдельного сообщения в программе Microsoft Outlook выполните следующие действия:

1. Создайте новое сообщение и укажите нужного получателя.
2. Установите функцию шифрования одним из способов:
   - В окне сообщения откройте вкладку **Параметры** и в группе **Разрешения** нажмите кнопку **Шифровать** (**Шифровать**).
   - В окне сообщения откройте вкладку **Параметры** и в группе **Дополнительные параметры** нажмите кнопку вызова диалогового окна **Свойства** . В окне **Свойства** нажмите кнопку **Параметры безопасности**.

     В окне **Свойства безопасности** установите флажок **Шифровать содержимое и вложения сообщений**.

     Чтобы изменить дополнительные параметры настройки (см. «Настройка дополнительных параметров электронной подписи и шифрования» на стр. 128), такие как выбор персонального сертификата из нескольких установленных, нажмите кнопку **Изменить параметры**.
3. Отправьте сообщение.

Для шифрования всех отправляемых сообщений выполните следующие действия:

1. В главном окне программы Microsoft Outlook откройте вкладку **Файл** и выберите пункт **Параметры**.
2. В окне **Параметры Outlook** перейдите в раздел **Центр управления безопасностью** и нажмите кнопку **Параметры центра управления безопасностью**.
3. В окне **Центр управления безопасностью** перейдите в раздел **Защита электронной почты** и в группе **Шифрованная электронная почта** установите флажок **Шифровать содержимое и вложения исходящих сообщений**.

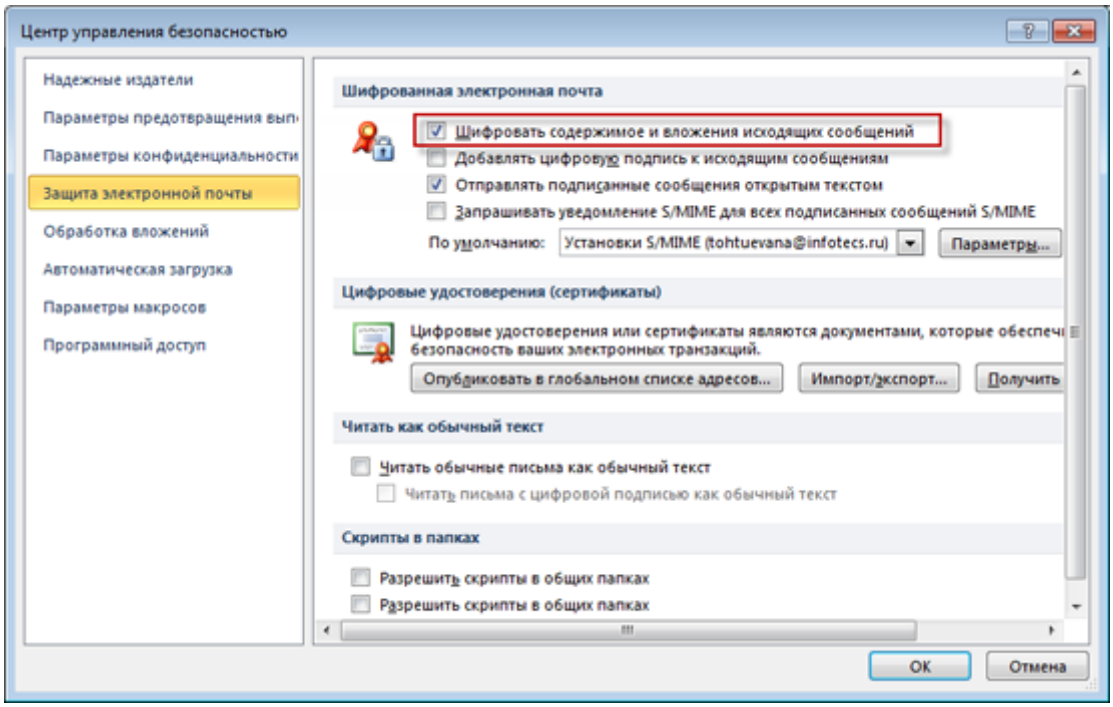


Рисунок 74. Установка параметра для шифрования всех сообщений

4 Чтобы изменить дополнительные параметры настройки (см. «Настройка дополнительных параметров электронной подписи и шифрования» на стр. 128), такие как выбор персонального сертификата из нескольких установленных, нажмите кнопку **Параметры**.

5 Два раза нажмите кнопку **OK**.

6 После этого все отправляемые сообщения будут зашифрованы, если для их получателей в карточке контактов добавлены сертификаты.

Просмотр зашифрованных сообщений

В программе Microsoft Outlook полученное зашифрованное сообщение в списке сообщений отмечено значком  .

При выборе зашифрованного сообщения в области чтения появится предупреждение: «Невозможно отобразить элемент в области чтения. Откройте элемент для чтения его содержимого».

Внимание! Для просмотра зашифрованного сообщения необходима программа ViPNet CSP.

Чтобы просмотреть зашифрованное сообщение, выполните следующие действия:

1. Дважды щелкните нужное сообщение в списке.
2. В окне **ViPNet CSP - пароль контейнера ключей** (см. Рисунок 42 на стр. 85) введите пароль, которым защищен ваш закрытый ключ.

   После этого сообщение со всеми вложениями будет расшифровано и показано на экране.

Шифрование документов и файлов

Если вам необходимо зашифровать определенные документы или файлы, воспользуйтесь следующим способом:

1. Создайте зашифрованное сообщение (см. «Шифрование сообщений электронной почты» на стр. 137).
2. В качестве вложений укажите нужные документы или файлы.
3. Отправьте сообщение на адрес получателя или на свой адрес. В первом случае зашифрованные документы сможет просмотреть только указанный вами получатель, во втором — только вы.

13

Электронная подпись макросов, форм и баз данных

Электронная подпись в Microsoft Office InfoPath

Разрешение подписывать форму InfoPath электронной подписью

При создании шаблона формы Microsoft Office InfoPath вы можете разрешить добавление к форме электронной подписи. Заполнив форму, пользователи смогут подписать всю форму или отдельные ее части.

Чтобы разрешить пользователям подписывать форму Microsoft Office InfoPath 2010 и 2013, выполните следующие действия:

1. В приложении Microsoft InfoPath Designer создайте или откройте шаблон формы.
2. На вкладке **Файл** в разделе **Сведения** нажмите кнопку **Параметры формы**.
3. В окне **Параметры формы** откройте раздел **Цифровые подписи**.

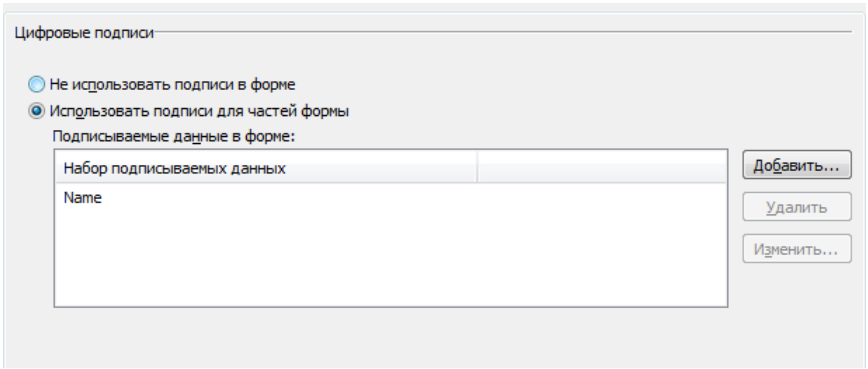


Рисунок 75. Вкладка «Цифровые подписи»

4. Чтобы указать подписываемые данные, нажмите кнопку **Добавить**.
5. В окне **Набор подписываемых данных** выполните следующие действия:
   - Введите имя для подписываемых данных в соответствующее поле.
   - Нажмите кнопку **Выбрать XPath** рядом с полем **Подписываемые поля и группы**.
   - В окне **Выбор поля или группы** выберите подписываемое поле и нажмите кнопку **ОК**.
   - Вы также можете указать тип взаимосвязи между несколькими подписями, установив переключатель в желаемое положение (по умолчанию **Допускать использование только одной подписи**) и добавить сообщение для подтверждения подписи.
   - Выполнив необходимые настройки, нажмите кнопку **ОК**. Выбранное поле появится в списке **Набор подписываемых данных**.

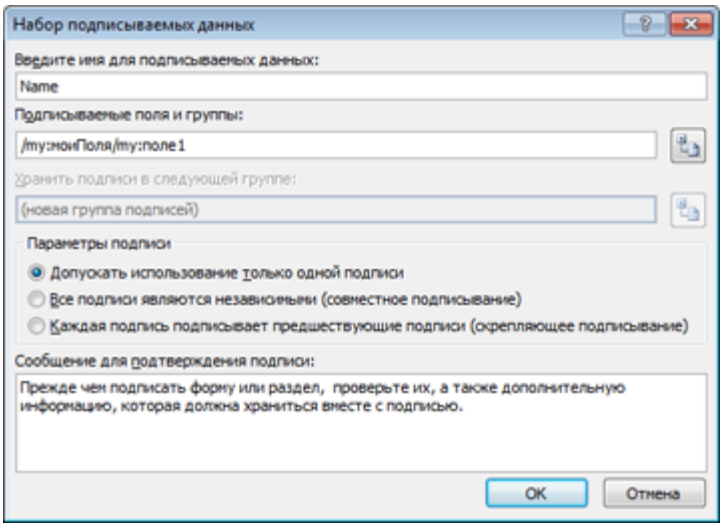


Рисунок 76. Окно «Набор подписываемых данных»

6 Чтобы сохранить настройки, нажмите кнопку **OK**.

Подписание формы InfoPath

Если при создании формы была предусмотрена возможность ее подписания, пользователь сможет добавить к форме свою электронную подпись. Чтобы подписать форму, выполните следующие действия:

1 Откройте форму или шаблон формы в программе InfoPath Filler 2010 или InfoPath Filler 2013.

2 Откройте вкладку **Файл** и в разделе **Сведения** нажмите кнопку **Подписать форму**.

Откроется окно **Цифровые подписи**.

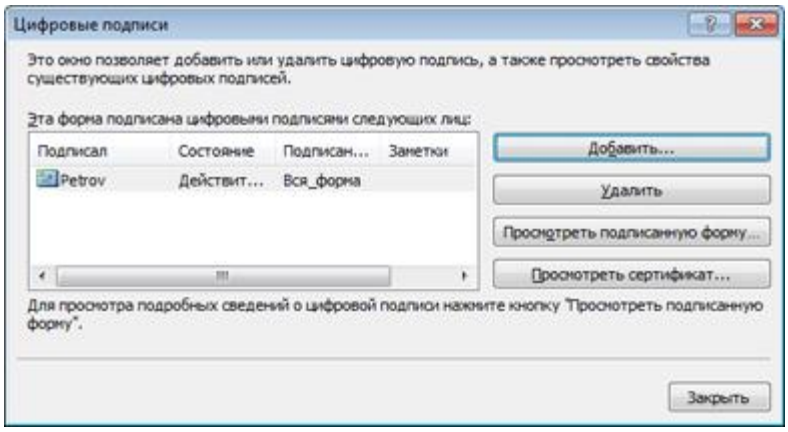


Рисунок 77. Окно «Цифровые подписи»

3 Нажмите кнопку **Добавить**. Откроется окно **Выбор данных для подписания**.

4 Если электронная подпись применяется для всей формы, выберите единственный пункт списка — **Вся_форма**. Если подпись применяется для отдельных данных, выберите из списка подписываемые данные.

5 Нажмите кнопку **OK**, откроется диалоговое окно **Подписание** (см. Рисунок 65 на стр. 123).

6 Если вы подписываете отдельные данные, введите свое имя в поле рядом с крестиком или щелкните ссылку **Выбрать рисунок**, чтобы вставить графическое изображение подписи.

7 При необходимости заполните поле **Цель подписания документа**. В программе InfoPath Filler 2013 в этом окне вы также при необходимости можете выбрать причину подписания из нескольких заданных вариантов в списке **Тип подтверждения**.

8 В нижней части окна **Подписание** приведены краткие сведения о сертификате, которым предполагается подписать данные. Если вы хотите подписаться другим сертификатом, нажмите кнопку **Изменить** и выберите сертификат.

9 Нажмите кнопку **Подписать**, откроется окно **ViPNet CSP – пароль контейнера ключей** (см. Рисунок 42 на стр. 85).

10 Введите пароль и нажмите кнопку **OK**.

После подписания внесение изменений в форму (или в поля) будет невозможно.

Просмотр подписи в форме InfoPath

Чтобы просмотреть подпись в форме Microsoft InfoPath, выполните следующие действия:

1 Откройте вкладку **Файл** и в разделе **Сведения** нажмите кнопку **Просмотр подписей**.

Откроется окно **Цифровые подписи**.

2 Если вы используете Microsoft InfoPath Filler 2010, выберите электронную подпись из списка и нажмите кнопку **Просмотреть подписанную форму**. Откроется окно **Состав подписи** (см. Рисунок 60 на стр. 118).

Если вы используете Microsoft InfoPath Filler 2013, выберите электронную подпись из списка и нажмите кнопку **Просмотреть подпись**. Откроется окно **Состав подписи** (см. Рисунок 60 на стр. 118).

- В окне **Состав подписи** содержатся краткие сведения о подписи и сертификате. Если при проверке сертификата возникли ошибки, сообщение об этом будет выведено под заголовком окна.
- Чтобы открыть сертификат, нажмите кнопку **Просмотр**.

Удаление подписи из формы InfoPath

Чтобы удалить подпись из формы Microsoft InfoPath, выполните следующие действия:

1 Откройте вкладку **Файл** и в разделе **Сведения** нажмите кнопку **Просмотр подписи**.

Откроется окно **Цифровые подписи**.

2 Выберите электронную подпись из списка. Чтобы просмотреть подпись перед удалением, нажмите кнопку **Просмотреть подпись**.

3 Выбрав электронную подпись, нажмите кнопку **Удалить**.

4 В окне подтверждения нажмите кнопку **Да**. Электронная подпись будет удалена из формы.

Электронная подпись макросов

Подписание макросов

Создав макрос в приложениях Microsoft Office, вы можете заверить его электронной подписью. Электронная подпись позволяет подтвердить происхождение макроса и его безопасность. Создать и подписать макрос позволяют приложения Microsoft Word, Excel, Outlook, PowerPoint, Publisher и Visio.

Внимание! Чтобы подписать макрос, нужно иметь сертификат с расширением «Подписывание кода» в поле «Расширенное использование ключа» («Улучшенный ключ»). Если такого сертификата нет, вы не сможете добавить электронную подпись к макросу. Для получения нужного сертификата обратитесь к администратору программы ViPNet Удостоверяющий и ключевой центр (см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора»).

Чтобы подписать макрос, выполните следующие действия:

1 Откройте редактор Microsoft Visual Basic. Для этого в приложении Microsoft Office Outlook, Publisher, Visio, Word, Excel или PowerPoint на вкладке **Разработчик** в группе **Код** нажмите кнопку **Visual Basic**.

2

Примечание. Вкладка **Разработчик** по умолчанию не отображается. Чтобы она появилась, в меню **Файл** выберите пункт **Параметры** и в открывшемся окне в разделе **Настроить ленту** добавьте вкладку **Разработчик**.

В любом из перечисленных приложений для вызова редактора Microsoft Visual Basic можно также воспользоваться сочетанием клавиш **Alt**+**F11**.

---

3 В окне редактора Microsoft Visual Basic в меню **Tools** (**Сервис**) выберите пункт **Digital Signature** (**Цифровая подпись**). Откроется окно **Цифровая подпись**.

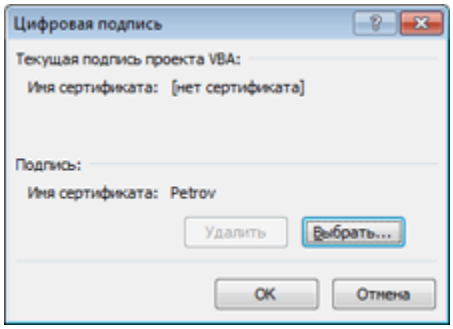


Рисунок 78. Добавление электронной подписи

4 Нажмите кнопку **Выбрать**, в открывшемся списке выберите сертификат электронной подписи и нажмите кнопку **OK**. Электронная подпись будет добавлена к макросу.

Проверка подписи макроса

Чтобы проверить электронную подпись макроса, выполните следующие действия:

1 В окне редактора Microsoft Visual Basic в меню **Сервис** выберите пункт **Цифровая подпись**. Откроется окно **Цифровая подпись**.

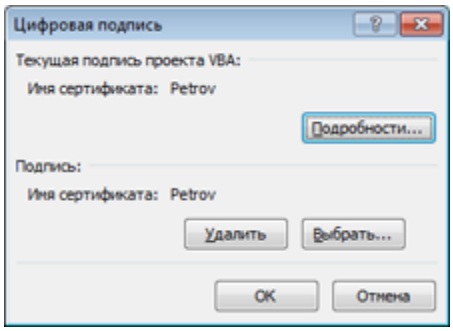


Рисунок 79. Окно «Цифровая подпись»

2 В окне **Цифровая подпись** указан текущий сертификат подписи. Чтобы просмотреть сертификат, нажмите кнопку **Подробности**.

Если сертификат ненадежен, то на вкладке **Общее** в окне **Сертификат** будет выведено сообщение о возникшей проблеме. Ненадежный сертификат помечается красным крестом.

Удаление подписи макроса

Чтобы удалить электронную подпись из проекта макроса, выполните следующие действия:

1 В окне редактора Microsoft Visual Basic в меню **Сервис** выберите пункт **Цифровая подпись**. Откроется окно **Цифровая подпись** (см. Рисунок 79 на стр. 147).

2 Чтобы удалить электронную подпись, нажмите кнопку **Удалить**. Электронная подпись будет удалена из проекта.

Подписание базы данных Microsoft Access

В приложении Microsoft Access предусмотрена возможность подписания базы данных при публикации. После создания файла базы данных в формате Microsoft Access его можно упаковать, добавить электронную подпись, а затем распространить подписанный пакет среди других пользователей. Пользователи, получившие пакет, могут извлечь из него базу данных и далее работать с ней.

Чтобы упаковать и подписать базу данных Microsoft Access, выполните следующие действия:

1 В программе Microsoft Access 2010 или 2013 откройте вкладку **Файл** и выберите раздел **Сохранить как** (в Access 2010 —**Сохранить и опубликовать**). В группе **Сохранить базу данных как** щелкните элемент **Упаковать и подписать**, а затем — **Сохранить как**.

   Откроется окно выбора сертификата.

2 Выберите сертификат электронной подписи и нажмите кнопку **ОК**. Откроется окно **Создать подписанный пакет Microsoft Office Access**.

Внимание! Для подписания базы данных электронной подписью необходимо выбрать сертификат, который имеет расширение «Подписывание кода» в поле «Расширенное использование ключа» («Улучшенный ключ»). Если в сертификате в поле «Расширенное использование ключа» не добавлено данное расширение, вы не сможете создать подписанный пакет. За необходимым сертификатом обратитесь к администратору удостоверяющего центра (см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора»).

3 Выберите папку для сохранения подписанного пакета.

4 В поле **Имя файла** введите имя для пакета и нажмите кнопку **Создать**.

   Подписанный пакет базы данных будет сохранен в указанной папке.

14

Организация защищенного соединения TLS

Организация доступа к защищенному веб-серверу

Чтобы с помощью криптопровайдера ViPNet CSP организовать доступ к защищенному веб-серверу, последовательно выполните настройку серверной и клиентской частей:

Таблица 5. Порядок организации доступа к защищенному веб-серверу

	Действие	Ссылка
☐	Настройте сервер IIS.	Настройка серверной части (на стр. 150)
☐	Установите криптопровайдер ViPNet CSP.	
☐	Установите в хранилище сертификатов компьютера сертификат пользователя (сервера), сертификат издателя и актуальный список CRL.	
☐	Установите криптопровайдер ViPNet CSP.	Настройка клиентской части (на стр. 151)
☐	Установите в хранилище сертификатов пользователя сертификат пользователя (клиента), сертификат издателя и актуальный список CRL.	
☐	При необходимости настройте браузер Internet Explorer для работы по протоколу TLS.	

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

Настройка серверной части

Для настройки серверной части выполните следующие действия:

1. Настройте сервер IIS (см. «Практическое руководство. Создание удаленных веб-узлов IIS» в библиотеке MSDN (https://msdn.microsoft.com/ru-ru/library/25fz9ck5%28v=vs.100%29.aspx)).
2. Установите криптопровайдер ViPNet CSP (см. «Установка и запуск программы» на стр. 28).
3. Создайте запрос на сертификат для веб-сервера IIS (см. «Создание запроса на сертификат и формирование закрытого ключа» на стр. 57) (используйте шаблон сертификата **Веб-сервер**) и отправьте его в удостоверяющий центр.
4. Получите у администратора удостоверяющего центра сертификат для сервера IIS, изданный по запросу, а также сертификат издателя и список аннулированных сертификатов (CRL).

Внимание! Сертификат пользователя для сервера должен иметь расширение «Шифрование данных» в поле «Использование ключа» и расширение «Проверка подлинности сервера» в поле «Расширенное использование ключа» («Улучшенный ключ»).

5 Установите полученный сертификат для сервера в контейнер ключей (см. «Установка сертификата в контейнер ключей» на стр. 70).

6 Установите в хранилище сертификатов локального компьютера сертификат сервера (см. «Установка сертификата в системное хранилище Windows» на стр. 72), а также сертификат издателя и список CRL (см. «Установка сертификата издателя и списка аннулированных сертификатов» на стр. 78).

7 Настройте права доступа к контейнеру ключей (см. «Настройка прав доступа к контейнеру ключей» на стр. 85). Мы рекомендуем задать следующие права:

- Для группы SYSTEM — **Полный доступ**, **Чтение**.
- Для группы Administrators — **Полный доступ**, **Чтение**.
- Для встроенной учетной записи, под которой работает приложение (LOCAL SYSTEM, LOCAL SERVICE, NETWORK SERVICE или IIS AppPool\Имя пула), — **Полный доступ**, **Чтение**.

8 Проверьте доступность веб-узла по защищенному протоколу HTTPS (см. «Проверка доступности веб-узла по защищенному протоколу HTTPS» на стр. 154).

Настройка клиентской части

Для настройки клиентской части выполните следующие действия:

1 Установите программу ViPNet CSP (см. «Установка и запуск программы» на стр. 28).

2 Создайте запрос на сертификат пользователя (см. «Создание запроса на сертификат и формирование закрытого ключа» на стр. 57) и отправьте его в удостоверяющий центр.

3 Получите у администратора удостоверяющего центра сертификат для веб-клиента, изданный по запросу, а также сертификат издателя и список CRL.

Внимание! Сертификат пользователя для веб-клиента должен иметь расширение «Проверка подлинности клиента» в поле «Расширенное использование ключа» («Улучшенный ключ»).

4 Установите полученный сертификат для клиента в контейнер ключей (см. «Установка сертификата в контейнер ключей» на стр. 70).

5 Установите в хранилище сертификатов текущего пользователя сертификат для веб-клиента (см. «Установка сертификата в системное хранилище Windows» на стр. 72), а также сертификат издателя и список CRL (см. «Установка сертификата издателя и списка аннулированных сертификатов» на стр. 78).

6 Выполните настройку веб-браузера Internet Explorer для работы по защищенному протоколу (см. «Настройка веб-браузера Internet Explorer для работы по протоколу TLS» на стр. 153).

7 Проверьте доступность веб-узла по защищенному протоколу HTTPS (см. «Проверка доступности веб-узла по защищенному протоколу HTTPS» на стр. 154).

Настройка веб-браузера Internet Explorer для работы по протоколу TLS

Примечание. В веб-браузере Google Chrome 26 и более поздних версий организовать защищенное соединение TLS с помощью криптопровайдера ViPNet CSP невозможно.

Настройки веб-браузера Internet Explorer по умолчанию позволяют работать по протоколу TLS. Если настройки браузера отличны от первоначальных или соединение с сервером не происходит, выполните следующие действия:

1. В меню **Сервис** веб-браузера Internet Explorer выберите пункт **Свойства обозревателя** (**Свойства браузера**).
2. В окне **Свойства обозревателя** (**Свойства браузера**) выполните следующие действия:
   - Откройте вкладку **Безопасность** и убедитесь, что флажок **Включить защищенный режим** снят.
   - Откройте вкладку **Дополнительно** и убедитесь, что установлены флажки **TLS 1.0** и **Использовать TLS 1.2**.
3. Проверьте доступность веб-узла по защищенному протоколу HTTPS (см. «Проверка доступности веб-узла по защищенному протоколу HTTPS» на стр. 154).

Проверка доступности веб-узла по защищенному протоколу HTTPS

Для доступа к веб-узлу по протоколу HTTPS выполните следующие действия:

1. В адресной строке обозревателя Internet Explorer введите `https://имя_сервера`.
2. При успешном соединении и аутентификации пользователя откроется страница веб-сервера.

Если соединение с веб-сервером установить не удалось, обратитесь к разделу Возможные неполадки и способы их устранения (на стр. 163).

15

Взаимодействие с сервером ViPNet HSM

Общие сведения о ViPNet HSM

Сервер ViPNet HSM (https://infotecs.ru/product/vipnet-hsm-1-0.html) представляет собой программно-аппаратный комплекс типа Hardware Security Module (HSM), предназначенный для выполнения криптографических операций по запросам клиентов, а также для защищенного хранения ключей и конфиденциальных данных клиентов.

Клиентами ViPNet HSM могут быть различные прикладные сервисы, на базе которых развернута инфраструктура открытых ключей (см. глоссарий, стр. 229).

С помощью ViPNet CSP вы можете подключаться к серверу ViPNet HSM и использовать его в качестве хранилища ключей, а также выполнять на сервере криптографические операции.

Подробнее о настройке программно-аппаратного комплекса ViPNet HSM см. документацию продукта ViPNet HSM.

Настройка ViPNet CSP для взаимодействия с сервером ViPNet HSM

Чтобы работать с ключами, хранящимися на сервере ViPNet HSM, предварительно настройте программу ViPNet CSP для взаимодействия с сервером. Для этого выполните следующие действия:

1 Запустите программу ViPNet CSP (см. «Запуск программы» на стр. 40).

2 В окне **ViPNet CSP** перейдите в раздел **Подключаемые устройства** (см. Рисунок 46 на стр. 95).

3 В списке **Подключаемые устройства** выполните следующие действия:

3.1 По умолчанию взаимодействие с сервером ViPNet HSM отключено, поэтому напротив типа устройств **ViPNet HSM** в столбце **Использование** отображается ссылка **Выключено**. Щелкните ссылку **Выключено** и в контекстном меню выберите пункт **Включить**.

3.2 Щелкните ссылку **Включено** и в контекстном меню выберите пункт **Параметры**.

4 В контекстном меню выберите пункт **Параметры**.

5 В окне **Параметры ViPNet HSM** выполните следующие действия:

5.1 В соответствующих полях укажите IP-адрес и порт для подключения к серверу ViPNet HSM.

5.2 Выполните одно из действий:

- Если вы хотите, чтобы к указанному серверу ViPNet HSM мог подключаться только текущий пользователь ОС Windows, в списке **Отображаемые параметры** выберите пункт **пользователя**.
- Если вы хотите, чтобы к указанному серверу ViPNet HSM могли подключаться все пользователи ОС Windows вашего компьютера, в списке **Отображаемые параметры** выберите пункт **общие**.

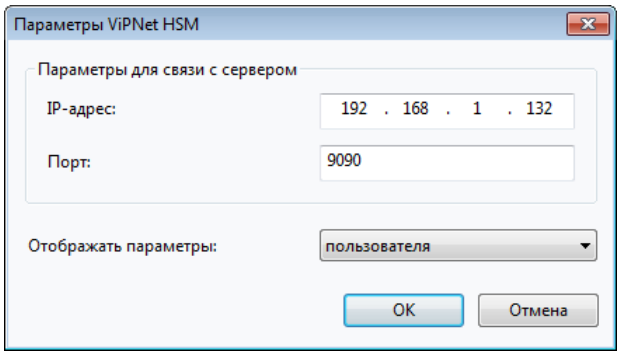


Рисунок 80. Настройка взаимодействия с сервером ViPNet HSM

Предварительная настройка ViPNet CSP для взаимодействия с сервером ViPNet HSM выполнена. Теперь вы можете работать с ключами, хранящимися на сервере ViPNet HSM, как если бы они находились на токене, подключенном к вашему компьютеру (см. «Работа с внешними устройствами» на стр. 93).

16

Работа с универсальной электронной картой

Общие сведения об универсальной электронной карте

Универсальная электронная карта (УЭК) предоставляет своему владельцу возможность получать все государственные и муниципальные услуги, оказываемые в электронной форме согласно законодательству Российской Федерации (см. «Авторизация на Едином портале государственных и муниципальных услуг РФ» на стр. 162). На УЭК содержатся персональные данные гражданина, страховой номер индивидуального лицевого счета в системе обязательного пенсионного страхования (СНИЛС), номер полиса обязательного медицинского страхования (ОМС), данные электронного банковского приложения. Кроме того, на УЭК может размещаться контейнер ключей (см. глоссарий, стр. 230) с квалифицированным сертификатом (см. глоссарий, стр. 230), который дает пользователю возможность совершать юридически значимые действия.

Во время подачи заявления на выдачу УЭК гражданин сам принимает решение о размещении на своей карте средств электронной подписи (см. глоссарий, стр. 232), и сотрудник пункта выдачи карт (ПВК) УЭК записывает контейнер ключей с квалифицированным сертификатом на УЭК.

Чтобы использовать квалифицированный сертификат, записанный на УЭК, вы можете использовать криптопровайдер ViPNet CSP. Для этого необходимо выполнить первоначальную настройку (см. «Настройка ViPNet CSP для взаимодействия с УЭК» на стр. 161).

Настройка ViPNet CSP для взаимодействия с УЭК

Чтобы воспользоваться Единым порталом государственных услуг или подписывать электронные документы с помощью вашей универсальной электронной карты (УЭК) (см. глоссарий, стр. 231), на которой размещены контейнер ключей и квалифицированный сертификат (см. «Работа с универсальной электронной картой» на стр. 159), предварительно установите ПО ViPNet UEC Client (распространяется ОАО «ИнфоТеКС Интернет Траст» (https://iitrust.ru/), рекомендуемая версия — 2.0.5.58).

Внимание! Для работы с картой УЭК на вашем компьютере должен быть доступ в Интернет.

Затем настройте программу ViPNet CSP для работы с УЭК. Для этого выполните следующие действия:

1. Запустите программу ViPNet CSP (см. «Запуск программы» на стр. 40).
2. Подключите к компьютеру любой PC/SC-совместимый считыватель контактных смарт-карт и установите его драйвер.
3. Поместите УЭК в считыватель.
4. В разделе **Контейнеры ключей** (см. Рисунок 31 на стр. 66) главного окна ViPNet CSP в раскрывающемся списке в верхней части окна выберите **UEC**.
5. В списке выберите контейнер ключей, записанный на вашу универсальную электронную карту, и нажмите кнопку **Свойства** либо дважды щелкните этот контейнер ключей.
6. В окне **Свойства контейнера ключей** (см. Рисунок 37 на стр. 76) нажмите кнопку **Проверить**, которая находится в нижней части окна напротив сведений о квалифицированном сертификате, содержащемся в контейнере ключей, и введите код ПИН2 вашей УЭК. Успешная проверка означает, что с сертификатом впоследствии можно работать.
7. В окне **Свойства контейнера ключей** нажмите кнопку **Открыть**.
8. В окне **Сертификат** нажмите кнопку **Установить сертификат** и установите сертификат в хранилище текущего пользователя операционной системы (см. «Установка сертификата из контейнера ключей» на стр. 75).

Предварительная настройка ViPNet CSP для работы с УЭК выполнена.

Авторизация на Едином портале государственных и муниципальных услуг РФ

Для того чтобы пройти авторизацию на Едином портале государственных и муниципальных услуг, используя УЭК, выполните следующие действия:

1 Перейдите на страницу авторизации Единого портала государственных услуг (https://esia.gosuslugi.ru).

2 В нижней части страницы в строке **Вход с помощью** щелкните ссылку **Электронных средств**.

3 Загрузите и установите плагин для работы с порталом государственных услуг.

Примечание. При использовании плагина версии 2.0.5.7 убедитесь, что в настройках браузера Internet Explorer на вкладке **Безопасность** снят флажок **Включить защищенный режим**, а также установлены все разрешения для элементов управления ActiveX.

4 Поместите УЭК в считыватель PC/SC-совместимый считыватель контактных смарт-карт.

5 Нажмите кнопку **Готово**.

6 Введите код ПИН2.

7 В окне **Безопасность Windows** выберите нужный квалифицированный сертификат.

После авторизации вы получаете доступ ко всем государственным и муниципальным услугам, представленным на портале.

A

Возможные неполадки и способы их устранения

Не удается запустить программу

Если при попытке запустить ViPNet CSP появляется сообщение о нарушении целостности или об отсутствии файлов программы, дальнейшая работа программы будет невозможна.

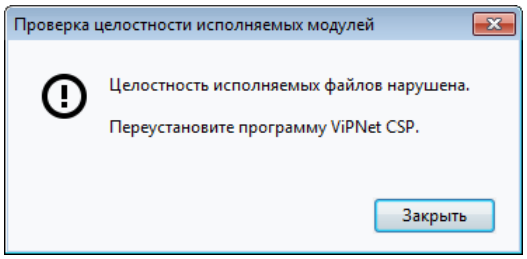


Рисунок 81. Сообщение о нарушении целостности файлов программы

Чтобы вернуть работоспособность ViPNet CSP, запустите установочный файл и восстановите установленные компоненты программы (см. «Добавление, удаление и восстановление компонентов программы» на стр. 34).

После перезагрузки программа ViPNet CSP будет полностью работоспособна. Если программа была зарегистрирована, повторная регистрация не требуется.

Не удается получить код регистрации через Интернет

Если при попытке получить код регистрации через Интернет соединение с сервером регистрации ОАО «ИнфоТеКС» установить не удается в течение 3 минут, появится окно с предупреждением.

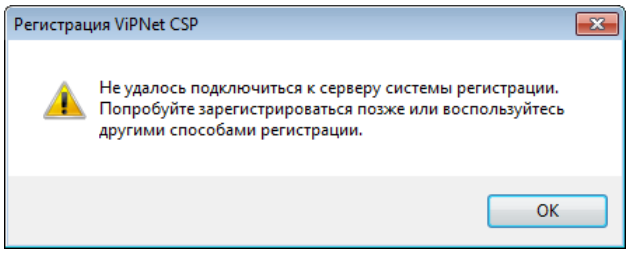


Рисунок 82. Не удалось соединиться с сервером регистрации ОАО «ИнфоТеКС»

В этом случае проверьте настройки вашего сетевого экрана. Доступ к серверу регистрации ОАО «ИнфоТеКС» (http://regboxproduct.infotecs.ru) по протоколу TCP, порт 80 не должен быть заблокирован.

Проблемы при использовании аппаратного модуля доверенной загрузки «Аккорд-АМДЗ»

Если на компьютере установлен аппаратный модуль доверенной загрузки «Аккорд-АМДЗ», но его не удается использовать в программе ViPNet CSP в качестве датчика случайных чисел, выполните следующие действия:

1. Убедитесь, что на компьютере установлены драйверы «Аккорд-АМДЗ».
2. Из папки установки драйверов (по умолчанию `C:\Accord`) скопируйте файл `tmdrv32.dll` в следующую папку:
   - При использовании 32-разрядной версии Windows — `C:\Windows\System32`.
   - При использовании 64-разрядной версии Windows — `C:\Windows\SysWOW64`.
3. В программе ViPNet CSP выберите «Аккорд-АМДЗ» в качестве датчика случайных чисел (см. «Использование датчика случайных чисел» на стр. 100).

Проблемы при использовании устройства типа SafeNet eToken (eToken Aladdin)

Если вы используете устройство типа SafeNet eToken (eToken Aladdin), и при формировании запроса на сертификат ваш компьютер зависает, убедитесь, что установлено программное обеспечение eToken PKI Client 5.1 SP1 или SafeNet Authentication Client.

Сертификат автоматически некорректно устанавливается в хранилище при подключении внешнего устройства

При подключении к компьютеру некоторых внешних устройств, например устройств семейства ESMART Token (см. «Список поддерживаемых внешних устройств» на стр. 214), сертификаты, хранящиеся на них, устанавливаются в системное хранилище автоматически. После такой установки работа программы ViPNet CSP с этими сертификатами будет невозможна. Чтобы отключить автоматическую установку сертификатов при подключении устройства, предварительно выполните следующие действия:

1. Откройте консоль MMC:
   - Нажмите сочетание клавиш **Win**+**R**.

     В меню **Пуск** также можно выбрать пункт **Выполнить**.
   - В поле **Открыть** введите `mmc` и нажмите кнопку **OK**.
2. В меню **Файл** окна консоли выберите пункт **Добавить или удалить оснастку**.
3. В окне **Добавление и удаление оснасткой** в списке **Доступные оснастки** выберите оснастку **Редактор объектов групповой политики** и нажмите кнопку **Добавить**.
4. В окне **Выбор объекта групповой политики** выберите объект **Локальный компьютер**. В результате будет добавлена оснастка **Политика «Локальный компьютер»**.
5. На левой панели окна консоли выберите раздел **Корень консоли** > **Политика «Локальный компьютер»** > **Конфигурация компьютера** > **Административные шаблоны** > **Компоненты Windows** > **Смарт-карта**.
6. На правой панели окна консоли дважды щелкните параметр **Включить распространение корневого сертификата со смарт-карты**.
7. В окне **Включить распространение корневого сертификата со смарт-карты** установите переключатель в положение **Отключить**.

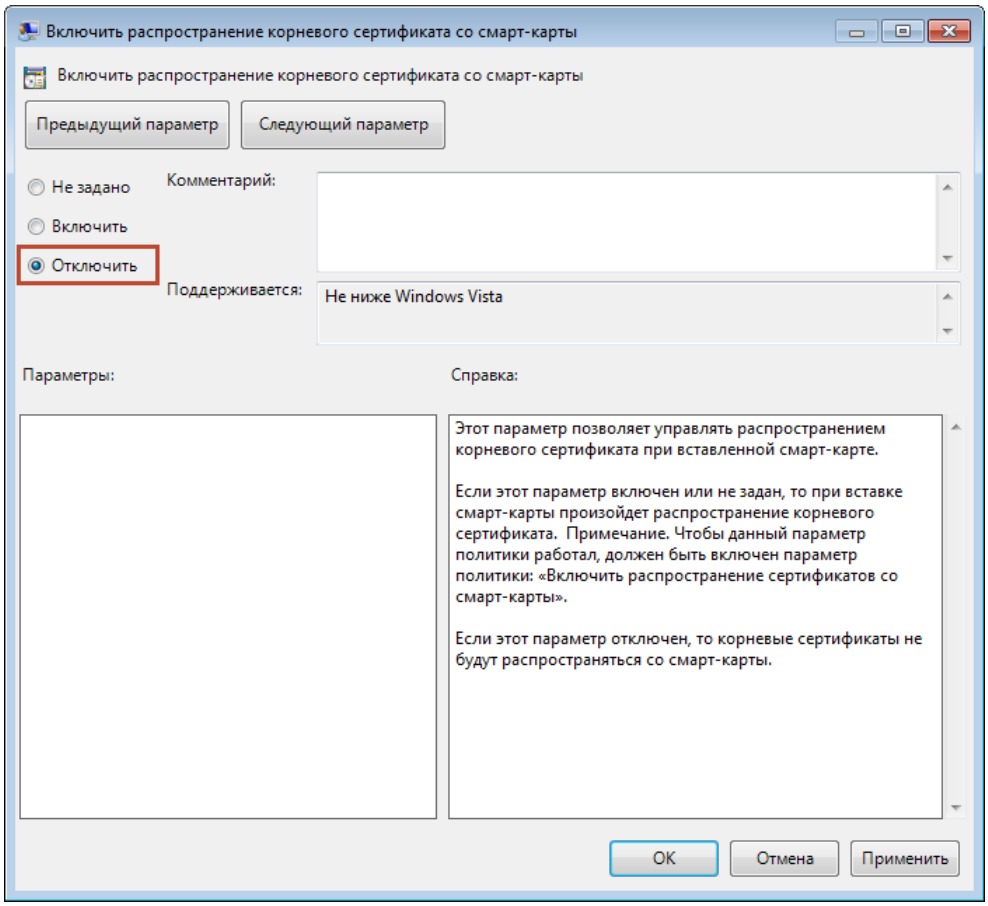


Рисунок 83. Отключение автоматической установки сертификатов в системное хранилище при подключении внешнего устройства к компьютеру

Теперь вы можете подключить внешнее устройство к компьютеру и установить нужные контейнеры ключей и сертификаты (см. «Установка контейнеров ключей и сертификатов» на стр. 64).

Не удается найти контейнер ключей, соответствующий сертификату

Подобная неполадка может возникнуть при выполнении следующих условий:

- Вы используете операционную систему Windows 7 или Windows Server 2008 R2.
- На вашем компьютере установлены контейнер ключей и соответствующий ему сертификат (см. глоссарий, стр. 64).
- При попытке выполнить одну из криптографических операций после указания сертификата не удается найти соответствующий ему контейнер ключей.

Это известная проблема, решенная специалистами компании Microsoft. Для устранения неполадки установите пакет исправлений для Windows KB977222 (https://support.microsoft.com/ru-ru/kb/977222).

Не удается зашифровать документ

Адрес электронной почты из сертификата не найден в списке адресов контакта

При импорте сертификата в карточку контакта Microsoft Outlook может появиться предупреждение о том, что сертификат не содержит адрес электронной почты, который бы соответствовал адресу данного контакта.

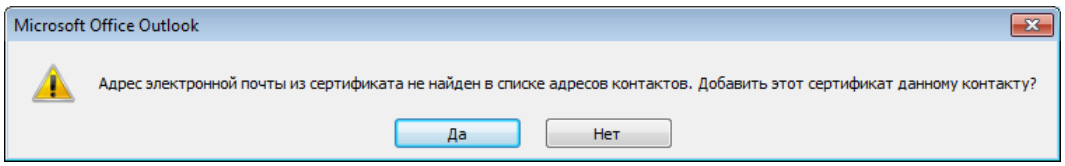


Рисунок 84. Предупреждение при импорте сертификата

В этом случае зашифровать сообщение на этом сертификате получателя не удастся.

Возможны следующие причины появления проблемы:

- Сертификат не принадлежит данному контакту, в этом случае выполните следующие действия:
  - Откройте окно **Сертификат**, дважды щелкнув файл сертификата.
  - На вкладке **Общие** удостоверьтесь, что сертификат принадлежит данному получателю. Если это не так, укажите для импорта нужный сертификат.

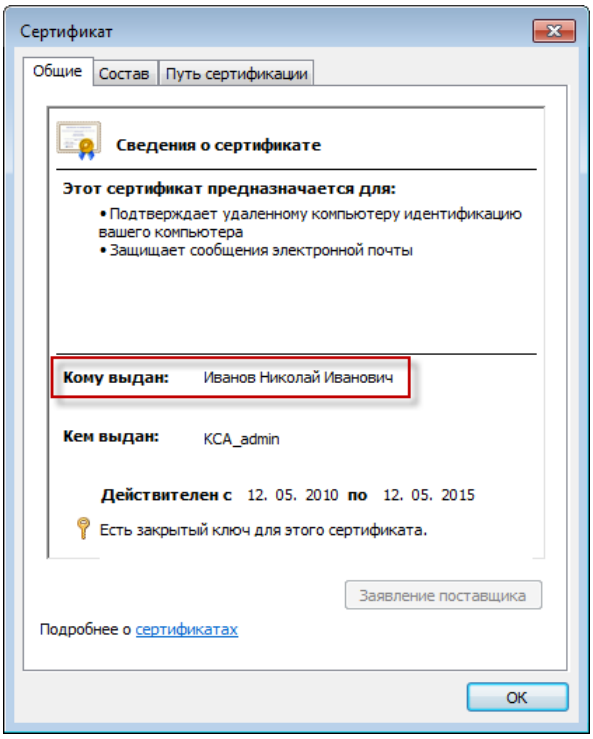


Рисунок 85. Проверка владельца сертификата

- В сертификате не прописан адрес электронной почты данного контакта, в этом случае выполните следующие действия:
  - Откройте окно **Сертификат**, дважды щелкнув файл сертификата на диске.
  - На вкладке **Состав** выберите поле **Субъект** и удостоверьтесь, в качестве значения параметра **E** задан нужный адрес электронной почты.

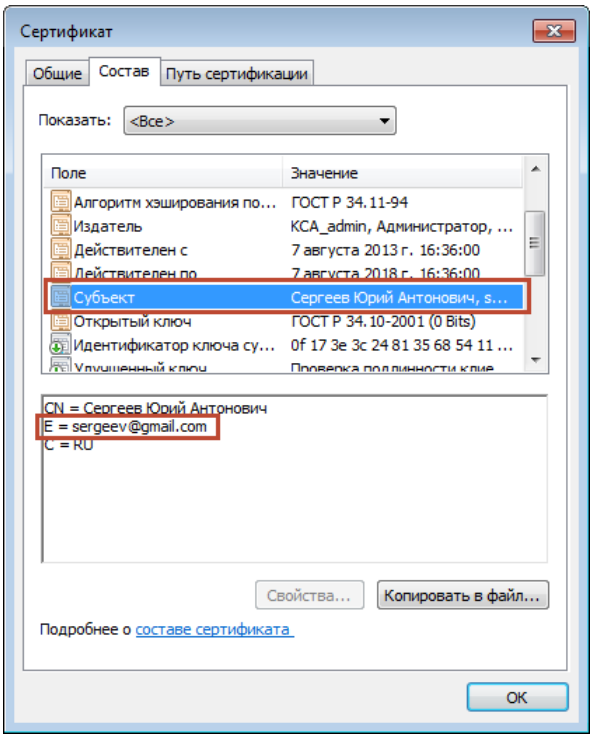


Рисунок 86. Проверка адреса электронной почты в сертификате

Если это не так, выполните следующие действия:

- Если вы импортировали сертификат контакта, запросите новый сертификат у получателя.
- Если вы добавляли в систему свой сертификат, запросите новый сертификат у администратора вашего удостоверяющего центра.

Недопустимый сертификат

При отправке зашифрованного сообщения может появиться предупреждение:

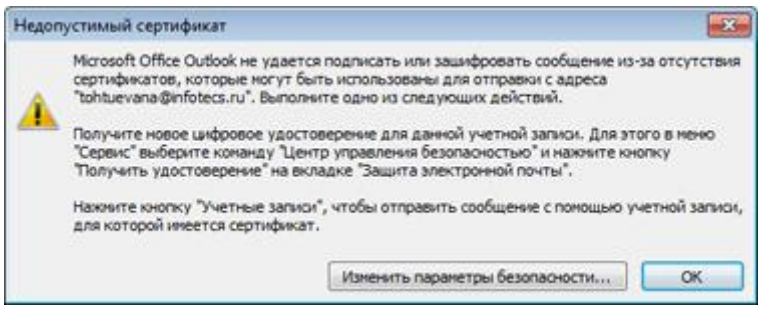


Рисунок 87. Недопустимый сертификат в Microsoft Outlook

Это может быть связано со следующими причинами:

- Сертификат получателя не содержит адреса электронной почты данного получателя (см. «Адрес электронной почты из сертификата не найден в списке адресов контакта» на стр. 171).

- Ваш сертификат не содержит адреса вашей электронной почты (см. «Адрес электронной почты из сертификата не найден в списке адресов контакта» на стр. 171).
- Сертификат получателя или ваш сертификат недействителен. Запросите новый сертификат у получателя или у администратора вашего удостоверяющего центра.
- Не указан персональный сертификат подписи и шифрования (см. «Настройка дополнительных параметров электронной подписи и шифрования» на стр. 128).
- В системное хранилище не был установлен сертификат издателя (см. «Установка сертификата издателя и списка аннулированных сертификатов» на стр. 78).

Не удается поставить электронную подпись

Не найден закрытый ключ, соответствующий сертификату

Если при выборе сертификата для подписания открывается окно **ViPNet CSP - инициализация контейнера ключей**, это значит, что не найден закрытый ключ, соответствующий выбранному сертификату. Это может произойти в том случае, если контейнер ключей был удален в программе ViPNet CSP (см. «Удаление контейнера ключей» на стр. 92).

Чтобы подписать документ выбранным сертификатом, в окне **ViPNet CSP - инициализация контейнера ключей** укажите путь к контейнеру, который содержит закрытый ключ, соответствующий сертификату. Если вы не знаете местоположение контейнера ключей, использование выбранного сертификата невозможно.

Если в окне **ViPNet CSP - инициализация контейнера ключей** вы укажете путь к контейнеру ключей, этот контейнер будет добавлен в список в разделе **Контейнеры ключей** окна **ViPNet CSP**.

Не удается подписать сообщение электронной почты

Если при попытке подписать сообщение электронной почты выводится сообщение о том, что отсутствуют сертификаты, которые могут быть использованы для отправки с данного адреса электронной почты, вам следует обратиться за таким сертификатом в удостоверяющий центр. В сертификате должен быть указан ваш адрес электронной почты и присутствовать расширение «Защищенная электронная почта» в поле «Расширенное использование ключа» («Улучшенный ключ»).

Не удалось подписать сообщение электронной почты нужным сертификатом

Если при попытке подписать сообщение электронной почты подписание происходит, но используется сертификат, отличный от выбранного, это означает, что указанный сертификат электронной подписи не содержит адреса электронной почты владельца сертификата или этот адрес не совпадает с адресом отправки сообщения электронной почты. При этом в момент

подписания сообщения из системного хранилища выбирается другой сертификат, содержащий адрес электронной почты, с которого отправляется сообщение.

Для устранения ошибки выполните следующие действия:

1 Создайте запрос на новый сертификат и укажите в нем корректный адрес электронной почты.

2 Отправьте запрос на сертификат администратору вашего удостоверяющего центра и дождитесь выполнения запроса.

3 Укажите в качестве сертификата для электронной подписи полученный сертификат.

Невозможно редактировать подписанный документ Microsoft Word или Excel

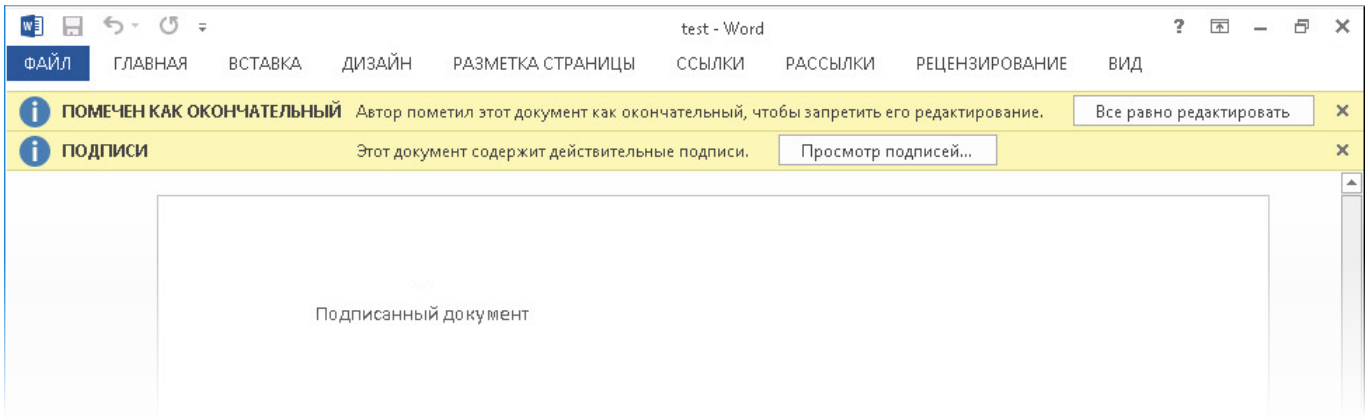


Рисунок 88. Предупреждения при открытии подписанного документа

Чтобы внести изменения в подписанный документ Microsoft Word или Excel, удалите электронную подпись (см. «Удаление электронной подписи в Microsoft Word, Excel и PowerPoint» на стр. 120) и внесите необходимые изменения. После этого вы можете снова подписать документ.

Внимание! Не следует удалять электронную подпись из документа, подписанного другим лицом, или если документ имеет юридическую значимость.

Нет соединения с сервером по протоколу TLS

На IIS-сервере и веб-клиенте установлены разные версии ViPNet CSP

Установите на веб-клиенте ту же версию программы ViPNet CSP, что установлена на сервере.

Если это невозможно и на сервере установлена более ранняя версия ViPNet CSP, чем 4.2, на веб-клиенте с последней версией ViPNet CSP выполните следующие действия:

1 В окне **ViPNet CSP** перейдите в раздел **Дополнительно**.

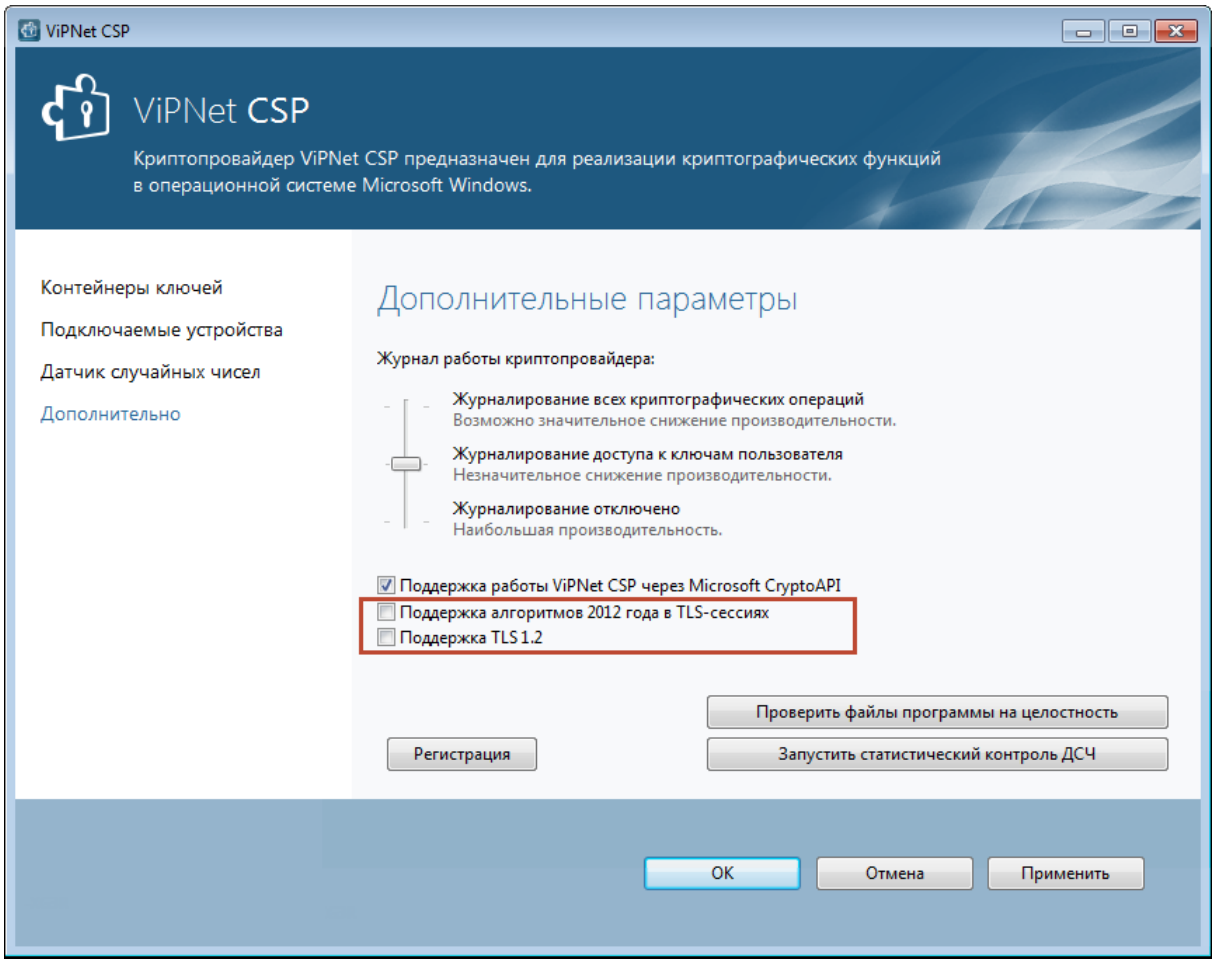


Рисунок 89. Отключение поддержки протокола TLS 1.2

2 Снимите флажки **Поддержка алгоритмов 2012 года в TLS-сессиях** и **Поддержка TLS 1.2**.

3 В окне **Свойства обозревателя** (**Свойства браузера**) вашего браузера Internet Explorer снимите флажок **Использовать TLS 1.2** и установите флажки **TLS 1.0**, **Использовать TLS 1.1** (см. «Настройка веб-браузера Internet Explorer для работы по протоколу TLS» на стр. 153).

4 Закройте программы перезагрузите компьютер.

Попробуйте снова организовать TLS-соединение.

Не установлены сертификаты пользователя, издателя, CRL в нужное хранилище

Проверьте корректность установки сертификатов в хранилище с помощью стандартной консоли MMC (Microsoft Management Console).

Чтобы просмотреть сертификаты, установленные в хранилище, выполните следующие действия:

1 Откройте консоль MMC:

- Нажмите сочетание клавиш **Win**+**R**.

  В меню **Пуск** также можно выбрать пункт **Выполнить**.

- В поле **Открыть** введите `mmc` и нажмите кнопку **OK**.

2 В меню **Файл** окна консоли выберите пункт **Добавить или удалить оснастку**.

3 В окне **Добавление и удаление оснасткой** в списке **Доступные оснастки** выберите оснастку **Сертификаты** и нажмите кнопку **Добавить**.

4 В окне **Оснастка диспетчера сертификатов** выберите нужный тип оснастки:

- **моей учетной записи пользователя** — для просмотра сертификатов веб-клиента;
- **учетной записи компьютера** — для просмотра сертификатов сервера.

Примечание. Чтобы не добавлять оснастку **Сертификаты** в консоль каждый раз, когда она вам понадобится, вы можете сохранить консоль. Для этого в меню **Консоль** выберите пункт **Сохранить**.

Сертификаты пользователя, издателя и список CRL должны быть установлены в нужное хранилище, и при их открытии не должно возникать ошибок.

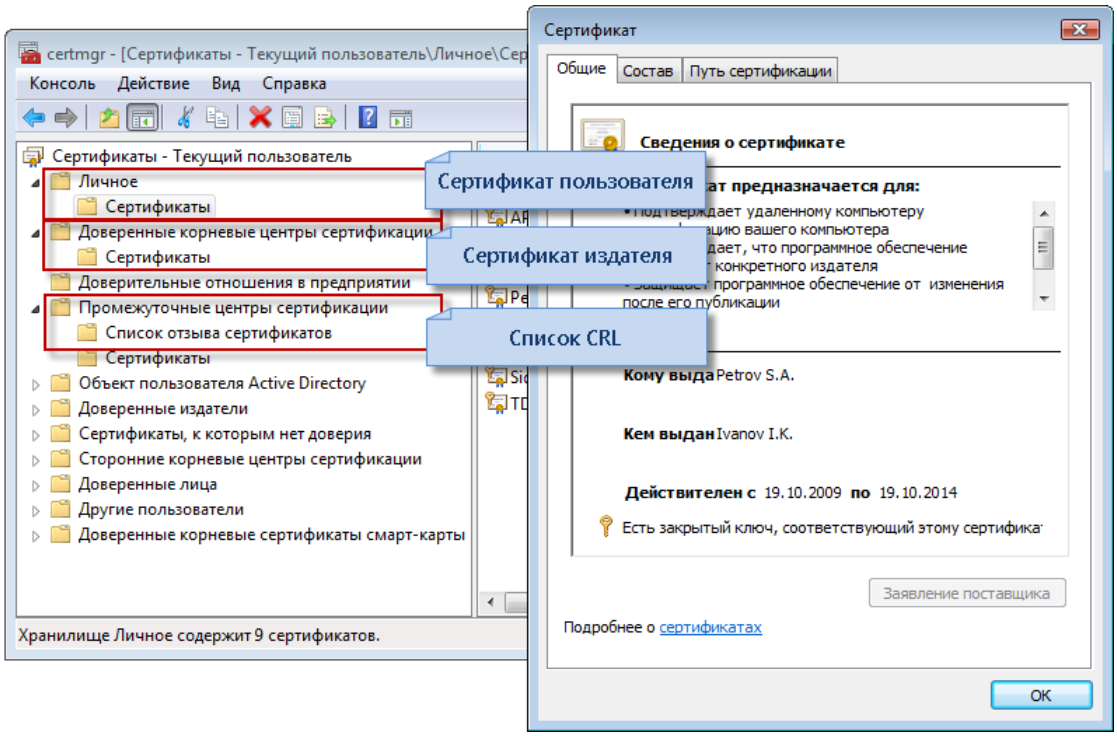


Рисунок 90. Сертификат веб-клиента в хранилище сертификатов текущего пользователя

Для сервера IIS в оснастке MMC сертификатов локального компьютера должны присутствовать следующие сертификаты:

- Раздел **Личные** > **Сертификаты** — сертификат пользователя (сервера).
- Раздел **Доверенные корневые центры сертификации** > **Сертификаты** — сертификат издателя.
- Раздел **Промежуточные центры сертификации** > **Список отзыва сертификатов** — список CRL.

Для веб-клиента в оснастке MMC сертификатов текущего пользователя должны присутствовать следующие сертификаты:

- Раздел **Личные** > **Сертификаты** — сертификат пользователя (веб-клиента).
- Раздел **Доверенные корневые центры сертификации** > **Сертификаты** — сертификат издателя.
- Раздел **Промежуточные центры сертификации** > **Список отзыва сертификатов** — список CRL.

Если сертификат не установлен или установлен некорректно, выполните установку сертификата в хранилище (см. «Установка сертификата издателя и списка аннулированных сертификатов» на стр. 78).

Веб-браузер не настроен на работу по протоколу TLS

Если после соответствующей настройки веб-браузера (см. «Настройка веб-браузера Internet Explorer для работы по протоколу TLS» на стр. 153) соединения с сервером не происходит, выполните следующие действия:

- Проверьте наличие нужного сертификата.
- Убедитесь, что в свойствах обозревателя разрешено использование протокола TLS (см. «Настройка веб-браузера Internet Explorer для работы по протоколу TLS» на стр. 153).

Для проверки наличия сертификата выполните следующие действия:

1. В меню **Сервис** веб-браузера Internet Explorer выберите пункт **Свойства обозревателя** (**Свойства браузера**).
2. В окне **Свойства обозревателя** (**Свойства браузера**) откройте вкладку **Содержание** и нажмите кнопку **Сертификаты**.
3. В окне **Сертификаты** откройте вкладку **Личное** и проверьте, что в списке сертификатов присутствует нужный.
4. Выберите нужный сертификат и нажмите кнопку **Просмотр**.
5. В окне **Сертификат** убедитесь, что сертификат содержит расширение **Проверка подлинности клиента** (см. Рисунок 91 на стр. 180). Если такой атрибут отсутствует, обратитесь в удостоверяющий центр за сертификатом, в котором будет указан данный параметр.

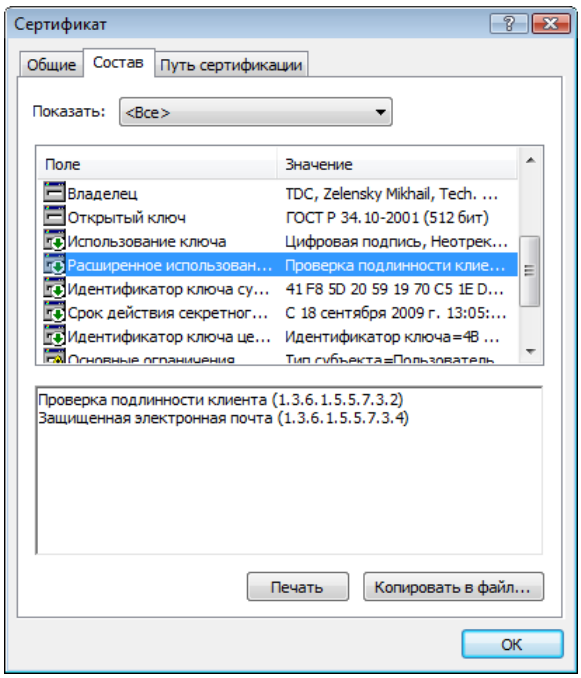


Рисунок 91. Состав сертификата веб-клиента

Требуется перезапуск службы сервера IIS

В некоторых случаях для доступа к серверу по вновь настроенному протоколу TLS необходимо перезапустить службу сервера. Для этого выполните следующие действия:

1 Откройте окно **Диспетчер задач Windows**.

2 Остановите службу `inetinfo.exe`.

3 После того как служба автоматически запустится, проверьте подключение к серверу.

Требуется сохранить пароль к сертификату сервера

Для доступа к серверу необходимо сохранить пароль к контейнеру ключей. Для этого выполните следующие действия:

В окне ViPNet CSP в разделе **Контейнеры ключей** (см. Рисунок 31 на стр. 66) выберите контейнер ключей, пароль к которому требуется сохранить, и нажмите кнопку **Свойства**.

1 В окне **Свойства контейнера ключей** (см. Рисунок 40 на стр. 83) нажмите кнопку **Проверить**.

2 В окне **ViPNet CSP - пароль контейнера ключей** (см. Рисунок 42 на стр. 85) укажите пароль к контейнеру ключей и установите флажок **Сохранить пароль**.

В результате пароль к контейнеру ключей будет сохранен на компьютере.

На компьютере установлен антивирус ESET

Если на вашем компьютере помимо ViPNet CSP установлен антивирус производства компании ESET, TLS-соединение на алгоритмах 2001 года может блокироваться антивирусом. Чтобы блокировка соединения не происходила, выполните следующие действия:

1 В области уведомлений Windows щелкните правой кнопкой мыши значок  с названием вашей антивирусной программы ESET.

2 В контекстном меню выберите пункт **Дополнительные настройки**.

3 В окне **Расширенные параметры** выполните следующие действия:

3.1 На левой панели выберите раздел **Интернет и электронная почта**.

3.2 На правой панели раскройте область **SSL/TLS** и снимите флажок **Включить фильтрацию протокола SSL/TLS**.

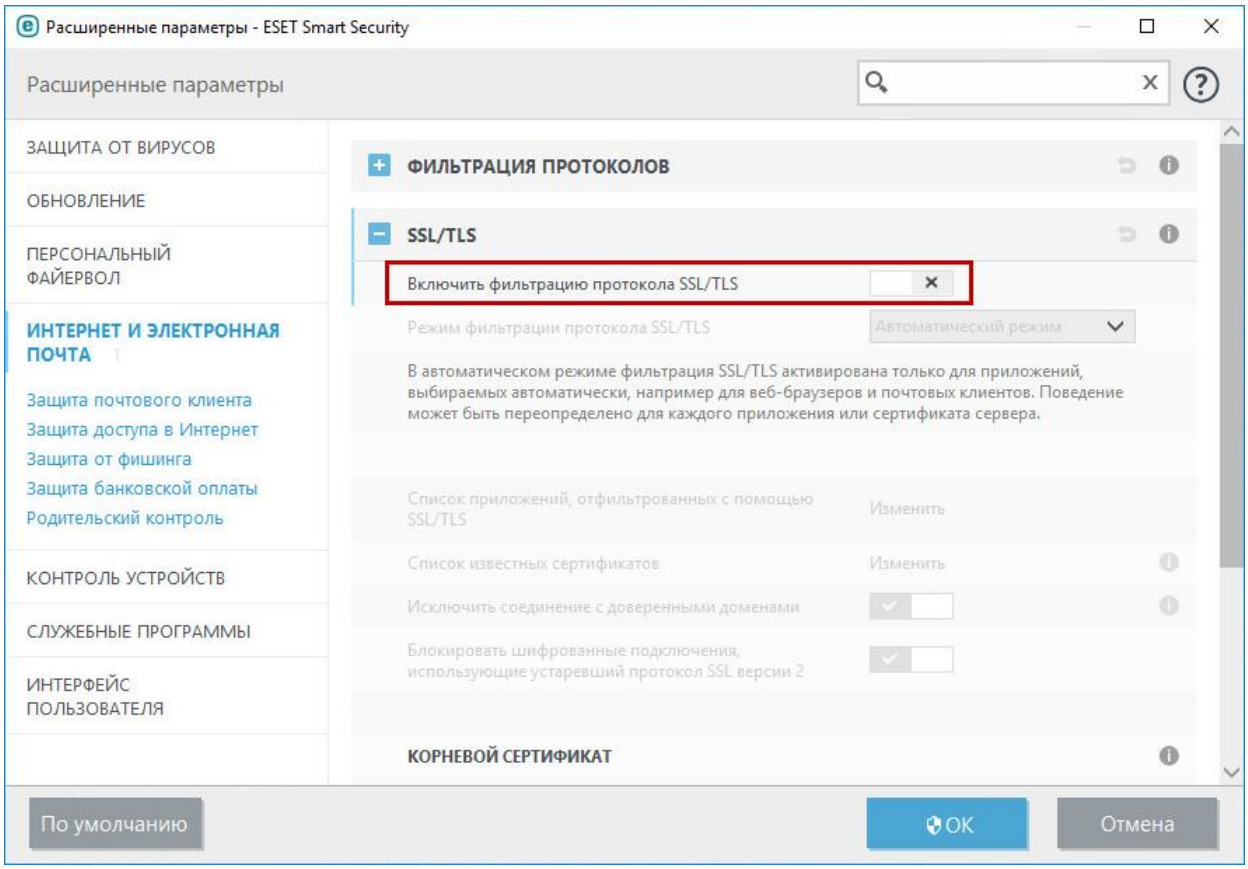


Рисунок 92. Устранение конфликта с антивирусом ESET

Попробуйте снова организовать TLS-соединение.

На компьютере установлен антивирус Kaspersky Internet Security

Если на вашем компьютере помимо ViPNet CSP установлен антивирус Kaspersky Internet Security 2017, TLS-соединение может блокироваться антивирусом. Чтобы блокировка соединения не происходила, выполните следующие действия:

1. В области уведомлений Windows щелкните правой кнопкой мыши значок **Kaspersky Internet Security**.
2. В контекстном меню выберите пункт **Настройка**.
3. В окне **Настройка** перейдите в раздел **Дополнительно** и на правой панели щелкните ссылку **Сеть**.

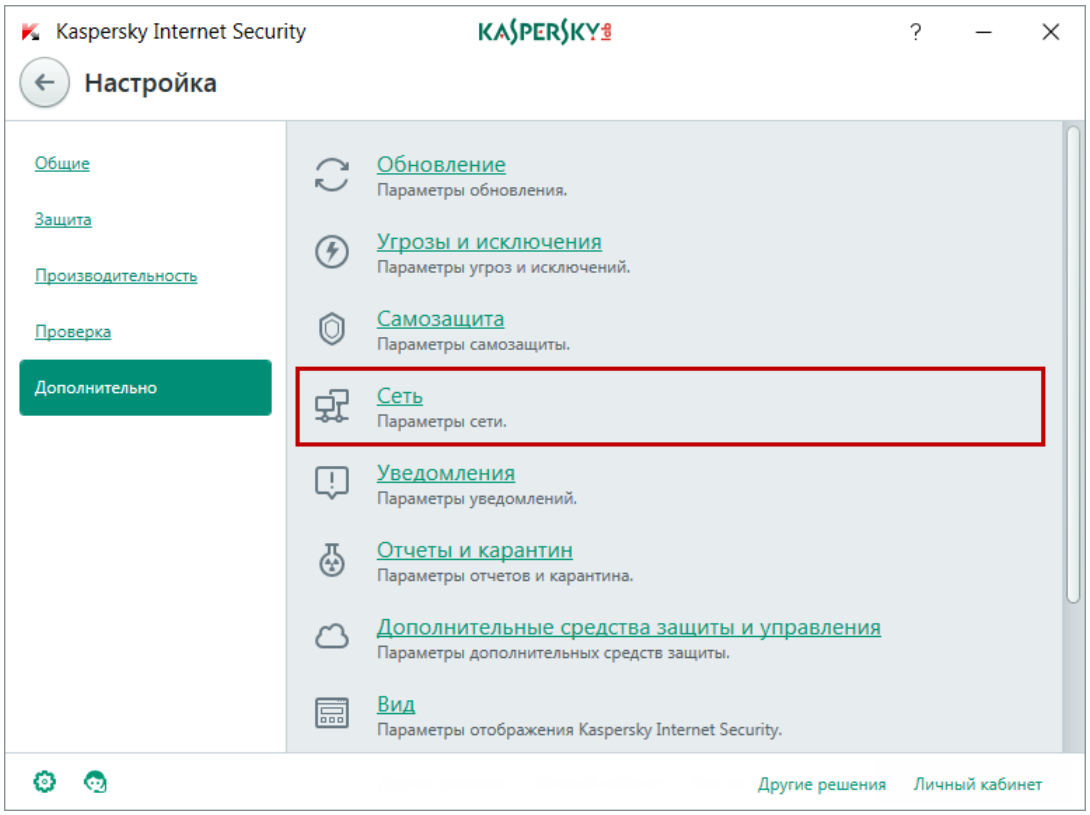


Рисунок 93. Начало настройки антивируса Kaspersky Internet Security для обеспечения совместной работы с ViPNet CSP

4 В окне **Параметры сети** снимите флажок **Внедрять в трафик скрипт взаимодействия с веб-страницами**.

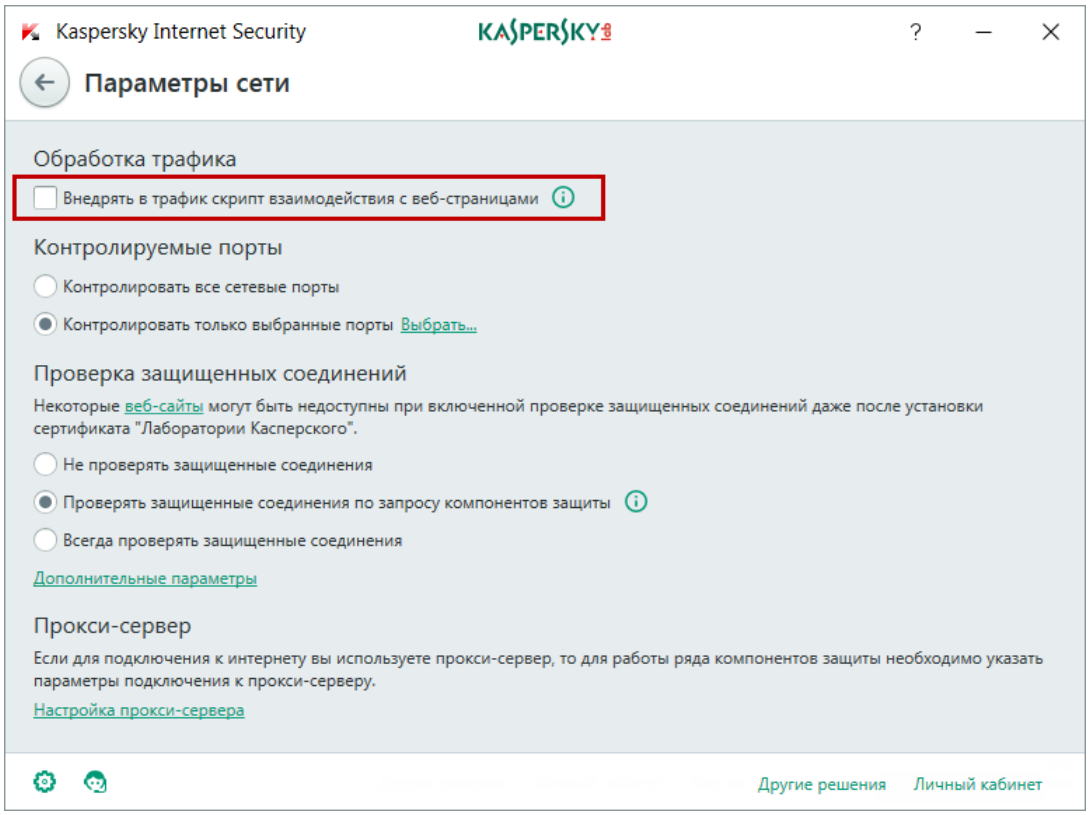


Рисунок 94. Настройка антивируса Kaspersky Internet Security для обеспечения совместной работы с ViPNet CSP

Попробуйте снова организовать TLS-соединение.

На компьютере установлен антивирус Avast Internet Security

Если на вашем компьютере помимо ViPNet CSP установлен антивирус Avast Internet Security, TLS-соединение на алгоритмах 2001 года может блокироваться антивирусом. Чтобы блокировка соединения не происходила, выполните следующие действия:

1. В главном окне программы Avast Internet Security нажмите кнопку **Настройки**.
2. В окне настроек в разделе **Компоненты** напротив параметра **Веб-экран** щелкните ссылку **Настройки**.

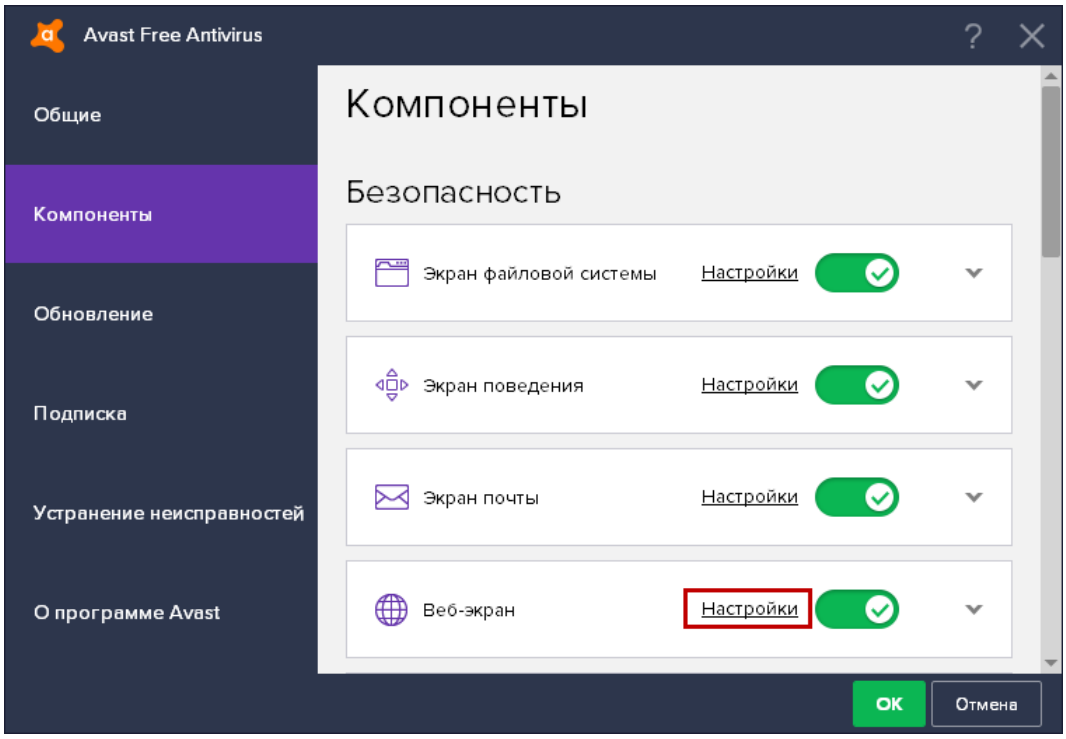


Рисунок 95. Основные настройки антивируса Avast Internet Security

3 В открывшемся окне в разделе **Основные настройки** снимите флажок **Включить сканирование HTTPS**.

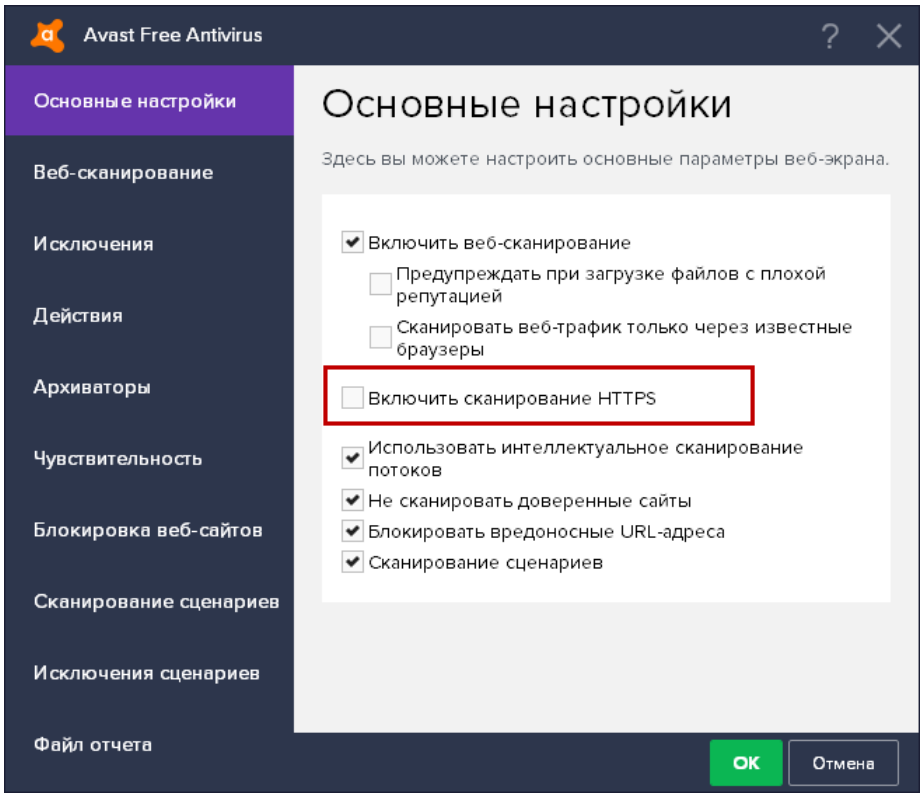


Рисунок 96. Устранение конфликта с антивирусом Avast Internet Security

Попробуйте снова организовать TLS-соединение.

На компьютере установлен антивирус AVG Internet Security

Если на вашем компьютере помимо ViPNet CSP установлен антивирус AVG Internet Security, TLS-соединение на алгоритмах 2001 года может блокироваться антивирусом. Чтобы блокировка соединения не происходила, выполните следующие действия:

1 В главном окне программы AVG Internet Security щелкните ссылку **Меню** и выберите пункт **Настройки**.

2 В окне настроек в разделе **Компоненты** напротив параметра **Online Shield** щелкните ссылку **Настройка**.

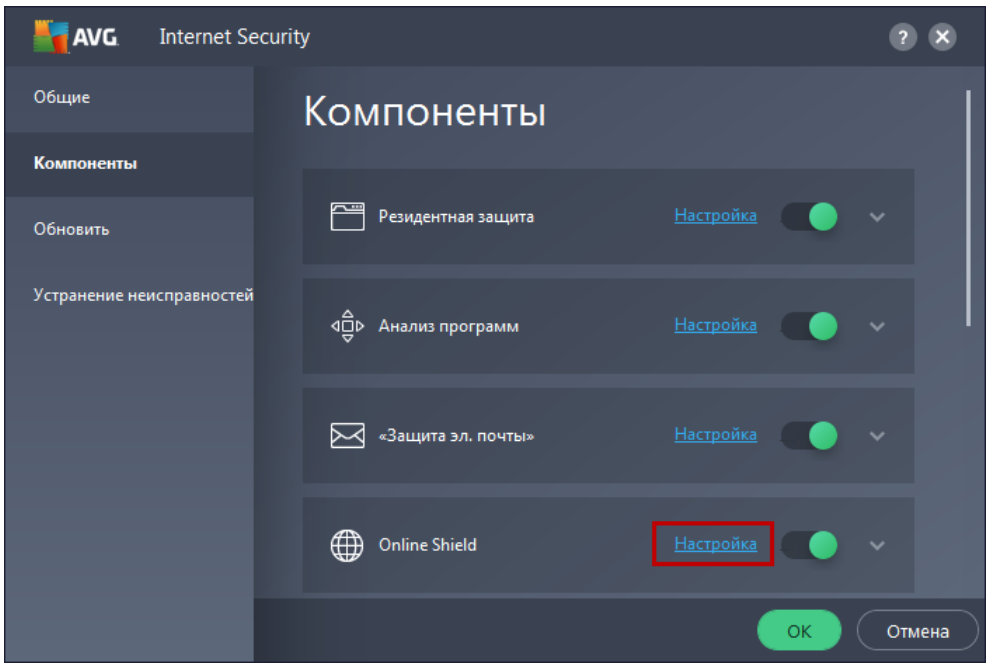


Рисунок 97. Основные настройки антивируса AVG Internet Security

3 В открывшемся окне в разделе **Основные настройки** снимите флажок **Включить сканирование HTTPS**.

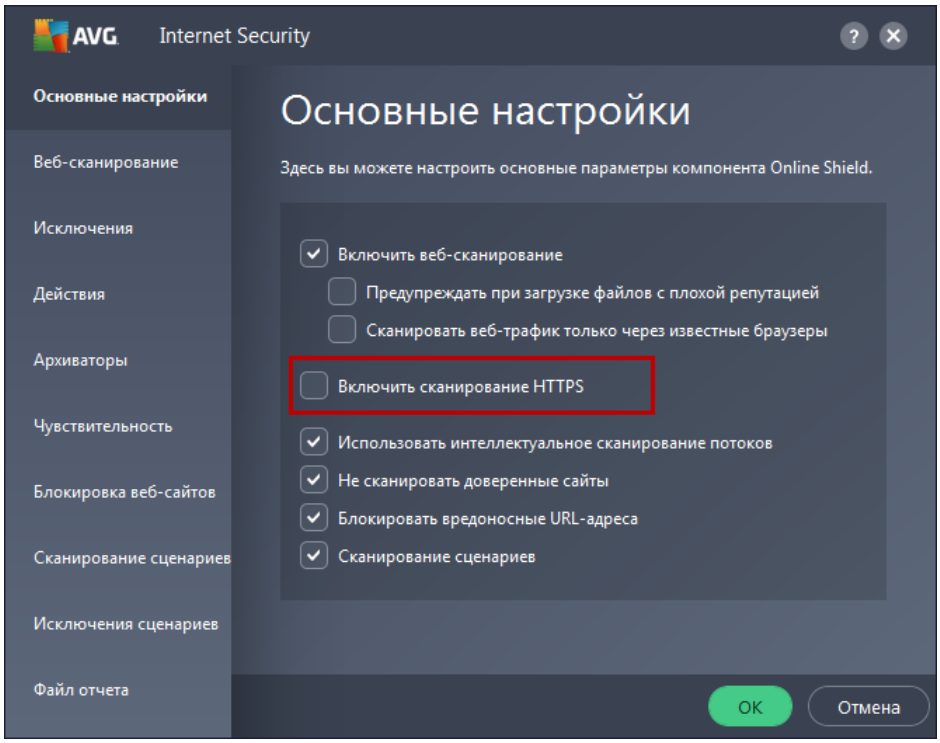


Рисунок 98. Устранение конфликта с антивирусом AVG Internet Security

Попробуйте снова организовать TLS-соединение.

После обновления Windows пропало соединение по протоколу TLS

После установки некоторых пакетов обновлений операционной системы Windows работа ViPNet CSP по протоколу TLS может быть прекращена.

В этому случае запустите установочный файл программы и выполните восстановление ее компонентов (см. «Добавление, удаление и восстановление компонентов программы» на стр. 34).

Не удается подключиться к центру сертификации Microsoft CA по протоколу HTTP

Для удаленного доступа к серверу, на котором развернут центр сертификации Microsoft CA с интегрированным ViPNet CSP (см. «Интеграция ViPNet CSP с центром сертификации на базе Microsoft CA» на стр. 109), по протоколу HTTPS пользователю не требуется выполнять каких-либо дополнительных настроек.

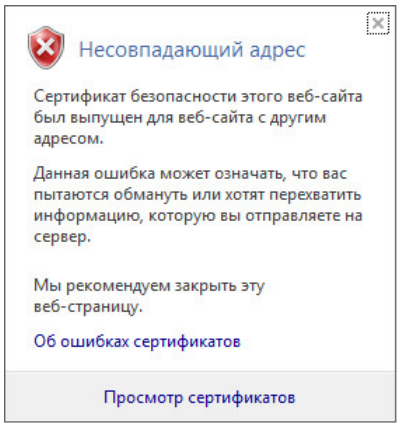
Для удаленного доступа к серверу, на котором развернут центр сертификации Microsoft CA с интегрированным ViPNet CSP, по протоколу HTTP выполните следующие действия:

1. Запустите веб-браузер Internet Explorer.
2. В окне **Свойства браузера** на вкладке **Безопасность** выполните следующие действия:
   - Нажмите кнопку **Сайты** и добавьте веб-сайт с центром сертификации в зону **Надежные сайты**.
   - Нажмите кнопку **Другой** и в окне **Параметры безопасности - зона надежных сайтов** для параметра **Использование элементов управления ActiveX, не помеченных как безопасные для использования** установите переключатель в положение **Включить**.

Примечание. Названия элементов интерфейса приведены для веб-браузера Internet Explorer 11.

При соединении с сервером выводится предупреждение системы безопасности

При попытке соединения с сервером в веб-браузере могут появляться предупреждения системы безопасности.



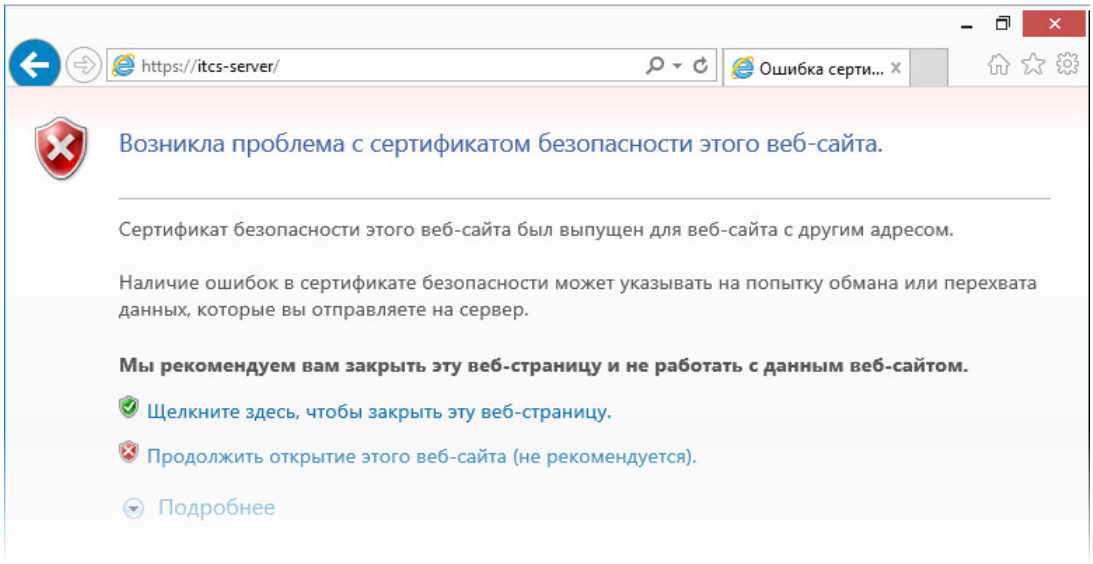


Рисунок 99. Предупреждения о несоответствии доменного имени сервера и имени владельца сертификата сервера

В этом случае проверьте, что доменное имя сервера и имя пользователя, на которое выдан сертификат сервера, совпадают.

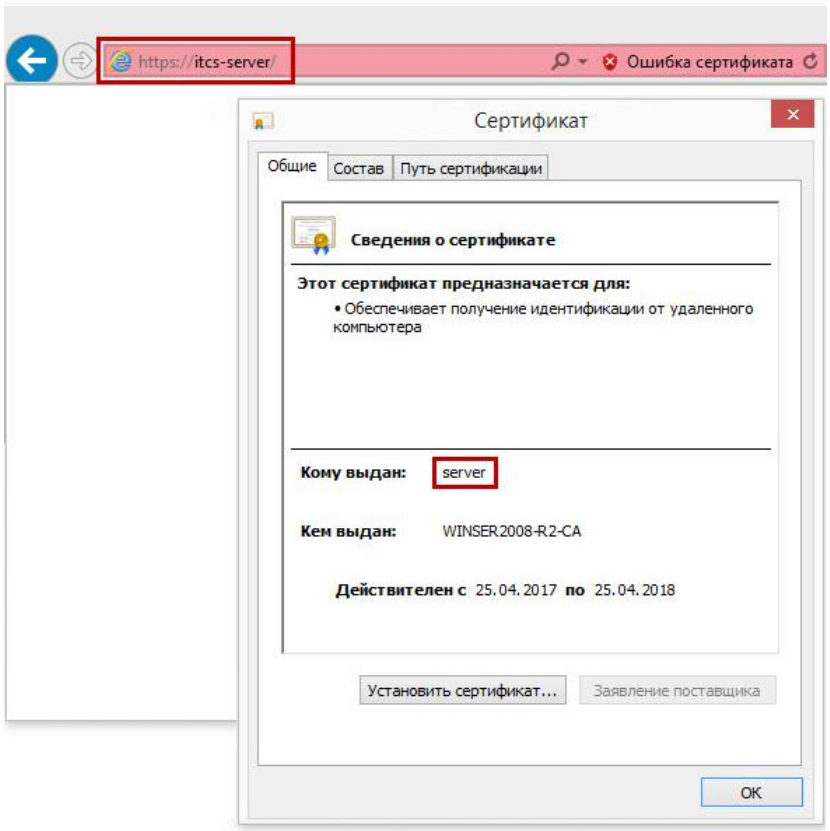


Рисунок 100. Проверка соответствия доменного имени сервера и имени владельца сертификата сервера

Аварийная остановка ViPNet CSP при одновременном использовании нескольких внешних устройств

Подобная неполадка может возникнуть из-за конфликта драйверов для внешних устройств eToken или JaCarta с драйверами для других поддерживаемых внешних устройств (см. «Внешние устройства» на стр. 214).

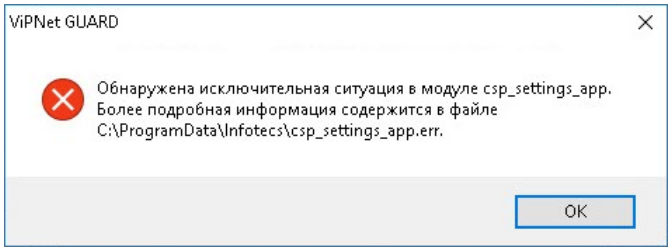


Рисунок 101. Ошибка при одновременном использовании нескольких внешних устройств

Аварийная остановка программы может произойти при одновременном выполнении следующих условий:

- На вашем компьютере установлены драйверы для внешнего устройства eToken или JaCarta, а также драйверы для хотя бы одного другого поддерживаемого внешнего устройства.
- В программе ViPNet CSP в списке опрашиваемых устройств включено использование нескольких внешних устройств, в том числе eToken или JaCarta.

Чтобы устранить неполадку, в главном окне ViPNet CSP на странице **Подключаемые устройства** отключите использование всех типов устройств, кроме требуемого (см. «Настройка списка опрашиваемых устройств» на стр. 95).

Не удается работать с внешним устройством, если на нем установлено сразу два апплета

Если на вашем внешнем устройстве установлено сразу два апплета, ViPNet CSP распознает внешнее устройство, соответствующее лишь одному из этих апплетов. Работа сразу с двумя апплетами не поддерживается. Чтобы использовать в ViPNet CSP какой-либо определенный апплет из записанных на вашем токене, в главном окне ViPNet CSP на странице **Подключаемые устройства** отключите использование всех типов устройств, кроме требуемого (см. «Настройка списка опрашиваемых устройств» на стр. 95).

Например, если на токене установлены апплеты JaCarta PKI и JaCarta ГОСТ, ViPNet CSP по умолчанию распознает устройство типа JaCarta. Чтобы использовать ваш токен как устройство JaCarta ГОСТ, в программе ViPNet CSP отключите поддержку всех типов внешних устройств, кроме eToken GOST/JaCarta GOST.

Не удается подключиться к компьютеру с ViPNet CSP по протоколу RDP

Указанная проблема может быть вызвана конфликтом с обновлением Windows KB2919355 (http://www.microsoft.com/ru-RU/download/details.aspx?id=42327).

Для решения проблемы восстановите установленные компоненты программы ViPNet CSP (см. «Добавление, удаление и восстановление компонентов программы» на стр. 34).

Проверка целостности файлов программы

При необходимости вы можете проверить целостность файлов программы. Для этого выполните следующие действия:

1 В окне **ViPNet CSP** перейдите в раздел **Дополнительно**.

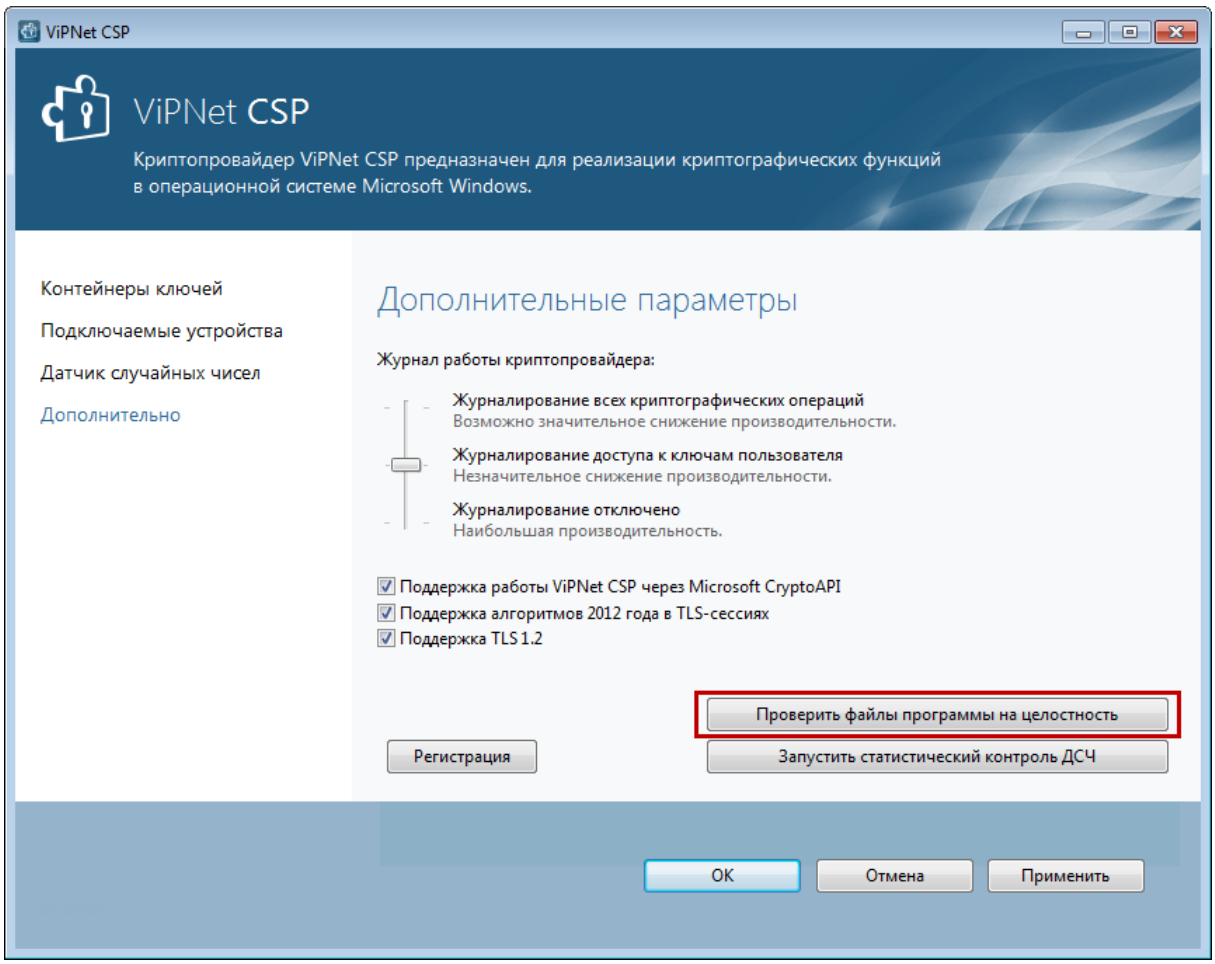


Рисунок 102. Проверка целостности файлов программы

2 Нажмите кнопку **Проверить файлы программы на целостность**.

При этом произойдет пересчет контрольных сумм и проверка их соответствия суммам, указанным в каждом из файлов программы.

По окончании проверки отобразится окно с сообщением о результатах проверки. В случае несоответствия контрольным суммам восстановите компоненты программы (см. «Добавление, удаление и восстановление компонентов программы» на стр. 34).

Статистический контроль датчиков случайных чисел программы

При необходимости вы можете провести статистический контроль датчиков случайных чисел программы. Для этого выполните следующие действия:

1 В окне **ViPNet CSP** перейдите в раздел **Дополнительно**.

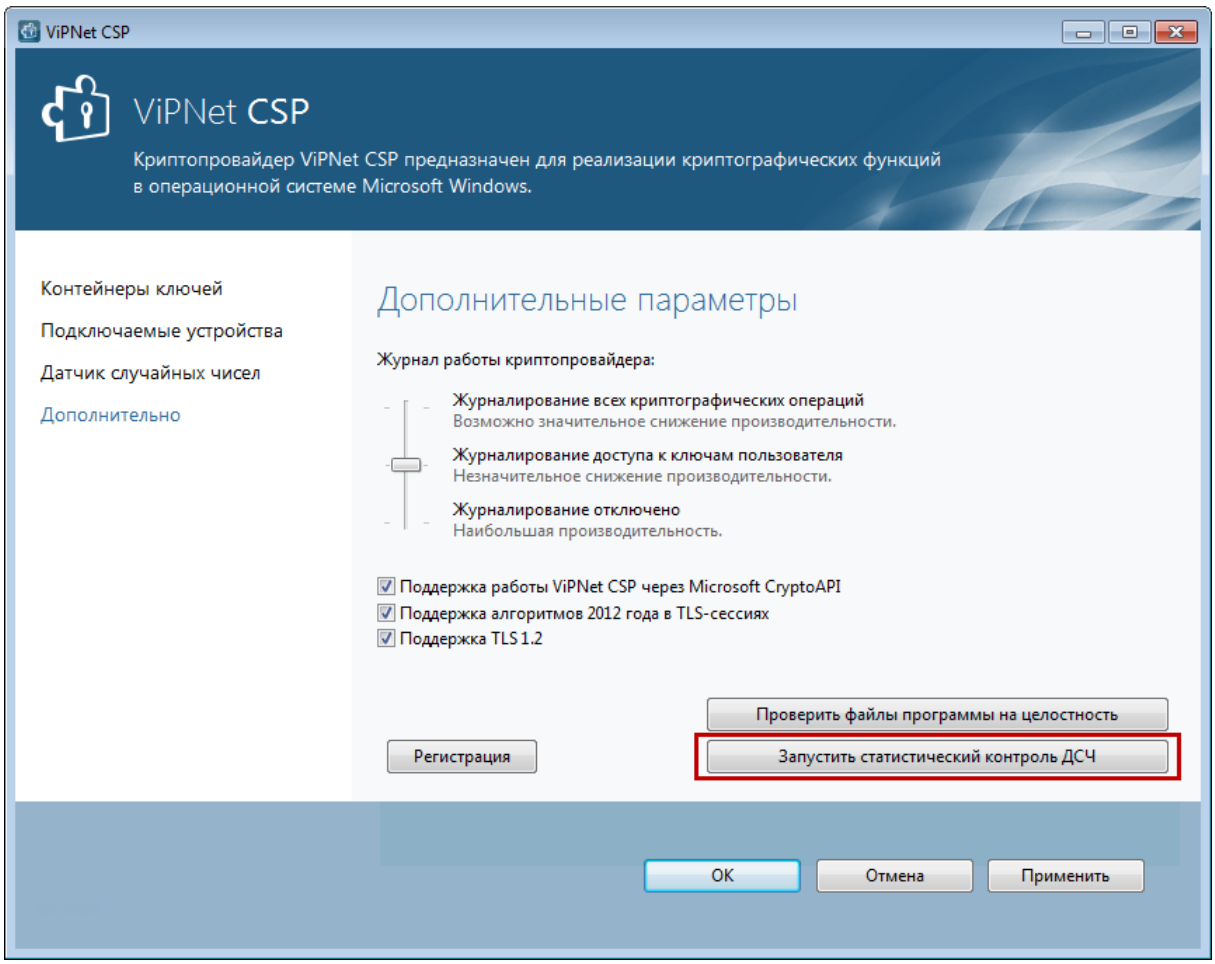


Рисунок 103. Запуск статистического контроля датчиков случайных чисел программы

2 Нажмите кнопку **Запустить статистический контроль ДСЧ**.

Восстановление системных файлов и параметров ОС Windows после неудачной установки ViPNet CSP

Если после установки ViPNet CSP ваш компьютер перестал загружаться либо если операционная система начала циклически перезагружаться, верните операционную систему в состояние, предшествующее установке программы ViPNet CSP с помощью точки восстановления, созданной во время установки программы. Например, если вы используете ОС Windows 10, выполните следующие действия:

1. Подключите к компьютеру накопитель с дистрибутивом операционной системы, установленной на вашем компьютере.
2. В программе настройки BIOS выберите в качестве загрузочного носителя подключенный носитель и перезагрузите компьютер.
3. В окне **Установка Windows** при необходимости измените предлагаемые параметры ввода и нажмите кнопку **Далее**. Затем щелкните ссылку **Восстановление системы**.

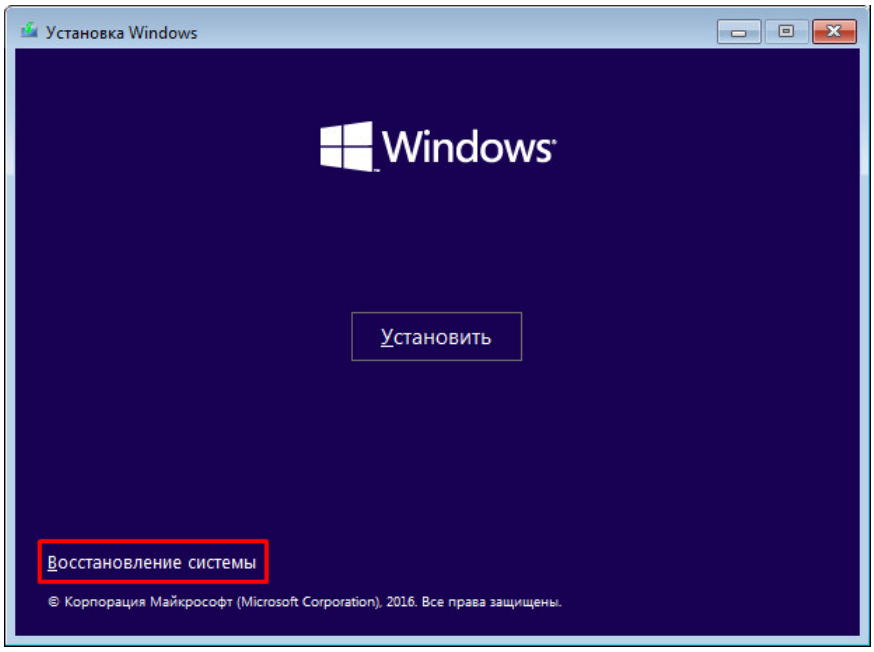


Рисунок 104. Запуск Windows для восстановления системы

4. На странице **Выбор действия** щелкните плитку **Поиск и устранение неисправностей**.
5. На странице **Дополнительные параметры** щелкните плитку **Восстановление системы**.

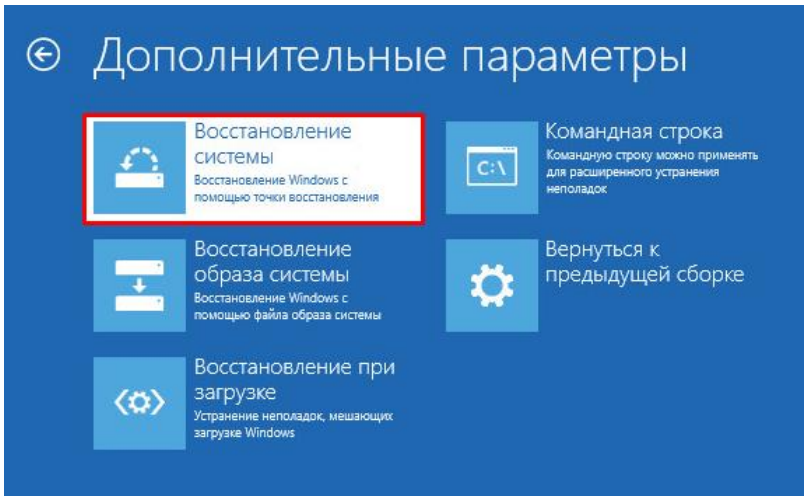


Рисунок 105. Выбор способа восстановления системы

6 На страницах мастера **Восстановление системы** выберите необходимую точку восстановления и подтвердите восстановление системы.

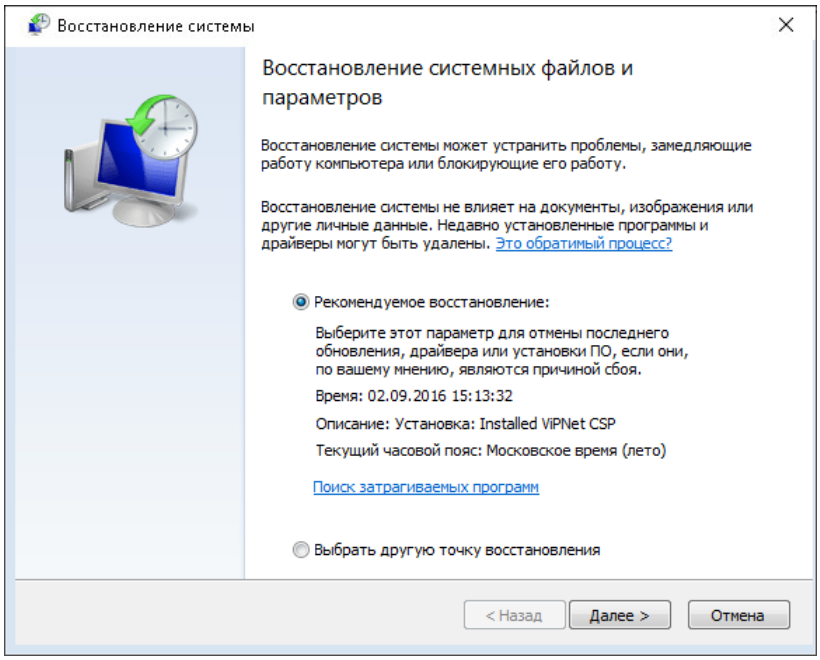


Рисунок 106. Выбор точки восстановления

По окончании восстановления компьютер перезагрузится.

Повторная регистрация для устранения неполадок

Для устранения некоторых неполадок может потребоваться повторная регистрация ViPNet CSP. В этом случае сотрудник технической поддержки ОАО «ИнфоТеКС» предоставит вам новый серийный номер. Чтобы заново зарегистрировать программу, выполните следующие действия:

1 В окне **ViPNet CSP** перейдите в раздел **Дополнительно**.

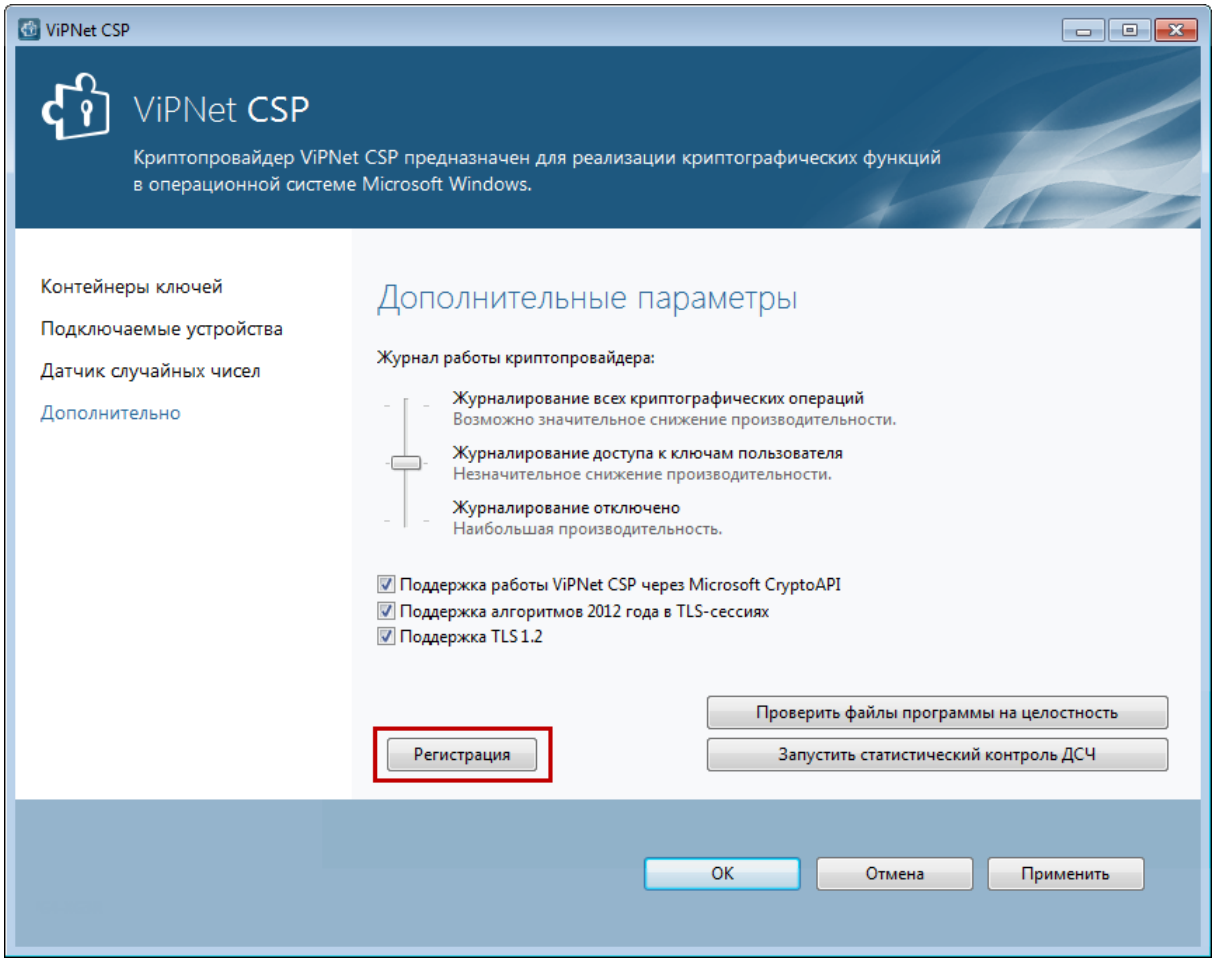


Рисунок 107. Запуск мастера регистрации

2 Нажмите кнопку **Регистрация**. Откроется окно мастера **Регистрация ViPNet CSP** (см. Рисунок 13 на стр. 43).

3 Повторно зарегистрируйте программу с помощью нового серийного номера, следуя инструкциям из раздела Регистрация ViPNet CSP (на стр. 41).

Предоставление дополнительной информации о неисправности

Для устранения неисправности сотрудник технической поддержки ОАО «ИнфоТеКС» может попросить вас предоставить дополнительную информацию для анализа.

Если неисправность возникает на этапе установки или обновления программы, выполните следующие действия:

1. Откройте следующую папку:

   `C:\ProgramData\InfoTeCS\InstallerData\ViPNet CSP\Logs`

2. Добавьте находящиеся в папке файлы журнала в архив и отправьте вместе с описанием неисправности в службу технической поддержки.

Если неисправность возникает во время работы программы, выполните следующие действия:

1. Нажмите сочетание клавиш **Win**+**R**.

   В меню **Пуск** также можно выбрать пункт **Выполнить**.

2. В поле **Открыть** введите команду `regedit` и нажмите клавишу **Enter**.

3. В программе «Редактор реестра» перейдите в раздел `Logs`, который находится по следующему пути:

   - в 32-разрядных операционных системах Windows: `HKEY_LOCAL_MACHINE\SOFTWARE\InfoTeCS\Logs`;
   - в 64-разрядных операционных системах Windows: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\InfoTeCS\Logs`.

4. Измените значения ключей `level` и `fields` на `0xff (255)` в следующих вложенных разделах:

   - в 32-разрядных операционных системах Windows: `itcspp, itccspbs, itccspex, itcssp`;
   - в 64-разрядных операционных системах Windows: `itcspp`, `itccspbs`, `itccspex`, `itcssp`, `itccsp64`, `itccspbs64`, `itccspex64`, `itcssp64`.

5. Перезагрузите компьютер.

   Примечание. В некоторых случаях запуск компьютера может занять более продолжительное время, чем обычно.

6. Нажмите сочетание клавиш **Win**+**R**.

   В меню **Пуск** также можно выбрать пункт **Выполнить**.

7. В поле **Открыть** введите команду `msinfo32` и нажмите клавишу **Enter**.

8. В программе «Сведения о системе» в меню **Файл** выберите пункт **Сохранить**.

9 Сохраните файл NFO с произвольным именем.

10 Скачайте программу DebugView (http://technet.microsoft.com/ru-ru/sysinternals/bb896647.aspx).

11 Запустите файл `DbgView.exe` от имени администратора.

12 Повторите действия, при которых у вас возникала неисправность.

13 В программе DebugView выделите все записи и скопируйте в текстовый файл.

14 Добавьте получившийся текстовый файл и файл NFO, сохраненный на шаге 9, в архив и отправьте вместе с описанием неисправности в службу технической поддержки.

Примечание. Если для воспроизведения ошибки необходимо стороннее ПО, укажите это в письме.

---

15 Присвойте ключам `level` и `fields` (см. пункт 4) значение 0.

16 Перезагрузите компьютер.

B

История версий

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

Версия 4.2.2

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet CSP версии 4.2.2 по сравнению с программой версии 4.2.

- **Соответствие требованиям ФСБ России к средствам криптографической защиты информации класса КС3 теперь обеспечивается утилитой ViPNet SysLocker, входящей в комплект поставки**

  Из программы ViPNet CSP удалены функции настройки замкнутой программной среды. Аналогичные функции администратор Windows теперь может выполнить в программе ViPNet SysLocker, которую при необходимости следует установить дополнительно.

- **Изменения в интерфейсе программы**

  В интерфейсе программы произошли следующие изменения:

  - Для экспорта сертификатов и закрытых ключей в файл теперь используется системный мастер Windows (см. «Экспорт сертификата и закрытого ключа в файл» на стр. 88).
  - Для отображения свойств сертификата теперь используется системное окно Windows. В этом окне, наряду с информацией, доступной в прошлых версиях ViPNet CSP, для аннулированных сертификатов вы можете просмотреть дату и время их аннулирования в поле **Расширенные сведения об ошибке.**

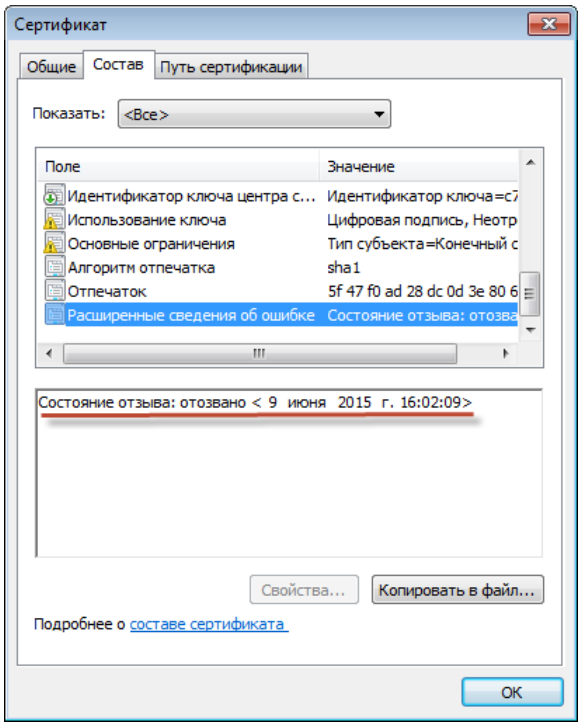


Рисунок 108. Информация о дате и времени отзыва сертификата

- **Изменение комплекта документации**

  В комплект добавлен документ «ViPNet SysLocker. Руководство администратора».

- **Изменения в списке поддерживаемых операционных систем**

  В связи с тем, что компания Microsoft прекратила поддержку операционной системы Windows XP (32-разрядная), работа ViPNet CSP на компьютерах с этой операционной системой также более не поддерживается ОАО «ИнфоТеКС».

- **Изменения в списке поддерживаемых пакетов программ Microsoft Office**

  В связи с тем, что компания Microsoft прекратила поддержку пакета программ Microsoft Office 2003, работа ViPNet CSP в этих программах также более не поддерживается ОАО «ИнфоТеКС».

- **Изменения в списке поддерживаемых веб-браузеров**

  Ввиду невостребованности прекращена поддержка веб-браузеров Internet Explorer 6 и 7.

- **Изменения в списке внешних устройств хранения данных**

  Реализована поддержка устройств линейки «ESMART Token ГОСТ».

  Ввиду невостребованности прекращена поддержка следующих типов внешних устройств: Shipka, iButton Accord, iButton Aladdin, KAZTOKEN.

Версия 4.2.0

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet CSP версии 4.2 по сравнению с программой версии 4.1.

- **Новый формат контейнеров ключей, созданных по алгоритму ГОСТ 34.10-2012**

  Для обеспечения соответствия рекомендациям Технического комитета по стандартизации (ТК 26) «Криптографическая защита информации» (http://www.tc26.ru/) изменен формат контейнеров ключей, созданных по алгоритму ГОСТ 34.10-2012.

- **Изменения в списке поддерживаемых внешних устройств**

  Ввиду невостребованности прекращена поддержка следующих типов внешних устройств: Mifare Standard4K, SmartCard RIK, Rosan Mifare, Smartcard Athena.

Версия 4.1.0

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet CSP версии 4.1 по сравнению с программой версии 4.0.

- **Обновленный пользовательский интерфейс**

  Полностью переработан дизайн пользовательского интерфейса программы.

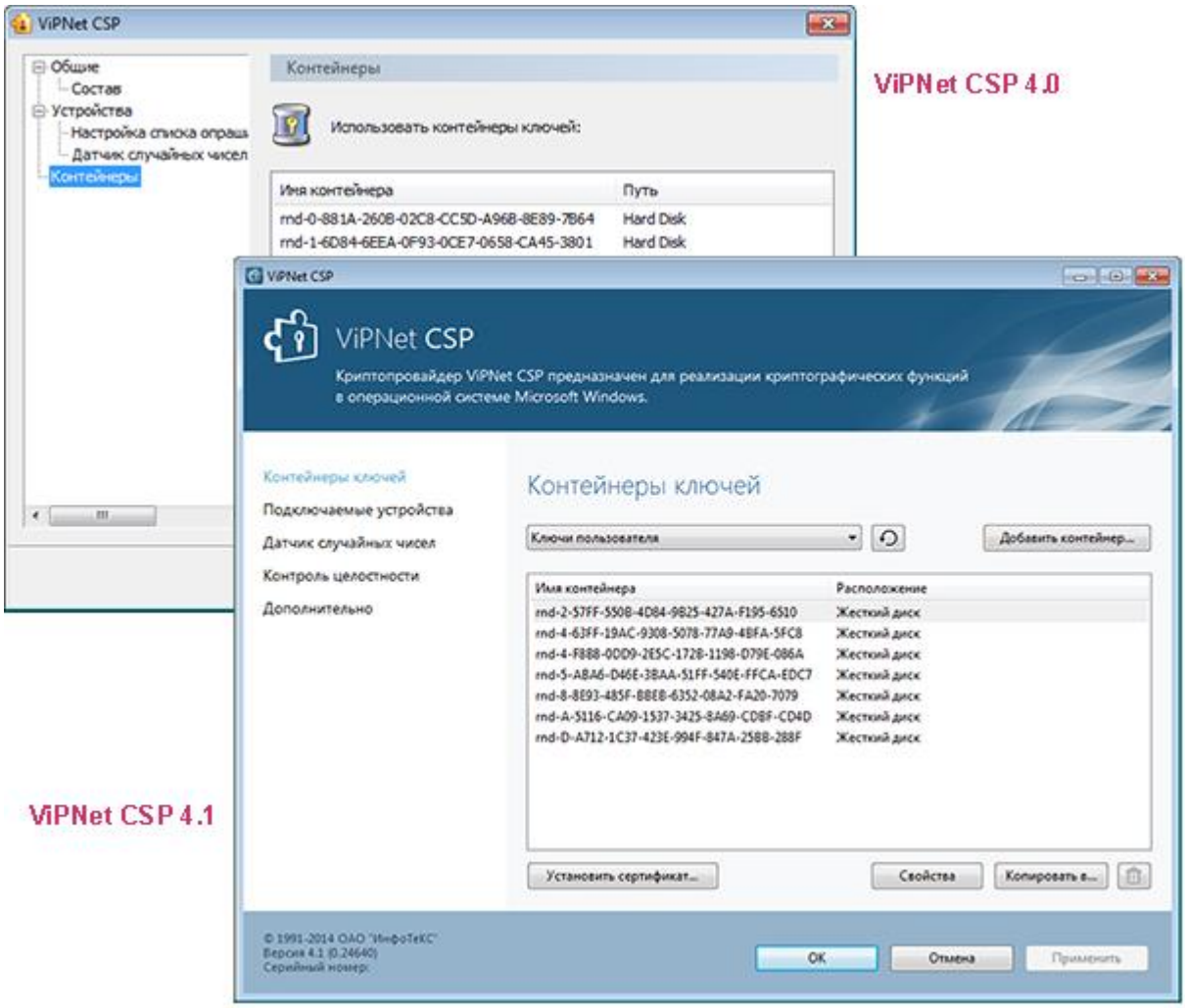


Рисунок 109. Пользовательский интерфейс программы ViPNet CSP 4.1

- **Соответствие рекомендациям Технического комитета по стандартизации (ТК 26) «Криптографическая защита информации»**

  Криптографические алгоритмы ViPNet CSP приведены в соответствие с рекомендациями ТК 26 «Криптографическая защита информации» (http://www.tc26.ru/).

- **Расширенная поддержка алгоритма ГОСТ 34.10-2012**
  - Добавлена возможность организации защищенного соединения TLS/SSL с использованием ключей, созданных по алгоритму ГОСТ 34.10-2012.
  - Добавлена возможность экспорта контейнеров ключей, созданных по алгоритму ГОСТ 34.10-2012, в файлы формата PKCS#12 (`*.pfx`), а также импорта таких контейнеров ключей из файлов PKCS#12.
  - Добавлена возможность работы с внешними устройствами, поддерживающими хранение ключей, созданных по алгоритму ГОСТ 34.10-2012.

- **Организация защищенного соединения TLS/SSL с использованием универсальной электронной карты (УЭК)**

  Добавлена возможность использования контейнера ключей, записанного на вашу универсальную электронную карту, для организации защищенного соединения TLS/SSL с помощью ViPNet CSP.

- **Новый порядок работы с внешними устройствами**

  В главном окне программы убран раздел **Устройства**. Теперь контейнеры ключей, сохраненные на внешнем устройстве, отображаются в разделе **Контейнеры ключей** при выборе названия устройства в раскрывающемся списке.

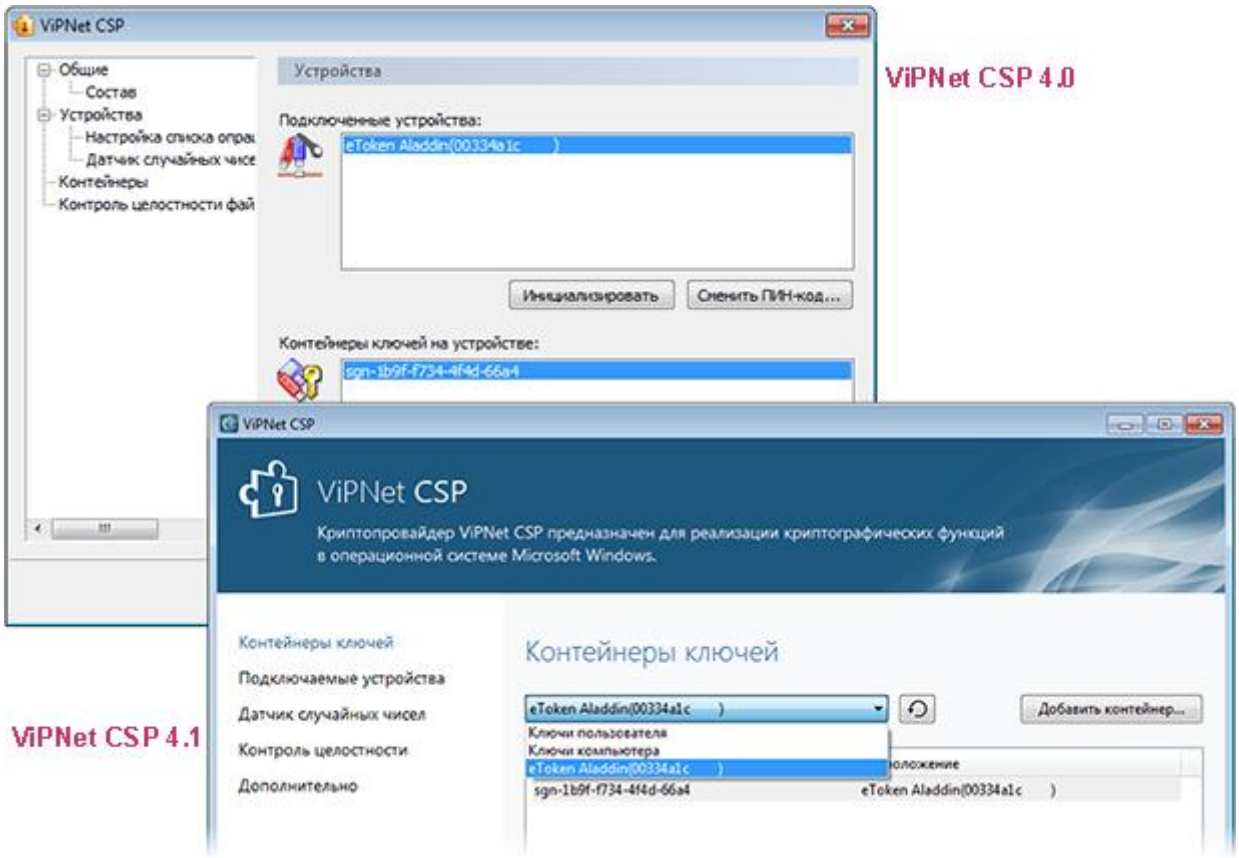


Рисунок 110. Изменение порядка работы с внешними устройствами

- **Новый интерфейс для настройки регистрации событий криптопровайдера**

  Функция настройки регистрации событий криптопровайдера перенесена в раздел **Другое**. Теперь режимы ведения журнала задаются с помощью ползунка, для каждого режима добавлена подсказка.

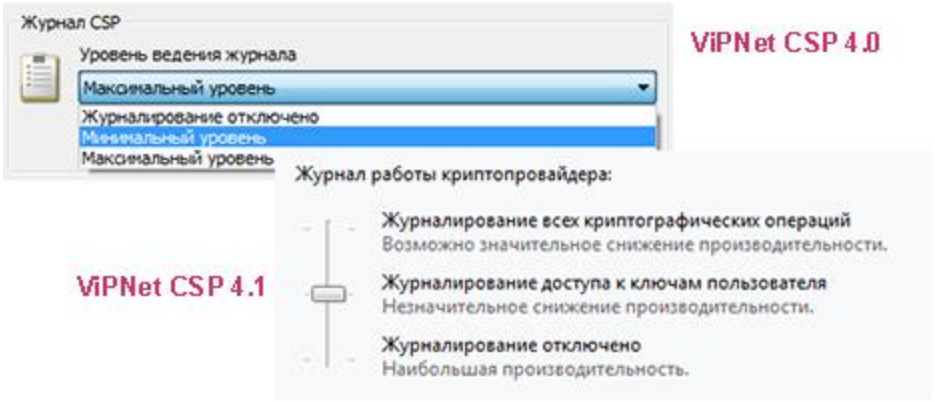


Рисунок 111. Настройка регистрации событий криптопровайдера

- **Автоматический поиск контейнера ключей, которому соответствует сертификат**

  В мастере установки сертификатов добавлена возможность автоматического поиска контейнера ключей, соответствующего устанавливаемому сертификату. Поиск осуществляется по контейнерам ключей, установленным в ViPNet CSP. Новая возможность позволяет значительно ускорить работу, если в ViPNet CSP установлено большое количество контейнеров ключей.

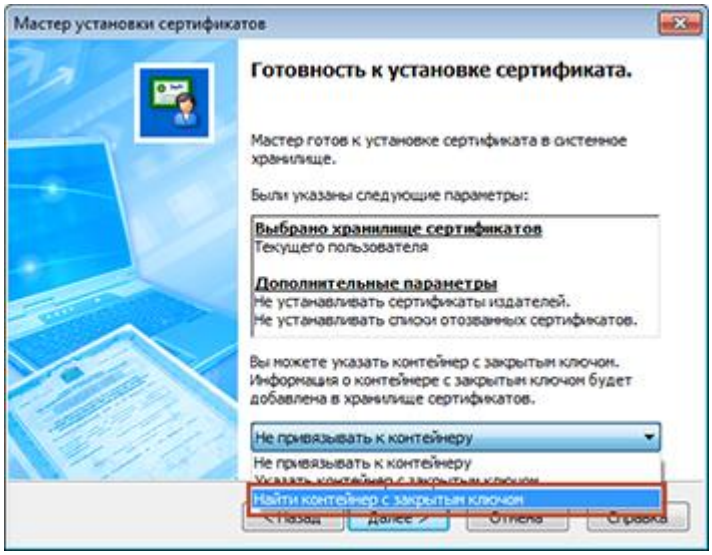


Рисунок 112. Задание автоматического поиска контейнера ключей

- **Комплект документации**

  В комплект документации добавлено руководство «ViPNet CSP. Быстрый старт».

Версия 4.0.0

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.0 по сравнению с версией 3.2.11.

- **Соответствие новым стандартам хэширования и работы с электронной подписью**

  Хэширование данных и работа с электронной подписью осуществляется в соответствии со стандартами ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012.

- **Поддержка новых операционных систем**

  В криптопровайдере реализована поддержка операционных систем Windows 8 (32-разрядная и 64-разрядная) и Windows Server 2012 (64-разрядная).

- **Поддержка интерфейса Cryptography API: Next Generation (CNG)**

  В программе реализована поддержка интерфейса CNG, пришедшего на смену CryptoAPI. Подробнее об интерфейсе CNG см. «Криптографический интерфейс ViPNet CNG. Руководство разработчика».

- **Поддержка стандарта PKCS #11 для 64-разрядной архитектуры**

  Реализована поддержка стандарта PKCS #11, определяющего интерфейс доступа к криптографическим устройствам.

- **Обновление программы создания запроса на сертификат**
  - Добавлена возможность формирования запроса на сертификат для ключей, созданных с помощью различных криптопровайдеров: как от ОАО «ИнфоТеКС», так и от корпорации Microsoft.
  - В список **Шаблон сертификата** добавлен пункт **WEB server**, позволяющий создать запрос на сертификат для установки на веб-сервере IIS.
  - Появилась возможность с помощью флажков **Экспортируемый** и **Системный** задавать следующие параметры издаваемого сертификата:
    - Будет ли возможно вместе с издаваемым сертификатом экспортировать соответствующий ему закрытый ключ.
    - Следует ли устанавливать издаваемый сертификат в системное хранилище локального компьютера.

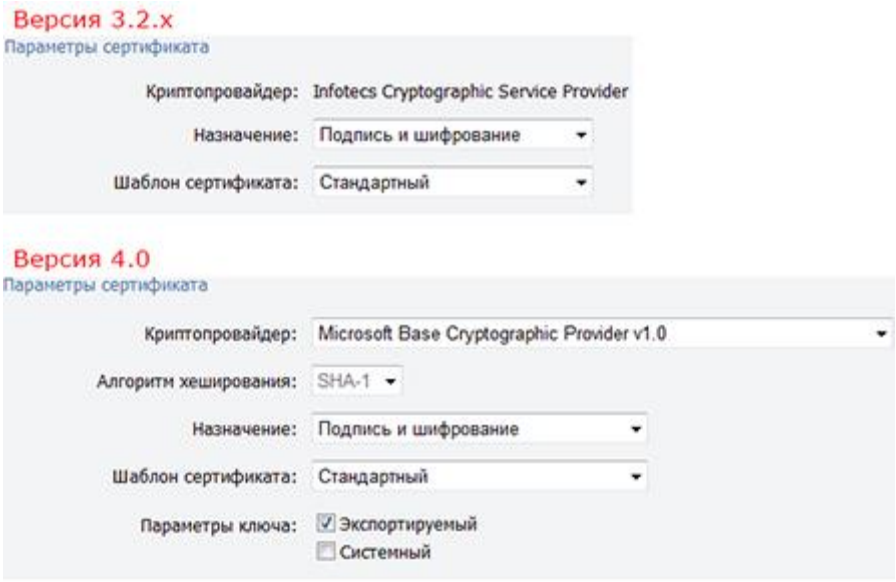


Рисунок 113. Новый интерфейс программы создания запроса на сертификат

- **Отдельное отображение контейнеров ключей, установленных в папку хранения контейнеров ключей пользователя и локального компьютера**

  В разделе **Контейнеры** добавлен переключатель, позволяющий фильтровать контейнеры ключей по месту их хранения.

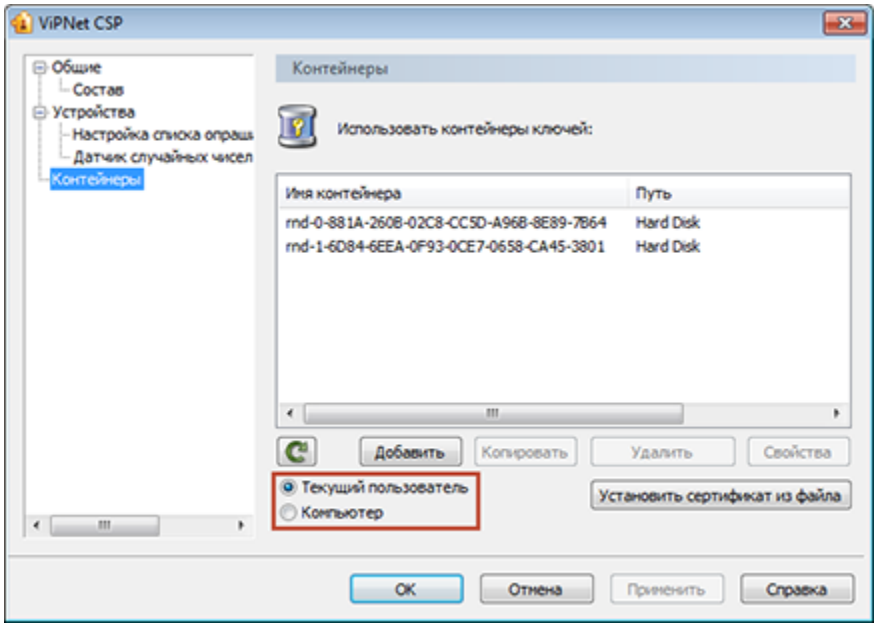


Рисунок 114. Переключатель для фильтрации контейнеров ключей

- **Настройка прав доступа к контейнеру ключей**

  Добавлена возможность задания прав доступа к контейнеру ключей для встроенных учетных записей операционной системы Windows.

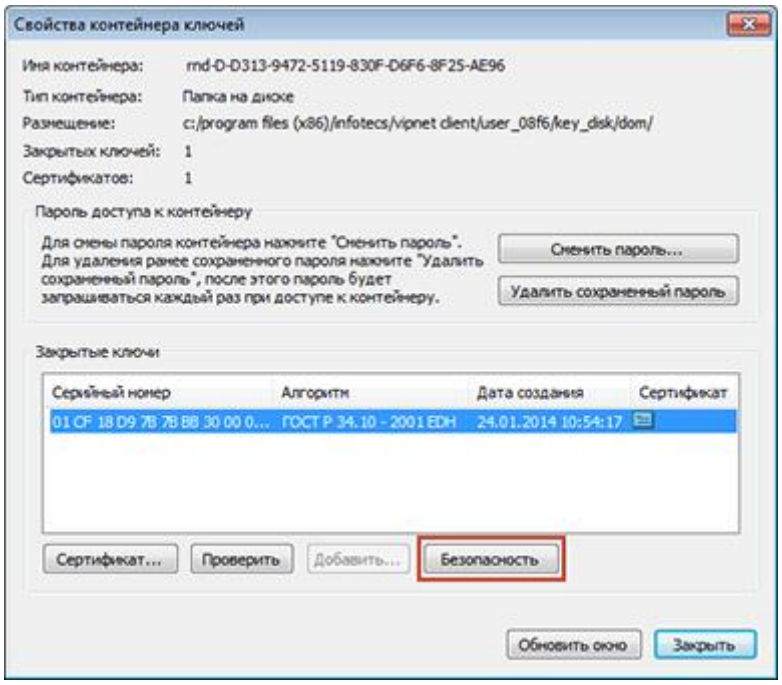


Рисунок 115. Настройка прав доступа к контейнеру ключей

- **Поддержка новых внешних устройств хранения данных**

  Реализована поддержка новых устройств хранения данных, таких как универсальные электронные карты (УЭК), смарт-карты Magistra и других (см. «Внешние устройства» на стр. 214).

- **Интеграция с пакетом программ Microsoft Office 2013**

  Реализована поддержка шифрования и работы с электронной подписью в программах пакета Microsoft Office 2013.

- **Поддержка новых веб-браузеров**

  Добавлена возможность использования ViPNet CSP для работы по протоколу TLS/SSL в веб-браузерах Google Chrome и Яндекс.Браузер (см. «Аутентичность и конфиденциальность соединений TLS» на стр. 26).

- **Регистрация событий криптопровайдера в журнале операционной системы Windows**

  Добавлена возможность ведения журнала событий криптопровайдера. Вы можете задать один из двух режимов ведения журнала (см. «Настройка регистрации событий криптопровайдера» на стр. 103).

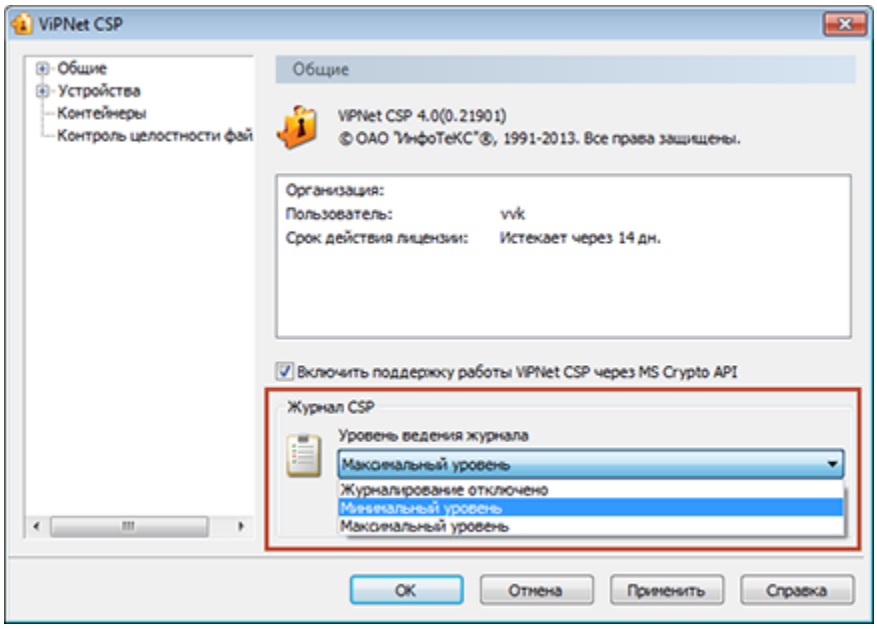


Рисунок 116. Выбор уровня ведения журнала событий криптопровайдера

- **Соответствие требованиям ФСБ России к средствам криптографической защиты информации класса КС3**

  Добавлен механизм контроля целостности файлов, позволяющий создать замкнутую программную среду. Параметры, необходимые для этого, можно настроить в специальном разделе **Контроль целостности**.

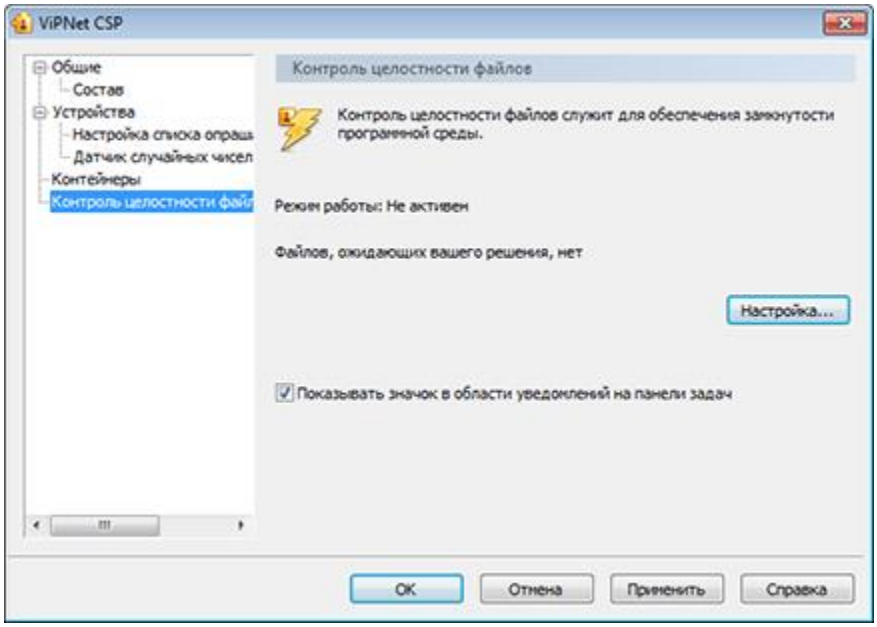


Рисунок 117. Настройка контроля целостности файлов

Примечание. Механизм контроля целостности файлов по умолчанию недоступен. Для его добавления выберите соответствующий компонент при установке программы (см. «Установка программы» на стр. 29).

- **Расширенный комплект документации**

  Комплект документации дополнен руководствами разработчика по криптографическим интерфейсам ViPNet CSP, ViPNet CNG и ViPNet PKCS11.

Версия 3.2.11

В версии 3.2.11 улучшена внутренняя функциональность программы, исправлены незначительные ошибки, выявленные в процессе эксплуатации версии 3.2.10.

Версия 3.2.10

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.2.10 по сравнению с версией 3.2.5.

- **Шаблон запроса на квалифицированный сертификат**

  В программе создания запроса на сертификат появился шаблон, с помощью которого можно создать запрос для получения квалифицированного сертификата (см. глоссарий, стр. 230).

- **Поддержка новых внешних устройств хранения данных**

  Реализована поддержка устройства аутентификации JaCarta, устройств компании Gemalto с апплетом «Аладдин Р.Д.», устройства ruToken Lite компании «Актив», устройства Kaztoken с поддержкой казахстанского стандарта электронной подписи.

- **Новые типы датчиков случайных чисел**

  Внешние устройства, поддерживающие стандарт PKCS#11, можно использовать в качестве датчика случайных чисел при создании закрытого ключа. Также для инициализации датчика случайных чисел можно использовать предварительно созданную последовательность чисел (гамму) с диска ДСДР.

- **Добавление сертификата в контейнер ключей**

  Реализована возможность добавления сертификата в контейнер ключей, содержащий соответствующий закрытый ключ, без его установки в системное хранилище сертификатов.

- **Улучшенная совместимость с КриптоПро CSP**

  Улучшена совместимость программы ViPNet CSP с программным обеспечением КриптоПро CSP.

Версия 3.2.5

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.2.5 по сравнению с версией 3.2.3.

- **Интеграция с пакетом программ Microsoft Office 2010**

  Реализована поддержка шифрования и работы с электронной подписью в программах пакета Microsoft Office 2010.

- **Поддержка серверной части протокола TLS на новых операционных системах**

  Реализована поддержка криптопровайдером защищенных соединений TLS на серверах на базе ОС Microsoft Windows Vista (32/64-разрядная)/Windows 7 (32/64-разрядная)/Server 2008 (32/64-разрядная)/Server 2008 R2.

- **Поддержка 64-разрядных приложений**

  Реализована поддержка приложений, ориентированных на 64-разрядную платформу, в том числе поддержка всех приложений из пакета Microsoft Office 2010.

- **Поддержка устройств Siemens CardOS и Аккорд-5MX**

  Реализована поддержка таких внешних устройств хранения данных, как Siemens CardOS и Аккорд-5MX.

Версия 3.2.3

В версии 3.2.3 улучшена внутренняя функциональность программы, исправлены незначительные ошибки, выявленные в процессе эксплуатации версии 3.2.2.

Версия 3.2.2

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.2.2 по сравнению с версией 3.2.1.

- **Поддержка нового внешнего устройства Mifare Standard4K**

  Реализована поддержка карт Mifare 4K через комбинированное устройство считывателя ACR128.

Версия 3.2.1

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.2.1.

- **Выпущена первая официальная версия программы ViPNet CSP**

Новая программа ViPNet CSP позволяет встроить функции криптопровайдера ViPNet в офисные приложения и работать с защищенными документами и устанавливать соединения TLS/SSL. Программа ViPNet CSP распространяется бесплатно для всех категорий пользователей.

- **Поддержка новых внешних устройств Mifare и eToken ГОСТ**

  Реализована поддержка карт Mifare через устройство считывателя SBSK-03 компании Rosan, а также поддержка устройств eToken ГОСТ компании Аладдин.

- **Поддержка работы с системой Docsvision**

  Реализована возможность интеграции криптопровайдера ViPNet CSP в систему электронного документооборота Docsvision.

- **Изменение срока действия незарегистрированной версии программы**

  Срок действия незарегистрированной версии программы ограничен до 14 дней. Регистрация программы по-прежнему бесплатна и доступна всем желающим на сайте ОАО «ИнфоТеКС».

Внешние устройства

Общие сведения

Внешние устройства предназначены для хранения контейнеров ключей (см. глоссарий, стр. 230), которые вы можете использовать для аутентификации, формирования электронной подписи (см. глоссарий, стр. 232) или для других целей.

На внешнем устройстве могут храниться ключи, созданные по различным алгоритмам в программном обеспечении ViPNet или в сторонних программах. Максимальное количество контейнеров ключей, которое может храниться на одном внешнем устройстве, зависит от объема памяти устройства.

Все операции с контейнерами ключей и внешними устройствами вы можете выполнить в программе ViPNet CSP. Чтобы использовать какое-либо внешнее устройство, на компьютер необходимо установить драйверы этого устройства. Перед записью ключей на устройство убедитесь, что оно отформатировано.

Список поддерживаемых внешних устройств

В следующей таблице перечислены внешние устройства, которые могут быть использованы в программном обеспечении ViPNet. Для каждого семейства устройств в таблице приведено описание, указаны условия и особенности работы с устройствами.

Таблица 6. Поддерживаемые внешние устройства

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
UEC	**Универсальная электронная карта (УЭК)**	На компьютере должен быть доступ в Интернет. На компьютере должно быть установлено ПО ViPNet UEC Client (рекомендуемая версия — 2.0.5.58). Должна быть выполнена настройка ViPNet CSP для взаимодействия УЭК (см. «Настройка ViPNet CSP для взаимодействия с УЭК» на стр. 161). В качестве ПИН-кода используется код ПИН2 вашей карты. В качестве считывателя смарт-карт следует использовать PC/SC-совместимый контактный считыватель.
ESMART Token	Смарт-карты и токены семейств **ESMART Token**, **ESMART Token ГОСТ**	На компьютере должно быть установлено ПО ESMART PKI Client для Windows (рекомендуемая версия — 4.2.33). С помощью ПО ESMART PKI Client для Windows вам может потребоваться отформатировать устройство с профилем ViPNet2. Перенос ключей подписи с устройства и на устройство ESMART Token ГОСТ невозможен, так как на устройстве используется аппаратная криптография с неизвлекаемым ключом. На устройстве ESMART Token ГОСТ нельзя создать запрос на сертификат, в поле «назначение» которого присутствует «шифрование».
Infotecs Software Token	**Infotecs Software Token** — программная реализация стандарта PKCS#11	Необходимое ПО входит в поставку ViPNet CSP. С помощью программы token_manager.exe на компьютере должен быть создан программный токен. Подробную информацию о работе с программным токеном см. в документе «Криптографический интерфейс ViPNet PKCS#11 VT. Руководство разработчика», раздел «Создание и удаление слотов и токенов в ViPNet PKCS#11 VT».

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
A-Key	Смарт-карты **aKey S1000**, **aKey S1003**, **aKey S1004** производства компании Ak Kamal Security	На компьютере должна быть установлена библиотека akpkcs11.dll, предоставленная компанией Ak Kamal Security. Устройство имеет два ПИН-кода: администратора и пользователя. Значение этих ПИН-кодов по умолчанию — `12345678`. Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.
ViPNet HSM	Программно-аппаратный комплекс **ViPNet HSM** производства ОАО «ИнфоТеКС»	В программе ViPNet CSP необходимо задать параметры подключения к серверу ViPNet HSM (см. «Настройка ViPNet CSP для взаимодействия с сервером ViPNet HSM» на стр. 157).
JaCarta	Персональные электронные ключи и смарт-карты **JaCarta PKI** и **JaCarta PKI/ГОСТ** производства компании «Аладдин Р.Д.»	На компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая версия — 2.9.0.1531). Устройства JaCarta PKI/ГОСТ определяются как принадлежащие одновременно к семействам JaCarta и eToken GOST/JaCarta GOST. Во избежание возникновения проблем рекомендуется запретить опрос неиспользуемого семейства устройств. При использовании устройства JaCarta PKI/ГОСТ во избежание появления ошибок не следует сохранять ПИН-коды этого устройства на компьютере.
JCDS	Смарт-карты **Gemalto Optelio Contactless D72**, **KONA 131 72K** и токен **JaCarta LT** с апплетом от компании «Аладдин Р.Д.»	На карту или токен должен быть загружен апплет Datastore, позволяющий модулю jcpkcs11ds.dll (рекомендуемая версия — 1.1.3.20) производства компании «Аладдин Р.Д.» работать с картой или токеном. Для администрирования токенов JaCarta LT на компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая версия — 2.9.0.1531).
Siemens CardOS	Смарт-карты **CardOS/M4.01a**, **CardOS V4.3B**, **CardOS V4.2B**, **CardOS V4.2B DI**, **CardOS V4.2C**, **CardOS V4.4** производства компании Atos (Siemens)	На компьютере должно быть установлено ПО Siemens CardOS API V5.0. Смарт-карты должны быть особым образом размечены. Обратитесь к производителю устройств.

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
eToken GOST/ **JaCarta GOST**	Персональные электронные ключи **eToken ГОСТ** и **JaCarta ГОСТ** , а также персональные электронные ключи и смарт-карты **JaCarta PKI/ГОСТ** производства компании «Аладдин Р.Д.»	Для работы с указанными устройствами на компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая версия — 2.9.0.1531). Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом. Устройства JaCarta PKI/ГОСТ определяются как принадлежащие одновременно к семействам JaCarta и eToken GOST/JaCarta GOST. Во избежание возникновения проблем рекомендуется запретить опрос неиспользуемого семейства устройств.
Rutoken ECP/ **Rutoken Lite**	Электронные идентификаторы **Рутокен ЭЦП**, **Рутокен ЭЦП 2.0** и **Рутокен Lite** производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.2.2.0). Перенос ключей подписи с устройств, а также на устройства Рутокен ЭЦП и Рутокен ЭЦП 2.0 невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.
Rutoken/ **Rutoken S**	Электронные идентификаторы **Рутокен** и **Рутокен S** производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.2.2.0).
SafeNet eToken (eToken Aladdin)	Персональные электронные ключи **Gemalto SafeNet eToken 5100/5105**, **5200/5205**, **5110**, **7300**, смарт-карта **Gemalto SafeNet eToken 4100** производства компании Gemalto (SafeNet) Персональные электронные ключи **eToken PRO (Java)**, **eToken PRO**, смарт-карты **eToken PRO (Java)**, **eToken PRO**, **JaCarta PRO** производства компании «Аладдин Р.Д.»	Если компьютер работает под управлением ОС Windows 10, на нем должно быть установлено ПО SafeNet Authentication Client (рекомендуемая версия — 10.0.43). Если компьютер работает под управлением другой ОС, на нем должно быть установлено либо ПО PKI Client версии 5.1 SP1, либо ПО SafeNet Authentication Client (рекомендуемая версия — 10.0.43). Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC-совместимым устройством считывания карт. Для работы смарт-карты JaCarta PRO на компьютере должно быть установлено ПО JC-PROClient версии 1.0.6 и должен быть включен режим совместимости с eToken.

Примечание. Список поддерживаемых операционных систем для каждого из приведенных устройств вы найдете на официальном веб-сайте производителя этого устройства.

Алгоритмы и функции, поддерживаемые внешними устройствами

В следующей таблице перечислены криптографические алгоритмы, поддерживаемые внешними устройствами, приведена информация о возможности использования устройств в качестве датчиков случайных чисел, а также информация о поддержке стандарта PKCS#11.

Примечание. Стандарт PKCS#11 (также известный как Cryptoki) — один из стандартов семейства PKCS (Public Key Cryptography Standards — криптографические стандарты ключа проверки электронной подписи), разработанных компанией RSA Laboratories. Стандарт определяет независимый от платформы интерфейс API для работы с криптографическими устройствами идентификации и хранения данных.

Таблица 7. Алгоритмы и функции, поддерживаемые внешними устройствами

Название семейства устройств в программе ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Использование ДСЧ в ViPNet CSP	Поддержка PKCS#11
UEC	ГОСТ Р 34.10-2001	отсутствует	Нет	Да
ESMART Token	**ESMART Token** — отсутствует; **ESMART Token ГОСТ** — ГОСТ Р 34.10-2001	**ESMART Token** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 **ESMART Token ГОСТ** — отсутствует	Нет	Да
Infotecs Software Token	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (изолированная программная реализация)	отсутствует	Нет	Да
A-Key	**aKey S1000**, **aKey S1003**, **aKey S1004** — ГОСТ Р 34.10-2012; **aKey S1000**, **aKey S1003** — ГОСТ Р 34.10-2001	отсутствует	Нет	Да

Название семейства устройств в программе ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Использование ДСЧ в ViPNet CSP	Поддержка PKCS#11
ViPNet HSM	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	отсутствует	Нет	Да
JaCarta	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
JCDS	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
Siemens CardOS	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
eToken GOST/ **JaCarta GOST**	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ)	отсутствует	Да	Да
Rutoken ECP/ **Rutoken Lite**	**Рутокен ЭЦП** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ); **Рутокен ЭЦП 2.0** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012; **Рутокен Lite** — отсутствует	**Рутокен ЭЦП** — отсутствует; **Рутокен ЭЦП 2.0** — отсутствует; **Рутокен Lite** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	**ЭЦП** — да; **ЭЦП 2.0** — да; **Lite** — нет	Да
Rutoken/ **Rutoken S**	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
SafeNet eToken (eToken Aladdin)	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да

Примечание. Шифрование поддерживается не всеми перечисленными устройствами. Для получения более подробной информации см. документацию по необходимому устройству.

D

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 понадобится 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 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**) > **Региональные стандарты** (**Region**).

2 В окне **Регион** (**Region**) перейдите на вкладку **Дополнительно** (**Administrative**).

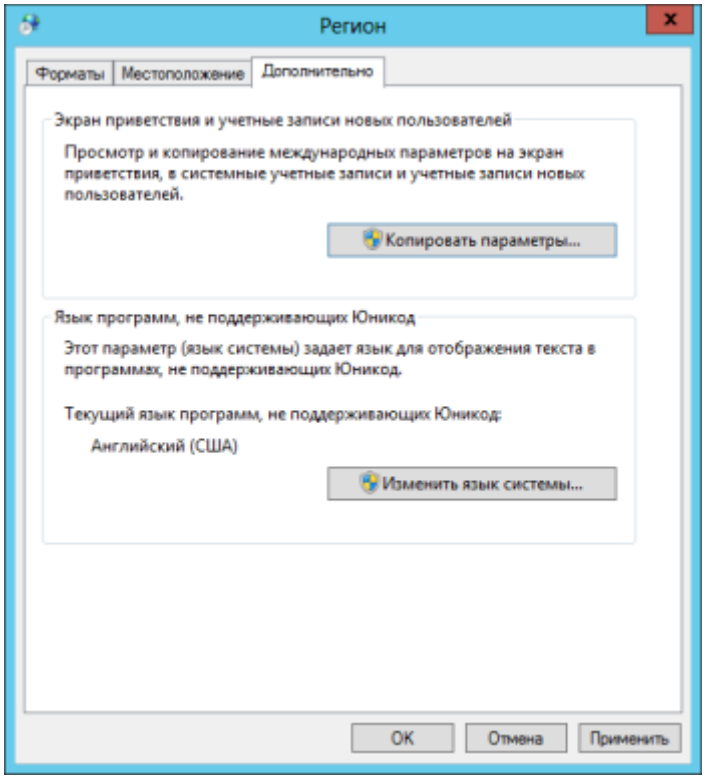


Рисунок 118. Дополнительные языковые параметры

3 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Изменить язык системы** (**Change system locale**).

4 В появившемся окне в списке выберите **Русский (Россия)** (**Russian (Russia)**).

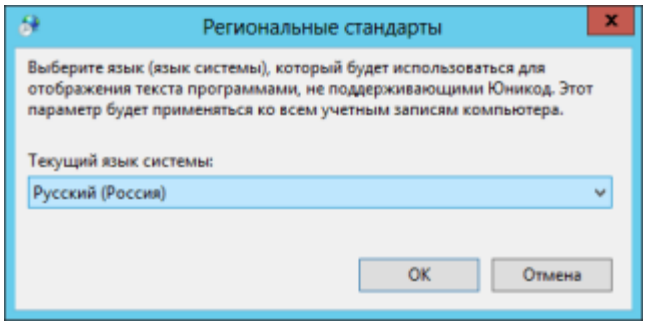


Рисунок 119. Выбор языка системы

5 Нажмите кнопку **OK**. Перезагрузите компьютер.

6 Дождитесь завершения перезагрузки компьютера и откройте **Панель управления** (**Control Panel**) > **Региональные стандарты** (**Region**).

7 В окне **Регион** (**Region**) перейдите на вкладку **Дополнительно** (**Administrative**).

8 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Копировать параметры** (**Copy settings**).

9 В открывшемся окне в списке **Копировать текущие параметры в**: установите флажок **Экран приветствия и системные учетные записи** (**Welcome screen and system accounts**) и нажмите кнопку **OK**.

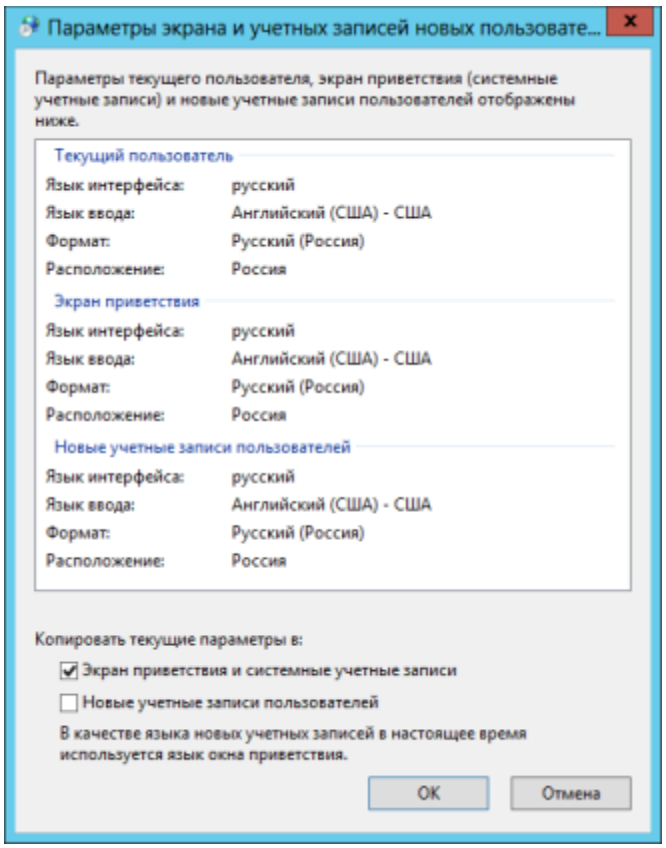


Рисунок 120. Копирование параметров

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)**).

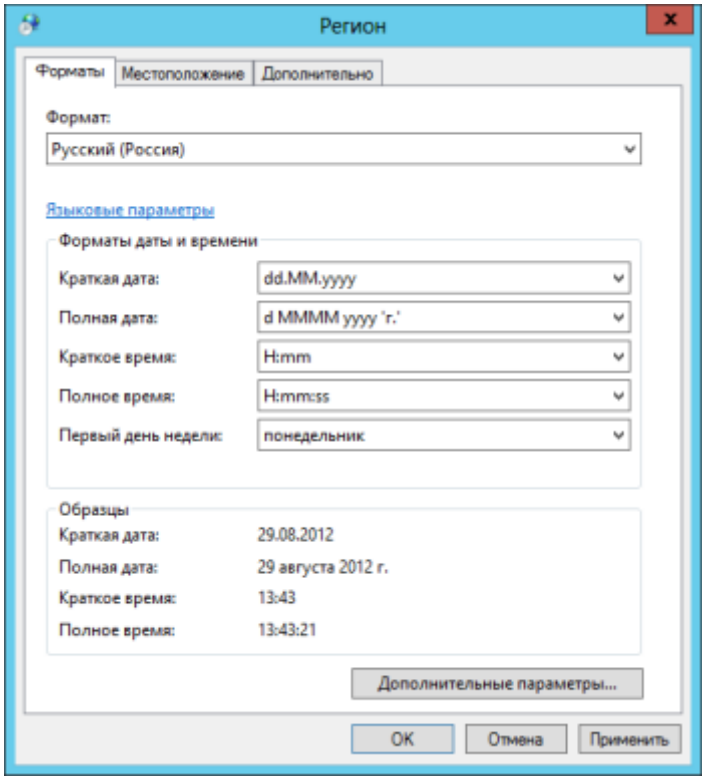


Рисунок 121. Настройка форматов

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

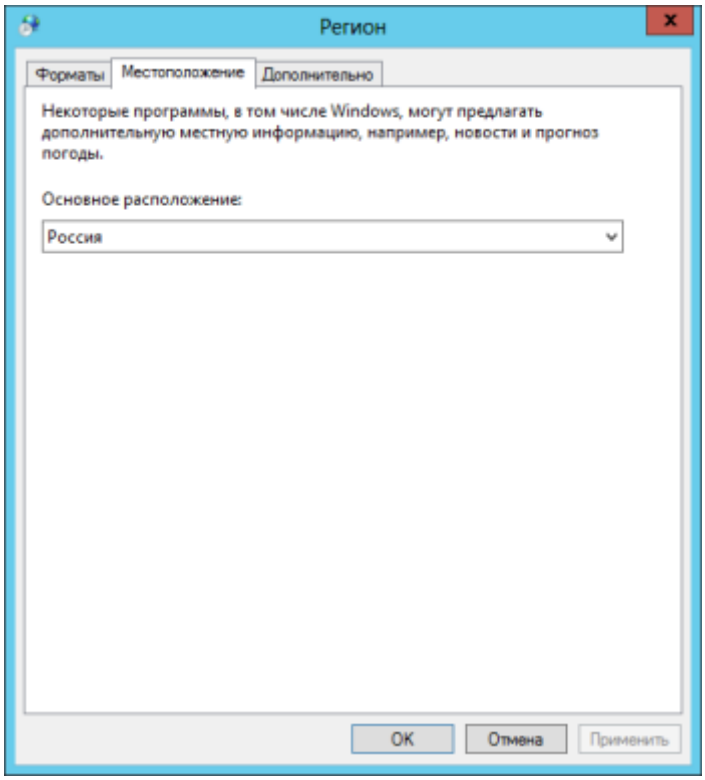


Рисунок 122. Выбор текущего расположения

Региональные настройки в ОС Windows 7, Windows Server 2008 R2

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

1 Откройте **Панель управления** (**Control Panel**) > **Часы, язык и регион** (**Clock, Language, and Region**) > **Язык и региональные стандарты** (**Region and Language**).

2 В окне **Язык и региональные стандарты** (**Region and Language**) перейдите на вкладку **Дополнительно** (**Administrative**).

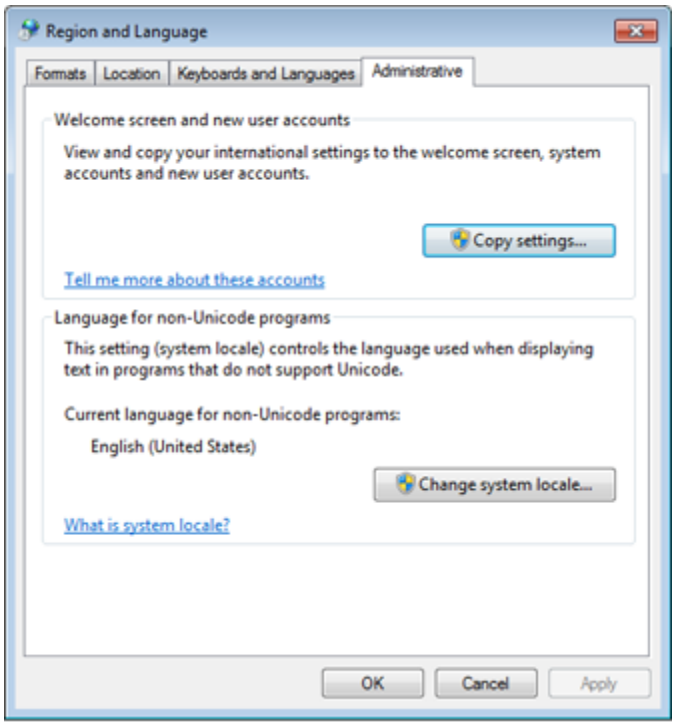


Рисунок 123. Дополнительные языковые параметры

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)**).

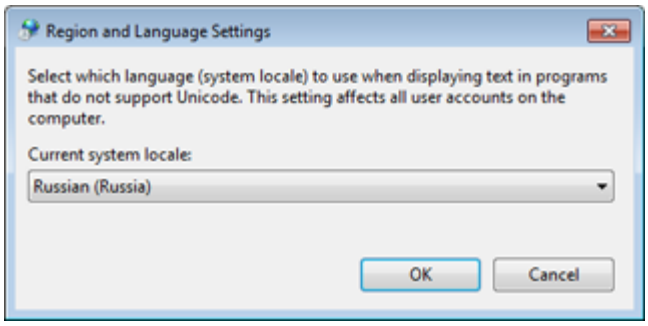


Рисунок 124. Выбор языка системы

5 Нажмите кнопку **OK**. Перезагрузите компьютер.

6 Дождитесь завершения перезагрузки компьютера и откройте **Панель управления** (**Control Panel**) > **Часы, язык и регион** (**Clock, Language, and Region**) > **Язык и региональные стандарты** (**Region and Language**).

7 В окне **Язык и региональные стандарты** (**Region and Language**) перейдите на вкладку **Дополнительно** (**Administrative**).

8 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Копировать параметры** (**Copy settings**).

9 В открывшемся окне установите флажок **Экран приветствия и системные учетные записи** (**Welcome screen and system accounts**) и нажмите кнопку **OK**.

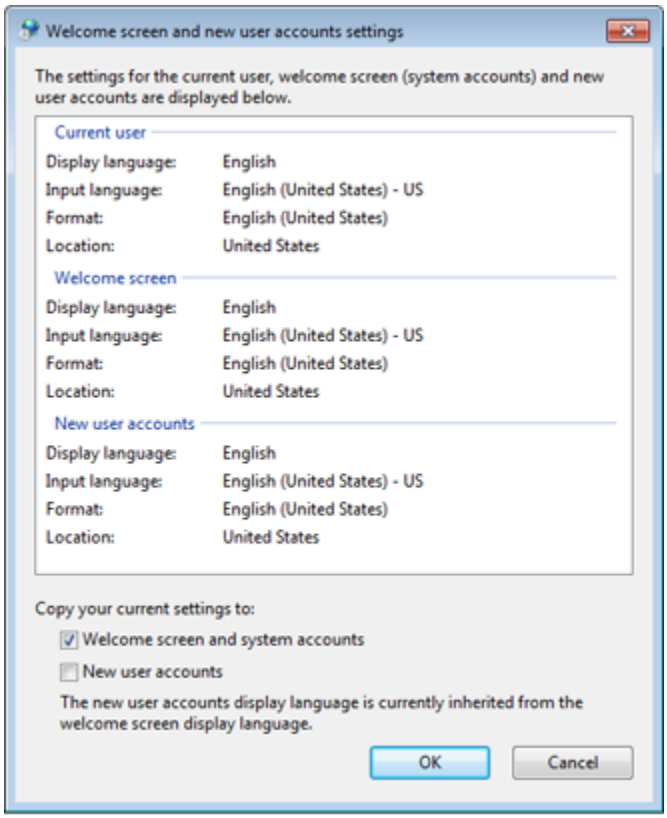


Рисунок 125. Копирование параметров

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)**).

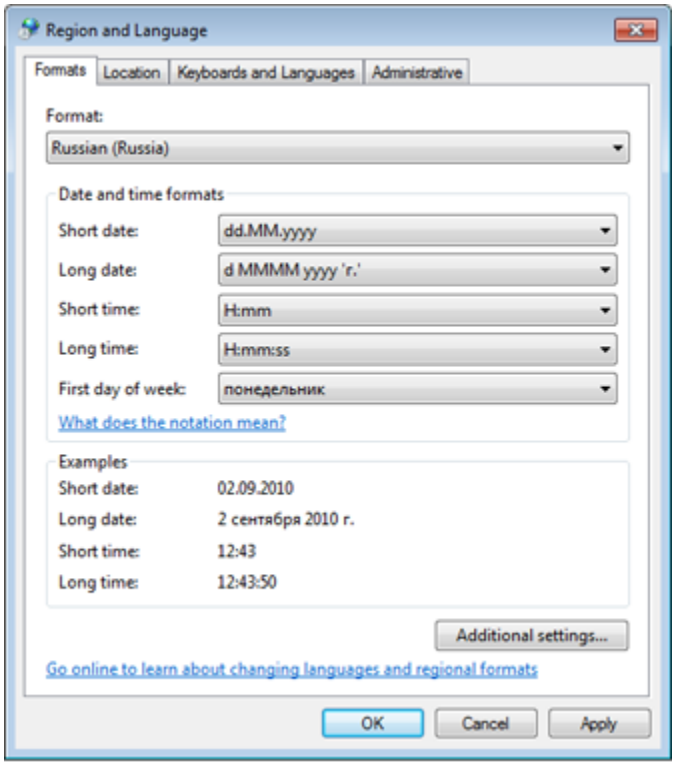


Рисунок 126. Настройка форматов

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

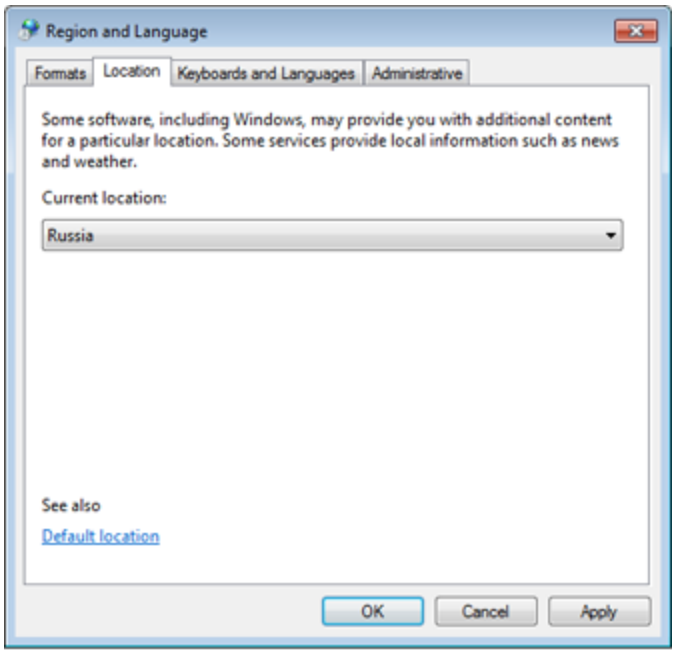


Рисунок 127. Выбор текущего расположения

E

Глоссарий

PKI (инфраструктура открытых ключей)

От англ. Public Key Infrastructure — инфраструктура открытых ключей. Комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам (в том числе ключам проверки электронной подписи) в распределенных системах через создание сертификатов ключей проверки электронной подписи и поддержание их жизненного цикла.

S/MIME (Secure Multipurpose Internet Mail Extensions)

Спецификация безопасных сообщений электронной почты, использующая стандарт X.509 и различные механизмы шифрования (ГОСТ 28147-89, 3DES и другие).

ViPNet HSM

Программно-аппаратный комплекс производства ОАО «ИнфоТеКС». Представляет собой сервер, который предоставляет клиентам защищенное хранилище ключей электронной подписи и обеспечивает выполнение основных криптографических операций в защищенном окружении. Взаимодействие клиентов с ViPNet HSM осуществляется по стандарту PKCS#11.

Асимметричное шифрование

Система шифрования, при которой алгоритмы используют два математически связанных ключа. Открытый ключ используется для зашифрования и передается по незащищенному каналу. Закрытый ключ служит для расшифрования.

Доверенное лицо (администратор) удостоверяющего центра

Лицо, обладающее правом издавать сертификаты от имени удостоверяющего центра.

Запрос на сертификат

Защищенное электронной подписью сообщение, содержащее имя пользователя, ключ проверки электронной подписи и его параметры, желаемый срок действия сертификата, предполагаемые назначения сертификата и другие параметры (полный набор параметров зависит от формата запроса и программного обеспечения, в котором он был сформирован).

Квалифицированный сертификат

Сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

Ключ проверки электронной подписи

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

Ключ электронной подписи

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

Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

Контейнер ключей терминала

Контейнер ключей, необходимый для работы с универсальными электронными картами. Формируется в пункте выдачи карт при первом развертывании рабочего места оператора.

Корневой сертификат

Сертификат администратора удостоверяющего центра, являющийся последним сертификатом в цепочке доверия. Другими словами, для корневого сертификата нет сертификата, с помощью которого можно было бы проверить его достоверность. С помощью корневого сертификата проверяется достоверность сертификатов (пользователей и издателей), заверенных этим сертификатом.

Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

Сертификат ключа проверки электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. сертификатом ключа проверки электронной подписи называется сертификат открытого ключа.

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

Сертификат оператора канала обслуживания

Сертификат, необходимый для работы с универсальными электронными картами. Выдается пользователю в пункте выдачи карт.

Сертификат терминала

Сертификат, необходимый для работы с универсальными электронными картами. Выдается пользователю в пункте выдачи карт.

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.

Точка распространения данных

Источник, доступный по общеизвестным протоколам (например, HTTP или LDAP), используемый для размещения сформированной в удостоверяющем центре информации (сертификатов издателей и списков аннулированных сертификатов).

Удостоверяющий центр

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

Универсальная электронная карта (УЭК)

Универсальная электронная карта (УЭК) дает возможность получать все государственные и муниципальные услуги, оказываемые в электронной форме согласно законодательству Российской Федерации. На УЭК может размещаться контейнер ключей с квалифицированным сертификатом, который дает пользователю возможность совершать юридически значимые действия.

Цепочка сертификации

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

Электронная подпись

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

Электронная рулетка

Встроенный компонент программного обеспечения ViPNet, который позволяет инициализировать датчик случайных чисел на основе действий пользователя. Полученная последовательность используется при формировании ключей узла.

Указатель

И

К

Н

О

П

Р

С

У

Ц

Ш

Э