ViPNet CSP 4.0

Руководство пользователя

ViPNet Virtual Private Network

infotecs

ФРКЕ.00106-01 34 01

ОАО «ИнфоТеКС»

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

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

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

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

Для кого предназначен документ

Данное руководство предназначено для пользователей программы ViPNet CSP — пользователей систем электронного документооборота, работающих с сертификатами для шифрования документов, сообщений электронной почты, для подписания и проверки подлинности электронной подписи, а также системных администраторов, организующих удаленный доступ к ресурсам по протоколам TLS/SSL.

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.

ViPNet CSP обеспечивает:

- Создание ключей электронной подписи (см. «Электронная подпись» на стр. 236) в соответствии с алгоритмами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.
- Формирование и проверку 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 имитозащиту данных в соответствии с алгоритмом ГОСТ 28147-89.
- Генерацию случайных и псевдослучайных чисел, сессионных ключей шифрования.
- Аутентификацию и выработку сессионного ключа при передаче данных по протоколам SSL/TLS.
- Хранение сертификатов открытых ключей непосредственно в контейнерах ключей.
- Поддержку различных устройств хранения электронных ключей (eToken, ruToken, Shipka и др.).

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).

Системные требования

Примечание. Совместимость криптопровайдера ViPNet CSP с ОС Windows 7 признана корпорацией Microsoft на официальном уровне.

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 — Microsoft XP (32-разрядная), Server 2003 (32-разрядная), Vista (32/64-разрядная), Windows 7 (32/64-разрядная), Windows Server 2008 (32/64-разрядная), Windows Server 2008 R2 (64-разрядная), Windows 8 (32/64-разрядная), Windows Server 2012 (64-разрядная).

  Для операционной системы должен быть установлен самый последний пакет обновлений.
- Internet Explorer — версия 6.0 или выше.
- При использовании программ Microsoft Office — версия 2003, 2007, 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. 216).

Совместимость с программным обеспечением 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. 28) требуется

использовать криптопровайдер ViPNet CSP, в программе ViPNet CSP в разделе **Общие** должен быть установлен флажок **Включить поддержку работы ViPNet CSP через MS Crypto API**. При этом убедитесь, что на компьютере не установлен компонент «Совместимость с продуктами Microsoft», входящий в ПО КриптоПро CSP версии 3.6.

- Если для выполнения криптографических операций в поддерживаемых приложениях требуется использовать криптопровайдер КриптоПро CSP, на компьютере должен быть установлен компонент КриптоПро CSP «Совместимость с продуктами Microsoft». При этом в программе ViPNet CSP в разделе **Общие** должен быть снят флажок **Включить поддержку работы ViPNet CSP через MS Crypto API**. Кроме того, для подписи документов Microsoft Office необходимо дополнительно установить программу КриптоПро Office Signature.

Внимание! Не следует одновременно устанавливать на компьютер компонент КриптоПро CSP «Совместимость с продуктами Microsoft» и в программе ViPNet CSP устанавливать флажок **Включить поддержку работы ViPNet CSP через MS Crypto API**.

Сертификаты пользователей, сформированные в удостоверяющем центре КриптоПро по запросу из программы ViPNet CSP, могут использоваться для подписи с помощью криптопровайдера ViPNet CSP. Аналогично сертификаты, сформированные с помощью программы ViPNet Удостоверяющий и ключевой центр по запросу из программы КриптоПро CSP, могут использоваться в КриптоПро CSP.

Примечание. Закрытые ключи, сформированные с помощью криптопровайдера ViPNet CSP, невозможно использовать в программном обеспечении КриптоПро CSP.

Комплект поставки

В комплект поставки программы ViPNet CSP входят:

- Установочный файл ViPNet CSP `setup.exe`.
- Документация в формате PDF, в том числе:
  - ViPNet CSP. Руководство пользователя.
  - Криптографический интерфейс ViPNet CSP. Руководство разработчика.
  - Криптографический интерфейс ViPNet CNG. Руководство разработчика.
  - Криптографический интерфейс ViPNet PKCS#11 VT. Руководство разработчика.

Новые возможности версии 4.0

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.0 по сравнению с версией 3.2.10.

- **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.

- **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. Для этого поле **Криптопровайдер** преобразовано в список.
  - Добавлена возможность выбора алгоритма хеширования. Для этого добавлен соответствующий список.
  - 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, будет ли создаваемый сертификат экспортируемым и следует ли его устанавливать в системное хранилище локального компьютера.

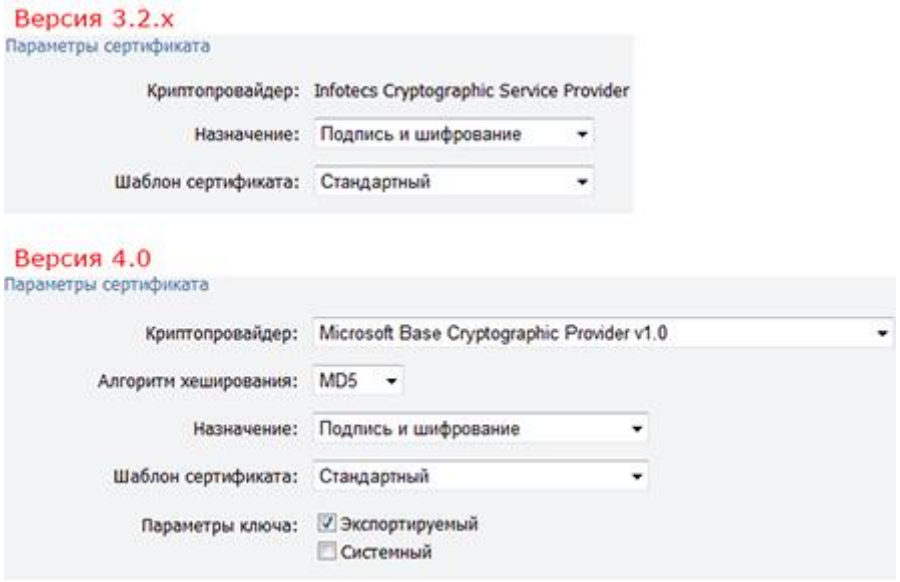


Рисунок 1: Новый интерфейс программы создания запроса на сертификат

- **Отдельное отображение контейнеров ключей, установленных в папку хранения контейнеров ключей пользователя и локального компьютера**

  В разделе **Контейнеры** добавлен переключатель, позволяющий фильтровать контейнеры ключей.

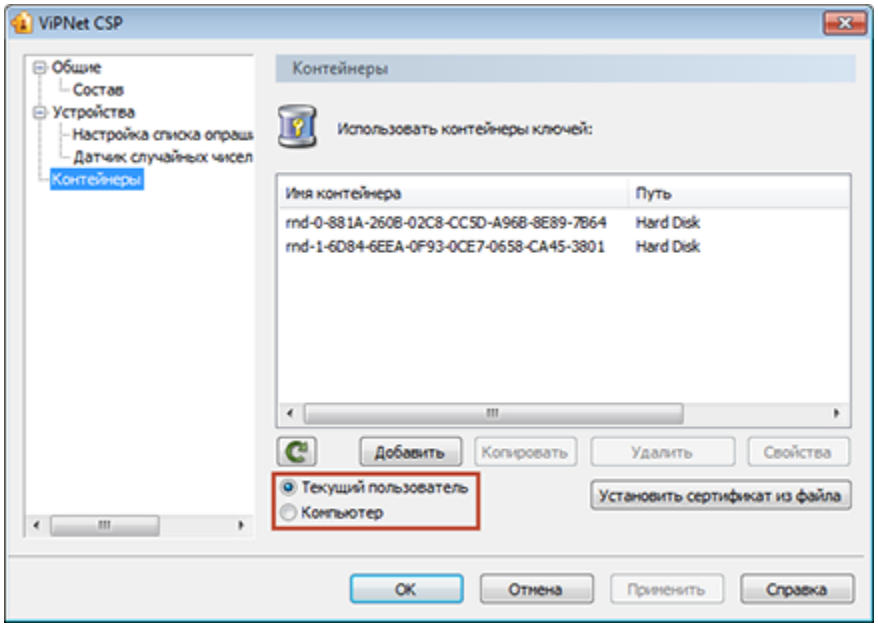


Рисунок 2: Переключатель для фильтрации контейнеров ключей

- **Поддержка новых внешних устройств хранения данных**

  Реализована поддержка новых устройств хранения данных, таких как смарт-карты Magistra и других (см. «Внешние устройства» на стр. 216).

- **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/SSL» на стр. 27).

- **Соответствие требованиям ФСБ России к средствам криптографической защиты информации класса КС3**

  Добавлен механизм контроля целостности файлов. Параметры, необходимые для создания замкнутой программной среды, можно настроить в специальном разделе **Контроль целостности**.

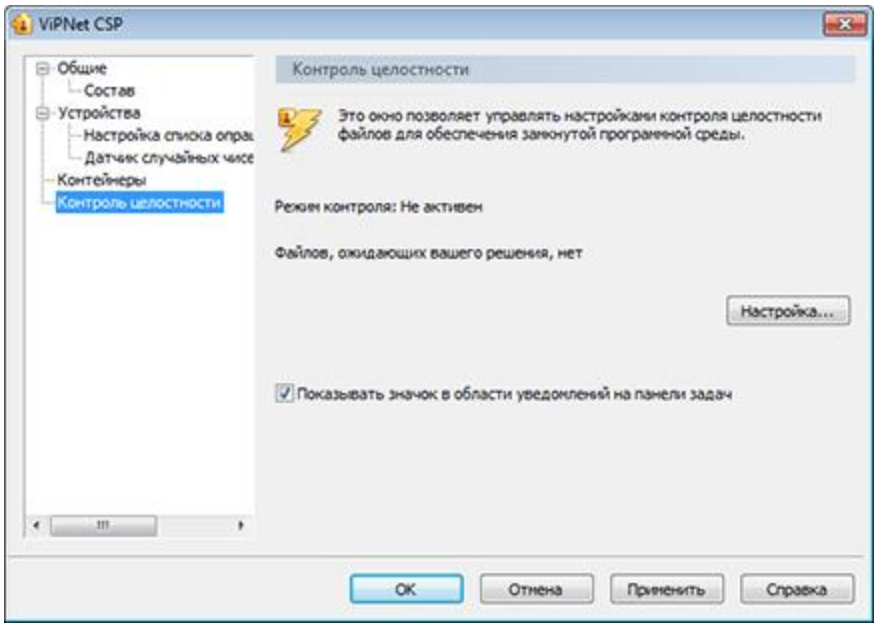


Рисунок 3: Настройка контроля целостности файлов

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.
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Законодательная база в сфере защиты информации http://www.infotecs.ru/laws/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/vpn/.

Контактная информация

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

- Электронный адрес службы поддержки: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки http://www.infotecs.ru/support/request/.
- Форум ОАО «ИнфоТеКС» http://www.infotecs.ru/forum.
- 8 (495) 737-6196 — «горячая линия» службы технической поддержки.
- 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.

Использование криптопровайдера в системах защиты данных

Назначение криптопровайдера

Криптопровайдер ViPNet CSP предназначен для реализации криптографических функций в операционной системе Windows.

Примечание. Поскольку криптопровайдер является независимым программным модулем, то для его работы не требуется запуск другого клиентского ПО ViPNet.

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/SSL.

Примечание. В ОС семейства Microsoft, начиная с Windows 2000, встроен криптопровайдер Microsoft Base Cryptographic Provider, который обладает набором основных криптографических функций. Алгоритмы, используемые данными функциями, не сертифицированы по требованиям ФСБ.

Шифрование и подпись документов

Для осуществления функций шифрования и проверки электронной подписи криптопровайдер ViPNet CSP использует открытый ключ, находящийся в сертификате (см. «Сертификат открытого ключа подписи пользователя» на стр. 235) 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 Microsoft Outlook.

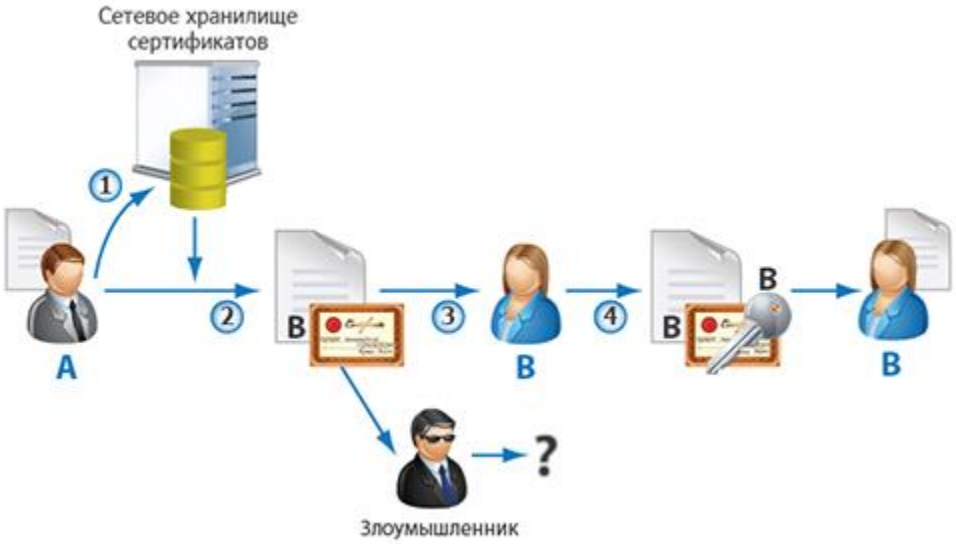


Рисунок 4: Схема обмена защищенными документами

Пользователю **A** необходимо передать пользователю **B** конфиденциальное сообщение Outlook:

1. Пользователь **A** запрашивает из сетевого хранилища сертификат открытого ключа пользователя **B** и сопоставляет его с контактом **B** в программе Microsoft Outlook.
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 письмо 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.

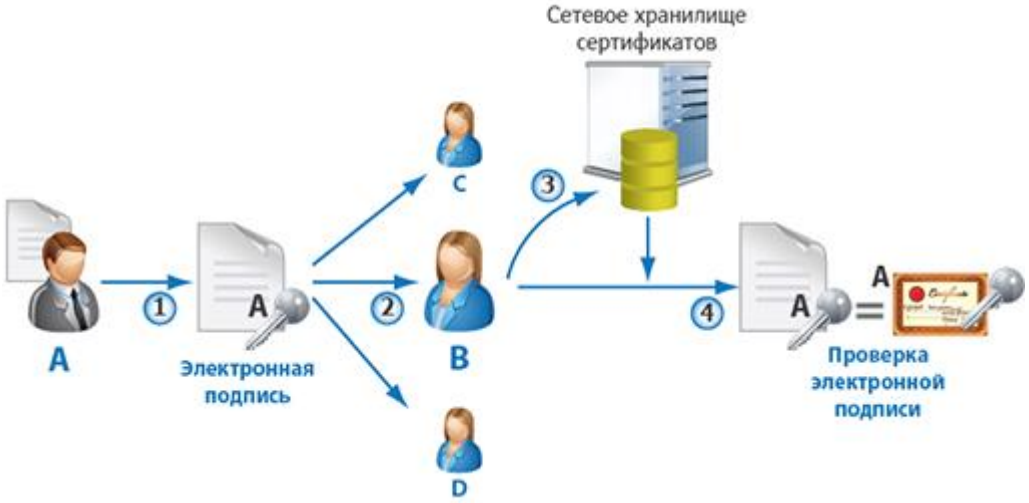


Рисунок 5: Процесс формирования и проверки электронной подписи документа

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

1 Пользователь **A** подписывает документ своим закрытым ключом.

2 Пользователь **A** отправляет данный документ всем заинтересованным лицам (пользователи **B**, **C** и **D**) или выкладывает для общего доступа.

3 Пользователь **B** запрашивает сертификат открытого ключа пользователя **A** в хранилище сертификатов.

4 Пользователь **B** проверяет документ 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 не удалась, это означает, что документ не принадлежит пользователю **A** или редактировался сторонними лицами, или был поврежден в процессе пересылки. В этом случае пользователь **B** может запросить у пользователя **A** документ повторно.

Контейнер ключей

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

Закрытый ключ генерируется 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. 63) или, в некоторых случаях, по инициативе администратора удостоверяющего центра. Запрос на выдачу или обновление сертификата пользователя вы можете сделать из клиентского ПО ViPNet CryptoService, ViPNet Client, программы «Создание запроса на сертификат» (см. «Порядок получения и ввода в действие закрытого ключа и сертификата» на стр. 62), входящей в пакет установки ViPNet CSP, или программ сторонних разработчиков.

Кроме этого необходимы цепочка сертификатов издателя (см. «Сертификат издателя» на стр. 234) и список отозванных сертификатов (см. «Список отозванных сертификатов (СОС)» на стр. 235) для проверки подлинности сертификата пользователя и его актуальности.

При организации защищенного документооборота приложение (программа из состава Microsoft Office, веб-браузер Internet Explorer, 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. 70).
- Сертификат издателя и СОС устанавливаются стандартными средствами операционной системы (см. «Установка сертификатов издателей и СОС» на стр. 84).

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. 72) или на внешнем устройстве (см. «Установка контейнера ключей с внешнего устройства» на стр. 75).

- Путем установки сертификата и сопоставление ему закрытого ключа из контейнера ключей в папке на диске или внешнем устройстве (см. «Установка сертификата в системное хранилище» на стр. 79).

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. Файлы сертификатов всегда создаются только в определенных стандартных форматах:

- Файл формата X.509, содержащий только сертификат (файлы с расширениями `.crt`, `.cer`);
- Файл формата PKCS#7 или PKCS#12. Эти форматы предназначены для хранения зашифрованных и подписанных сообщений вместе с соответствующими сертификатами. Файл одного из этих форматов также может использоваться для передачи наборов сертификатов и списков отозванных сертификатов (файлы с расширениями `.p7r`, `.p7b`, `.pfx`, `.p12`).

Примечание. 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.

Электронная подпись

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

Электронная подпись позволяет подтвердить:

- 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».

Чтобы иметь возможность ставить электронную подпись, необходимо получить в компетентном удостоверяющем центре сертификат электронной подписи (см. «Контейнер ключей» на стр. 24).

Если проверка сертификата по базе данных удостоверяющего центра показала, что он является законным, действующим, не был просрочен или отозван, то сертификат считается действительным. Документы, подписанные действительным сертификатом электронной подписи и не изменявшиеся с момента их подписания, также считаются действительными.

Аутентичность и конфиденциальность соединений TLS/SSL

Протокол TLS/SSL 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 для другой функциональности.

Взаимодействие двух узлов при защищенном соединении представлено на схеме ниже.

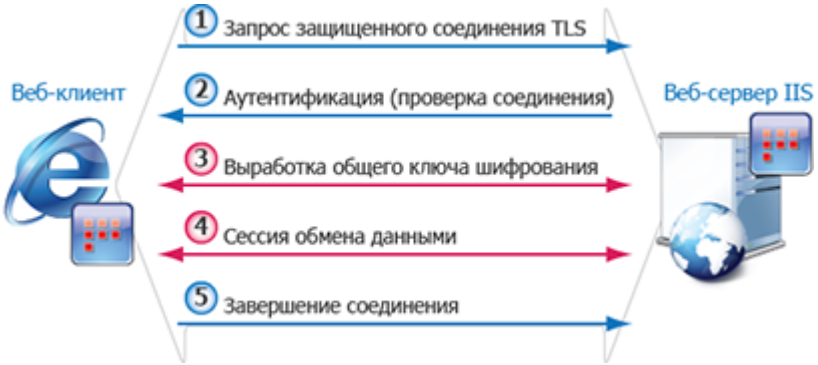


Рисунок 6: Схема взаимодействия узлов при TLS-соединении

Примечание. В качестве веб-клиента помимо Microsoft Internet Explorer могут использоваться браузеры Google Chrome и Яндекс.Браузер. Однако для этого в свойствах ярлыка браузера в поле **Объект** необходимо после пути к программе добавить команду `--use-system-ssl`.

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

Практическое применение ViPNet CSP

С помощью программы ViPNet CSP вы можете выполнять следующие операции:

- Зашифровывать сообщения Microsoft Outlook, Microsoft Outlook Express/Почта Microsoft Windows/Почта Microsoft Windows Live и вложенные файлы (см. «Шифрование сообщений электронной почты» на стр. 157).
- Формировать и проверять электронную подпись в приложениях Microsoft Office (см. «Электронная подпись в документах Microsoft Office» на стр. 117).
- Подписывать сообщения Microsoft Outlook, Outlook Express/Почта Microsoft Windows/Почта Microsoft Windows Live (см. «Электронная подпись и шифрование в почтовых программах Microsoft» на стр. 136).
- Подписывать формы Microsoft Office InfoPath (см. «Электронная подпись в Microsoft Office InfoPath» на стр. 165).
- Подписывать макросы в программах Microsoft Word, Excel, Outlook, PowerPoint, Access, Publisher и Visio (см. «Электронная подпись макросов и баз данных» на стр. 175).
- Устанавливать защищенные веб-соединения TLS/SSL, используя сервер IIS и браузер Microsoft Internet Explorer, Google Chrome или Яндекс.Браузер (см. «Организация защищенного соединения TLS/SSL» на стр. 184).
- Выполнять криптографические функции в системе электронного документооборота Docsvision.
- Выполнять аутентификацию в ОС Windows с помощью протокола Kerberos.
- Выполнять криптографические операции, необходимые для работы службы сертификатов Active Directory.

2

Быстрый старт

Если существует необходимость защищать электронные документы средствами криптографии, подписывать документы электронной подписью, обеспечивая их подлинность и целостность, необходимо установить специализированные модули — криптопровайдеры (см. «Назначение криптопровайдера» на стр. 20). Все версии операционной системы Windows, начиная с Windows 2000, имеют встроенный криптопровайдер. Однако во многих случаях Закон РФ «Об электронной подписи» требует применения сертифицированных криптографических средств, таких как ViPNet CSP.

Для подготовки к использованию криптопровайдера ViPNet CSP выполните следующие действия:

1. Установите программу ViPNet CSP (см. «Установка программы» на стр. 33).
2. Получите сертификат открытого ключа и контейнер с закрытым ключом:
   - Файл сертификата и файл контейнера с закрытым ключом (либо файл контейнера, содержащий и закрытый ключ, и сертификат) могли быть выданы вам ранее администратором вашего удостоверяющего центра. Убедитесь, что вы располагаете этими файлами.
   - Если файлов контейнера и сертификата нет, создайте запрос на получение сертификата (см. «Порядок получения и ввода в действие закрытого ключа и сертификата» на стр. 62).

   Вместе с сертификатом и контейнером поставляется сертификат издателя (на стр. 234) и список отозванных сертификатов (СОС) (на стр. 235).

Примечание. Сертификат содержит открытый ключ, которому соответствует единственный закрытый ключ. Закрытый ключ хранится у пользователя и предназначен для формирования электронной подписи и расшифрования зашифрованных сообщений. Открытый ключ используется для проверки подписи и зашифрования сообщений и свободно распространяется в составе сертификата.

Сертификат издателя и СОС предназначены для подтверждения подлинности вашего сертификата.

3 Установите сертификат открытого ключа и соответствующий ему закрытый ключ или несколько сертификатов и ключей (см. «Способы установки закрытого ключа и сертификата» на стр. 71).

Примечание. При добавлении контейнера программа автоматически предлагает установить сертификат в системное хранилище. Если сертификат не был установлен, установите его самостоятельно (см. «Установка сертификата из контейнера ключей» на стр. 82).

4 Установите в системное хранилище сертификат издателя и СОС (см. «Установка сертификатов издателей и СОС» на стр. 84).

Примечание. Если вы являетесь администратором веб-сервера, с которым требуется организовать защищенные соединения TLS/SSL, подготовьте сервер и веб-клиенты к работе по протоколу TLS/SSL (см. «Организация защищенного соединения TLS/SSL» на стр. 184).

5 Выполнив перечисленные выше действия, вы можете использовать любые приложения, которые в своей работе используют криптопровайдер (см. «Практическое применение ViPNet CSP» на стр. 28). Это могут быть программы для работы с электронной подписью, шифрования данных, защищенной передачи информации и другие.

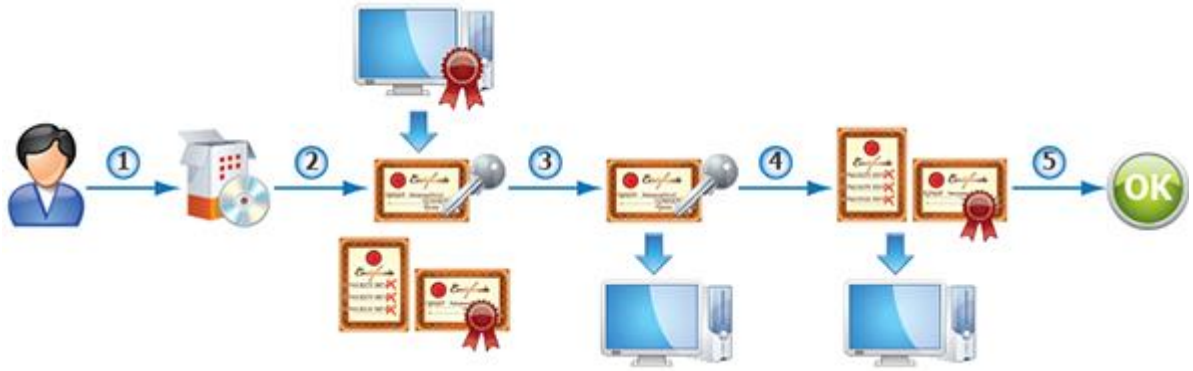


Рисунок 7: Порядок подготовки к использованию криптопровайдера

3

Установка и запуск программы

Установка программы

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! Если ViPNet CSP устанавливается на компьютер с операционной системой Windows, локализация которой отличается от русской, для правильного отображения кириллицы в интерфейсе ViPNet CSP следует изменить 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:

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. Если вы хотите настроить параметры установки, на странице **Способ установки** нажмите кнопку **Настроить** и укажите:
   - 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:
   - **Поддержка работы ViPNet CSP через MS Crypto API** — 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.

- **Контроль целостности по классу КС3** — добавляет функции, позволяющие осуществлять контроль целостности файлов. Это необходимо для соответствия классу криптографической защиты КС3. По умолчанию компонент отключен.

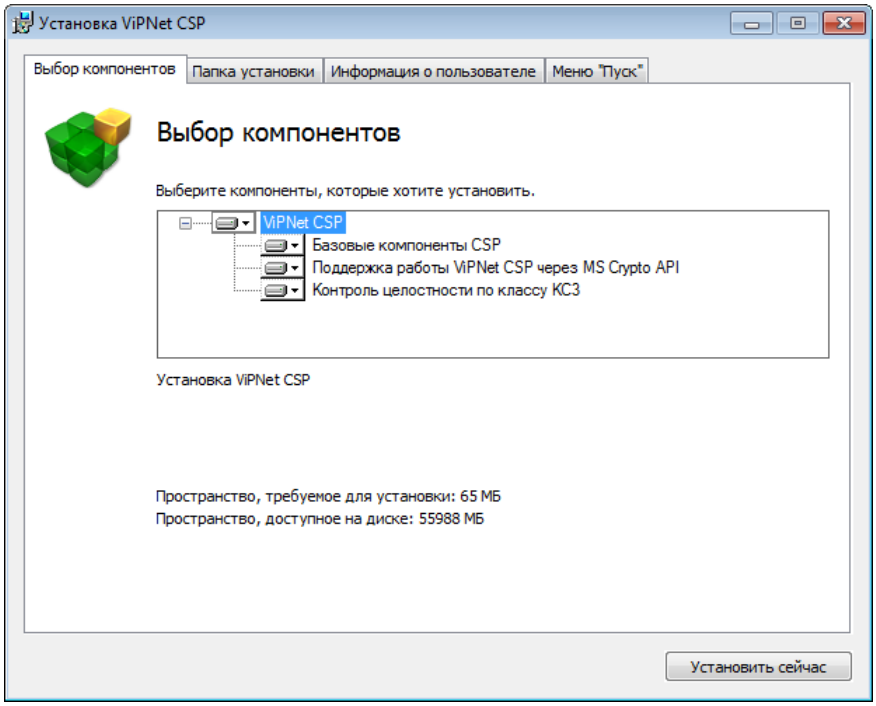
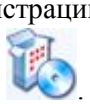


Рисунок 8: Настройка параметров установки ViPNet CSP

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

5 По окончании установки программа предложит перезагрузить компьютер. В окне сообщения о перезагрузке нажмите кнопку **Да**.

Если у вас уже есть серийный номер ViPNet CSP, вы можете зарегистрировать программу без демонстрации интерфейса (Silent mode). Для этого необходимо предварительно подготовить файл регистрации `cspreg.txt` и разместить его в одной папке с установочным файлом  . Файл `cspreg.txt` должен иметь вид:

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

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

Добавление, удаление и восстановление компонентов программы

При необходимости вы можете установить или удалить компоненты программы ViPNet CSP, а также восстановить ПО 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 программы выберите **Восстановить**;
   - для удаления всех компонентов программы выберите **Удалить все компоненты**.

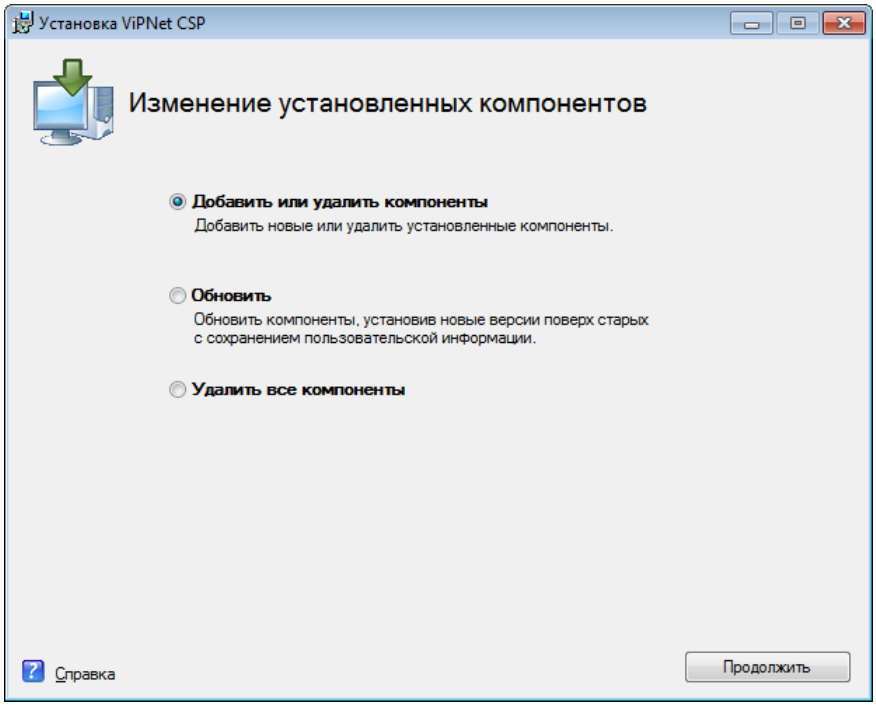


Рисунок 9: Изменение установленных компонентов

Затем нажмите кнопку **Продолжить**.

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

4 Дождитесь завершения установки (восстановления, удаления) компонентов программы. Затем нажмите кнопку **Закрыть**.

Установка с использованием командной строки

Приложение ViPNet CSP может быть установлено 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`.

Пример команды установки:

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

Запуск программы

Для запуска программы ViPNet CSP выполните одно из действий:

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

При запуске незарегистрированной версии программы откроется окно **ViPNet CSP** с предложением зарегистрировать программу. Вы можете перейти к регистрации программы либо начать работу с демо-версией программы (см. «Лицензирование программы» на стр. 40).

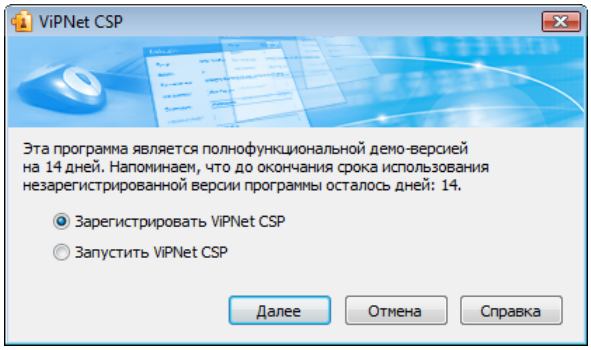


Рисунок 10: Запуск незарегистрированной версии программы

После запуска программы откроется раздел **Общие** главного окна ViPNet CSP. Здесь содержится информация о версии программы, владельце лицензии и режиме работы ViPNet CSP.

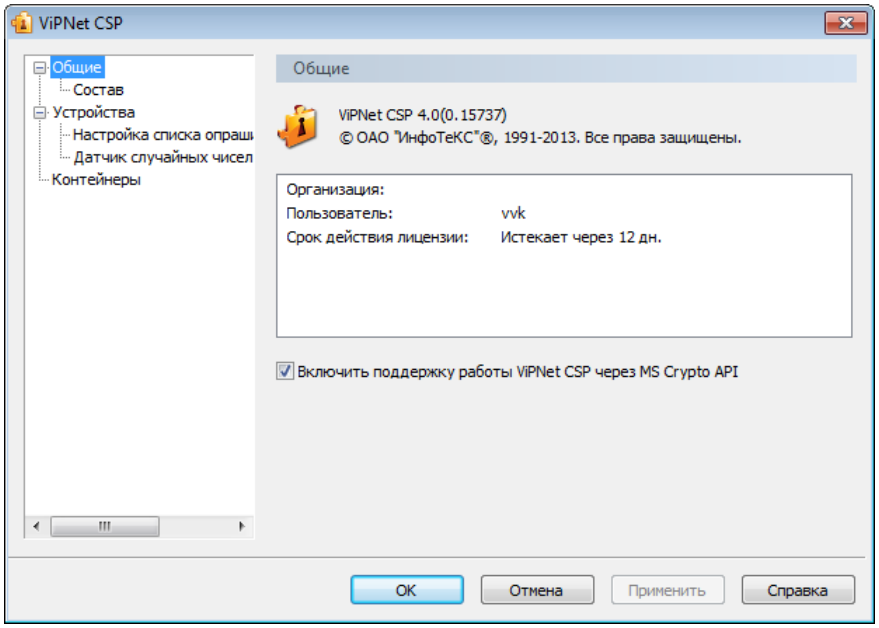


Рисунок 11: Раздел общей информации о программе

Начните работу с программой с установки контейнера ключей и сертификата (см. «Установка контейнеров ключей и сертификатов» на стр. 70).

Лицензирование программы

При установке программы ViPNet CSP в составе другого ПО ViPNet отдельной регистрации программы не требуется. При отдельной установке криптопровайдера ViPNet CSP требуется его регистрация.

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

Особенности демо-лицензии:

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

По истечении срока действия демо-лицензии работа с незарегистрированной программой ViPNet CSP невозможна. Чтобы продолжить работу с ViPNet CSP, зарегистрируйте программу (см. «Регистрация ViPNet CSP» на стр. 41). Регистрация осуществляется бесплатно.

Внимание! При обновлении программы ViPNet CSP с версии 3.2.x на версию 4.x необходима повторная регистрация.

4

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 (см. «Лицензирование программы» на стр. 40). 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.

Начало регистрации

Вы можете зарегистрировать ViPNet CSP самостоятельно (обычная регистрация). Для этого следуйте приведенным ниже указаниям.

Если вы системный администратор и хотите одновременно зарегистрировать несколько копий программы, вы можете использовать возможность регистрации через файл, чтобы собрать запросы на регистрацию от всех пользователей, отправить их в одном сообщении электронной почты и получить все регистрационные коды одновременно. Подробнее см. раздел Порядок действий системного администратора при регистрации через файл (на стр. 60).

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. 58).

Если вы провели обновление конфигурации компьютера, на котором будете использовать ViPNet CSP, ознакомьтесь с разделом Если конфигурация вашего компьютера изменилась (на стр. 58).

Чтобы зарегистрировать ViPNet CSP:

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

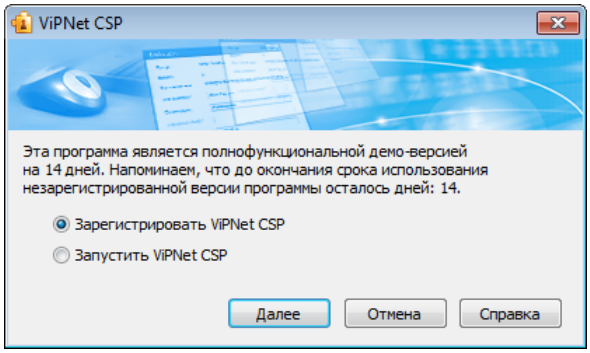


Рисунок 12: Вызов мастера регистрации

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

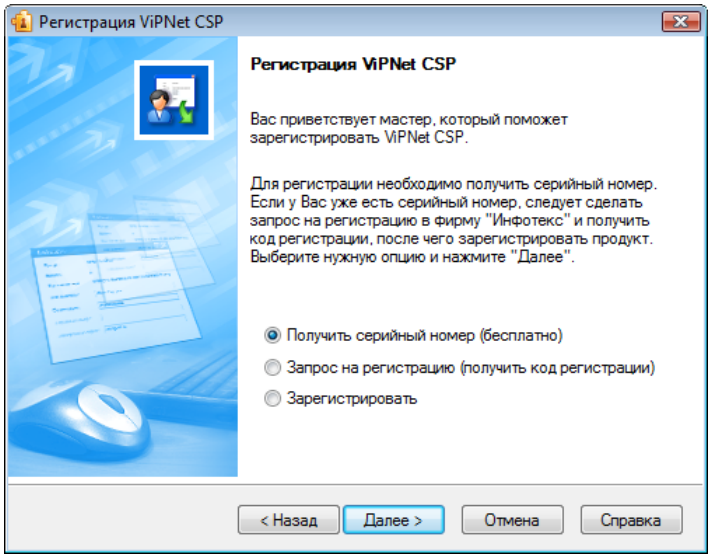


Рисунок 13: Первая страница регистрации

3 Если перед этим:

- вы не получили серийный номер ViPNet CSP, выберите пункт **Получить серийный номер (бесплатно)** (см. «Получение серийного номера» на стр. 45).
- вы уже имеете серийный номер, выберите пункт **Запрос на регистрацию (получить код регистрации)** (см. «Получение кода регистрации» на стр. 46).

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

- вы уже получили серийный номер и код регистрации, выберите пункт **Зарегистрировать** (см. «Регистрация ViPNet CSP» на стр. 56).

Получение серийного номера

Для получения серийного номера:

1. На странице **Регистрация ViPNet CSP** выберите пункт **Получить серийный номер (бесплатно)** и нажмите кнопку **Далее**.

   В окне вашего браузера откроется страница загрузки бесплатных продуктов ViPNet на сайте компании «ИнфоТеКС».

2. Выбрав версию продукта, заполните форму запроса и отправьте данные. Ссылка для загрузки продукта и серийный номер будут отправлены на указанный адрес электронной почты.

3. Получив серийный номер, вернитесь на страницу **Регистрация ViPNet CSP** (см. «Начало регистрации» на стр. 42) и сделайте запрос на получение кода регистрации (см. «Получение кода регистрации» на стр. 46).

Получение кода регистрации

Чтобы запросить код регистрации для ViPNet CSP:

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. 46).
   - **По электронной почте** (см. «Получение кода регистрации по электронной почте» на стр. 49).
   - **По телефону** (см. «Получение кода регистрации по телефону» на стр. 51).
   - **Через файл** (см. «Регистрация через файл» на стр. 52).

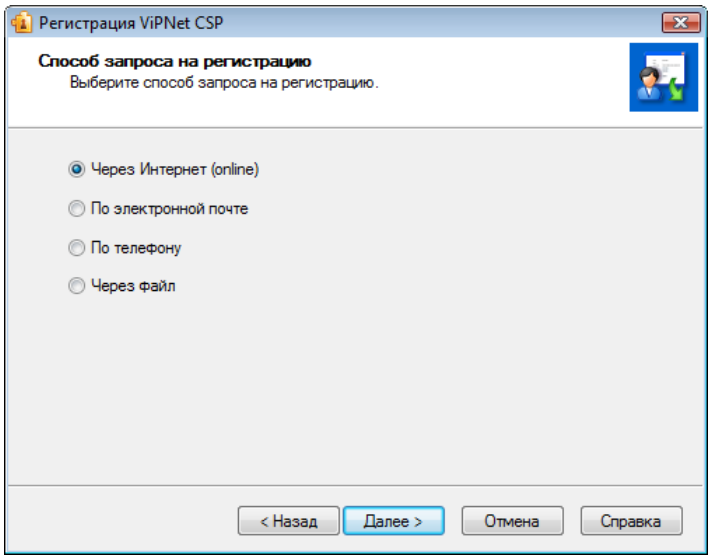


Рисунок 14: Выбор типа запроса на регистрацию

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**.

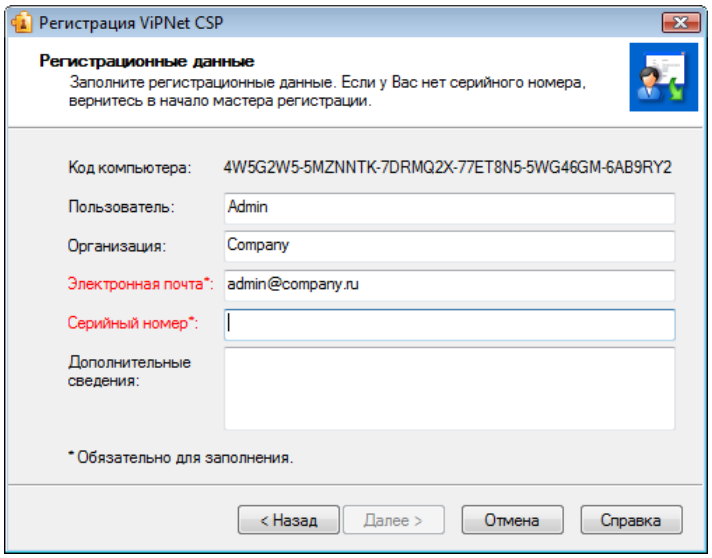


Рисунок 15: Ввод регистрационных данных

На странице **Регистрационные данные**:

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

Примечание. Если у вас нет серийного номера, сделайте запрос на его получение (см. «Получение серийного номера» на стр. 45).

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.

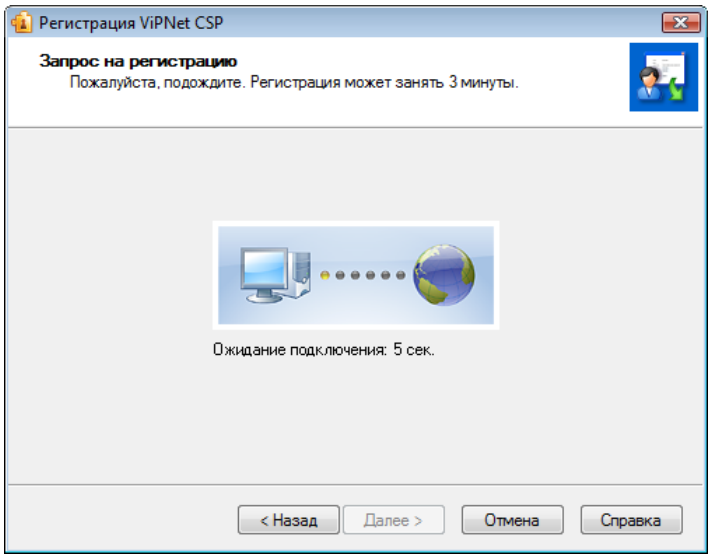


Рисунок 16: Запрос на регистрацию через Интернет

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

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 (см. «Получение серийного номера» на стр. 45).

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. 58).

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:

1 Введите все данные, как описано в разделе

Получение кода регистрации через Интернет (на стр. 46).

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.

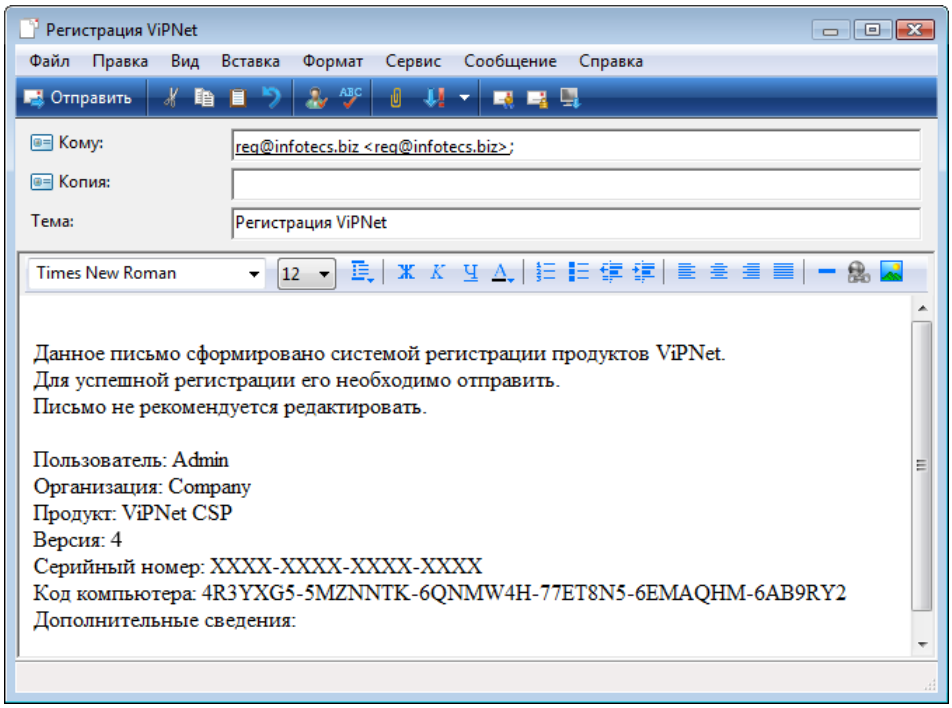


Рисунок 17: Запрос на регистрацию по электронной почте

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. 56).

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».

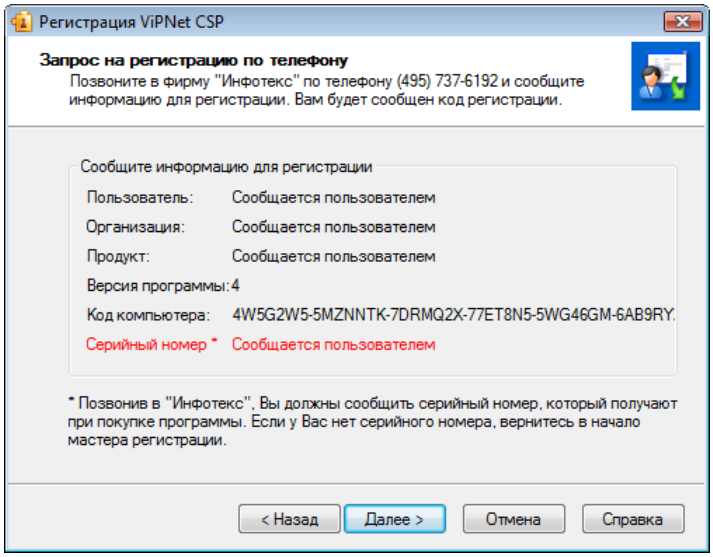


Рисунок 18: Запрос на регистрацию по телефону

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.**

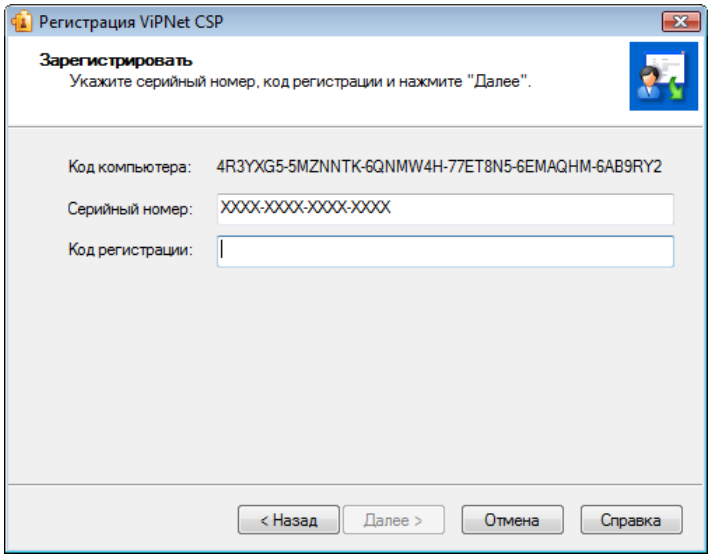


Рисунок 19: Ввод регистрационного кода

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

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

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. 58).

4 Нажмите кнопку **Готово**.

Регистрация через файл

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

Примечание. Если требуется провести регистрацию через файл только одной копии программы ViPNet CSP, сначала выполните действия 1–6, описанные в данном разделе, затем выполните действия системного администратора из раздела Порядок действий системного администратора при регистрации через файл (на стр. 60). После этого выполните действие 7 данного раздела, зарегистрировав свою копию ViPNet CSP (см. «Регистрация ViPNet CSP» на стр. 56).

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

Чтобы воспользоваться регистрацией через файл:

1. На странице **Способ запроса на регистрацию** выберите **Через файл** и нажмите кнопку **Далее**.
2. На странице **Регистрационные данные** введите все данные, как описано в разделе

Получение кода регистрации через Интернет (на стр. 46). Нажмите кнопку **Далее**.

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

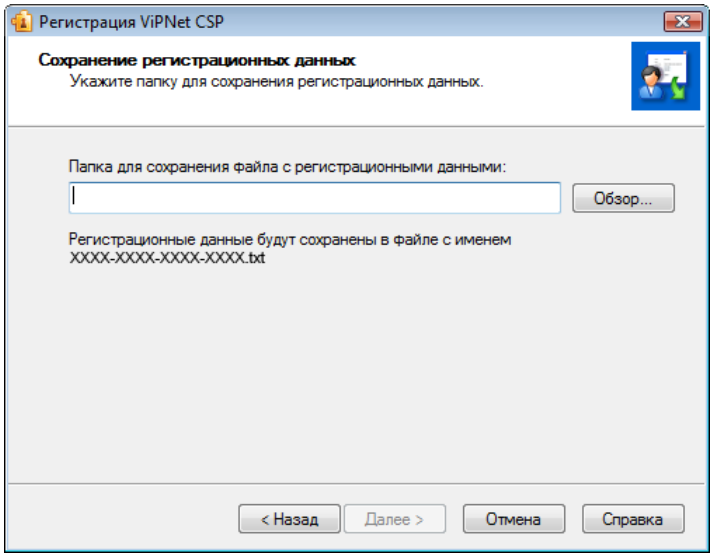


Рисунок 20: Сохранение регистрационных данных

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

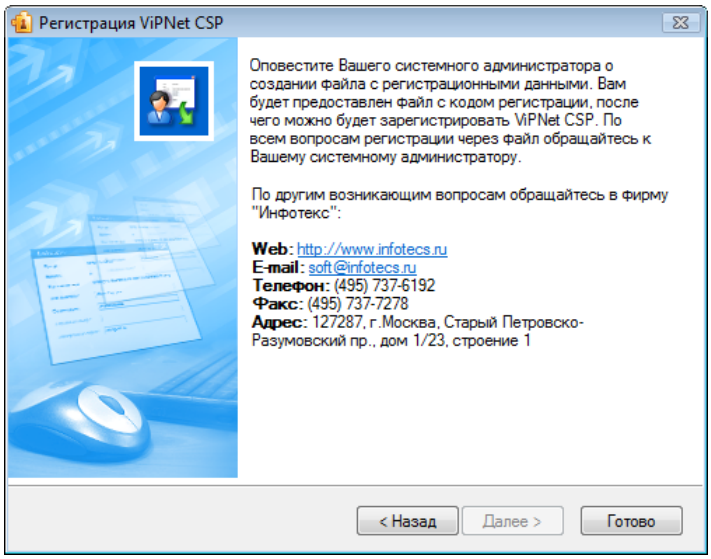


Рисунок 21: Данные для регистрации через файл сохранены

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

6 Передайте файл, содержащий регистрационные данные, своему системному администратору.

7 Получив от администратора код регистрации, зарегистрируйте свою копию ViPNet CSP (см. «Регистрация ViPNet CSP» на стр. 56).

Регистрация ViPNet CSP

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

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**.

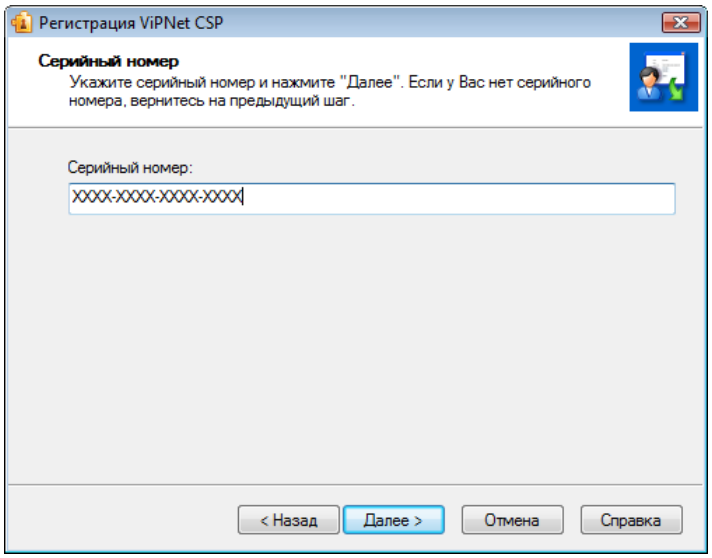


Рисунок 22: Ввод серийного номера

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

4 На странице **Код регистрации**:

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

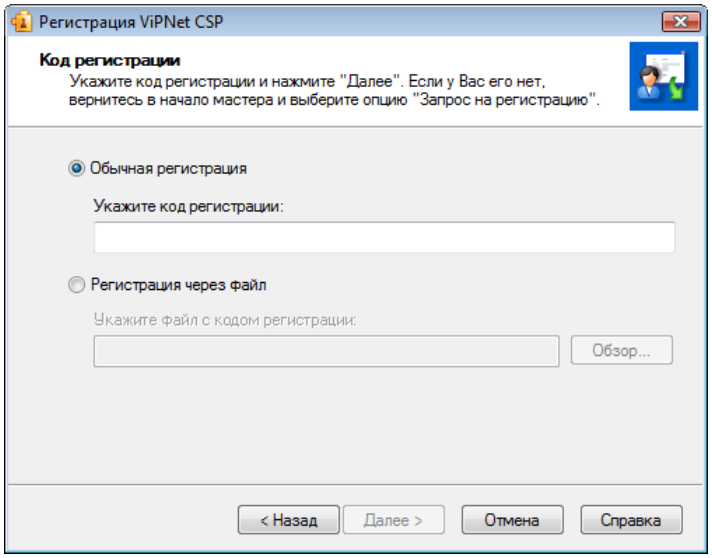


Рисунок 23: Ввод кода регистрации

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

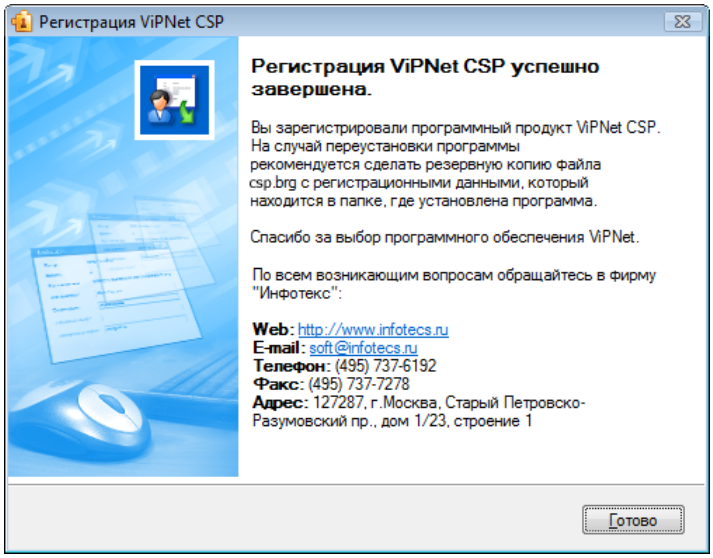


Рисунок 24: Завершение регистрации

6 Нажмите кнопку **Готово**.

7 Сохраните регистрационные данные (см. «Сохранение регистрационных данных на стр. 58»), 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\`, если используется операционная система Windows Vista, Windows 7, Windows Server 2008, Windows 8 или Windows Server 2012;
- `C:\Documents and Settings\All Users\Application Data\InfoTeCS\ViPNet CSP\`, если используется операционная система Windows XP или Windows Server 2003.

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 папке установки ViPNet CSP. 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. 46). 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.

Порядок действий системного администратора при регистрации через файл

Процедура регистрации через файл позволяет представителю организации (обычно это системный администратор) запросить коды регистрации для нескольких пользователей ViPNet.

Чтобы воспользоваться регистрацией через файл, все пользователи должны иметь серийные номера своих продуктов ViPNet. Если у пользователей нет серийных номеров, их следует получить с помощью мастера **Регистрация ViPNet CSP** (см. «Получение серийного номера» на стр. 45).

Каждый пользователь на своем компьютере должен создать запрос на регистрацию через файл (см. «Регистрация через файл» на стр. 52). В итоге должен быть создан файл `*.txt`, содержащий регистрационные данные, который пользователь передает системному администратору.

Если вы являетесь системным администратором:

1. Сохраните файлы с регистрационными данными, полученные от пользователей ViPNet, в одну папку.
2. Объедините все файлы в один с помощью команды: `copy *.txt registration.all`. Вместо `registration.all` вы можете задать любое другое имя файла.
3. Отправьте получившийся файл на адрес электронной почты reg@infotecs.biz. В теме сообщения укажите: ViPNet Registration Using File.
4. После обработки запроса компанией ОАО «ИнфоТеКС» вы получите сообщение с прикрепленным файлом `*.txt`. Файл будет содержать коды регистрации для всех пользователей, участвующих в регистрации через файл. После того как вы передадите этот файл пользователям (например, с помощью сетевого диска), они смогут зарегистрировать свои программы ViPNet.

5

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:

1. Сформируйте файл запроса на сертификат в программе «Создание запроса на сертификат» (см. «Создание запроса на сертификат и формирование закрытого ключа» на стр. 63).
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. 77).
5. Установите в системное хранилище полученный сертификат (см. «Установка сертификата в системное хранилище» на стр. 79), а также сертификаты издателей и СОС (см. «Установка сертификатов издателей и СОС» на стр. 84).

Создание запроса на сертификат и формирование закрытого ключа

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

1. В меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet CSP** > **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:
     - В окне **Обновление сертификата** выберите сертификат, который требуется обновить, и нажмите кнопку **OK**.
     - Если требуется выбрать другой сертификат или просмотреть выбранный сертификат, воспользуйтесь кнопками **Выбрать сертификат** и **Выбранный сертификат**.
     - Если необходимо, укажите новые параметры сертификата и данные о владельце или оставьте реквизиты предыдущего сертификата.

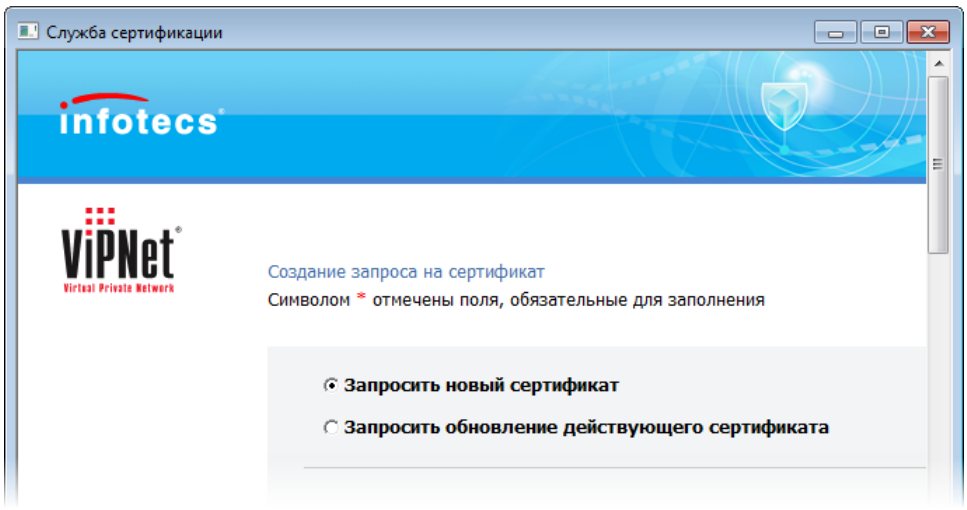


Рисунок 25: Выбор типа запроса на сертификат

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

- В списке **Криптопровайдер** выберите криптопровайдер, с помощью которого вы хотите создать закрытый и открытый ключи.
- Выберите алгоритм хеширования в соответствующем списке.
- 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:
  - **Квалифицированный ViPNet CSP** (по умолчанию) — чтобы создать запрос на квалифицированный сертификат (на стр. 233), 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.
  - **WEB server** — чтобы создать запрос на сертификат для установки на веб-сервере IIS.
  - **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 сертификат, установите флажок **Экспортируемый.**
- Чтобы создать сертификат для установки в хранилище локального компьютера, установите флажок **Системный.**

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

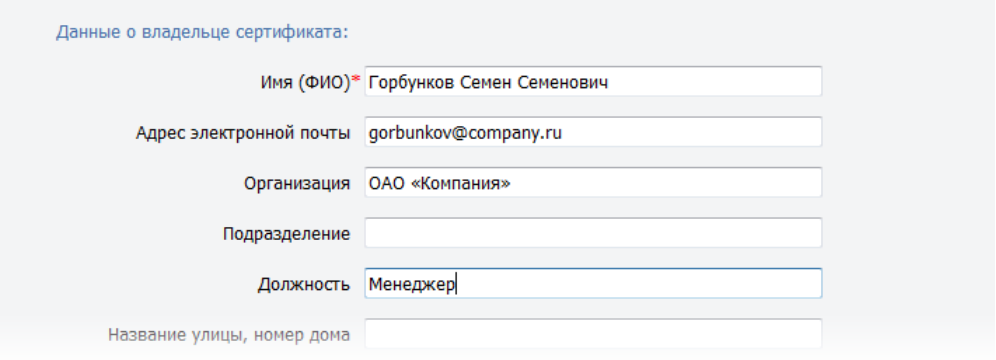


Рисунок 26: Указание данных о владельце сертификата

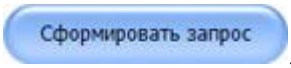
Внимание! Если сертификат планируется использовать для подписания сообщений электронной почты программы Microsoft Outlook, обязательно укажите адрес электронной почты. Сертификат, не содержащий адреса электронный почты, не может быть использован для подписания сообщений электронной почты.

---

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 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 **Общие** (см. рисунок на стр. 39) установлен флажок **Включить поддержку работы ViPNet CSP через MS Crypto API**.

Далее выполните следующие шаги, необходимые для создания контейнера ключей.

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

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

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

8 В окне **ViPNet CSP - пароль контейнера ключей** задайте пароль доступа к контейнеру ключей.

9 Появится электронная рулетка (на стр. 236), если она еще не запускалась в рамках текущего сеанса работы программы. Поводите указателем в пределах окна **Электронная рулетка**.

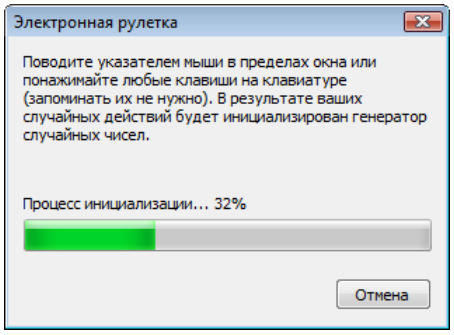


Рисунок 27: Электронная рулетка

Примечание. Если в программе ViPNet CSP был выбран датчик случайных чисел, отличный от биологического (см. «Использование датчика случайных чисел» на стр. 104), электронная рулетка не появится.

Если для сохранения контейнера выбрано ГОСТ-устройство, 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 страницу браузера **Служба сертификации** можно закрыть.

После создания запроса на сертификат передайте файл запроса администратору вашего удостоверяющего центра и получите от него изданный сертификат. Далее в программе **Настройка ViPNet CSP** установите полученный сертификат (см. «Установка сертификата в системное хранилище» на стр. 79) 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:

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

2. В группе **Подпись** нажмите кнопку **Перенести**.

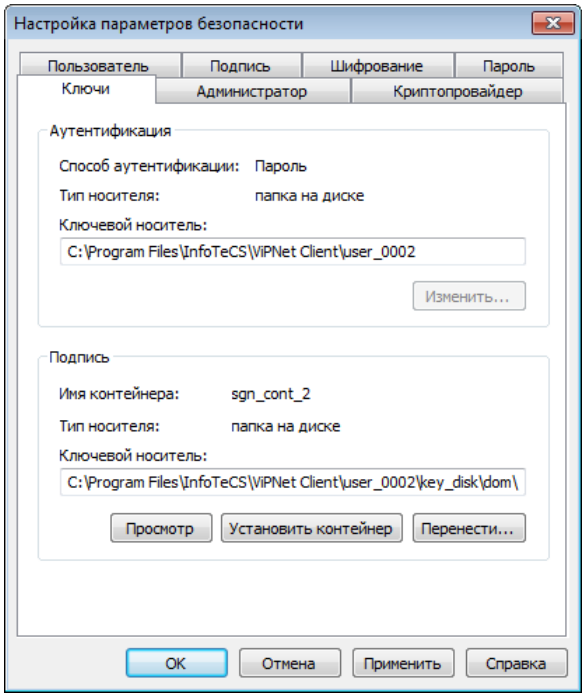


Рисунок 28: Работа с контейнером ключей

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. 72).

6

Установка контейнеров ключей и сертификатов

Способы установки закрытого ключа и сертификата

Для того чтобы начать работу с механизмами электронной подписи:

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. 72).
   - Если закрытый ключ и сертификат находятся в одном контейнере и размещены на внешнем устройстве, см. раздел Установка контейнера ключей с внешнего устройства (на стр. 75).
   - 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. 77).
2. Установите сертификат в системное хранилище (см. «Установка сертификата в системное хранилище» на стр. 79).
3. Установите сертификаты издателей и список отозванных сертификатов (СОС) в системное хранилище (см. «Установка сертификатов издателей и СОС» на стр. 84).

Установка контейнера ключей из папки

Для работы с защищенными документами и организации соединений по протоколу TLS/SSL необходимы закрытый ключ и соответствующий ему сертификат. Установка закрытого ключа и сертификата может выполняться в одном контейнере ключей или путем установки сертификата и контейнера ключей по отдельности (см. «Установка сертификата в системное хранилище» на стр. 79).

Для установки в программу контейнера ключей из папки на диске:

1 В окне программы **ViPNet CSP** выберите раздел **Контейнеры**.

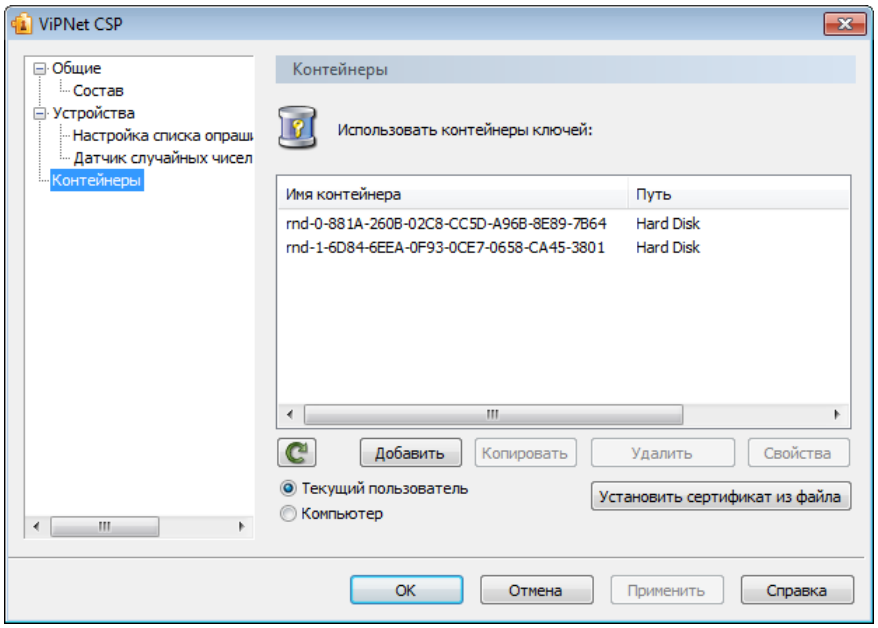


Рисунок 29: Управление контейнерами

2 В разделе **Контейнеры** нажмите кнопку **Добавить**.

3 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.

- 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`.

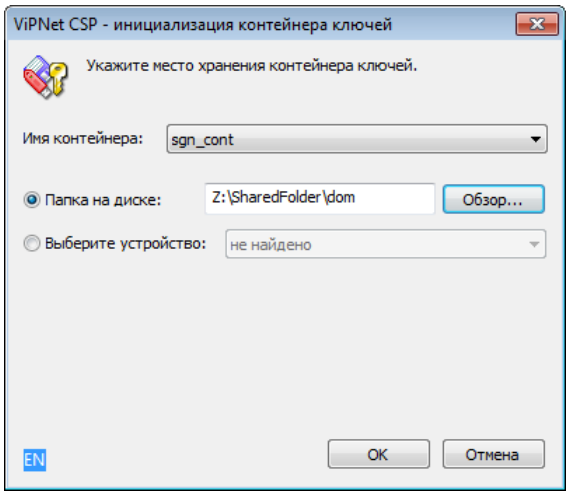


Рисунок 30: Инициализация контейнера ключей из папки

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

5 Нажмите кнопку **ОК**. В окне **Контейнер ключей** появится сообщение об успешном добавлении контейнера ключей и предложение установить сертификат в 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/SSL, сертификат необходимо устанавливать в хранилище локального компьютера вручную (см. «Установка сертификата из контейнера ключей» на стр. 82).

Нажмите кнопку **Да**. Сертификаты будут автоматически установлены в хранилище пользователя.

Если сертификаты устанавливать не требуется (или установка будет происходить вручную), нажмите кнопку **Нет**.

Для просмотра списка сертификатов в контейнере ключей нажмите кнопку **Сертификаты**.

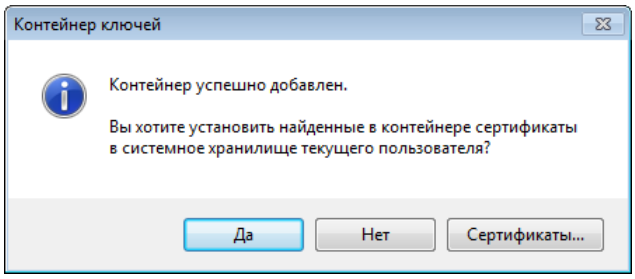


Рисунок 31: Установка сертификатов из контейнера ключей в хранилище

6 После установки (или отмены установки) сертификатов в хранилище в списке доступных контейнеров ключей (см. рисунок на стр. 72) 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. 82).

После добавления контейнера ключей установите сертификат издателя и СОС (см. «Установка сертификатов издателей и СОС» на стр. 84) и приступайте к выполнению криптографических операций (см. «Практическое применение ViPNet CSP» на стр. 28).

Установка контейнера ключей с внешнего устройства

Для установки в программу контейнера ключей с внешнего устройства:

1. В окне программы **ViPNet CSP** выберите раздел **Контейнеры** (см. рисунок на стр. 72).
2. В разделе **Контейнеры** нажмите кнопку **Добавить**.
3. В окне **ViPNet CSP - инициализация контейнера ключей** установите переключатель **Выберите устройство** и в списке выберите нужное устройство.

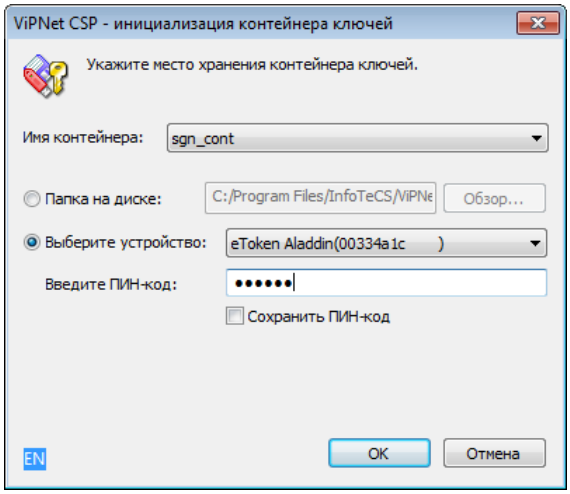


Рисунок 32: Инициализация контейнера ключей с внешнего устройства

4. В поле **Введите ПИН-код** укажите ПИН-код устройства. Чтобы не вводить ПИН-код каждый раз при обращении к устройству, установите флажок **Сохранить ПИН-код**.

Примечание. Сохранение ПИН-кода к устройству в системе ведет к снижению уровня безопасности.

Подробную информацию о работе с внешними устройствами см. в разделе Внешние устройства (на стр. 216).

---

5 Нажмите кнопку **ОК**. В окне **Контейнер ключей** (см. рисунок на стр. 74) появится сообщение об успешном добавлении контейнера ключей и предложение по установке сертификата в хранилище. Для работы с сертификатами их необходимо установить в хранилище текущего пользователя.

Нажмите кнопку **Да**. Сертификаты будут автоматически установлены в хранилище.

Если сертификаты устанавливать не требуется, нажмите кнопку **Нет.**

Для просмотра списка сертификатов в контейнере ключей нажмите кнопку **Сертификаты.**

6 После установки (или отмены установки) сертификатов в хранилище в списке доступных контейнеров ключей (см. рисунок на стр. 72) появится добавленный контейнер.

Примечание. Установить сертификаты из контейнера ключей можно вручную через окно настройки свойств контейнера (см. «Установка сертификата из контейнера ключей» на стр. 82).

После добавления контейнера ключей установите сертификат издателя и СОС (см. «Установка сертификатов издателей и СОС» на стр. 84) и приступайте к выполнению криптографических операций (см. «Практическое применение ViPNet CSP» на стр. 28).

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

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:

1. В окне программы **ViPNet CSP** выберите раздел **Контейнеры** (см. рисунок на стр. 72).
2. В разделе **Контейнеры** выберите контейнер, в который требуется установить сертификат, и нажмите кнопку **Свойства** либо дважды щелкните нужный контейнер.
3. В окне **Свойства контейнера ключей** нажмите кнопку **Добавить.**

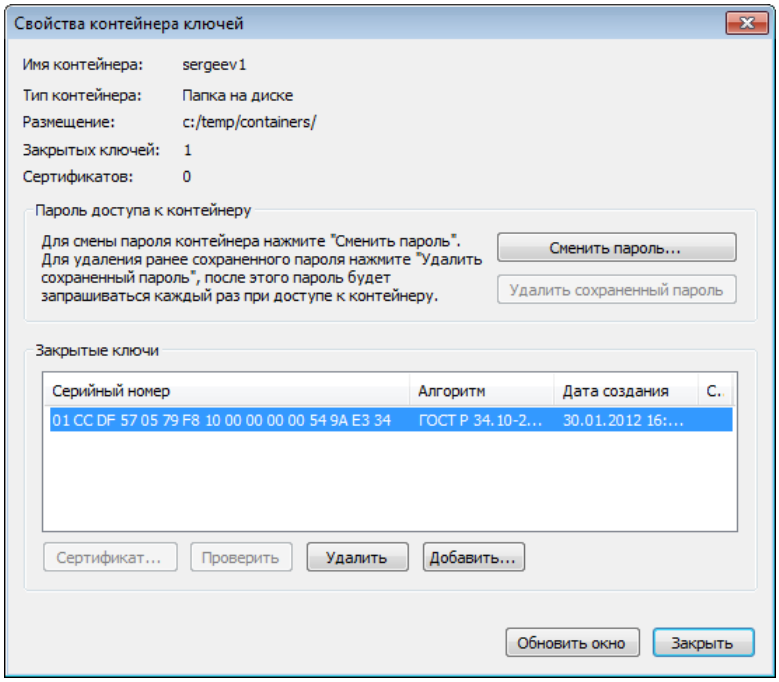


Рисунок 33: Добавление сертификата в контейнер ключей

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 «Ключ не найден».

Примечание. Чтобы после добавления сертификата увидеть его в окне **Свойства контейнера ключей**, нажмите кнопку **Обновить окно**.

Установка сертификата в системное хранилище

Чтобы использовать сертификат в различных приложениях, следует установить его в системное хранилище сертификатов. Вы можете сделать это двумя способами:

- Если сертификат еще не установлен в контейнер ключей, содержащий соответствующий закрытый ключ, установку сертификата в системное хранилище следует выполнять в разделе **Контейнеры** (см. «Установка сертификата, не добавленного в контейнер ключей» на стр. 79).
- Если сертификат уже установлен в контейнер ключей, установку сертификата в системное хранилище следует выполнять в окне просмотра сертификата (см. «Установка сертификата из контейнера ключей» на стр. 82).

Установка сертификата, не добавленного в контейнер ключей

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

1. В окне программы ViPNet CSP выберите раздел **Контейнеры** (см. рисунок на стр. 72).
2. В разделе **Контейнеры** нажмите кнопку **Установить сертификат из файла**.
3. В окне **Открыть** укажите путь к файлу сертификата на диске (см. «Контейнер ключей» на стр. 24).
4. На странице приветствия мастера установки сертификатов нажмите кнопку **Далее**.
5. На странице **Выбор хранилища сертификатов** укажите, в какое хранилище будет установлен ваш сертификат.

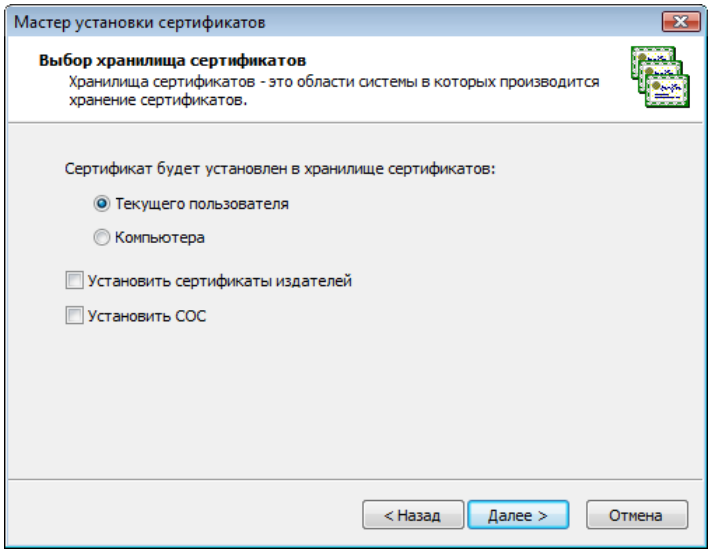


Рисунок 34: Выбор хранилища сертификатов

Сертификат следует устанавливать в хранилище текущего пользователя для целей шифрования, расшифрования и подписания файлов, а также для доступа к защищенным ресурсам через веб-браузер. В хранилище компьютера следует устанавливать сертификаты, которые будут использоваться службами данного компьютера.

Сертификат следует устанавливать в хранилище компьютера при использовании ViPNet CSP на веб-сервере для организации доступа к защищенным ресурсам.

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

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

Нажмите кнопку **Далее**.

6 На странице **Готовность к установке сертификата**:

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

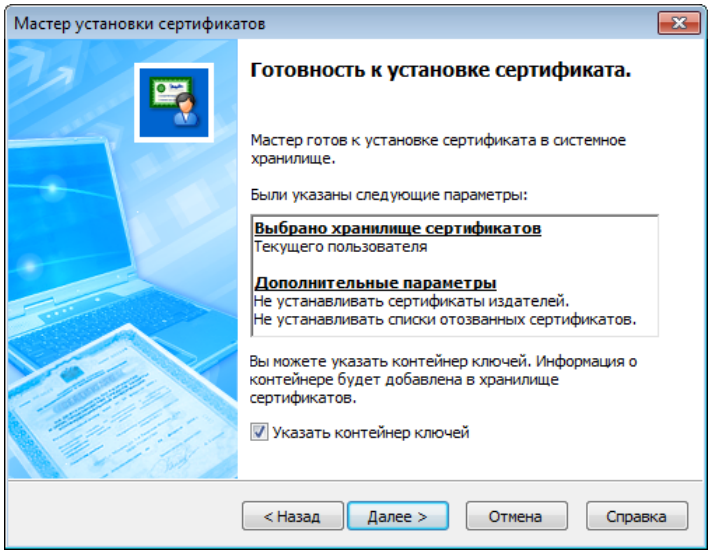


Рисунок 35: Сертификат готов к установке

- Если сертификат хранится в файле отдельно от закрытого ключа, установите флажок **Указать контейнер ключей**.

Примечание. Флажок **Указать контейнер ключей** можно не устанавливать. В этом случае необходимо указать расположение контейнера позже, после завершения работы мастера установки сертификата.

- Нажмите кнопку **Далее**.

7 Если флажок **Указать контейнер ключей** установлен и контейнер не найден либо недоступен, в появившемся окне **ViPNet CSP – инициализация контейнера ключей** укажите расположение контейнера ключей:

- папку на диске (см. «Установка контейнера ключей из папки» на стр. 72);
- устройство с указанием его параметров и ПИН-кода (см. «Установка контейнера ключей с внешнего устройства» на стр. 75).

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 использовании устройств содержится в разделе Внешние устройства (на стр. 216).

После этого 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 флажок **Указать контейнер ключей** установлен и контейнер доступен, в появившемся окне **ViPNet CSP – пароль контейнера ключей** в поле **Пароль** введите пароль доступа к контейнеру, после чего нажмите кнопку **ОК**.

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. В случае если в процессе установки сертификата ему не был сопоставлен закрытый ключ, необходимо установить контейнер ключей, соответствующий этому сертификату.

Если в процессе установки сертификату был сопоставлен закрытый ключ, контейнер с закрытым ключом, соответствующим этому сертификату, появится в списке контейнеров (см. рисунок на стр. 72). Вы можете установить еще один сертификат и закрытый ключ либо приступать к работе с защищенными документами (см. «Практическое применение ViPNet CSP» на стр. 28), предварительно установив сертификат издателя и СОС (см. «Установка сертификатов издателей и СОС» на стр. 84).

Установка сертификата из контейнера ключей

Для установки сертификата:

1 В окне программы **ViPNet CSP** выберите раздел **Контейнеры** (см. рисунок на стр. 72).

2 В разделе **Контейнеры** выберите контейнер ключей, сертификат из которого требуется установить, и нажмите кнопку **Свойства** либо дважды щелкните нужный контейнер ключей.

3 В окне **Свойства контейнера ключей** (см. рисунок на стр. 89) выберите закрытый ключ и нажмите кнопку **Сертификат**.

4 В окне **Сертификат** на вкладке **Общие** нажмите кнопку **Установить сертификат**. Будет запущен мастер установки сертификатов (см. «Установка сертификата в системное хранилище» на стр. 79).

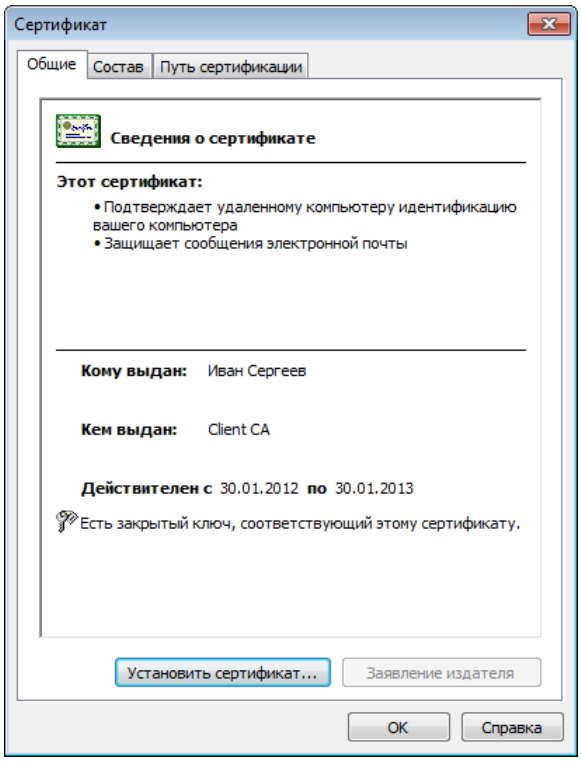


Рисунок 36: Окно свойств сертификата

5 На странице приветствия **Мастера установки сертификатов** нажмите кнопку **Далее**.

6 На странице **Выбор хранилища сертификатов** укажите нужное хранилище.

7 На странице **Готовность к установке сертификата** снимите флажок **Указать контейнер ключей** и нажмите кнопку **Далее**.

8 На странице **Завершение работы мастера установки сертификатов** нажмите кнопку **Готово**. Сертификат установлен в хранилище.

Кроме сертификата пользователя, для работы с защищенными файлами и организации соединений TLS/SSL необходимо установить сертификат издателя и СОС (см. «Установка сертификатов издателей и СОС» на стр. 84).

Установка сертификатов издателей и СОС

Для выполнения операций с защищенными файлами и организации соединений TLS/SSL требуется установить в системное хранилище сертификат пользователя, издателя и СОС. Установка сертификата пользователя осуществляется средствами программы ViPNet CSP в контейнер ключей или отдельно.

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

Для установки сертификатов и СОС:

1. Откройте папку, содержащую файл сертификата или СОС. Щелкните нужный файл правой кнопкой мыши и в контекстном меню выберите пункт **Установить сертификат** или **Установить список отзыва (CRL)**.
2. На первой странице мастера импорта сертификатов нажмите кнопку **Далее**.
3. На странице **Хранилище сертификатов** выберите вариант **Поместить все сертификаты в следующее хранилище**.

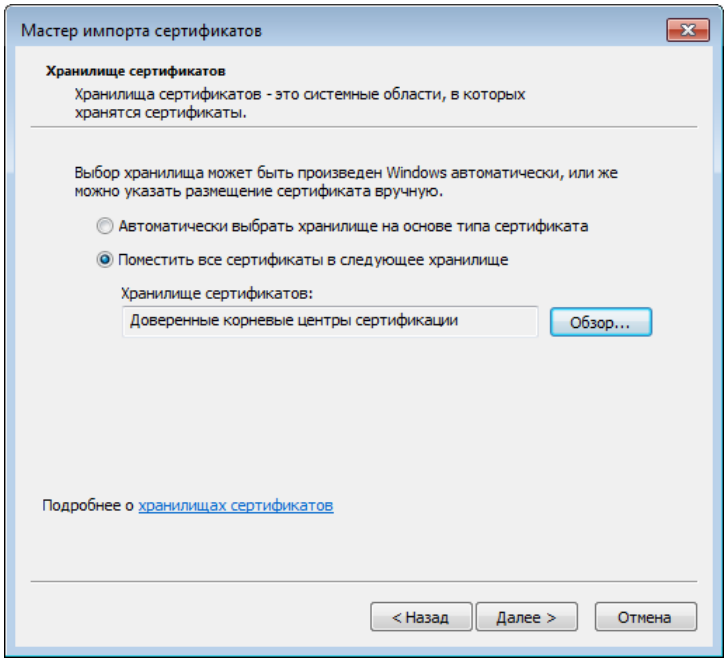


Рисунок 37: Выбор хранилища для сертификата издателя

4 Нажмите кнопку **Обзор**, затем в окне **Выбор хранилища сертификатов** выберите:

- **Доверенные корневые центры сертификации**, если вы устанавливаете сертификат издателя.
- **Промежуточные центры сертификации**, если вы устанавливаете СОС.

Нажмите кнопку **OK**.

5 Выбрав хранилище сертификатов, нажмите кнопку **Далее**.

6 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.

---

7 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. 28).

7

Операции с контейнерами ключей

Просмотр и настройка свойств контейнера ключей

В окне свойств контейнера ключей вы можете:

- Просмотреть информацию о закрытом ключе и сертификате, которые находятся в контейнере.
- Сменить пароль доступа к контейнеру.
- Удалить сохраненный пароль доступа к контейнеру.
- Произвести установку сертификата пользователя.
- Проверить или удалить закрытый ключ, хранящийся в контейнере.

Смена пароля к контейнеру ключей

Для смены пароля к контейнеру ключей в папке на диске:

1. В окне программы **ViPNet CSP** выберите раздел **Контейнеры** (см. рисунок на стр. 72).
2. Чтобы выбрать контейнер ключей из папки хранения контейнеров ключей текущего пользователя, установите переключатель в положение **Текущий пользователь.** Чтобы выбрать контейнер ключей из папки хранения контейнеров ключей компьютера, установите переключатель в положение **Компьютер.**
3. Выберите контейнер ключей, к которому требуется сменить пароль, и нажмите кнопку **Свойства** либо дважды щелкните нужный контейнер ключей.
4. В окне **Свойства контейнера ключей** нажмите кнопку **Сменить пароль.**

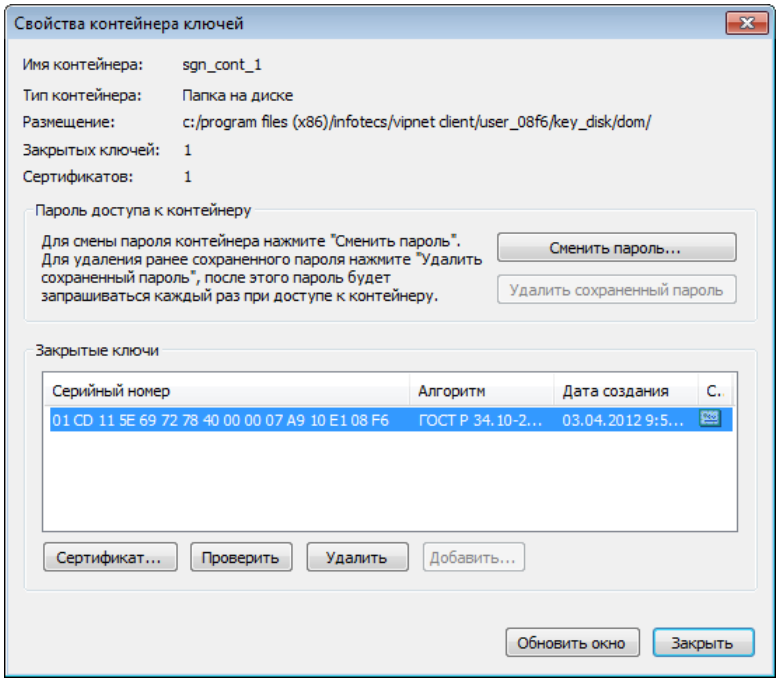


Рисунок 38: Информация о контейнере ключей

5 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.

---

6 В окне **ViPNet CSP - пароль контейнера ключей** укажите и подтвердите новый пароль. Нажмите кнопку **OK**.

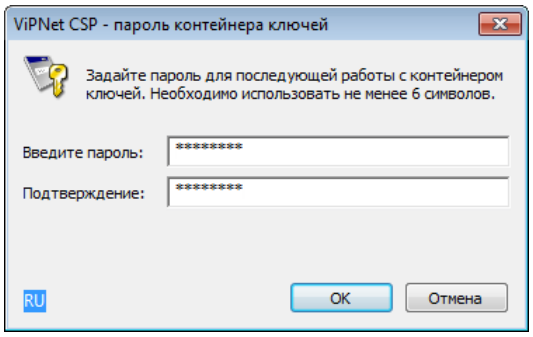


Рисунок 39: Смена пароля доступа к контейнеру ключей

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:

1. В окне программы **ViPNet CSP** выберите раздел **Контейнеры** (см. рисунок на стр. 72).
2. Чтобы выбрать контейнер ключей из папки хранения контейнеров ключей текущего пользователя, установите переключатель в положение **Текущий пользователь.** Чтобы выбрать контейнер ключей из папки хранения контейнеров ключей компьютера, установите переключатель в положение **Компьютер.**
3. Выберите контейнер ключей, сохраненный пароль к которому требуется удалить, и нажмите кнопку **Свойства** либо дважды щелкните нужный контейнер ключей.
4. В окне **Свойства контейнера ключей** (см. рисунок на стр. 89) нажмите кнопку **Удалить сохраненный пароль**. Пароль будет удален.

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

Проверка контейнера ключей

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

Чтобы проверить контейнер ключей:

1. В окне **Свойства контейнера ключей** (см. рисунок на стр. 89) в списке **Закрытые ключи** выберите нужный закрытый ключ.
2. Нажмите кнопку **Проверить.**
3. В окне **ViPNet CSP - пароль контейнера ключей** введите пароль доступа к контейнеру и нажмите кнопку **OK.**

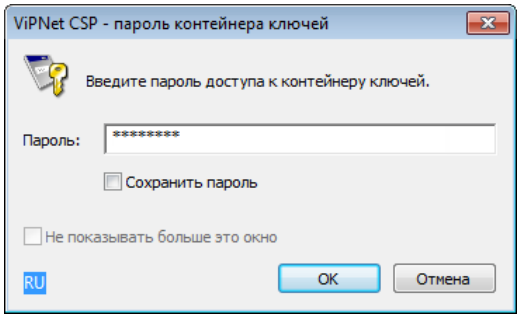


Рисунок 40: Ввод пароля доступа к контейнеру ключей

4 Будет сформирован фрагмент данных, который будет подписан с помощью закрытого ключа, после чего будет выполнена проверка электронной подписи с помощью сертификата открытого ключа. Таким образом, будет проверена пригодность закрытого ключа и его соответствие сертификату, хранящемуся в контейнере.

Примечание. Проверка возможна только в том случае, если в контейнере ключей есть сертификат, соответствующий закрытому ключу. 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 закрытого ключа проверка действительности сертификата (срок его действия, отсутствие в списках отозванных сертификатов и прочее) не выполняется.

Удаление закрытого ключа

Удаление закрытого ключа (и сертификата, при его наличии) из контейнера ключей требуется в следующих случаях:

- если в этом закрытом ключе нет больше необходимости — например, вследствие истечения срока его действия;
- при компрометации или отзыве сертификата, соответствующего закрытому ключу.

Чтобы удалить закрытый ключ и сертификат из контейнера ключей:

1 В окне **Свойства контейнера ключей** (см. рисунок на стр. 89) в списке **Закрытые ключи** выберите строку закрытого ключа.

2 Нажмите кнопку **Удалить**. Появится предупреждение о том, что удаленный закрытый ключ невозможно восстановить.

3 В окне предупреждения нажмите кнопку **Да**.

Выбранный закрытый ключ и соответствующий ему сертификат будут удалены из контейнера ключей. После этого необходимо удалить контейнер.

Создание резервной копии контейнера ключей

Вы можете скопировать контейнер ключей в папку на диске или на внешнее устройство. Эта функция полезна для создания резервной копии контейнера ключей и повышения уровня защиты данных.

Примечание. Копирование контейнера ключей подписи с внешних ГОСТ-устройств невозможно.

Для копирования контейнера:

1. В окне программы **ViPNet CSP** откройте раздел **Контейнеры** (см. рисунок на стр. 72).
2. Чтобы выбрать контейнер ключей из папки хранения контейнеров ключей текущего пользователя, установите переключатель в положение **Текущий пользователь.** Чтобы выбрать контейнер ключей из папки хранения контейнеров ключей компьютера, установите переключатель в положение **Компьютер.**
3. Выберите контейнер для копирования и нажмите кнопку **Копировать.**
4. В окне **ViPNet CSP - инициализация контейнера ключей** укажите новое имя для контейнера и место его расположения. Вы можете скопировать контейнер ключей в папку на диске или на внешнее устройство.
5. В окне **ViPNet CSP - пароль контейнера ключей** (см. рисунок на стр. 91) 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.**
6. В окне **ViPNet CSP - пароль контейнера ключей** (см. рисунок на стр. 89) 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.

7 Копия контейнера ключей появится в списке контейнеров ключей и в указанной папке (либо на устройстве).

Удаление контейнера ключей

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

1. В окне программы **ViPNet CSP** выберите раздел **Контейнеры** (см. рисунок на стр. 72).
2. Чтобы выбрать контейнер ключей из папки хранения контейнеров ключей текущего пользователя, установите переключатель в положение **Текущий пользователь**. Чтобы выбрать контейнер ключей из папки хранения контейнеров ключей компьютера, установите переключатель в положение **Компьютер**.
3. Выберите контейнер ключей, который требуется удалить, и нажмите кнопку **Удалить**.

Внимание! Удаленный контейнер ключей невозможно будет использовать. Перед удалением рекомендуется создать резервную копию контейнера (см. «Создание резервной копии контейнера ключей» на стр. 93).

4. Чтобы подтвердить удаление контейнера ключей, в открывшемся окне нажмите кнопку **OK**.

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

8

Работа с внешними устройствами

Просмотр списка подключенных устройств

ViPNet CSP позволяет работать с контейнерами ключей, которые хранятся на внешних устройствах (см. «Внешние устройства» на стр. 216).

Для просмотра подключенных устройств и хранящихся на них контейнеров ключей:

1 В окне программы **ViPNet CSP** откройте раздел **Устройства**.

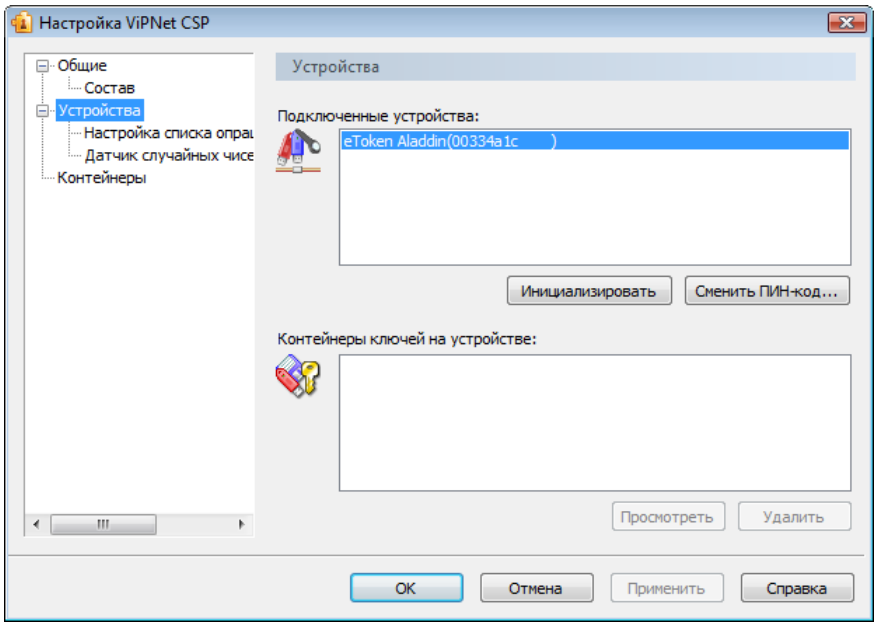


Рисунок 41: Раздел «Устройства»

2 В списке **Подключенные устройства** выберите нужное устройство.

Примечание. В списке **Подключенные устройства** отображаются только те устройства, которые в данный момент подключены или вставлены в соответствующий считыватель.

3 В списке **Контейнеры ключей на устройстве** выберите контейнер.

- Чтобы просмотреть свойства выбранного контейнера, нажмите кнопку **Просмотреть** (см. «Просмотр и настройка свойств контейнера ключей» на стр. 88).
- Чтобы удалить контейнер ключей с устройства, нажмите кнопку **Удалить**.

Примечание. Если список **Контейнеры ключей на устройстве** пуст, это значит, что на выбранном устройстве нет контейнеров.

Настройка списка опрашиваемых устройств

В программе ViPNet CSP вы можете указать типы устройств, которыми будете пользоваться, в разделе **Настройка списка опрашиваемых устройств**. Если флажок напротив какого-либо типа устройств снят, работа таких устройств с программой будет невозможна.

По умолчанию ViPNet CSP проводит поиск устройств всех поддерживаемых типов. Чтобы сократить время поиска нужного ключа, отключите неиспользуемые устройства. Для этого:

1 В окне программы **ViPNet CSP** откройте раздел **Настройка списка опрашиваемых устройств**.

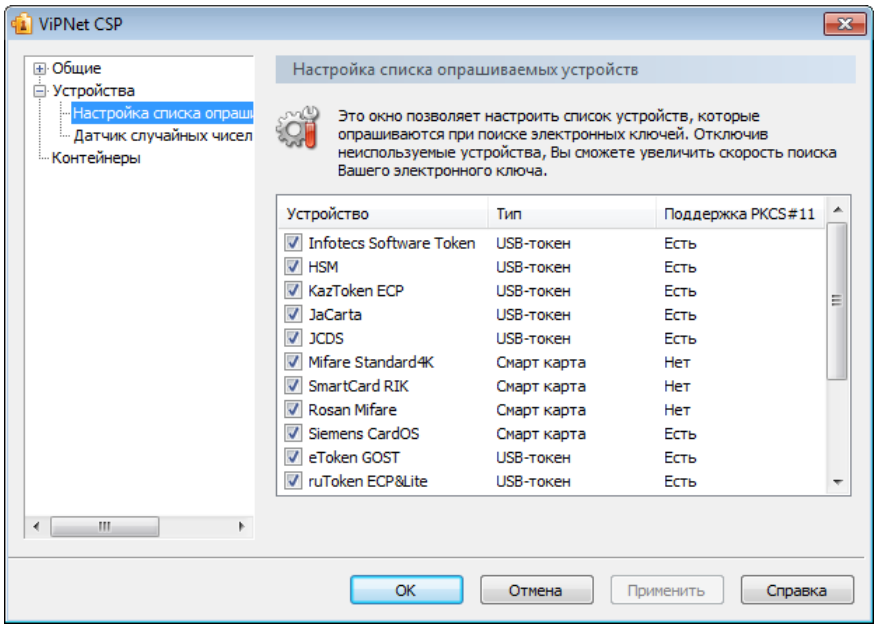


Рисунок 42: Настройка списка опрашиваемых устройств

2 Снимите флажки напротив типов устройств, которые не используются.

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.

Для инициализации подключенного устройства:

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 программы **ViPNet CSP** откройте раздел **Устройства** (см. рисунок на стр. 97).
3. Выберите устройство из списка **Подключенные устройства**.

Примечание. В списке **Подключенные устройства** отображаются только те устройства, которые в данный момент подключены или вставлены в соответствующий считыватель.

4. Нажмите кнопку **Инициализировать**.
5. В окне с предупреждением об удалении данных с устройства нажмите кнопку **Да**.
6. В появившемся окне **Инициализация**:
   - Введите ПИН-код администратора.
   - При необходимости смены ПИН-кода пользователя введите в двух других полях окна также новый ПИН-код пользователя.

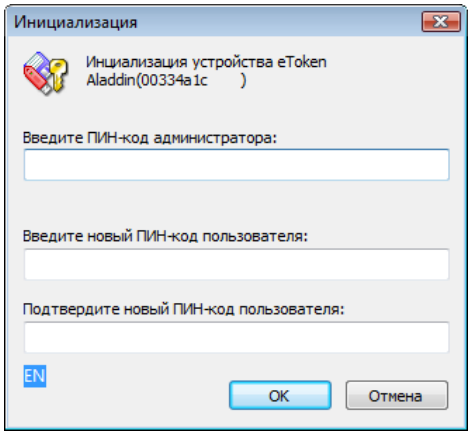


Рисунок 43: Окно «Инициализация»

7 Нажмите кнопку **OK**.

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

Внимание! Перед инициализацией устройства Rutoken или Rutoken ЭЦП в приложении ViPNet следует предварительно инициализировать устройство с помощью программы «Панель управления Рутокен», установив для параметра **Политика смены PIN-кода Пользователя** значение **Администратором**.

В случае если вы используете устройство ОКБ САПР Шипка (Shipka) и произвели инициализацию в приложении ViPNet, для корректной работы устройства вам также необходимо выполнить инициализацию с помощью утилиты ОКБ САПР «Параметры авторизации» (см. «Внешние устройства» на стр. 216).

Программы «Панель управления Рутокен» и «Параметры авторизации» не входят в комплект поставки продуктов ViPNet.

Смена ПИН-кода

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

Чтобы сменить ПИН-код устройства:

1. В окне программы **ViPNet CSP** откройте раздел **Устройства** (см. рисунок на стр. 97).
2. Выберите устройство из списка **Подключенные устройства**.

> **Примечание.** В списке **Подключенные устройства** отображаются только те устройства, которые в данный момент подключены или вставлены в соответствующий считыватель.

3. Нажмите кнопку **Сменить ПИН-код**.
4. В окне **Смена ПИН-кода** выберите тип изменяемого ПИН-кода.
5. В поле **Введите старый ПИН-код** укажите прежний ПИН-код, а в оставшихся двух полях — новый ПИН-код, после чего нажмите кнопку **ОК**.

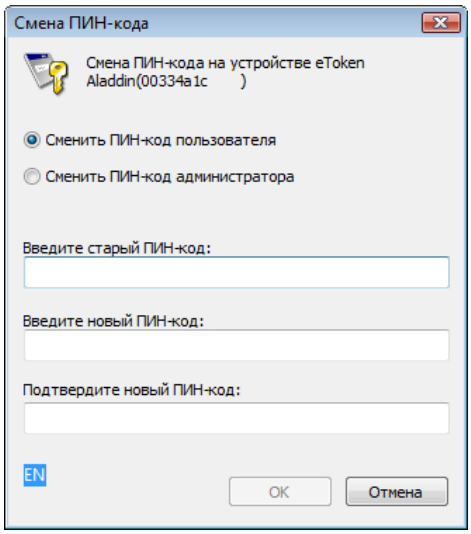


Рисунок 44: Смена ПИН-кода

Примечание. Для некоторых устройств, например для RuToken Lite и Magistra, вы можете задавать и изменять только ПИН-код пользователя.

В результате ПИН-код устройства будет изменен.

Использование датчика случайных чисел

Датчик случайных чисел позволяет генерировать 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»), аппаратный датчик случайных чисел или предварительно сгенерированную последовательность случайных чисел.

Чтобы выбрать используемый датчик случайных чисел:

1 В окне программы **ViPNet CSP** откройте раздел **Датчик случайных чисел**.

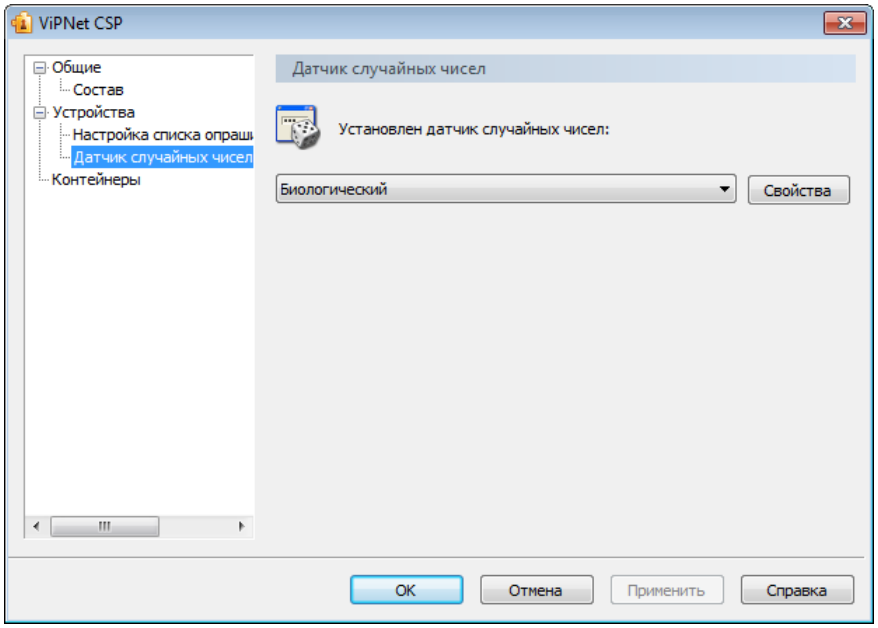


Рисунок 45: Вкладка «Датчик случайных чисел»

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

- **Биологический** — чтобы использовать для генерации случайных чисел «Электронную рулетку».

- **Внешнее устройство (Token) PKCS#11** — чтобы использовать для генерации случайных чисел внешнее устройство eToken Aladdin или eToken ГОСТ (см. «Внешние устройства» на стр. 216).

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 внешнее устройство.

При использовании ГОСТ-устройств генерация случайных чисел всегда осуществляется средствами этих устройств вне зависимости от выбранного датчика случайных чисел.

- **ДСДР** — чтобы использовать предварительно сгенерированную последовательность случайных чисел (гамму). Выбрав данный вариант:
  - Нажмите кнопку **Свойства**.
  - В окне **Свойства** нажмите кнопку **Добавить гамму**.
  - В окне **Просмотр каталогов** укажите папку, в которой находятся файлы, содержащие последовательность случайных чисел.
- Аппаратный датчик случайных чисел, установленный на компьютере.

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

4 Для просмотра информации о выбранном датчике случайных чисел нажмите кнопку **Свойства**.

Чтобы проверить работоспособность биологического или аппаратного датчика случайных чисел, в окне **Свойства** нажмите кнопку **Тестировать**. После проведения теста программа выдаст сообщение о его результате.

Настройка ViPNet CSP для работы с универсальной электронной картой (УЭК)

Если вы являетесь владельцем универсальной электронной карты (УЭК), на которой размещены контейнер ключей и квалифицированный сертификат (см. «Общие сведения об универсальной электронной карте» на стр. 182), для того чтобы воспользоваться Единым порталом государственных услуг или подписывать электронные документы с помощью вашей карты, предварительно настройте программу ViPNet CSP для работы с УЭК. Для этого выполните следующие действия:

1. Скопируйте на жесткий диск сертификат оператора канала обслуживания (ОКО), а также контейнер ключей и сертификат терминала, полученные в пункте выдачи карт.
2. Запустите программу `Uec_pkcs11_settings.exe`, которая находится в следующей папке:
   - Для 32-разрядных операционных систем:
     `C:\Program Files\InfoTeCS\ViPNet CSP`.
   - Для 64-разрядных операционных систем:
     `C:\Program Files (x86)\InfoTeCS\ViPNet CSP`.
3. В окне **Настройка УЭК** укажите расположение сертификата открытого ключа ОКО, сертификата открытого ключа терминала, а также контейнера ключей терминала в соответствующих полях и нажмите кнопку **Сохранить**.

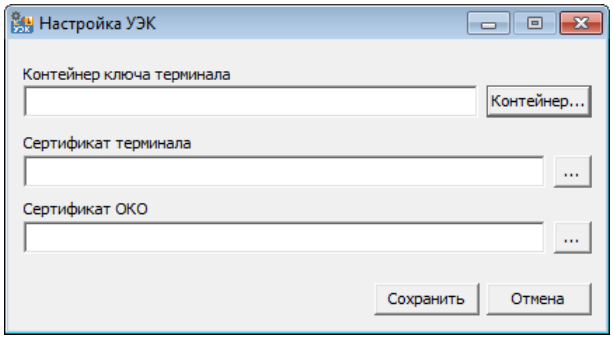


Рисунок 46: Первичная настройка УЭК

4. Запустите программу ViPNet CSP.

5 Убедитесь, что в разделе **Настройка списка опрашиваемых устройств** (см. рисунок на стр. 99) главного окна программы установлен флажок напротив устройства **UEC**.

6 Подключите к компьютеру любой PC/SC-совместимый считыватель контактных смарт-карт и установите его драйвер.

7 Поместите УЭК в считыватель.

8 В главном окне ViPNet CSP перейдите в раздел **Устройства** (см. рисунок на стр. 97). Откроется окно **ViPNet CSP - пароль контейнера ключей.**

9 Введите пароль доступа к установленному контейнеру ключей терминала, полученный в пункте выдачи карт. Чтобы впоследствии не указывать этот пароль, установите также флажок **Запомнить пароль.**

10 В списке **Контейнеры ключей на устройстве** выберите контейнер ключей, записанный на УЭК, и нажмите кнопку **Просмотреть.**

11 В окне **Свойства контейнера ключей** (см. рисунок на стр. 89) нажмите кнопку **Проверить** и введите код PIN2 вашей УЭК. Успешная проверка означает, что с данным сертификатом впоследствии можно работать.

Примечание. В случае если в пункте выдачи карт на вашу УЭК был записан сертификат электронной подписи, но в окне **Свойства контейнера ключей** показано, что на УЭК не записано ни одного сертификата, в разделе **Настройка списка опрашиваемых устройств** снимите все флажки, кроме **UEC**, и повторите подключение карты.

12 В окне **Свойства контейнера ключей** нажмите кнопку **Сертификат** и установите сертификат в хранилище **Личное** операционной системы.

Теперь вы можете использовать вашу электронную подпись для подписания документов, получения государственных, муниципальных и других услуг (см. «Авторизация на Едином портале государственных и муниципальных услуг Российской Федерации» на стр. 183).

9

Создание замкнутой программной среды

Общая информация

Программа ViPNet CSP соответствует требованиям ФСБ России к средствам криптографической защиты информации классов КС1, КС2 и КС3. Класс (уровень) криптографической защиты персональных данных КС3 предусматривает не только необходимость контроля самого средства криптографической защиты информации, но и функционирование этого средства в замкнутой программной среде, то есть в такой среде, где пользователь может запускать только явно разрешенные ему приложения. Замкнутая программная среда представляет собой заданную совокупность файлов, целостность которых регулярно проверяется. Поэтому если в вашей организации требуется использовать средства криптографической защиты, соответствующие классу КС3, вам необходимо выбрать файлы для включения в замкнутую среду и настроить проверку их целостности. Если же в вашей организации допускается работа со средствами криптографической защиты, соответствующими классу защиты КС1 или КС2, создание замкнутой среды необязательно.

Внимание! Для того чтобы механизм контроля целостности файлов был доступен, необходимо в мастере установки ViPNet CSP выбрать компонент **Контроль целостности по классу КС3** (см. «Установка программы» на стр. 33). Если данный компонент отсутствует, его необходимо добавить (см. «Добавление, удаление и восстановление компонентов программы» на стр. 35).

Чтобы организовать замкнутую программную среду, выполните следующие действия:

1. Добавьте файлы в список контроля целостности (см. «Добавление файлов в список контроля целостности» на стр. 110).
2. Задайте параметры контроля для каждого конкретного файла (см. «Настройка параметров контроля целостности» на стр. 113).
3. Запустите программу ViPNet CSP в режиме контроля файлов (см. «Выбор режима контроля» на стр. 112).

Добавление файлов в список контроля целостности

Внимание! Для настройки контроля целостности файлов необходимы права администратора операционной системы Windows.

Для организации замкнутой программной среды необходимо выбрать файлы, из которых она должна состоять, включить эти файлы в список контроля целостности и настроить проверку их целостности. Чтобы добавить файлы в список, выполните следующие действия:

1 В окне программы ViPNet CSP перейдите в раздел **Контроль целостности** и нажмите кнопку **Настройка**.

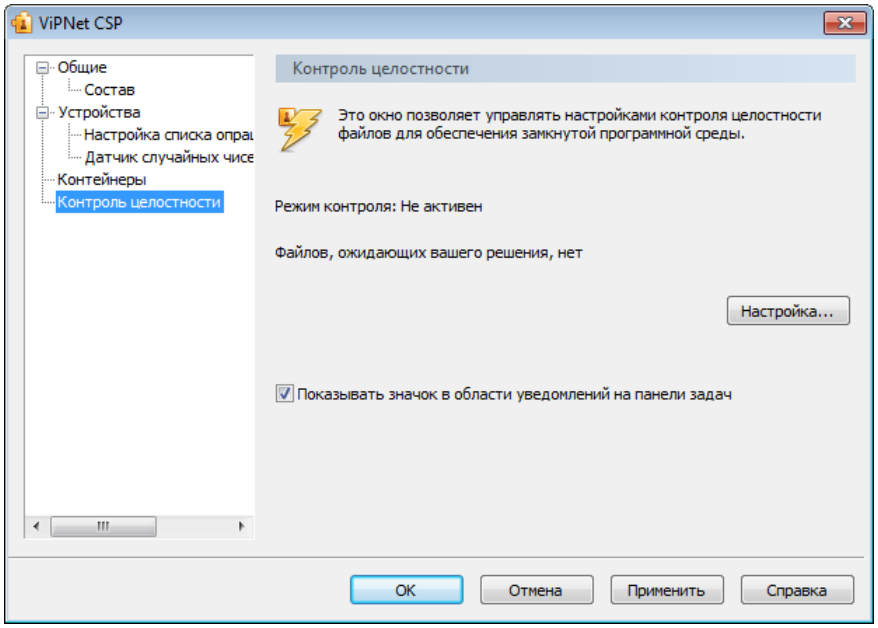


Рисунок 47: Настройка контроля целостности файлов

Примечание. Чтобы добавить в область уведомлений значок, с помощью которого можно в реальном времени просматривать состояние замкнутой программной среды (см. «Мониторинг состояния замкнутой программной среды» на стр. 115), установите флажок **Показывать значок в области уведомлений на панели задач**.

2 В окне **Контроль файлов** напротив строки **Режим контроля** нажмите кнопку **Сменить** и выберите режим **Обучение** (см. «Выбор режима контроля» на стр. 112).

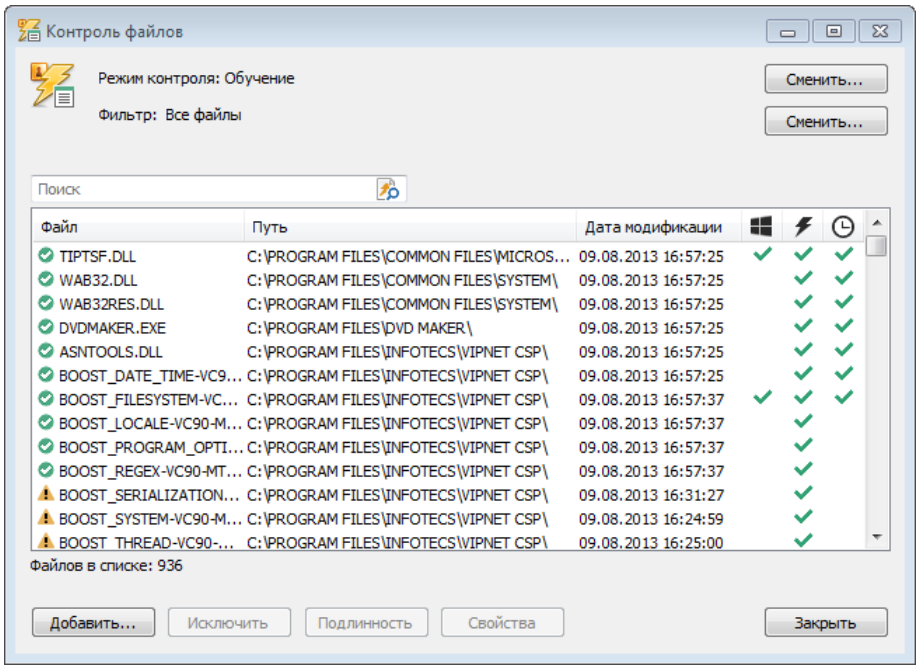


Рисунок 48: Окно «Контроль файлов»

3 Перезагрузите компьютер.

4 После перезагрузки файлы будут добавляться в список контроля целостности по мере обращения к ним.

5 Чтобы добавить файлы в список контроля целостности вручную, нажмите кнопку **Добавить** и выберите нужные файлы.

6 Чтобы удалить файлы из списка контроля целостности, выберите нужные файлы и нажмите кнопку **Исключить**.

После добавления всех нужных файлов в список перейдите к настройке параметров контроля целостности (см. «Настройка параметров контроля целостности» на стр. 113).

Выбор режима контроля

Для функционирования замкнутой программной среды и осуществления контроля целостности файлов необходимо, чтобы программа ViPNet CSP работала в режиме **Контроль файлов**, однако изменить список контролируемых файлов можно только в специальном режиме — **Обучение**. Чтобы выбрать режим работы программы, выполните следующие действия:

1. В окне **Контроль файлов** (см. рисунок на стр. 111) напротив строки **Режим контроля** нажмите кнопку **Сменить.**
2. В окне **Настройка режима контроля** в списке **Режим контроля** выберите нужный режим:
   - **Обучение** — для удобного добавления файлов в список контроля целостности.
   - **Контроль файлов** — для регулярной проверки целостности файлов. В этом режиме пользователь может работать только с теми файлами и программами, которые были включены администратором в состав замкнутой программной среды.

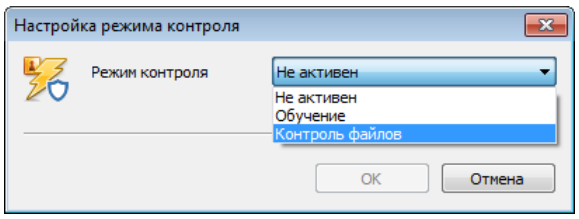


Рисунок 49: Настройка режима контроля целостности файлов

3. Перезагрузите компьютер.

Чтобы отключить функцию контроля целостности файлов, выберите режим работы программы **Не активен**.

Настройка параметров контроля целостности

После добавления файлов в список контроля целостности (см. «Добавление файлов в список контроля целостности» на стр. 110) необходимо для каждого из них задать параметры проверки. Для этого выполните следующие действия:

1 Для первичного подтверждения подлинности, находясь в режиме обучения, в окне **Контроль файлов** (см. рисунок на стр. 111) выберите все файлы из списка и нажмите кнопку **Подлинность**. Значок перед названием файла сменится с ⚠ на ✔.

2 Задайте один из вариантов периодичности проверки. Для этого:

2.1 Выберите файлы, для которых необходимо задать настройки.

> **Примечание.** Для удобства выбора файлов вы можете воспользоваться функцией фильтрации списка (см. «Фильтрация списка контроля целостности» на стр. 115).

2.2 Нажмите кнопку **Свойства**.

2.3 В окне **Свойства** установите нужные флажки:

- **Проверять при старте ОС** — для автоматической проверки выбранных файлов при загрузке операционной системы.
- **Проверять при запуске** — для автоматической проверки выбранных файлов при обращении к ним.
- **Периодическая проверка** — для автоматической проверки выбранных файлов через определенный интервал времени.

Затем нажмите кнопку **OK**.

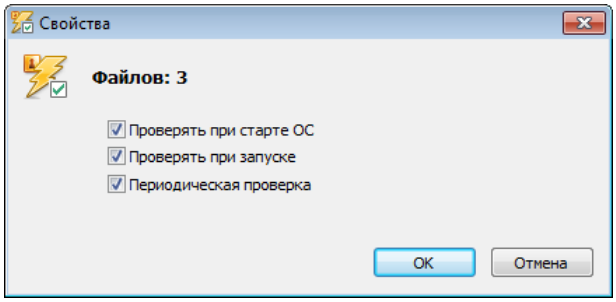


Рисунок 50: Задание периодичности проверки файлов

Выбранные флажки будут отображены в соответствующих столбцах списка контроля файлов.

После задания параметров проверки перейдите в режим **Контроль файлов** и перезагрузите компьютер (см. «Выбор режима контроля» на стр. 112).

Внимание! Перед тем как перейти в режим **Контроль файлов**, в Центре обновления Windows необходимо отключить получение обновлений операционной системы.

После запуска программы ViPNet CSP в режиме контроля пользователь будет иметь доступ только к файлами, выбранным в режиме обучения, и эти файлы будут проверяться в соответствии с заданными параметрами, а результаты проверки будут в режиме реального времени доступны в списке контроля целостности файлов. Для отображения только определенных категорий записей в списке вы можете использовать функцию фильтрации (см. «Фильтрация списка контроля целостности» на стр. 115). Краткие сведения о состоянии замкнутой программной системы вы можете просматривать в окне **Контроль целостности** (см. «Мониторинг состояния замкнутой программной среды» на стр. 115).

Примечание. В случае если какой-либо файл, необходимый для загрузки, изменился, операционная система Windows может не запуститься в режиме **Контроль целостности**. В этом случае загрузите операционную систему в безопасном режиме (Safe Mode), проанализируйте журнал загрузки и подтвердите подлинность изменившихся файлов либо замените их.

Фильтрация списка контроля целостности

Для более удобного просмотра списка контролируемых файлов, образующих замкнутую программную среду, вы можете воспользоваться функцией фильтрации. Для этого выполните следующие действия:

1. В окне **Контроль файлов** (см. рисунок на стр. 111) напротив строки **Фильтр** нажмите кнопку **Сменить.**
2. В окне **Настройка фильтра контроля файлов** выберите файлы, которые должны отображаться в списке:
   - В группе **Статус файла** выберите, файлы с какими статусами вы хотели бы увидеть в списке.
   - В группах **Специальный статус** и **Статус проверки** выберите параметры фильтрации, учитывая следующие особенности установки флажков:
     - ☑ — в списке должны присутствовать только файлы с данным статусом.
     - ■ — файлы присутствуют в списке вне зависимости от значения данного статуса.
     - ☐ — в списке должны присутствовать только файлы, не имеющие данный статус.

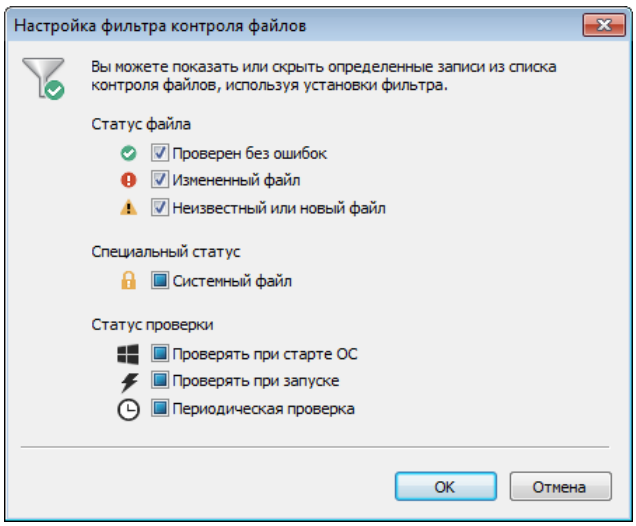


Рисунок 51: Фильтрация списка контроля файлов

Мониторинг состояния замкнутой программной среды

Если в главном окне ViPNet CSP в разделе **Контроль целостности** вы установили флажок **Показывать значок в области уведомлений на панели задач**, то вы можете в

режиме реального времени получать актуальные данные о состоянии замкнутой программной среды. Для этого выполните одно из действий:

- В области уведомлений щелкните значок **ViPNet CSP Контроль целостности**. Появится сообщение о состоянии замкнутой программной среды.

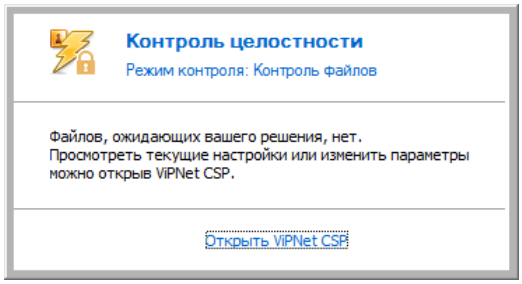


Рисунок 52: Сообщение с информацией о состоянии замкнутой программной среды

- В области уведомлений щелкните значок **ViPNet CSP Контроль целостности** правой кнопкой мыши и в контекстном меню выберите пункт **Просмотр**. Появится окно с информацией о состоянии замкнутой программной среды.

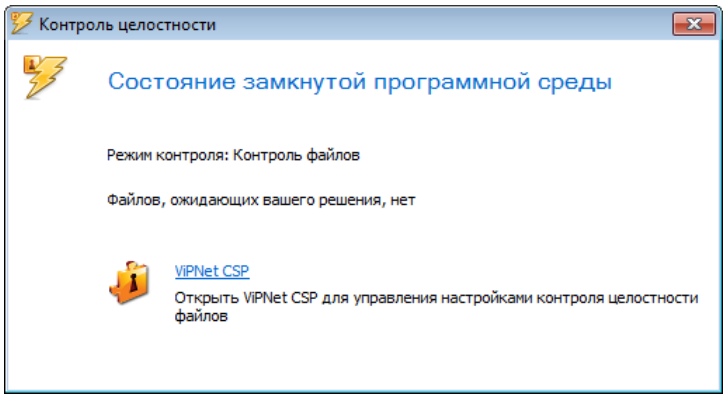


Рисунок 53: Окно с информацией о состоянии замкнутой программной среды

В сообщении и в окне приводится следующая информация:

- Текущий режим контроля.
- Информация о файлах по результатам проверки целостности.

10

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 2003

Чтобы добавить электронную подпись в документ Microsoft Word, Excel или PowerPoint:

1. Сохраните документ.
2. В меню **Сервис** выберите пункт **Параметры**.
3. В окне **Параметры** на вкладке **Безопасность** нажмите кнопку **Цифровые подписи**.
4. В окне **Цифровая подпись** нажмите кнопку **Добавить**.

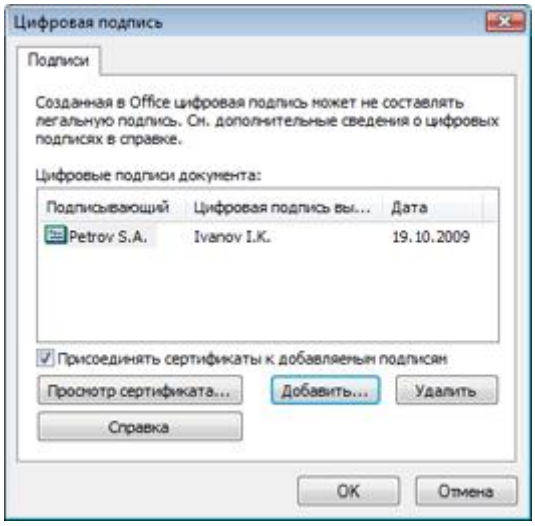


Рисунок 54: Добавление цифровой подписи

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

5 Откроется окно **Выбор сертификата** со списком доступных сертификатов электронной подписи. Чтобы просмотреть сведения о сертификате, выберите его и нажмите кнопку **Просмотр сертификата.**

6 В окне **Выбор сертификата** выберите нужный сертификат и нажмите кнопку **OK.** Откроется окно **ViPNet CSP – пароль контейнера ключей** (см. рисунок на стр. 91).

7 Введите пароль и нажмите кнопку **OK**. Выбранный сертификат появится в списке **Цифровые подписи документа** окна **Цифровая подпись.**

8 Дважды нажмите кнопку **OK**, чтобы закрыть диалоговые окна. В строке состояния в окне документа появится значок , обозначающий, что документ содержит электронную подпись.

Если после подписания документа в него были внесены какие-либо правки, при попытке сохранить документ появится предупреждение о том, что при сохранении все электронные подписи будут удалены. При необходимости вы можете снова подписать документ после сохранения изменений.

Microsoft Office 2007

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

1 Сохраните документ.

2 Нажмите кнопку **Microsoft Office** , выберите пункт **Подготовка**, а затем нажмите **Добавить цифровую подпись.** Откроется окно **Подписание.**

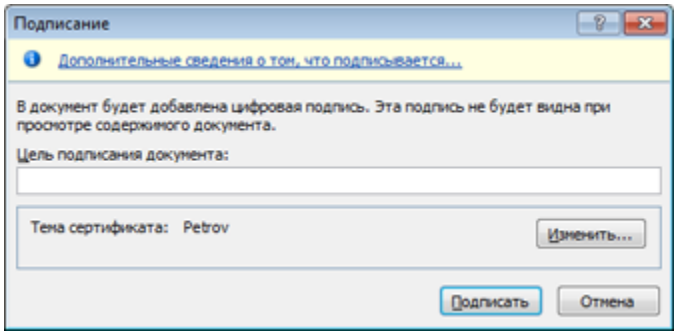


Рисунок 55: Добавление электронной подписи

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

3 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.

4 Выбрав сертификат, нажмите кнопку **Подписать**. Откроется окно **ViPNet CSP – пароль контейнера ключей** (см. рисунок на стр. 91).

5 Введите пароль и нажмите кнопку **OK**. Появится сообщение об успешном добавлении электронной подписи и сохранении документа. В строке состояния документа появится значок , обозначающий, что документ содержит электронную подпись.

Совет. При внесении каких-либо правок в подписанный документ все электронные подписи удаляются, однако при необходимости вы можете внести правки и затем подписать документ снова.

Microsoft Office 2010

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

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.

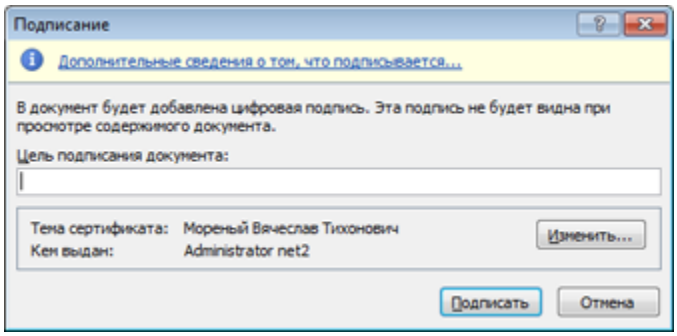


Рисунок 56: Добавление электронной подписи

5 Выбрав сертификат, нажмите кнопку **Подписать**. Откроется окно **ViPNet CSP – пароль контейнера ключей** (см. рисунок на стр. 91).

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.

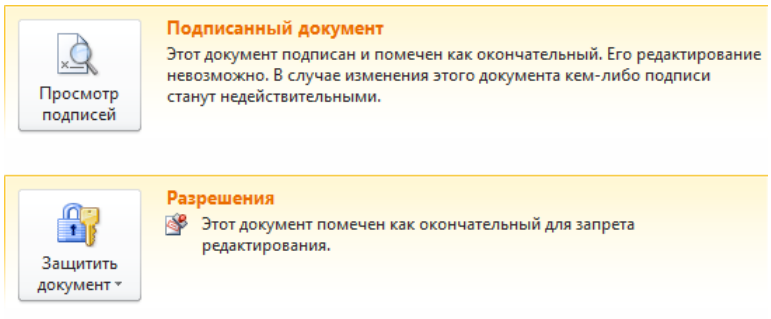


Рисунок 57: Информация о том, что документ помечен как окончательный

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

Совет. При внесении каких-либо правок в подписанный документ все электронные подписи удаляются, однако при необходимости вы можете внести правки и затем подписать документ снова.

Microsoft Office 2013

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

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.

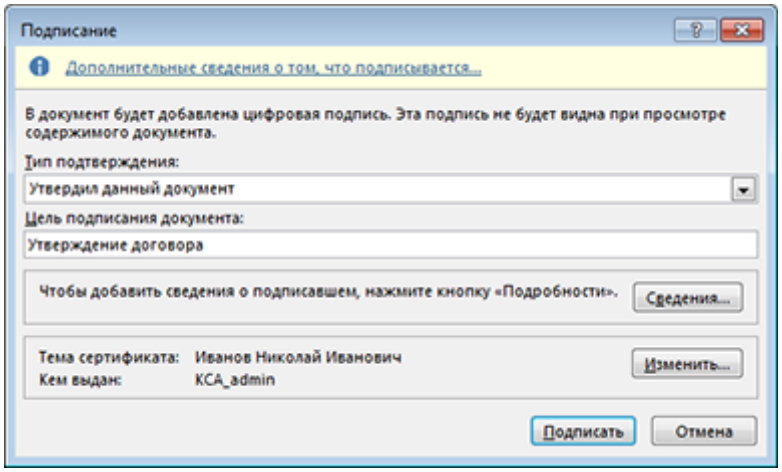


Рисунок 58: Добавление электронной подписи

5 Выбрав сертификат, нажмите кнопку **Подписать**. Откроется окно **ViPNet CSP – пароль контейнера ключей** (см. рисунок на стр. 91).

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.

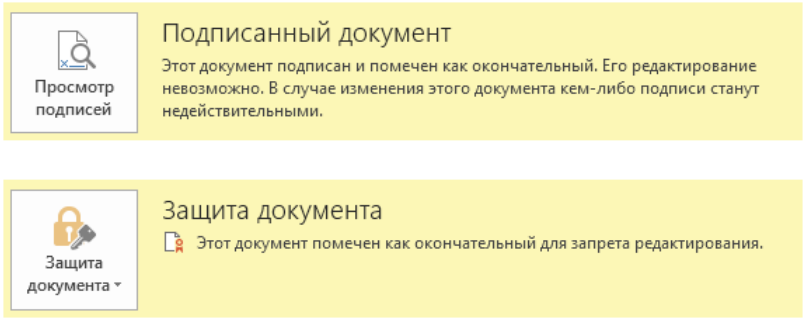


Рисунок 59: Информация о том, что документ помечен как окончательный

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

Совет. При внесении каких-либо правок в подписанный документ все электронные подписи удаляются, однако при необходимости вы можете внести правки и затем подписать документ снова.

Просмотр электронной подписи в Microsoft Word, Excel и PowerPoint

Microsoft Office 2003

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

1. В меню **Сервис** выберите пункт **Параметры**.
2. В окне **Параметры** на вкладке **Безопасность** нажмите кнопку **Цифровые подписи**.
3. В окне **Цифровая подпись** выберите сертификат подписи и нажмите кнопку **Просмотр сертификата** (см. рисунок на стр. 118).

   Если сертификат ненадежен, то в окне **Сертификат** на вкладке **Общее** будет выведено сообщение о возникшей проблеме (см. рисунок на стр. 124). Ненадежный сертификат помечается красным крестом.

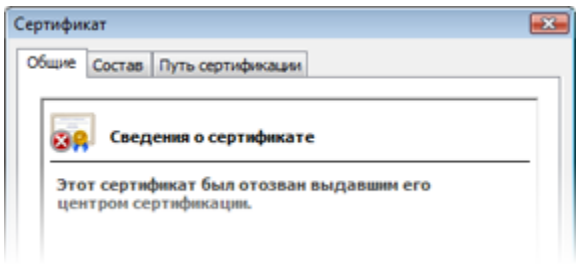


Рисунок 60: Отозванный сертификат

Microsoft Office 2007

Внимание! Документы, подписанные в программах пакета Microsoft Office 2010 или 2013, не могут быть корректно распознаны в программах пакета Microsoft Office 2007 до сборки 12.0.6554. Рекомендуется использовать эту или более позднюю сборку пакета программ.

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

1 Нажмите кнопку **Microsoft Office**  , выберите пункт **Подготовка**, а затем нажмите **Просмотр подписей**. Откроется панель **Подписи** (см. рисунок на стр. 125).

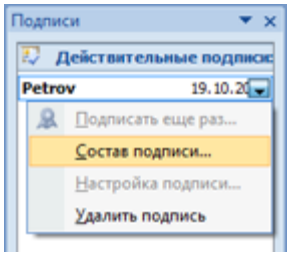


Рисунок 61: Панель «Подписи»

Примечание. Вы можете также 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** (см. рисунок на стр. 127) содержатся краткие сведения о подписи и сертификате. В этом окне 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.

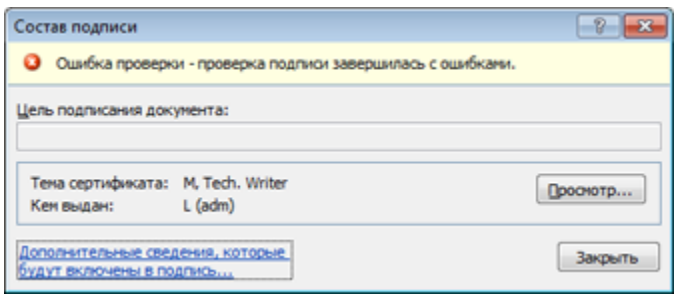


Рисунок 62: Состав подписи

Microsoft Office 2010

Внимание! Документы, подписанные в программах пакета Microsoft Office 2003 или 2007, не могут быть корректно распознаны в программах пакета Microsoft Office 2010 до сборки 14.0.6023. Рекомендуется использовать эту или более позднюю сборку пакета программ.

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

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

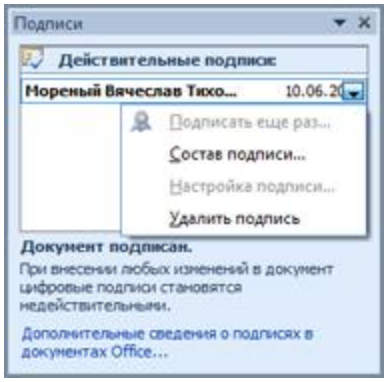


Рисунок 63: Панель «Подписи»

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** (см. рисунок на стр. 127) 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.

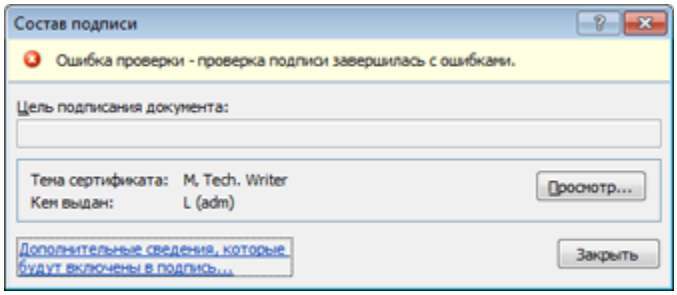


Рисунок 64: Состав подписи

Microsoft Office 2013

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

1 Сохраните документ.

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

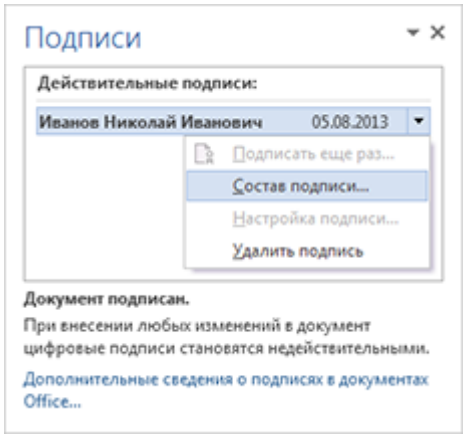


Рисунок 65: Панель «Подписи»

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** (см. рисунок на стр. 127) 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.

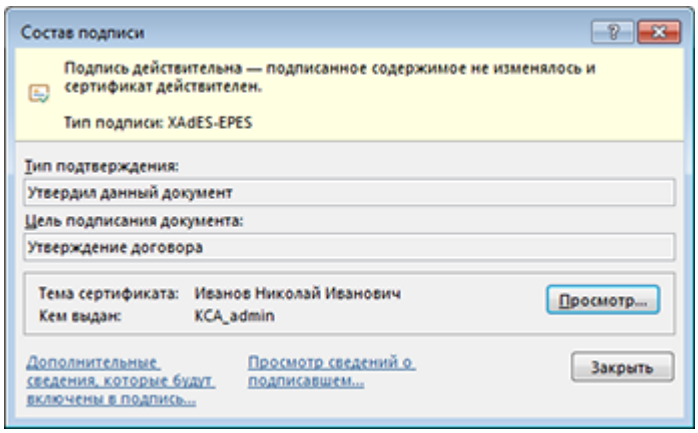


Рисунок 66: Состав подписи

Удаление электронной подписи в Microsoft Word, Excel и PowerPoint

Microsoft Office 2003

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

1. В меню **Сервис** выберите пункт **Параметры**.
2. В окне **Параметры** на вкладке **Безопасность** нажмите кнопку **Цифровые подписи**.
3. В окне **Цифровая подпись** (см. рисунок на стр. 118) выберите подпись для удаления. Вы можете просмотреть сертификат подписи, нажав кнопку **Просмотр сертификата**.
4. Выбрав электронную подпись, нажмите кнопку **Удалить**. Подпись будет удалена из документа.

Microsoft Office 2007

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

1. Откройте панель **Подписи**. Для этого нажмите кнопку **Microsoft Office**  , выберите пункт **Подготовка**, а затем нажмите **Просмотр подписей**.

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

2. На панели **Подписи** (см. рисунок на стр. 125) 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 2010

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

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 на стр. 126) 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:

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 на стр. 127) 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 из пакетов программ Office 2007, 2010 и 2013 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:

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**.

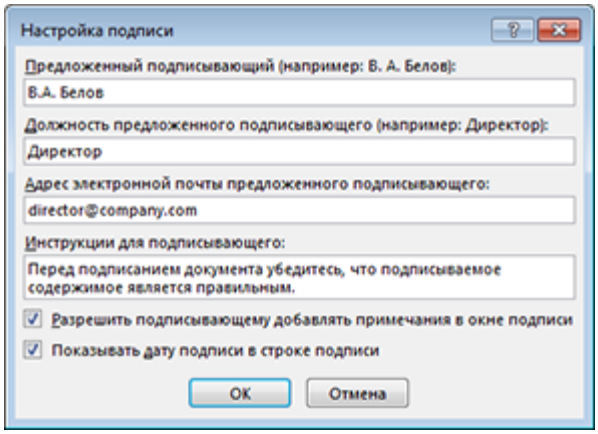


Рисунок 67: Окно «Настройка подписи»

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 68: 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:

1. В зависимости от используемой версии программы выполните одно из действий:
   - В программе Microsoft Word 2007 или Microsoft Excel 2007 нажмите кнопку **Microsoft Office**, выберите пункт **Подготовка**, а затем нажмите **Просмотр подписей**. Откроется панель **Подписи** (см. рисунок на стр. 125).

     На панели **Подписи** щелкните правой кнопкой мыши название строки подписи (или щелкните правой кнопкой мыши саму строку подписи в документе), в меню выберите пункт **Настройка подписи**.
   - В программе Microsoft Word или Microsoft Excel версии 2010 или 2013 щелкните правой кнопкой мыши строку подписи и в контекстном меню выберите пункт **Настройка подписи**.
2. В окне **Настройка подписи** (см. рисунок на стр. 131) внесите необходимые изменения и нажмите кнопку **OK**.

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 версий 2007, 2010 и 2013 вы можете подписать документ, используя видимую строку подписи.

Примечание. Если открыть документ с видимой строкой подписи в приложении, входящем в пакет Microsoft Office более ранней версии, чем 2007, строка подписи будет заменена обычным рисунком, и ее невозможно будет подписать.

Чтобы добавить электронную подпись в строку подписи:

1 В зависимости от версии программы выполните одно из действий:

- В программе Microsoft Word 2007 или Microsoft Excel 2007:

  1. Нажмите кнопку **Microsoft Office**  , выберите пункт **Подготовка**, а затем нажмите **Просмотр подписей**. Откроется панель **Подписи** (см. рисунок на стр. 125).

  2. На панели **Подписи** щелкните правой кнопкой мыши строку подписи (или щелкните правой кнопкой мыши саму строку подписи в документе) и в меню выберите пункт **Подписать.**

- В программе Microsoft Word или Microsoft Excel версии 2010 или 2013 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.

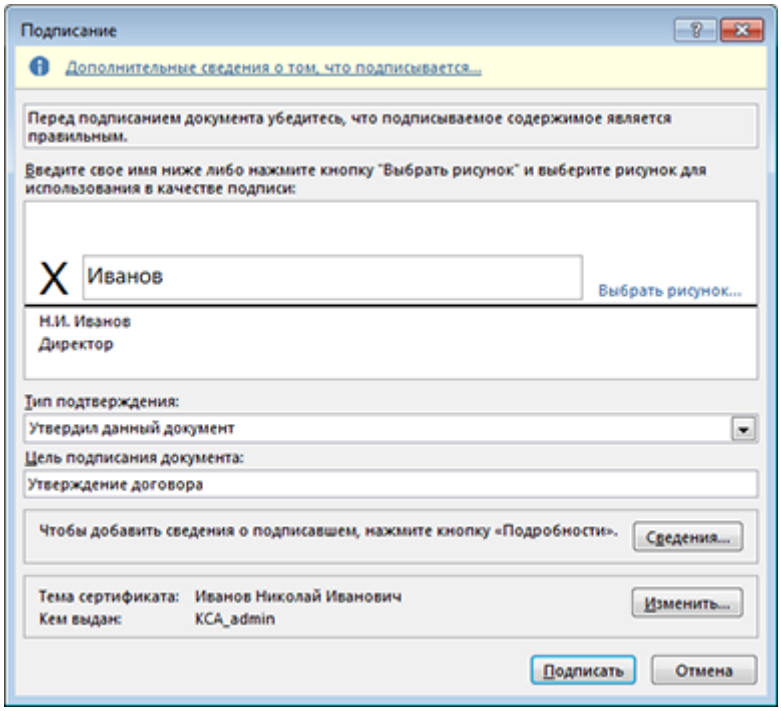


Рисунок 69: Подписание строки подписи в приложениях Microsoft Office 2013

3 После ввода имени и выбора сертификата нажмите кнопку **Подписать**. Откроется диалоговое окно **ViPNet CSP – пароль контейнера ключей** (см. рисунок на стр. 91).

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.**

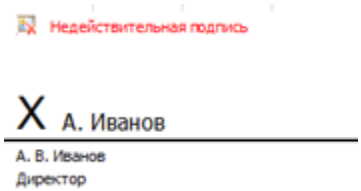


Рисунок 70: Недействительная подпись

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. 124) или удалить подпись (см. «Удаление электронной подписи в Microsoft Word, Excel и PowerPoint» на стр. 129) из видимой строки подписи можно так же, как в случае невидимой подписи.

11

Электронная подпись и шифрование в почтовых программах Microsoft

Порядок организации обмена защищенными сообщениями

В данном разделе описывается взаимодействие ViPNet CSP с почтовыми программами Microsoft Outlook (версии 2003, 2007, 2010 или 2013) и Почта Windows Live (версии 2009). Для того чтобы организовать обмен защищенными сообщениями с помощью ViPNet CSP в какой-либо из этих программ, выполните следующие действия:

1. Установите (см. «Способы установки закрытого ключа и сертификата» на стр. 71) контейнер ключей и сертификат в программе ViPNet CSP, а также корневой сертификат и список отозванных сертификатов (см. «Установка сертификатов издателей и СОС» на стр. 84).
2. Обменяйтесь сертификатами с получателем (отправителем) сообщения (см. «Обмен сертификатами с получателем сообщения» на стр. 139).
3. При необходимости настройте почтовую программу для работы с цифровой подписью и зашифрованными сообщениями (см. «Настройка дополнительных параметров электронной подписи и шифрования» на стр. 142).
4. В зависимости от того, являетесь вы отправителем или получателем зашифрованного сообщения:
   - Подпишите сообщение электронной подписью (см. «Добавление электронной подписи ко всем сообщениям» на стр. 145, «Добавление подписи к отдельному сообщению» на стр. 150).
   - Создайте и отправьте зашифрованное сообщение (см. «Шифрование сообщений электронной почты» на стр. 157).
   - Расшифруйте полученное сообщение (см. «Просмотр зашифрованных сообщений» на стр. 163).

Внимание! Чтобы подписывать сообщения электронной почты, нужно 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 или Почты Windows Live можно шифровать документы и файлы (см. «Шифрование документов и файлов» на стр. 164).

Обмен сертификатами с получателем сообщения

Чтобы зашифровать сообщение электронной почты для определенного получателя, вам необходим сертификат этого получателя. Обмен сертификатами может быть произведен несколькими способами:

- Путем отправки сообщения с электронной подписью (см. «Добавление подписи к отдельному сообщению» на стр. 150). 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. 199).

Чтобы импортировать сертификат в карточку контактов:

1. В программе Microsoft Outlook или в Почте Windows Live откройте представление **Контакты** (в Microsoft Outlook — представление **Люди**).
2. Двойным щелчком откройте нужный контакт.
3. Откройте окно управления сертификатами пользователя:
   - В программе Microsoft Outlook 2003 выберите вкладку **Сертификаты**.
   - В программе Microsoft Outlook 2007 или 2010 на вкладке **Контакт** в группе **Показать** нажмите кнопку **Сертификаты**  .
   - В программе Microsoft Outlook 2013 на вкладке **Контакт** в группе **Показ** нажмите кнопку **Сертификаты** .
   - В Почте Windows Live выберите раздел **Удостоверения**.
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. 199), 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:

1 В программе Microsoft Outlook или в Почте Windows Live создайте новый контакт и заполните карточку своими данными.

2 Импортируйте в контакт ваш сертификат.

3 В контекстном меню контакта:

- В программе Microsoft Outlook 2003 выберите пункт **Переслать**.
- В программе Microsoft Outlook 2007 выберите пункт **Отправить полные контактные сведения** и затем **В формате Outlook**.
- В программе Microsoft Outlook 2010 или 2013 выберите пункт **Переслать контакт** и затем **Как контакт Outlook**.

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

Примечание. В программе Почта Windows Live отправка контакта невозможна.

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:

1. Вызовите окно **Изменения настройки безопасности**:
   - В Microsoft Outlook 2003 выберите в меню **Сервис** пункт **Параметры**, откройте вкладку **Безопасность** и нажмите кнопку **Параметры**.
   - В Microsoft Outlook 2007 выберите в меню **Сервис** пункт **Центр управления безопасностью**, перейдите в раздел **Защита электронной почты** и нажмите кнопку **Параметры**.
   - В Microsoft Outlook 2010 или 2013 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. «S/MIME (Secure Multipurpose Internet Mail Extensions)» на стр. 232).
3. Нажмите **Выбрать** напротив поля **Сертификат подписи** и укажите нужный сертификат.

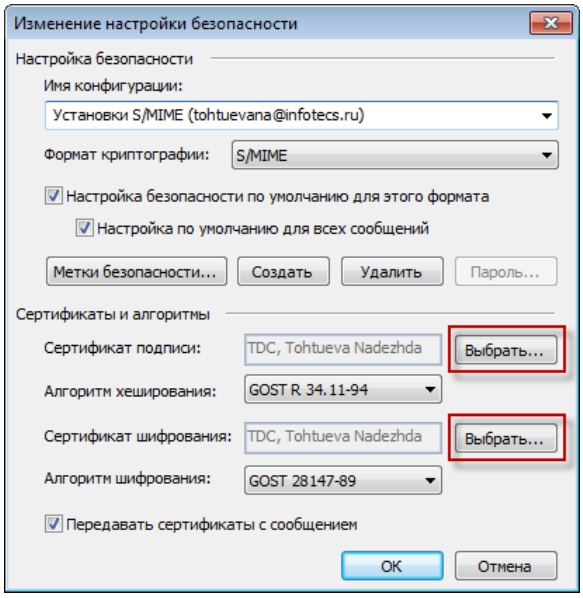


Рисунок 71: Выбор сертификатов для подписи и шифрования

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**.

Чтобы выбрать сертификаты подписи и шифрования в программе Почта Windows Live, выполните следующие действия:

1 В меню **Сервис** выберите пункт **Учетные записи**.

2 В окне **Учетные записи** выберите учетную запись и нажмите кнопку **Свойства**.

3 В окне свойств учетной записи откройте вкладку **Безопасность**.

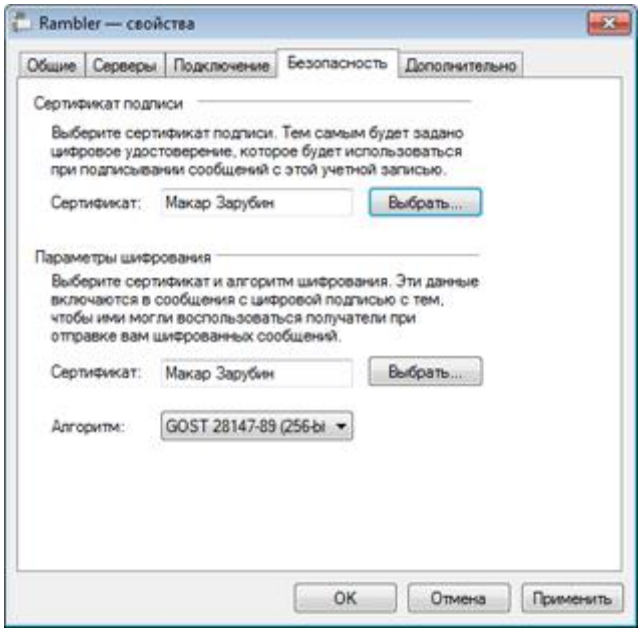


Рисунок 72: Выбор сертификатов подписи и шифрования

4 Нажмите кнопку **Выбрать** напротив поля **Сертификат подписи** и укажите нужный сертификат, который будет использоваться для подписания сообщений.

5 Нажмите кнопку **Выбрать** напротив поля **Сертификат шифрования** и укажите сертификат, который будет использоваться для шифрования сообщений.

6 В списке **Алгоритм** выберите алгоритм шифрования.

7 Нажмите кнопку **OK**.

Добавление электронной подписи ко всем сообщениям

Почтовые программы Microsoft позволяют 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. 157).

Примечание. Более подробные сведения о защите электронной почты средствами криптографии можно получить на веб-узле Office Online http://office.microsoft.com/ru-ru/outlook/HP010461711049.aspx.

Ниже описано, как настроить добавление электронной подписи к исходящим сообщениям в Microsoft Outlook и в Почте Windows Live.

Внимание! Чтобы подписывать сообщения электронной почты, нужно 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.

Microsoft Outlook

Чтобы добавлять электронную подпись ко всем сообщениям:

1. Откройте окно управления безопасностью электронной почты. Для этого:

   Если вы используете Microsoft Outlook 2003:

   - В меню **Сервис** выберите пункт **Параметры**.
   - В окне **Параметры** откройте вкладку **Безопасность**.

Если вы используете Microsoft Outlook 2007:

- В меню **Сервис** выберите пункт **Центр управления безопасностью**.
- В окне **Центр управления безопасностью** откройте вкладку **Защита электронной почты**.

Если вы используете Microsoft Outlook 2010 или 2013:

- 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**.

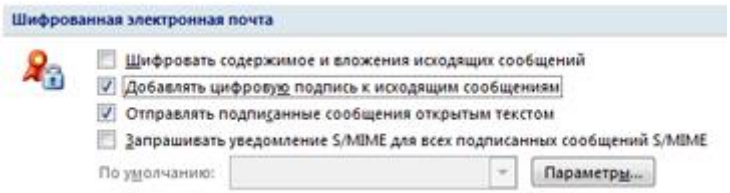


Рисунок 73: Группа «Шифрованная электронная почта» в окне управления безопасностью

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**.

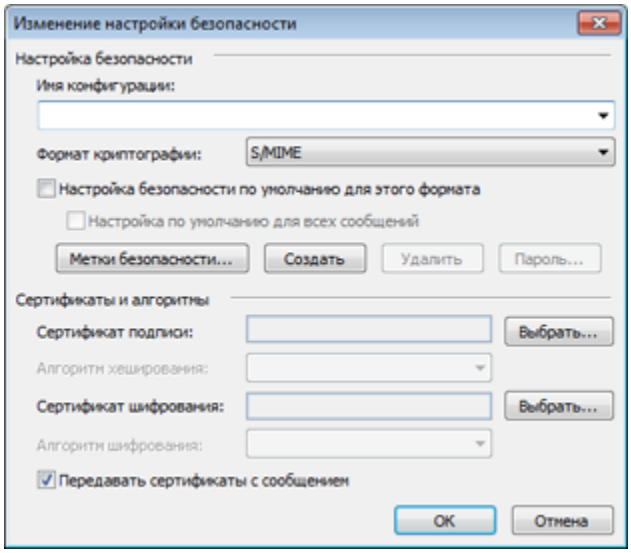


Рисунок 74: Окно «Изменение настройки безопасности»

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, нажмите кнопку **Просмотр сертификата**.

Выбрав сертификат подписи, нажмите кнопку **ОК**. 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 **ОК**.

Почта Windows Live

Чтобы добавлять электронную подпись ко всем сообщениям:

1 В главном окне программы Почта Windows Live в меню **Сервис** выберите пункт **Параметры безопасности**.

2 В окне **Параметры безопасности** откройте вкладку **Безопасность**.

3 В группе **Безопасная почта** установите флажок **Подписывать все отправляемые сообщения**.

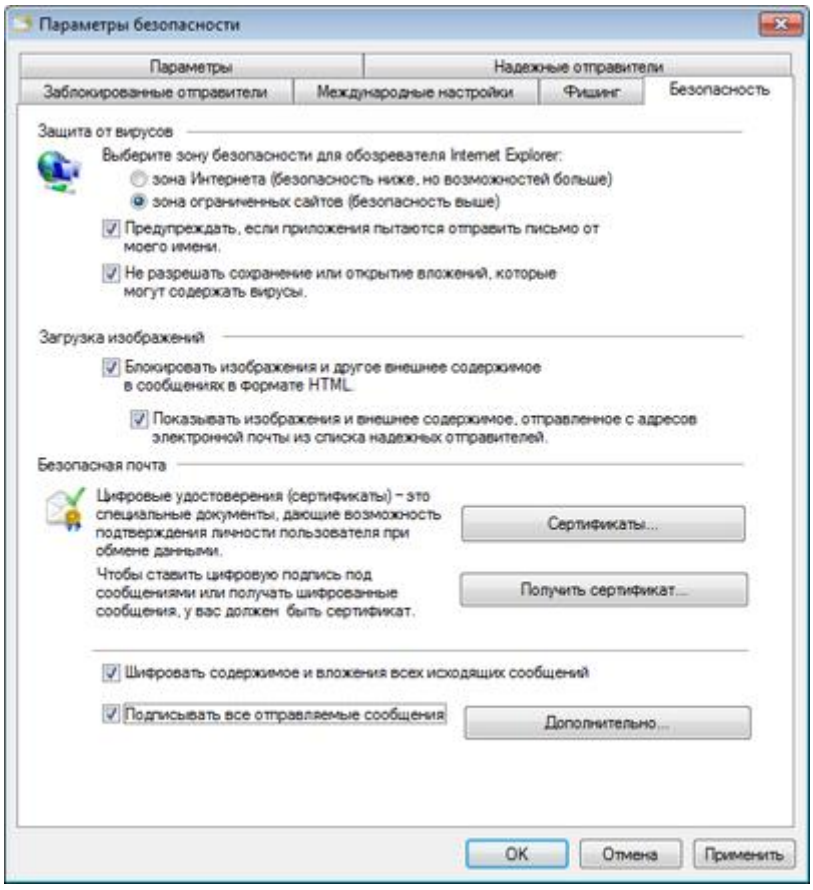


Рисунок 75: Добавление электронной подписи ко всем сообщениям

4 Нажмите кнопку **Дополнительно**. Откроется окно **Дополнительные параметры безопасности**.

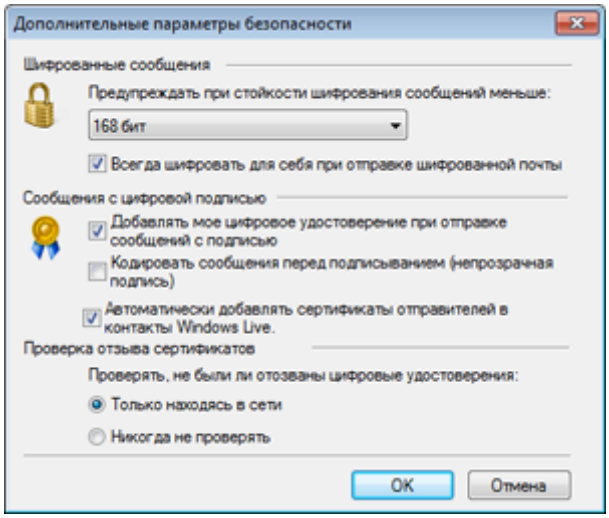


Рисунок 76: Дополнительные настройки безопасности

5 Убедитесь, что установлен флажок **Добавлять мое цифровое удостоверение при отправке сообщений с подписью**.

6 Убедитесь, что установлен флажок **Автоматически добавлять сертификаты отправителей в контакты Windows Live**.

7 Чтобы сохранить настройки, дважды нажмите кнопку **ОК**.

Добавление подписи к отдельному сообщению

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

Внимание! Чтобы подписывать сообщения электронной почты, нужно 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.

Microsoft Outlook

Чтобы подписать сообщение электронной подписью:

1. Создайте новое сообщение и в зависимости от версии программы Microsoft Outlook выполните одно из действий:
   - в программе Microsoft Outlook 2003 нажмите кнопку **Сообщение с цифровой подписью**  на панели инструментов;
   - в программе Microsoft Outlook 2007 откройте вкладку **Сообщение** и в группе **Параметры** нажмите кнопку **Сообщение с цифровой подписью**  ;
   - 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. 145).

2 Если на панели инструментов нет кнопки **Сообщение с цифровой подписью**  (или кнопки **Подписать**  (**Подписать** )), обратитесь к разделу Если отсутствует кнопка «Сообщение с цифровой подписью» («Подписать») (на стр. 151).

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 на стр. 91).

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

Если отсутствует кнопка «Сообщение с цифровой подписью» («Подписать»)

В случае если кнопка **Сообщение с цифровой подписью** (**Подписать**) отсутствует:

1 Откройте окно **Свойства безопасности**. Для этого в зависимости от версии программы Microsoft Outlook выполните одно из действий:

- В программе Microsoft Outlook 2003 нажмите кнопку **Параметры**, затем в окне **Параметры сообщения** нажмите кнопку **Параметры безопасности**.
- В программе Microsoft Outlook 2007 нажмите кнопку вызова диалогового окна группы **Параметры** на вкладке **Сообщение**. В окне **Параметры сообщения** нажмите кнопку **Параметры безопасности**.
- В программе Microsoft Outlook 2010 или 2013 откройте вкладку **Параметры** и в группе **Дополнительные параметры** нажмите кнопку вызова диалогового окна **Свойства**  . В окне **Свойства** нажмите кнопку **Параметры безопасности**.

Откроется окно **Свойства безопасности**.

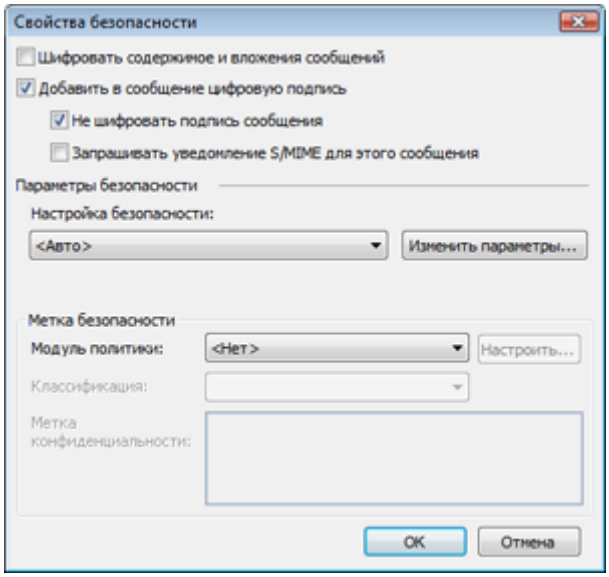


Рисунок 77: Окно «Свойства безопасности»

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

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

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. 142).

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

Почта Windows Live

Чтобы подписать сообщение электронной подписью:

1 В программе Почта Windows Live создайте новое сообщение.

2 В окне **Новое сообщение** в меню **Сервис** выберите пункт **Цифровая подпись**.

Примечание. Если меню в окне **Новое сообщение** скрыто, нажмите кнопку  на панели инструментов и выберите пункт **Отображать строку меню**.

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 на стр. 91).

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

Просмотр электронной подписи сообщения

Microsoft Outlook

Для проверки электронной подписи сообщения в программе Microsoft Outlook:

1. Откройте сообщение с электронной подписью.
2. В строке **Подписано** проверьте адрес электронной почты лица, подписавшего сообщение.

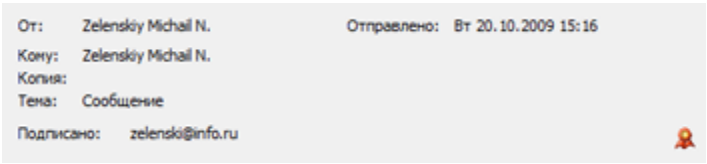


Рисунок 78: Проверка электронной подписи в сообщении

> **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.

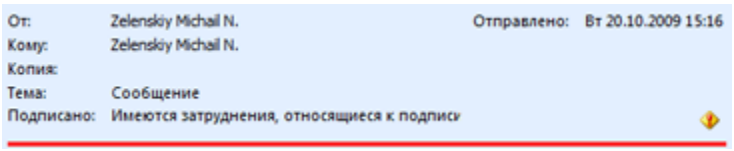


Рисунок 79: Сообщение с недействительной электронной подписью

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**.

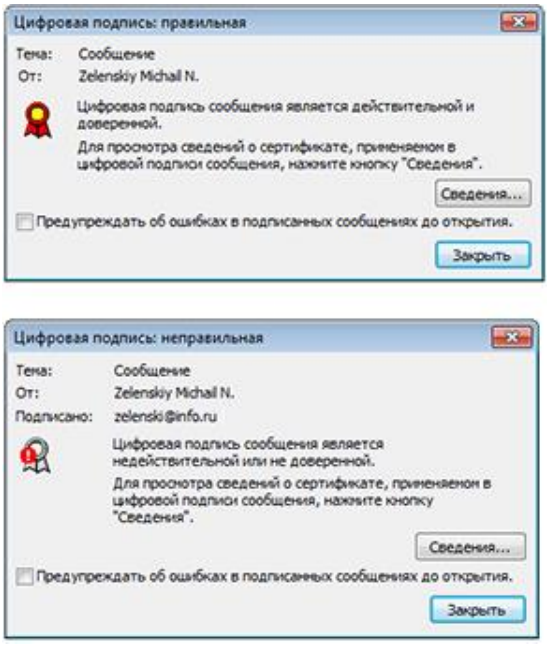


Рисунок 80: Сведения о действительности электронной подписи

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

Почта Windows Live

Для проверки электронной подписи сообщения в программе Почта Windows Live:

1 Выберите в списке сообщений подписанное сообщение.

2 В области чтения в заголовке сообщения будет отображаться значок электронной подписи.

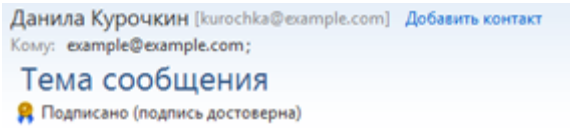


Рисунок 81: Сообщение подписано достоверной электронной подписью

Если при проверке электронной подписи возникли какие-либо проблемы, в заголовке сообщения на красном фоне будет выведено предупреждение об отсутствии доверия к сертификату электронной подписи. Вместо текста сообщения будет отображено предупреждение безопасности.

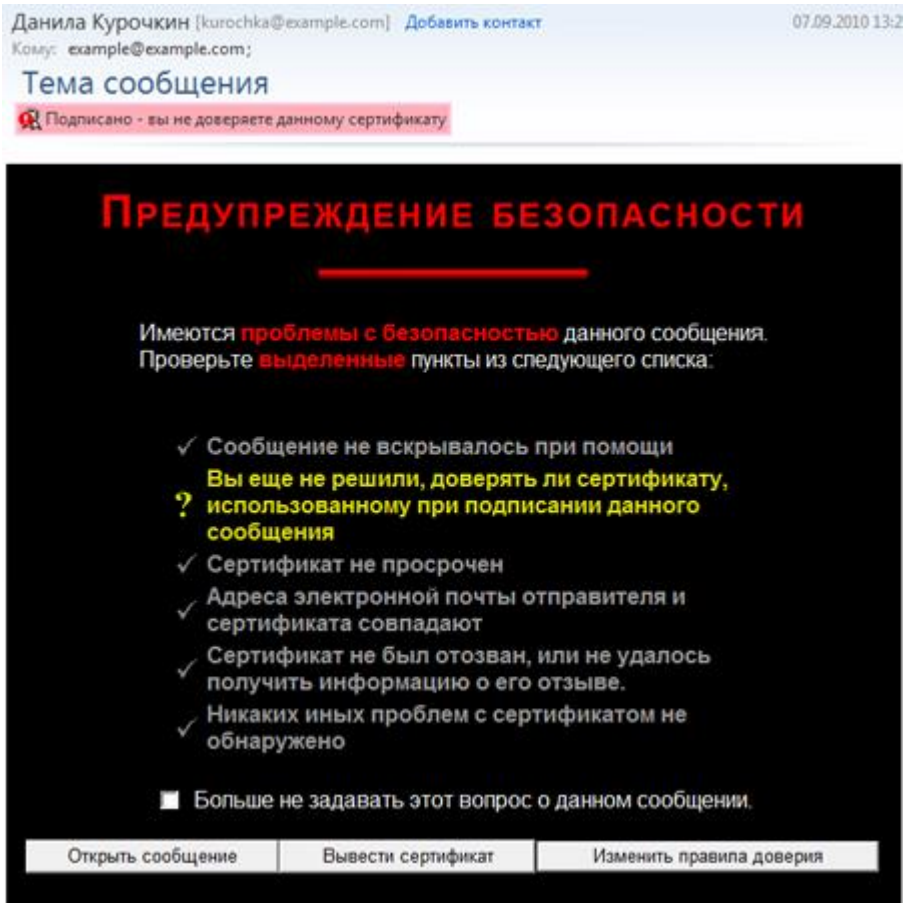


Рисунок 82: Сообщение подписано недостоверной электронной подписью

Если письмо подписано недостоверной электронной подписью, доступны следующие действия:

- Чтобы просмотреть сообщение, нажмите кнопку **Открыть сообщение**.
- Чтобы просмотреть сертификат, которым подписано сообщение, нажмите кнопку **Вывести сертификат**.
- Чтобы сделать сертификат, которым подписано сообщение, доверенным, нажмите кнопку **Изменить правила доверия**.

Шифрование сообщений электронной почты

Шифрование сообщений Microsoft Outlook 2003

Для шифрования отдельного сообщения:

1. В программе Microsoft Outlook создайте новое сообщение и укажите нужного получателя.
2. В окне сообщения выполните одно из действий:
   - на панели инструментов нажмите кнопку **Зашифровать сообщение** .
   - нажмите кнопку **Параметры**, в окне **Параметры сообщения** нажмите **Параметры безопасности** и установите флажок **Шифровать содержимое сообщения и вложения**.

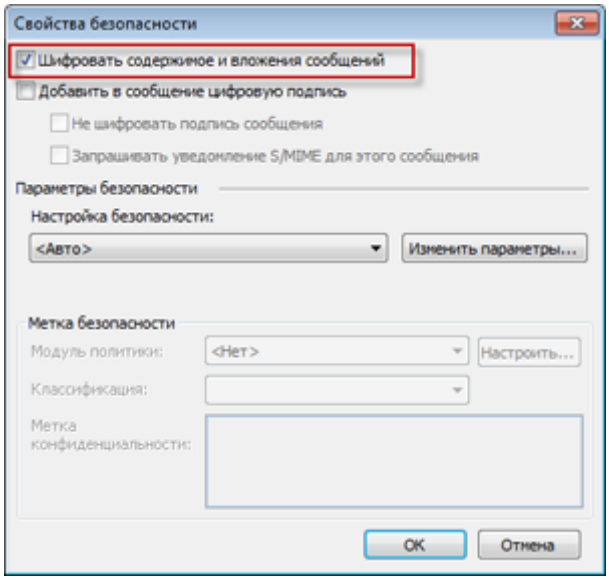


Рисунок 83: Установка параметра для шифрования отдельного сообщения

3. Чтобы изменить дополнительные параметры электронной подписи (см. «Настройка дополнительных параметров электронной подписи и шифрования» на стр. 142), такие как выбор персонального сертификата из нескольких установленных, нажмите кнопку **Изменить параметры**.

4 Нажмите кнопку **OK** три раза.

5 Отправьте получателю зашифрованное сообщение.

Совет. Если при отправке зашифрованного сообщения появилось предупреждение об ошибке, см. раздел Проблемы и неисправности (на стр. 190).

Для шифрования всех отправляемых сообщений:

1 В главном окне программы Microsoft Outlook выберите в меню **Сервис** команду **Параметры** и откройте вкладку **Безопасность**.

2 Установите флажок **Шифровать содержимое и вложения исходящих сообщений**.

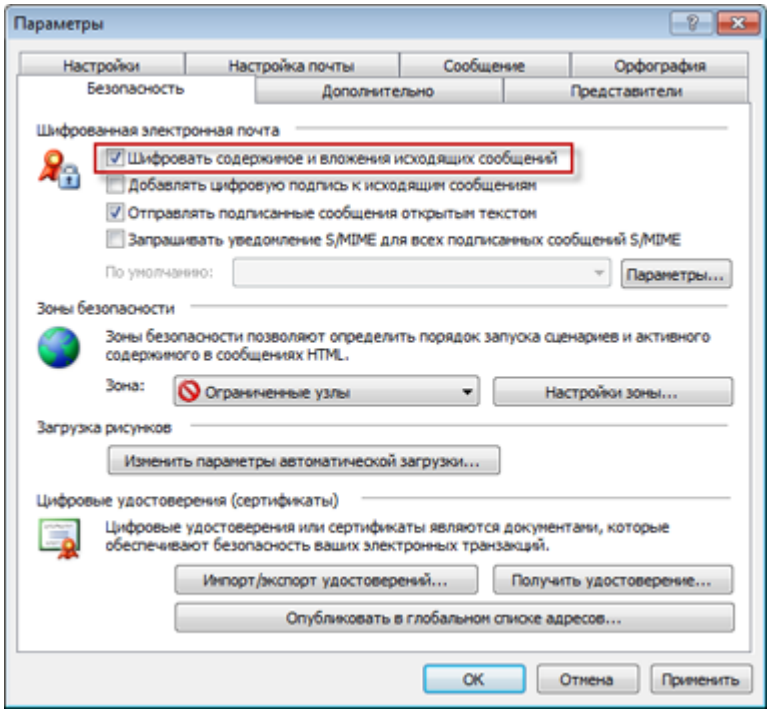


Рисунок 84: Установка параметра для шифрования всех сообщений

3 Чтобы указать для подписи и шифрования ваш сертификат, в окне **Изменение настройки безопасности** нажмите кнопку **Параметры** и выберите нужные сертификаты.

4 После этого все отправляемые сообщения будут зашифрованы, если в карточку контакта получателя сообщения добавлен сертификат.

Шифрование сообщений Microsoft Outlook 2007

Для шифрования отдельного сообщения:

1. В программе Microsoft Outlook создайте новое сообщение и укажите нужного получателя.
2. Установите функцию шифрования одним из способов:
   - В окне сообщения на ленте **Сообщение** в группе **Параметры** нажмите кнопку **Шифровать**  .
   - В окне сообщения на ленте **Сообщение** в группе **Параметры** откройте окно **Свойства безопасности** (см. рисунок на стр. 157) и установите флажок **Шифровать содержимое сообщения и вложения**.

     Чтобы изменить дополнительные параметры настройки (см. «Настройка дополнительных параметров электронной подписи и шифрования» на стр. 142), такие как выбор персонального сертификата из нескольких установленных, нажмите кнопку **Изменить параметры**.
3. Отправьте сообщение.

Для шифрования всех отправляемых сообщений:

1. В главном окне программы Microsoft Outlook в меню **Сервис** выберите команду **Центр управления безопасностью**, а затем перейдите в раздел **Защита электронной почты**.
2. В группе **Защита электронной почты** установите флажок **Шифровать содержимое и вложения исходящих сообщений**.

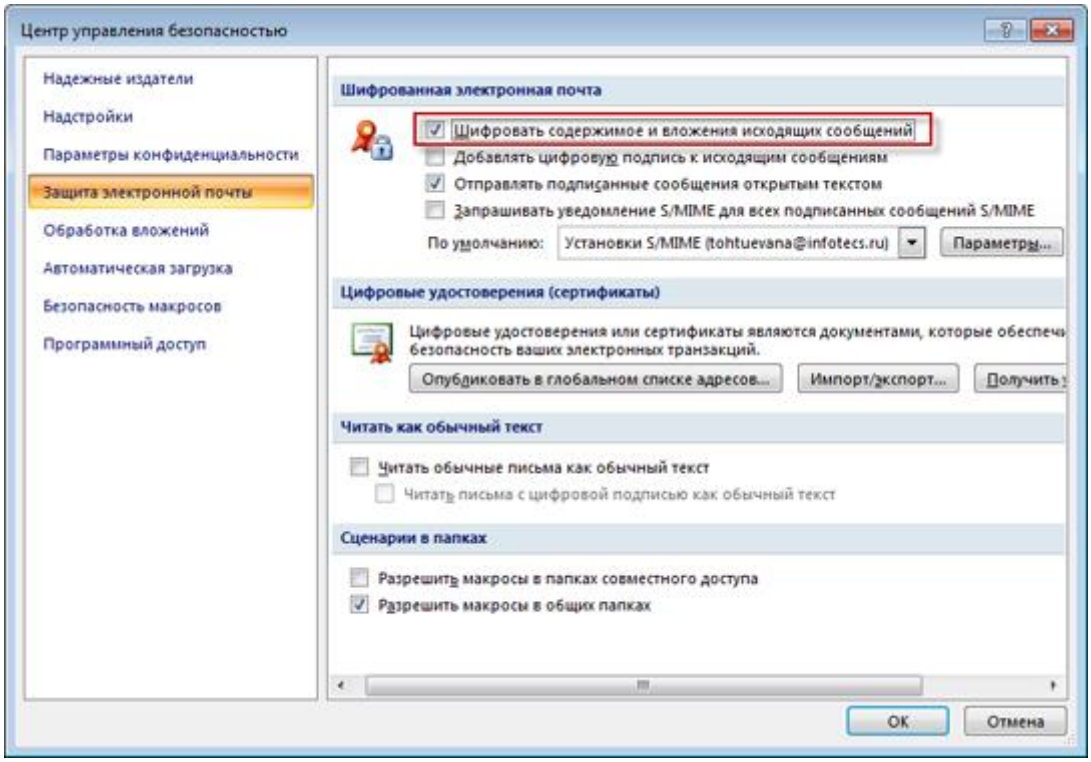


Рисунок 85: Установка параметра для шифрования всех сообщений

3 Чтобы изменить дополнительные параметры настройки (см. «Настройка дополнительных параметров электронной подписи и шифрования» на стр. 142), такие как выбор персонального сертификата из нескольких установленных, нажмите кнопку **Параметры**.

4 Два раза нажмите кнопку **OK**.

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

Шифрование сообщений Microsoft Outlook 2010 и 2013

Для шифрования отдельного сообщения:

1 В программе Outlook 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** (см. рисунок на стр. 157) установите флажок **Шифровать содержимое и вложения сообщений**.

  Чтобы изменить дополнительные параметры настройки (см. «Настройка дополнительных параметров электронной подписи и шифрования» на стр. 142), такие как выбор персонального сертификата из нескольких установленных, нажмите кнопку **Изменить параметры**.

3 Отправьте сообщение.

Для шифрования всех отправляемых сообщений:

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**.

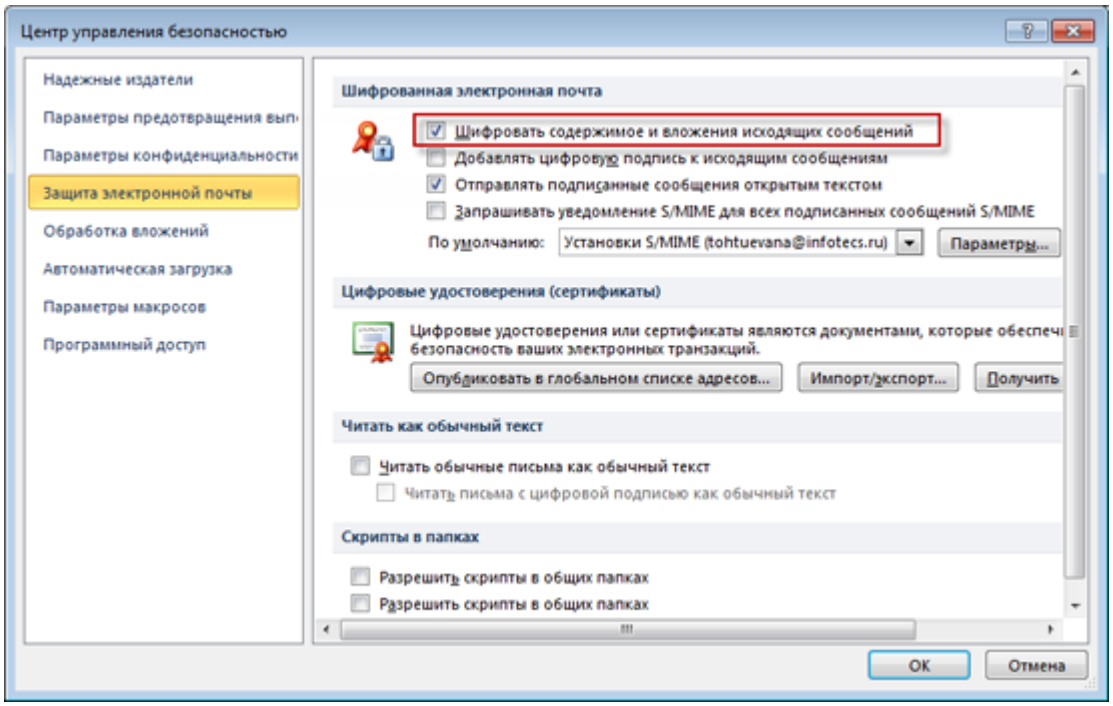


Рисунок 86: Установка параметра для шифрования всех сообщений

4 Чтобы изменить дополнительные параметры настройки (см. «Настройка дополнительных параметров электронной подписи и шифрования» на стр. 142), 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.

Шифрование сообщений Почты Windows Live

Для шифрования отдельного сообщения:

1 В программе Почта Windows Live создайте новое сообщение и укажите нужного получателя.

2 В окне **Новое сообщение** в меню **Сервис** выберите пункт **Зашифровать**.

Примечание. Если меню в окне **Новое сообщение** скрыто, на панели инструментов нажмите кнопку  и выберите пункт **Отображать строку меню**.

---

3 Отправьте сообщение.

Для шифрования всех отправляемых сообщений:

1 В главном окне программы Почта Windows Live в меню **Сервис** выберите пункт **Параметры безопасности**.

2 В окне **Параметры безопасности** откройте вкладку **Безопасность** (см. рисунок на стр. 148).

3 В группе **Безопасная почта** установите флажок **Шифровать содержимое и вложения исходящих сообщений**.

4 Нажмите кнопку **OK**.

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

Просмотр зашифрованных сообщений

Полученное зашифрованное сообщение в списке сообщений отмечено значком  (в Microsoft Outlook) или  (в Почте Windows Live).

В программе Microsoft Outlook при выборе зашифрованного сообщения в области чтения появится предупреждение: «Невозможно отобразить элемент в области чтения. Откройте элемент для чтения его содержимого». В почте Windows Live при выборе зашифрованного сообщения сразу открывается окно ввода пароля доступа к контейнеру. Таким образом, исключается возможность прочтения данного сообщения посторонним лицом.

Внимание! Для просмотра зашифрованного сообщения необходима программа ViPNet CSP.

Чтобы просмотреть зашифрованное сообщение:

1. В Microsoft Outlook дважды щелкните нужное сообщение в списке. В Почте Windows Live выберите сообщение в списке.
2. В окне **ViPNet CSP - пароль контейнера ключей** (см. рисунок на стр. 91) 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. 157).
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.

12

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.

Microsoft Office InfoPath 2003

Чтобы разрешить пользователям подписывать форму Microsoft Office InfoPath 2003:

1. Создайте или откройте шаблон формы в режиме конструктора.
2. В меню **Сервис** выберите пункт **Параметры формы**.
3. В окне **Параметры формы** на вкладке **Цифровые подписи** установите переключатель в положение **Разрешить пользователям подписывать эту форму цифровой подписью**.
4. При необходимости установите флажок **При отправке этой формы без цифровой подписи запрашивать подпись**.
5. Чтобы сохранить настройки, нажмите кнопку **ОК**.

Microsoft Office InfoPath 2007

Чтобы разрешить пользователям подписывать форму Microsoft Office InfoPath 2007:

1. Создайте или откройте шаблон формы в режиме конструктора.
2. В меню **Сервис** выберите пункт **Параметры формы.**
3. В окне **Параметры формы** откройте вкладку **Цифровые подписи**.

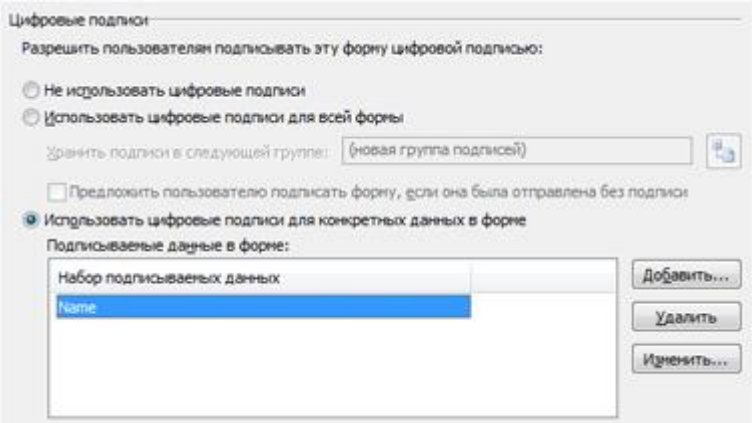


Рисунок 87: Вкладка «Цифровые подписи»

4 Если вы хотите, чтобы пользователь мог подписать всю форму, выберите опцию **Использовать цифровые подписи для всей формы**.

Если вы используете электронные подписи для всей формы, вы можете установить флажок **Предложить пользователю подписать форму, если она была отправлена без подписи**.

5 Если вы хотите, чтобы пользователь мог подписывать отдельные элементы формы, выберите **Использовать цифровые подписи для конкретных данных в форме**.

- Чтобы указать подписываемые данные, нажмите кнопку **Добавить**. Откроется окно **Набор подписываемых данных**.

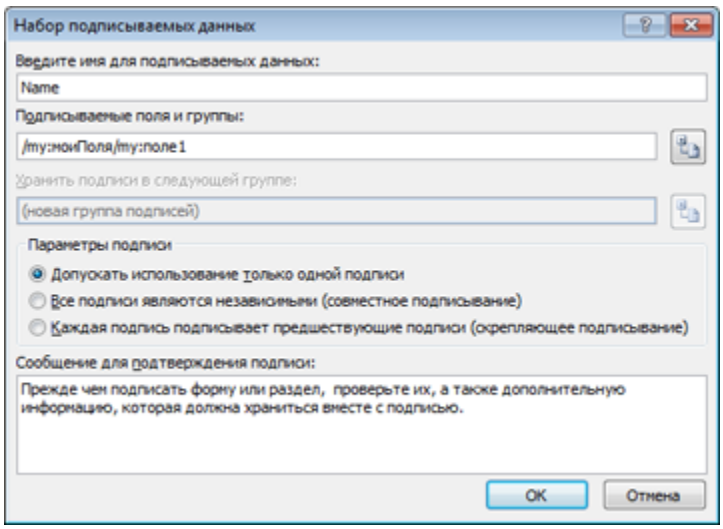


Рисунок 88: Окно «Набор подписываемых данных»

- 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** (см. рисунок на стр. 167).
- Если требуется разрешить подписывать несколько полей формы, повторите описанные в шаге 5 действия необходимое число раз.

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

Microsoft Office InfoPath 2010 и 2013

Чтобы разрешить пользователям подписывать форму Microsoft Office InfoPath 2010:

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**.

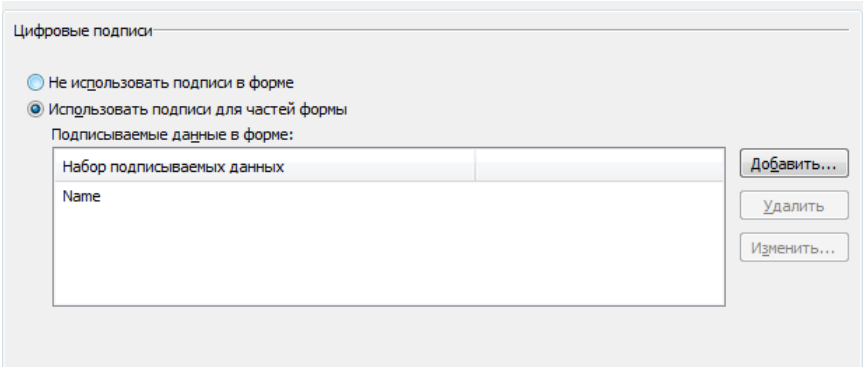


Рисунок 89: Вкладка «Цифровые подписи»

4 Чтобы указать подписываемые данные, нажмите кнопку **Добавить**.

5 В окне **Набор подписываемых данных**:

- 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 **OK**.
- 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 **OK**. Выбранное поле появится в списке **Набор подписываемых данных** (см. рисунок на стр. 167).

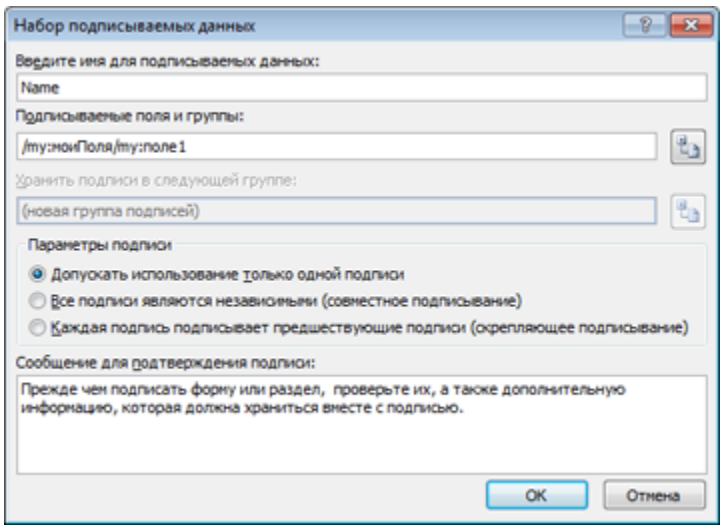


Рисунок 90: Окно «Набор подписываемых данных»

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. Ниже описано, как это сделать.

Microsoft Office InfoPath 2003

Чтобы подписать форму:

1. Откройте форму или шаблон формы.
2. В меню **Сервис** выберите пункт **Цифровые подписи** (или нажмите на панели инструментов кнопку **Цифровые подписи**). Откроется окно **Цифровые подписи**.

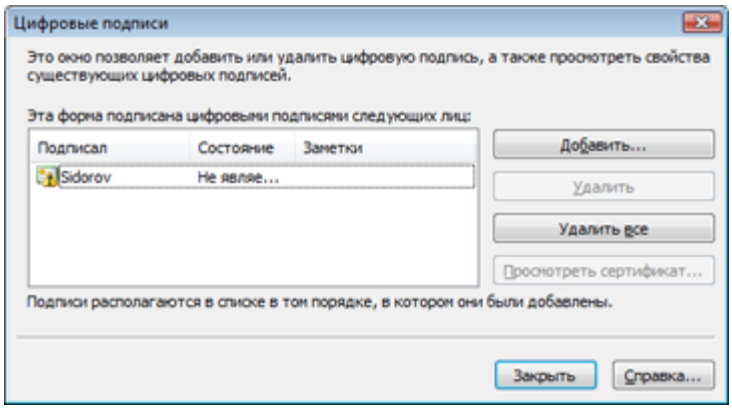


Рисунок 91: Окно «Цифровые подписи»

3. Нажмите кнопку **Добавить**, в открывшемся окне **Добавление подписи** нажмите кнопку **Выбор сертификата**.
4. Из списка выберите сертификат. Вы можете открыть его, нажав кнопку **Просмотр сертификата**. Выбрав сертификат, нажмите кнопку **OK**.
5. В окне **Добавление подписи** при необходимости введите заметки, которые будут добавлены в подпись. Нажмите кнопку **OK**.
6. В открывшемся окне **ViPNet CSP – пароль контейнера ключей** (см. рисунок на стр. 91) введите пароль и нажмите кнопку **OK**.

После подписания внесение изменений в форму невозможно.

Microsoft Office InfoPath 2007, 2010 и 2013

Чтобы подписать форму:

1. Откройте форму или шаблон формы в программе InfoPath 2007, InfoPath Filler 2010 или InfoPath Filler 2013.

2. В зависимости от версии Microsoft Office InfoPath выполните одно из действий:

   - в программе InfoPath 2007 в меню **Сервис** выберите пункт **Цифровые подписи** (или нажмите кнопку **Цифровые подписи** на панели инструментов);
   - в программе InfoPath Filler 2010 или 2013 откройте вкладку **Файл** и в разделе **Сведения** нажмите кнопку **Подписать форму**.

   Откроется окно **Цифровые подписи**.

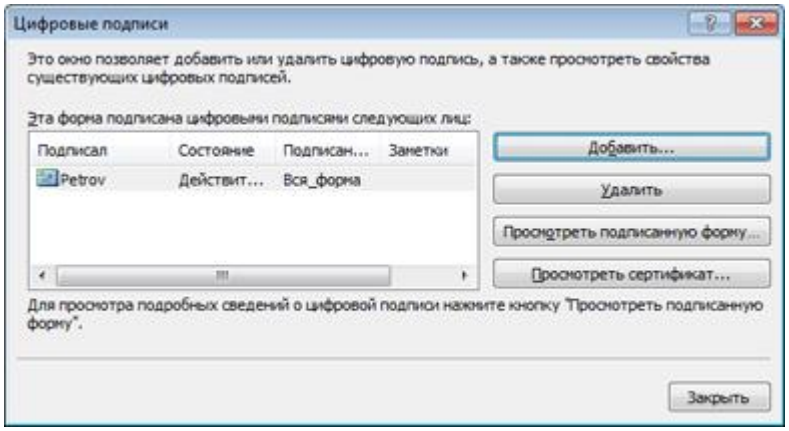


Рисунок 92: Окно «Цифровые подписи»

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 на стр. 134).

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 на стр. 91).

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:

1. В зависимости от версии программы Microsoft InfoPath выполните одно из действий:
   - В программе Microsoft InfoPath 2003 или Microsoft InfoPath 2007 в меню **Сервис** выберите пункт **Цифровые подписи** (или нажмите кнопку **Цифровые подписи**  на панели инструментов).
   - В программе Microsoft InfoPath Filler 2010 откройте вкладку **Файл** и в разделе **Сведения** нажмите кнопку **Цифровые подписи**.
   - В программе Microsoft InfoPath Filler 2013 откройте вкладку **Файл** и в разделе **Сведения** нажмите кнопку **Просмотр подписей**.

   Откроется окно **Цифровые подписи**.
2. Если вы используете Microsoft InfoPath 2003, выберите сертификат подписи из списка и нажмите кнопку **Просмотреть сертификат**.

   Если сертификат ненадежен, то на вкладке **Общее** в окне **Сертификат** (см. рисунок на стр. 124) будет выведено сообщение о возникшей проблеме. Ненадежный сертификат помечен красным крестом.
3. Если вы используете Microsoft InfoPath 2007 или Microsoft InfoPath Filler 2010, выберите электронную подпись из списка и нажмите кнопку **Просмотреть подписанную форму**. Откроется окно **Состав подписи** (см. рисунок на стр. 127).

   Если вы используете Microsoft InfoPath Filler 2013, выберите электронную подпись из списка и нажмите кнопку **Просмотреть подпись**. Откроется окно **Состав подписи** (см. рисунок на стр. 127).
   - 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**. Чтобы просмотреть дополнительные сведения о подписи, щелкните ссылку **Дополнительные сведения, которые будут включены в подпись.**

Удаление подписи из формы InfoPath

Чтобы удалить подпись из формы Microsoft InfoPath:

1. В зависимости от версии программы Microsoft InfoPath выполните одно из действий:
   - В программе Microsoft InfoPath 2003 или 2007 в меню **Сервис** выберите пункт **Цифровые подписи** (или нажмите на панели инструментов кнопку **Цифровые подписи** ).
   - В программе Microsoft InfoPath Filler 2010 или 2013 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:
   - В Microsoft InfoPath 2003 и Microsoft InfoPath Filler 2013 нажмите кнопку **Просмотреть сертификат**. Откроется окно **Сертификат**.
   - В Microsoft InfoPath 2007 или Microsoft InfoPath Filler 2010 нажмите кнопку **Просмотреть подписанную форму**. Откроется окно **Состав подписи**. Чтобы открыть сертификат, нажмите кнопку **Просмотр**.
3. Выбрав электронную подпись, нажмите кнопку **Удалить**.

Примечание. В Microsoft InfoPath 2003 вы можете удалить сразу все электронные подписи, нажав кнопку **Удалить все**.

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

13

Электронная подпись макросов и баз данных

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, Access, 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:

1. Откройте редактор Microsoft Visual Basic.
   - Если вы используете любое из перечисленных приложений версии Microsoft Office 2003 или Microsoft Outlook 2007, Publisher 2007, Visio 2007: в меню **Сервис** выберите пункт **Макрос**, затем щелкните команду **Редактор Visual Basic**.
   - Если вы используете Microsoft Word 2007, Excel 2007 или PowerPoint 2007: на вкладке **Разработчик** в группе **Код** нажмите кнопку **Visual Basic**.

Примечание. Вкладка **Разработчик** по умолчанию не отображается. Чтобы она появилась, в меню **Файл** выберите пункт **Параметры** и в открывшемся окне в разделе **Настройка ленты** (**Настроить ленту**) установите флажок **Разработчик**.

   - Если вы используете Microsoft Access 2007, 2010 или 2013: на вкладке **Работа с базами данных** в группе **Макрос** нажмите кнопку **Visual Basic**.
   - Если вы используете любое из перечисленных приложений, кроме Microsoft Access, версии Microsoft Office 2010 или 2013: на вкладке **Разработчик** в группе **Код** нажмите кнопку **Visual Basic**.

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

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

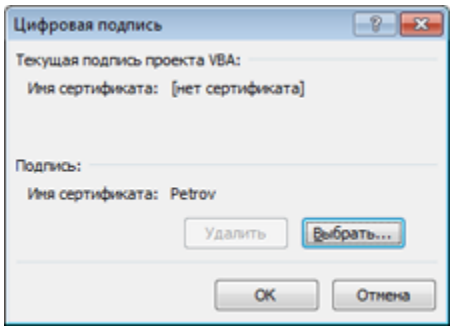


Рисунок 93: Добавление электронной подписи

3 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:

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

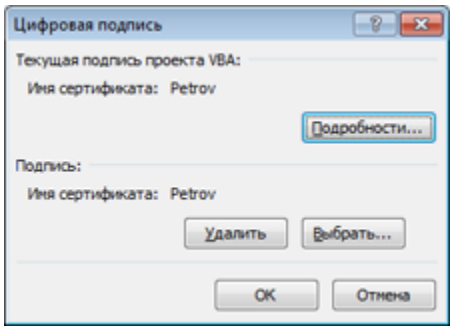


Рисунок 94: Окно «Цифровая подпись»

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** (см. рисунок на стр. 124) будет выведено сообщение о возникшей проблеме. Ненадежный сертификат помечается красным крестом.

Удаление подписи макроса

Чтобы удалить электронную подпись из проекта макроса:

1. В окне редактора Microsoft Visual Basic в меню **Сервис** выберите пункт **Цифровая подпись.** Откроется окно **Цифровая подпись** (см. рисунок на стр. 177).
2. Чтобы удалить электронную подпись, нажмите кнопку **Удалить**. Электронная подпись будет удалена из проекта.

Подписание базы данных Microsoft Access 2007, 2010 или 2013

В приложении Microsoft Access версий 2007, 2010 и 2013 предусмотрена возможность подписания базы данных при публикации. После создания файла базы данных в формате Microsoft Access 2007, 2010 или 2013 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.

Примечание. Базы данных более ранних версий, чем Microsoft Access 2007, невозможно заверить электронной подписью, однако в этом случае вы можете подписать отдельные компоненты базы данных. Подробнее см. в главе Подписание макросов (см. «Электронная подпись макросов и баз данных» на стр. 175).

Чтобы упаковать и подписать базу данных Microsoft Access:

1. В зависимости от версии программы выполните одно из действий:

   - В программе Microsoft Access 2007 нажмите кнопку **Microsoft Office**  , выберите пункт **Опубликовать**, а затем нажмите **Упаковать и подписать.**
   - 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 **OK**. 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

Работа с универсальной электронной картой

Общие сведения об универсальной электронной карте

Универсальная электронная карта (УЭК) — это ключ доступа к широкому спектру электронных услуг и сервисов — государственных, муниципальных и коммерческих (см. «Авторизация на Едином портале государственных и муниципальных услуг Российской Федерации» на стр. 183). УЭК дает возможность получать все государственные и муниципальные услуги, оказываемые в электронной форме согласно законодательству Российской Федерации. 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 (на стр. 234) с квалифицированным сертификатом (см. «Квалифицированный сертификат» на стр. 233), 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. «Электронная подпись» на стр. 236), 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 предварительно настроить программу (см. «Настройка ViPNet CSP для работы с универсальной электронной картой (УЭК)» на стр. 106).

Авторизация на Едином портале государственных и муниципальных услуг Российской Федерации

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/idp/Authn/CommonLogin).
2. Выберите способ авторизации **Через криптопровайдер/УЭК**.
3. Загрузите и установите плагин для работы с порталом государственных услуг.
4. Поместите УЭК в считыватель PC/SC-совместимый считыватель контактных смарт-карт.
5. Нажмите кнопку **Войти**.
6. Введите код PIN2.
7. В окне **Безопасность Windows** выберите нужный квалифицированный сертификат.

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

15

Организация защищенного соединения TLS/SSL

Организация доступа к защищенному веб-серверу

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

1. Для настройки серверной части:
   - Настройте сервер IIS.
   - Установите криптопровайдер ViPNet CSP.
   - Установите в хранилище сертификатов компьютера сертификат пользователя (сервера), сертификат издателя и актуальный список отозванных сертификатов.

   Подробнее см. раздел Настройка серверной части (на стр. 186).
2. Для настройки клиентской части:
   - Установите криптопровайдер ViPNet CSP.
   - Установите в хранилище сертификатов пользователя сертификат пользователя (клиента), сертификат издателя и актуальный список отозванных сертификатов.
   - При необходимости настройте браузер Internet Explorer для работы по протоколу TLS/SSL.

   Подробнее см. раздел Настройка клиентской части (на стр. 187).

Настройка серверной части

Для настройки серверной части:

1. Настройте сервер IIS (см. «Практическое руководство. Создание удаленных веб-узлов IIS» в библиотеке MSDN http://msdn.microsoft.com/ru-ru/library/default.aspx).
2. Установите криптопровайдер ViPNet CSP (см. «Установка и запуск программы» на стр. 32).
3. Создайте запрос на сертификат для сервера (см. «Создание запроса на сертификат и формирование закрытого ключа» на стр. 63) 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 отозванных сертификатов (СОС).

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. 77).
6. Установите в хранилище сертификатов локального компьютера сертификат сервера (см. «Установка сертификата в системное хранилище» на стр. 79), а также сертификат издателя и СОС (см. «Установка сертификатов издателей и СОС» на стр. 84).
7. Проверьте доступность веб-узла по защищенному протоколу HTTPS (см. «Проверка доступности веб-узла по защищенному протоколу HTTPS» на стр. 189).

Настройка клиентской части

Для настройки клиентской части:

1. Установите программу ViPNet CSP (см. «Установка и запуск программы» на стр. 32).
2. Создайте запрос на сертификат пользователя для веб-клиента (см. «Создание запроса на сертификат и формирование закрытого ключа» на стр. 63) 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 отозванных сертификатов (СОС).

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. 77).
5. Установите в хранилище сертификатов текущего пользователя сертификат для веб-клиента (см. «Установка сертификата в системное хранилище» на стр. 79), а также сертификат издателя и СОС (см. «Установка сертификатов издателей и СОС» на стр. 84).
6. Выполните настройку обозревателя Internet Explorer для работы по защищенному протоколу.
7. Проверьте доступность веб-узла по защищенному протоколу HTTPS (см. «Проверка доступности веб-узла по защищенному протоколу HTTPS» на стр. 189).

Настройка веб-браузеров Internet Explorer, Google Chrome и Яндекс.Браузер для работы по протоколу TLS/SSL

Настройки браузеров по умолчанию позволяют работать по протоколу TLS/SSL. Если настройки браузера отличны от первоначальных или соединение с сервером не происходит:

1. Откройте окно **Свойства обозревателя** (**Свойства: Интернет**). Для этого:
   - В меню **Сервис** браузера Internet Explorer выберите пункт **Свойства обозревателя**.
   - В окне настроек браузера Google Chrome или Яндекс.Браузер нажмите кнопку **Изменить настройки прокси-сервера**.
2. Откройте вкладку **Дополнительно**.
3. Установите флажки **SSL 3.0**, **TLS 1.0**.
4. Снимите флажок **SSL 2.0**.
5. Проверьте доступность веб-узла по защищенному протоколу HTTPS (см. «Проверка доступности веб-узла по защищенному протоколу HTTPS» на стр. 189).

Примечание. Для корректной работы по протоколу TLS/SSL в браузерах Google Chrome и Яндекс.Браузер в свойствах ярлыка браузера в поле **Объект** необходимо после пути к программе добавить команду `--use-system-ssl`.

Проверка доступности веб-узла по защищенному протоколу HTTPS

Для доступа к веб-узлу по протоколу HTTPS:

1. В адресной строке обозревателя Internet Explorer наберите: `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 Проблемы и неисправности (на стр. 190).

16

Проблемы и неисправности

Проверка целостности модулей программы

Для контроля наличия необходимых библиотек:

1 В окне программы ViPNet CSP на панели навигации выберите раздел **Состав**.

2 В таблице **Исполняемые модули** проверьте состав библиотек.

Для проверки целостности библиотек:

1 В окне программы ViPNet CSP на панели навигации выберите раздел **Состав**.

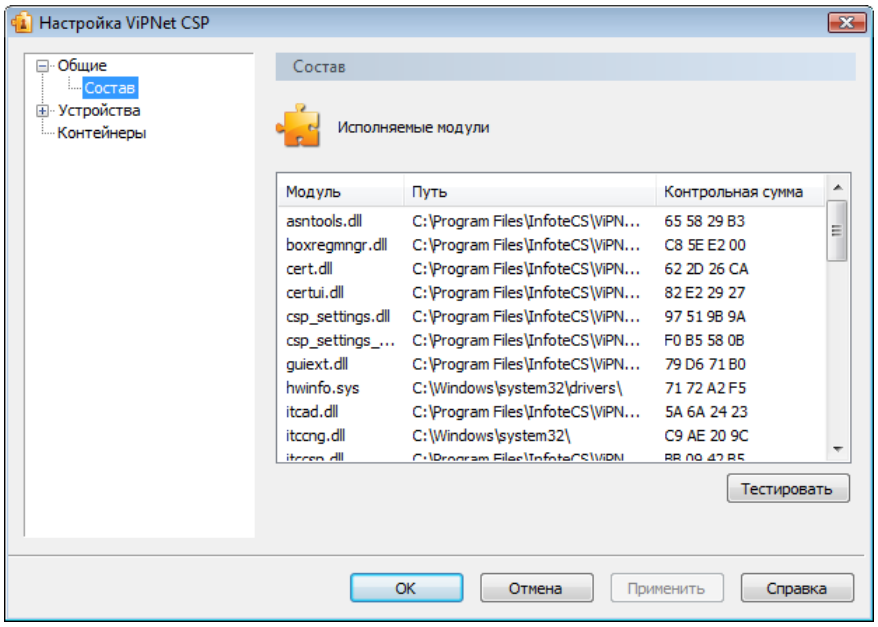


Рисунок 95: Панель «Состав»

2 Нажмите кнопку **Тестировать**.

При этом произойдет пересчет контрольных сумм и проверка их соответствия суммам, указанным в каждом из модулей.

По окончании проверки отобразится окно с сообщением о результатах проверки.

Не удается запустить программу

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

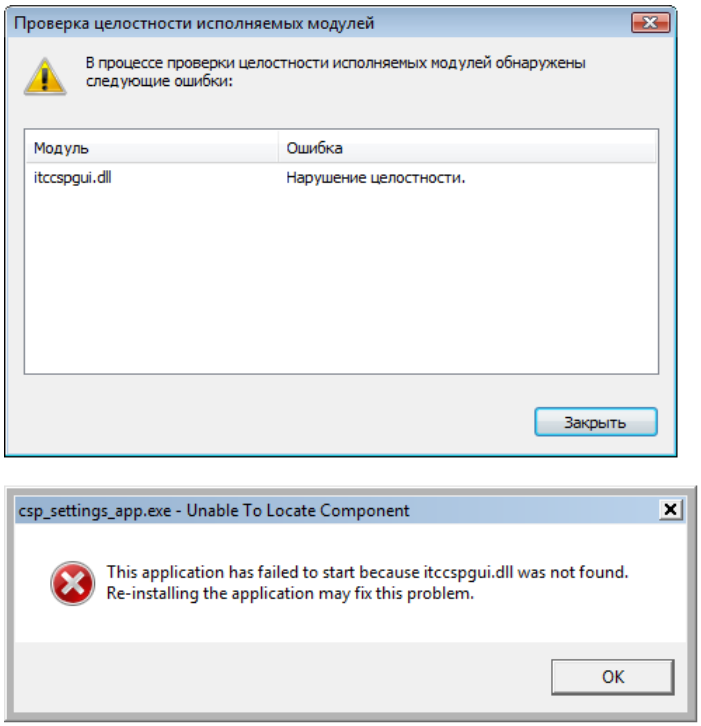


Рисунок 96: Сообщения об ошибках при запуске ViPNet CSP

Чтобы восстановить работоспособность ViPNet CSP, снова установите программу «поверх» уже установленной копии ViPNet CSP (не удаляя ее):

1. Запустите установочный файл `Setup.exe`  .
2. В окне **Установка ViPNet CSP** с помощью переключателя выберите **Обновить**, затем нажмите кнопку **Продолжить**. Начнется обновление компонентов программы.

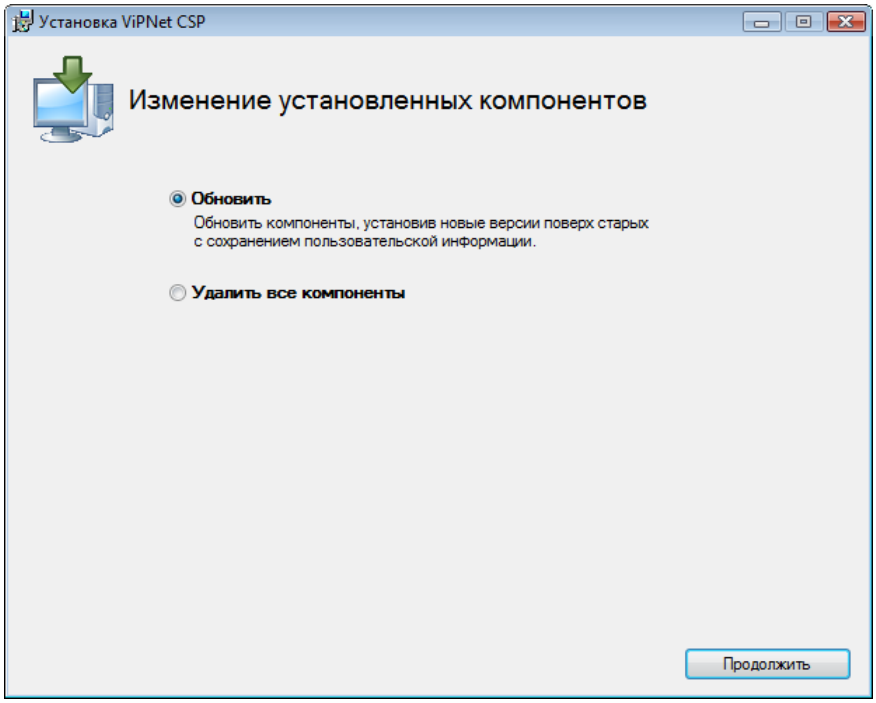


Рисунок 97: Обновление ViPNet CSP

3 По завершении обновления программа предложит перезагрузить компьютер. В окне сообщения о перезагрузке нажмите кнопку **Да.**

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

Конфликт ViPNet CSP с другими программами

Из-за специфики работы программного обеспечения ViPNet может быть нарушена работа сторонних приложений.

Для устранения конфликта ПО ViPNet со сторонними приложениями внесите изменения в системный реестр Windows:

1. В меню **Пуск** выберите пункт **Выполнить**.
2. В окне **Выполнить** в поле **Открыть** введите `regedit` и нажмите кнопку **OK**. Откроется окно **Редактор реестра**.

Внимание! Неправильное редактирование реестра может привести к возникновению неполадок в работе операционной системы, поэтому обязательно создайте резервную копию реестра. Это позволит восстановить реестр при возникновении неполадок.

3. В разделе реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Infotecs\PatchEngine` присвойте параметру `Flags` значение 0.
4. Перезагрузите компьютер.

   Если после выполнения указанных действий проблема не будет решена, обратитесь в службу технической поддержки компании «ИнфоТеКС» (см. «Обратная связь» на стр. 18).

Если ViPNet CSP конфликтует с криптопровайдерами других разработчиков, можно отключить поддержку работы ViPNet CSP через интерфейс Microsoft CryptoAPI.

Внимание! После отключения поддержки интерфейса Microsoft CryptoAPI невозможно будет использовать криптографические функции ViPNet CSP в Microsoft Office и других приложениях, использующих этот интерфейс. Однако сохранится возможность использовать ViPNet CSP в различных приложениях ViPNet.

Чтобы отключить поддержку интерфейса Microsoft CryptoAPI, в разделе **Общие** (см. рисунок на стр. 39) снимите флажок **Включить поддержку работы ViPNet CSP через MS Crypto API**. Изменения полностью вступят в силу после перезагрузки компьютера.

Не удается использовать электронный замок «Аккорд-АМДЗ»

Если на компьютере установлен электронный замок «Аккорд-АМДЗ», но его не удается использовать в программе ViPNet CSP в качестве датчика случайных чисел:

1. Убедитесь, что на компьютере установлены драйверы электронного замка «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. 104).

При использовании устройства типа eToken Aladdin происходит зависание компьютера

Если вы используете устройство типа eToken Aladdin, и при формировании запроса на сертификат ваш компьютер зависает, убедитесь, что установлено программное обеспечение eToken PKI Client 5.1 или более поздних версий.

Ошибка проверки сертификата

Если при установке сертификата пользователя появляется системное сообщение о невозможности проверить сертификат, это означает, что в системе не установлены сертификат издателя и список отозванных сертификатов (см. «Установка сертификатов издателей и СОС» на стр. 84).

Не удается зашифровать документ

Адрес электронной почты из сертификата не найден в списке адресов контакта

При импорте сертификата в карточку контакта может появиться сообщение:

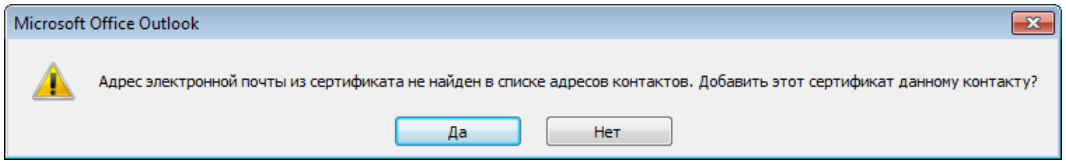


Рисунок 98: Ошибка импорта сертификата

Это означает, что сертификат не содержит адрес электронной почты, который бы соответствовал адресу данного контакта. Поэтому зашифровать сообщение на этом сертификате для получателя не удастся.

Возможны следующие причины появления проблемы:

- Сертификат не принадлежит данному контакту:
  - Откройте окно **Сертификат**, дважды щелкнув файл сертификата на диске.
  - На вкладке **Общие** удостоверьтесь, что сертификат принадлежит данному получателю. Если это не так, укажите для импорта нужный сертификат.

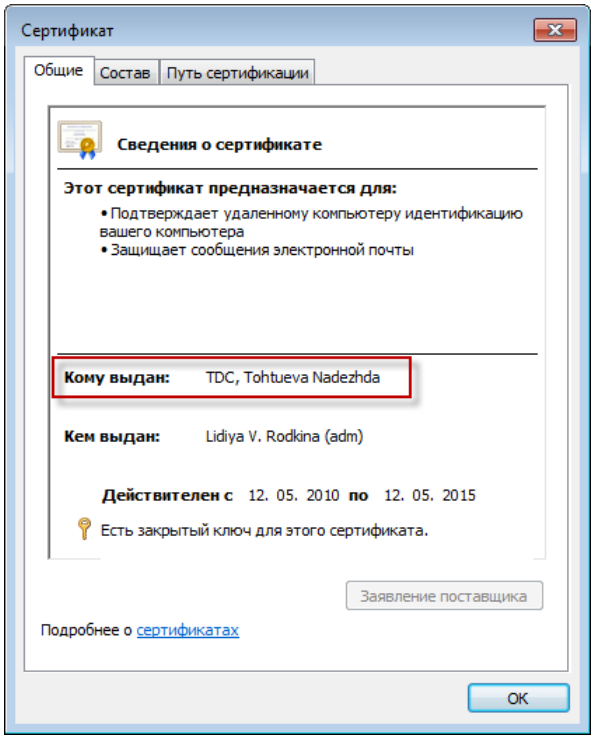


Рисунок 99: Проверка владельца сертификата

- В сертификате не прописан адрес электронной почты данного контакта:
  - 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.

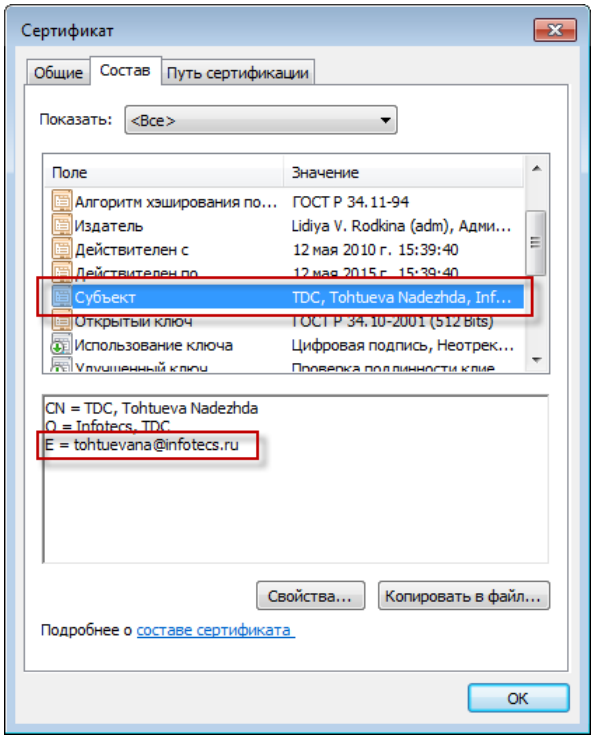


Рисунок 100: Проверка адреса электронной почты в сертификате

- Если это не так, запросите новый сертификат:
  - у получателя, в случае если вы импортировали сертификат контакта.
  - у администратора вашего удостоверяющего центра, если вы добавляли в систему свой сертификат.

Недопустимый сертификат

При отправке зашифрованного сообщения может появиться предупреждение:

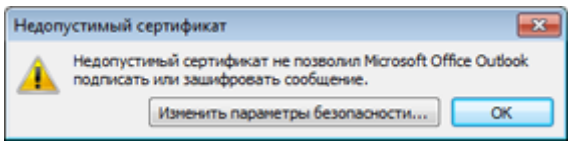


Рисунок 101: Предупреждение о недопустимом сертификате в Outlook 2003

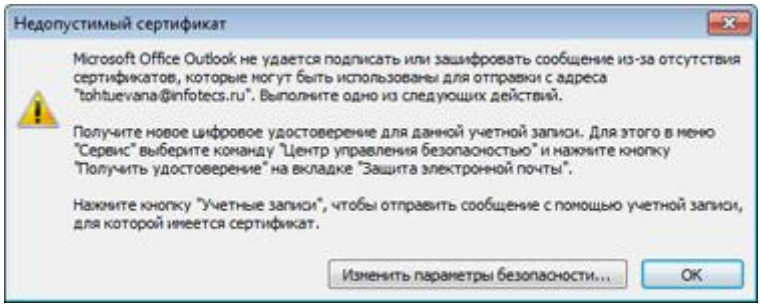


Рисунок 102: Предупреждение о недопустимом сертификате в Outlook 2007

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. 199).
- Ваш сертификат не содержит адреса вашей электронной почты (см. «Адрес электронной почты из сертификата не найден в списке адресов контакта» на стр. 199).
- 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. 142).
- В системное хранилище не был установлен сертификат издателя (см. «Установка сертификатов издателей и СОС» на стр. 84).

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. 95).

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 на вкладке **Контейнеры**.

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:

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.

Не удается подписать макрос или базу данных Microsoft Access 2007

Если при попытке подписать макрос или создать подписанный пакет Microsoft Access 2007 в окне выбора сертификата электронной подписи нет доступных сертификатов, это значит, что вы не можете подписывать код. Обратитесь в удостоверяющий центр за сертификатом, который имеет атрибут «Подписывание кода» в расширенном использовании ключа.

Не удается подписать видимую строку подписи в Microsoft Word 2003 или Excel 2003

Приложения Microsoft Word и Excel более ранних версий, чем Microsoft Office 2007, не позволяют подписывать видимые строки подписи. Чтобы подписать строку подписи, откройте документ с помощью приложения Microsoft Office 2007.

Невозможно редактировать подписанный документ Microsoft Word или Excel

Чтобы внести изменения в подписанный документ Microsoft Word или Excel, удалите электронною подпись (см. «Удаление электронной подписи в Microsoft Word, Excel и PowerPoint» на стр. 129) 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 HTTPS

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.

Не установлены сертификаты пользователя, издателя, СОС в нужное хранилище

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

Чтобы просмотреть сертификаты, установленные в хранилище:

1. Откройте консоль MMC. Для этого:
   - 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 **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 СОС должны быть установлены в нужное хранилище, и при их открытии не должно возникать ошибок.

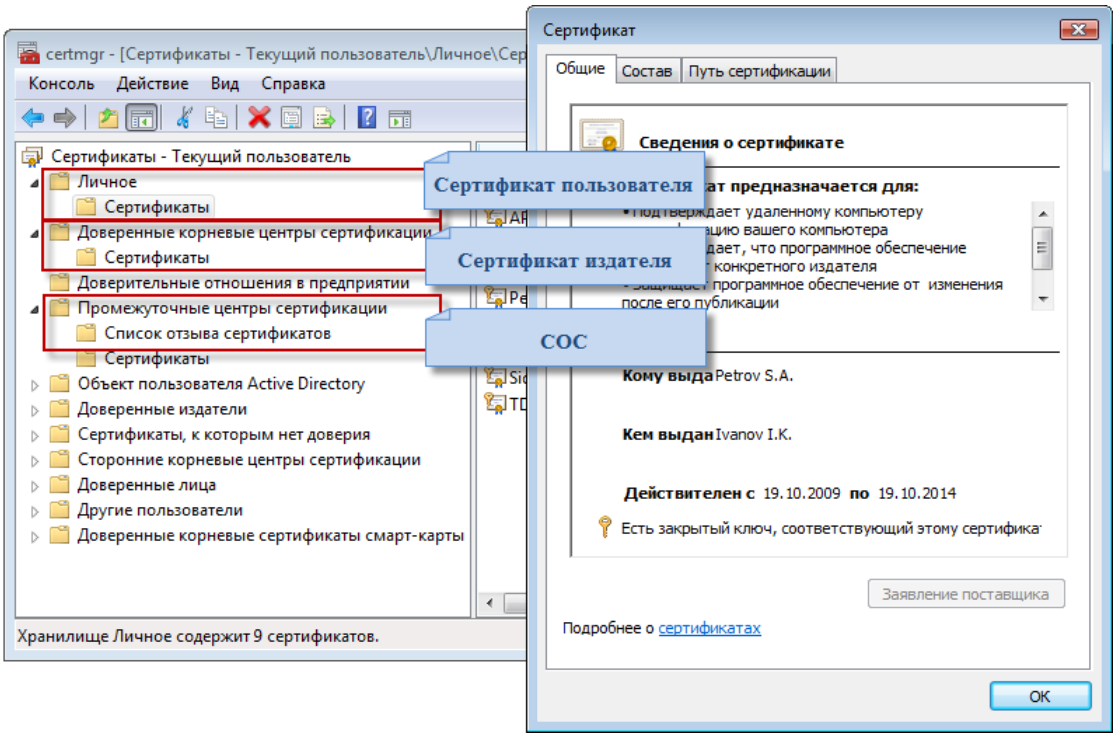


Рисунок 103: Сертификат веб-клиента в хранилище сертификатов текущего пользователя

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

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

Для веб-клиента в оснастке MMC сертификатов текущего пользователя должны присутствовать сертификаты:

- Раздел **Личные > Сертификаты** — сертификат пользователя (веб-клиента).

- Раздел **Доверенные корневые центры сертификации > Сертификаты** — сертификат издателя.
- Раздел **Промежуточные центры сертификации > Список отзыва сертификатов** — СОС.

Если сертификат не установлен или установлен некорректно, выполните установку сертификата в хранилище (см. «Установка сертификатов издателей и СОС» на стр. 84).

Веб-браузер не настроен на работу по протоколу TLS

По умолчанию настройки веб-браузера Internet Explorer позволяют работать по защищенному протоколу TLS. Если соединения с сервером не происходит, проверьте наличие в браузере нужного сертификата и убедитесь, что в свойствах обозревателя разрешено использование протоколов TLS/SSL.

Для проверки наличия сертификата:

1. В меню **Сервис** веб-браузера Internet Explorer выберите пункт **Свойства обозревателя**.
2. В окне **Свойства обозревателя** 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 на стр. 208). Если такой атрибут отсутствует, обратитесь в удостоверяющий центр за сертификатом, в котором будет указан данный параметр (см. «ViPNet Удостоверяющий и ключевой центр. Руководство администратора»).

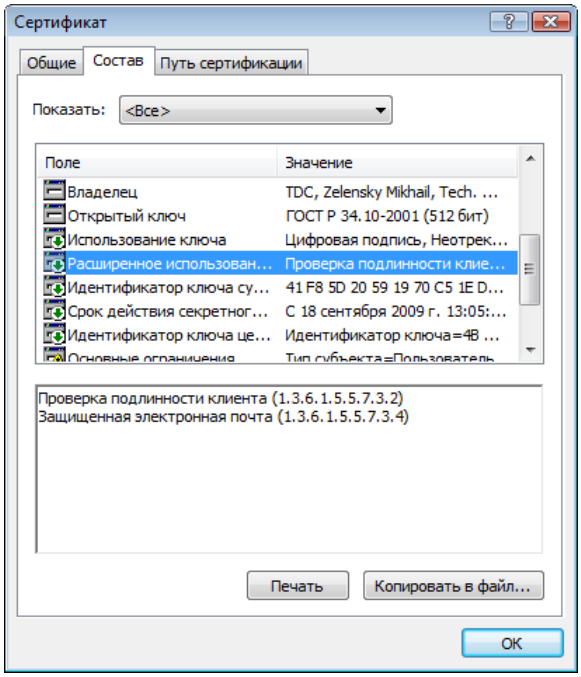


Рисунок 104: Состав сертификата веб-клиента

Для проверки активности протоколов TLS/SSL:

1. В меню **Сервис** веб-браузера Internet Explorer выберите пункт **Свойства обозревателя**.
2. В диалоговом окне **Свойства обозревателя** откройте вкладку **Дополнительно**.
3. Убедитесь, что флажки **SSL 3.0**, **TLS 1.0** установлены, а флажок **SSL 2.0** снят.
4. Проверьте подключение к веб-серверу.

Требуется перезапуск службы сервера IIS

В некоторых случаях для доступа к серверу по вновь настроенному протоколу TLS необходимо перезапустить службу сервера. Для этого:

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

В некоторых случаях для доступа к серверу требуется сохранить пароль к контейнеру ключей. Для этого:

1. В оснастке консоли MMC откройте нужный сертификат.
2. На вкладке **Состав** окна **Сертификат** нажмите кнопку **Копировать в файл**.
3. На странице приветствия **Мастера экспорта сертификатов** нажмите кнопку **Далее**.
4. В окне ввода пароля к контейнеру ключей введите пароль пользователя серверной части, установите флажки **Сохранить пароль** и **Не показывать больше это окно**.
5. Нажмите кнопку **OK**. Теперь работу мастера можно завершить — пароль сохранен.

При соединении с сервером выводится предупреждение системы безопасности

Если при попытке соединения с сервером обозреватель выводит предупреждение системы безопасности **Указанное в сертификате название неправильно или не совпадает с названием узла**, проверьте, что название домена сервера и имя пользователя, на которое выдан сертификат сервера, совпадают.

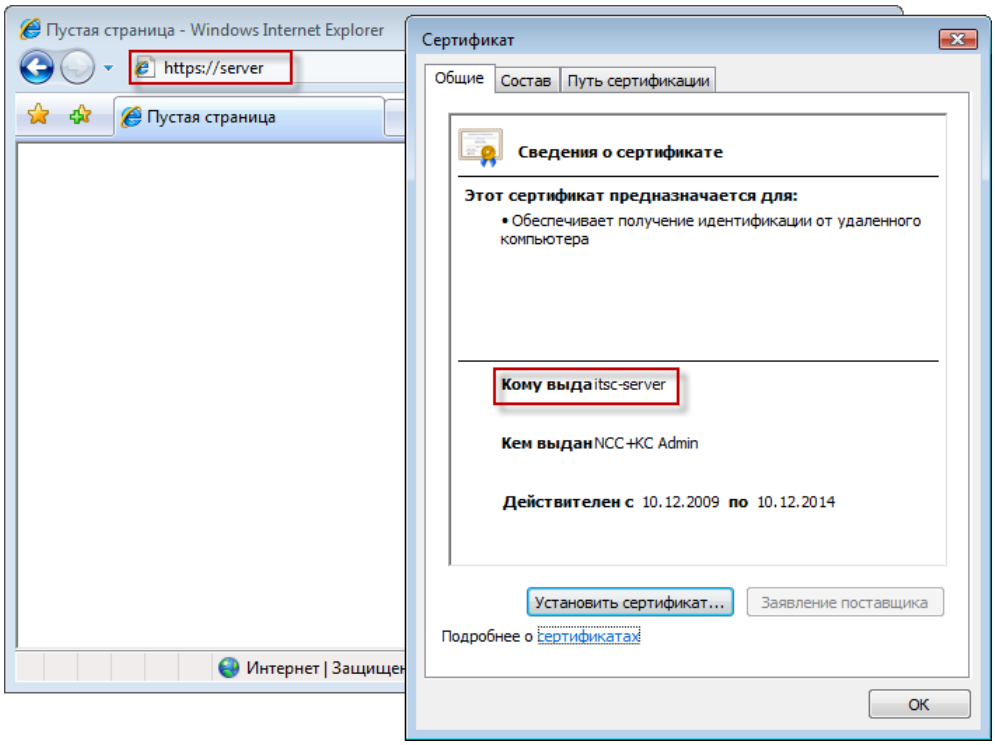


Рисунок 105: Предупреждение системы безопасности о несовпадении имен

Предоставление дополнительной информации о неисправности

Для устранения неисправности сотрудник технической поддержки ОАО «ИнфоТеКС» может попросить вас предоставить дополнительную информацию для анализа. В этом случае:

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 папку `Logs`, которая находится по следующему адресу:

   - 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 `dbg_level` на `0xff (255)`.

5. Перезагрузите компьютер.

   Примечание. В некоторых случаях запуск компьютера может занять продолжительное время.

6. Скачайте программу DebugView http://technet.microsoft.com/ru-ru/sysinternals/bb896647.aspx.

7. Запустите файл `DbgView.exe` от имени администратора.

8. Повторите действия, при которых у вас возникала неисправность.

9. В программе DebugView выделите все записи и скопируйте в текстовый файл.

10. Добавьте получившийся текстовый файл в архив и отправьте вместе с описанием неисправности в службу технической поддержки.

Примечание. Если для воспроизведения ошибки необходимо стороннее ПО, укажите это в письме.

11 Присвойте ключу `dbg_level` (см. пункт 4) значение 0.

12 Перезагрузите компьютер.

История версий

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

Версия 3.2.10

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.2.10.

- **Шаблон запроса на квалифицированный сертификат**

  В программе создания запроса на сертификат появился шаблон, с помощью которого можно создать запрос для получения квалифицированного сертификата (см. «Квалифицированный сертификат» на стр. 233).

- **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 генерации закрытого ключа. Также для инициализации датчика случайных чисел можно использовать предварительно сгенерированную 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.

- **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

Улучшена внутренняя функциональность программы, исправлены недочеты.

Версия 3.2.2

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

- **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. «Контейнер ключей» на стр. 234), которые вы можете использовать для аутентификации, формирования электронной подписи (см. «Электронная подпись» на стр. 236) 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 внешнего устройства в таблице приведено описание, условия и особенности работы с устройством, 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 открытого ключа), разработанных компанией RSA Laboratories. Стандарт определяет независимый от платформы интерфейс API для работы с криптографическими устройствами идентификации и хранения данных.

Таблица 5. Поддерживаемые внешние устройства

Название устройства в программе ViPNet CSP	Полное название и тип устройства	Необходимые условия работы с устройством	Поддержка стандарта PKCS#11
UEC	**Универсальная электронная карта**	На компьютере необходимо указать расположение сертификатов и контейнера ключей, полученных в пункте выдачи карт (см. «Настройка ViPNet CSP для работы с универсальной электронной картой (УЭК)» на стр. 106).	Да
ESMART CryptoToken 64K	Смарт-карты **ESMART CryptoToken 64K**	На компьютере должно быть установлено программное обеспечение ESMART PKI Client.	Да
Infotecs Software Token	**Infotecs Software Token** — программная реализация стандарта PKCS#11	Входит в поставку программы ViPNet CSP.	Да
A-Key S1000	Смарт-карта **AkToken** производства компании Ak Kamal Security	На компьютере должны быть установлены драйверы, предоставленные компанией Ak Kamal Security. Перенос ключей подписи на данный тип устройств невозможен.	Да
Magistra	Смарт-карты **Магистра** производства компании «СмартПарк»	Устройство не поддерживает ГОСТ 34.10-2012; создание ключей по этому алгоритму невозможно, перенос ключей, созданных по этому алгоритму, на данный тип устройств невозможен.	Да
ViPNet HSM	Виртуальный токен **ViPNet HSM** производства компании «ИнфоТеКС»	Необходимо установить клиентское приложение ViPNet HSM и проинициализировать виртуальный токен.	Да

KAZTOKEN	**KAZTOKEN**, электронный идентификатор производства компании «Цифровой поток»	На компьютере должны быть установлены драйверы ktDrivers.x64.v.2.73.00.04.08 (для 64-разрядной ОС) или ktDrivers.x86.v.2.73.00.04.08. Перенос ключей подписи на данный тип устройств невозможен.	Да
JaCarta	Персональные электронные ключи **JaCarta Laser** производства компании «Аладдин Р.Д.»	На компьютере должно быть установлено программное обеспечение JC-Client компании «Аладдин Р.Д.».	Да
JCDS	Смарт-карты **Gemalto Optelio Contactless D72**, **KONA 131 72K** с апплетом от компании «Аладдин Р.Д.»	На карту должен быть загружен апплет, позволяющий модулю jcpkcs11ds.dll компании «Аладдин Р.Д.» работать с картой.	Да
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 или более поздних версий.	Да
eToken GOST	Персональные электронные ключи **eToken ГОСТ** и **JaCarta ГОСТ** производства компании «Аладдин Р.Д.»	Создание ключей подписи возможно только по ГОСТ 34.10-2001, ГОСТ 34.10-2012 не поддерживается; перенос ключей подписи на данный тип устройств невозможен.	Да

Rutoken ECP/Rutoken Lite	**Рутокен ЭЦП**, **Рутокен Lite** — электронные идентификаторы производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken версии 2.89.00.0491. В программе ViPNet CSP настоятельно рекомендуется отключить поддержку устройств Рутокен. Создание ключей подписи возможно только по ГОСТ 34.10-2001, ГОСТ 34.10-2012 не поддерживается; перенос ключей подписи на данный тип устройств невозможен.	Да
Rutoken/ Rutoken S	**Рутокен**, **Рутокен S** — электронные идентификаторы производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken версии 2.89.00.0491. Постоянная корректная работа ПО ViPNet при использовании устройств Рутокен с драйверами указанной версии не гарантирована. Для гарантированной корректной работы ПО ViPNet рекомендуется использовать устройства другого типа.	Да
Shipka	ПСКЗИ **ШИПКА** (любой версии) производства компании «ОКБ САПР»	На компьютере должно быть установлено программное обеспечение ACShipka Environment версии не ниже 3.3.2.7. Проведите инициализацию устройства с помощью утилиты производителя «Параметры авторизации».	Да
eToken Aladdin	Персональные электронные ключи **eToken PRO (Java)**, **eToken PRO**, смарт-карты **eToken PRO (Java)**, **eToken PRO** производства компании «Аладдин Р.Д.»	На компьютере должно быть установлено программное обеспечение PKI Client версии 5.1 и выше. Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC совместимым USB-устройством считывания с карт.	Да

Примечание. Список поддерживаемых операционных систем для каждого из приведенных устройств вы найдете на официальном веб-сайте производителя этого устройства.

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, Server 2012

Для установки поддержки кириллицы на ОС Windows 8, Server 2012:

1. Откройте **Панель управления** (**Control Panel**) > **Региональные стандарты** (**Region**).
2. В окне **Регион** (**Region**) перейдите на вкладку **Дополнительно** (**Administrative**).

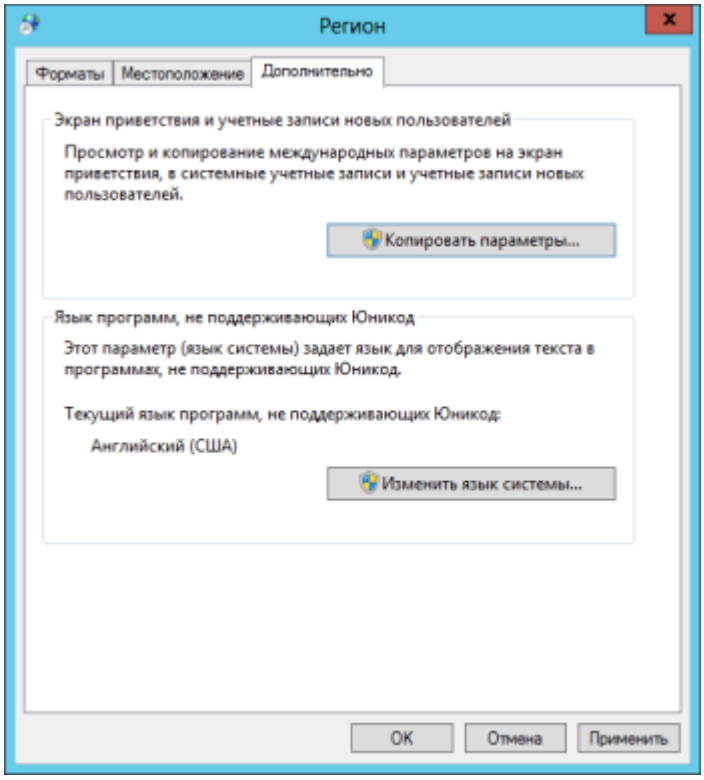


Рисунок 106: Дополнительные языковые параметры

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

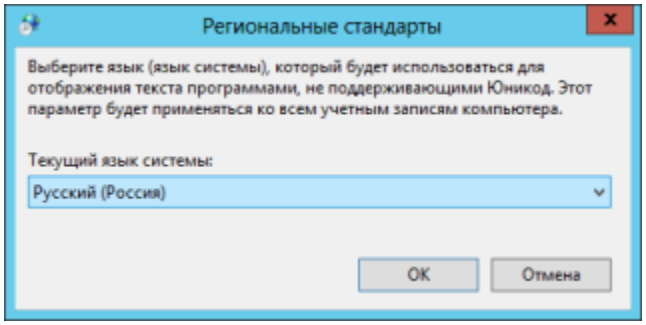


Рисунок 107: Выбор языка системы

5 Нажмите кнопку **OK**. Потребуется перезагрузка.

6 После перезагрузки 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 установите флажок **Экран приветствия и системные учетные записи** (**Welcome screen and system accounts**) и нажмите кнопку **OK**.

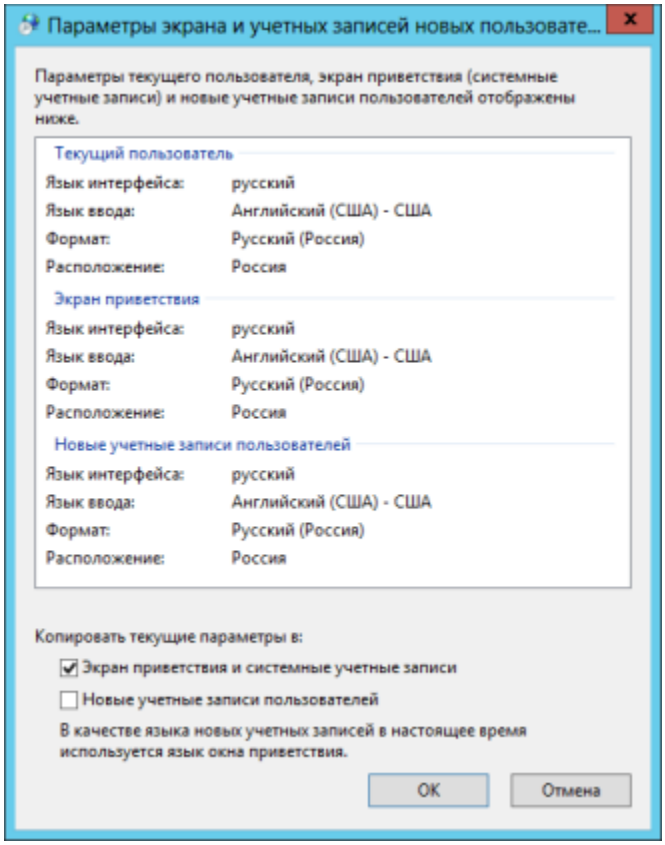


Рисунок 108: Копирование параметров

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))**.

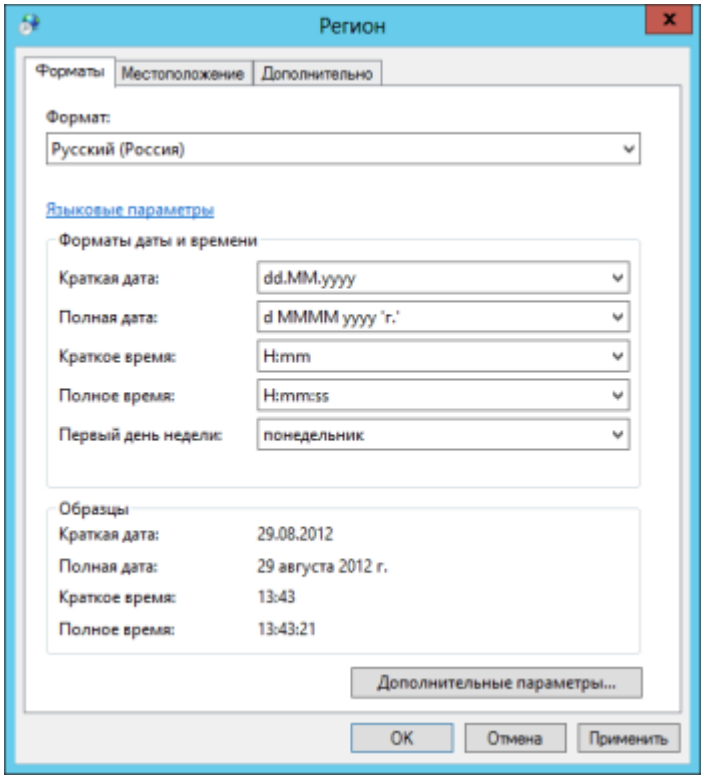


Рисунок 109: Настройка форматов

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

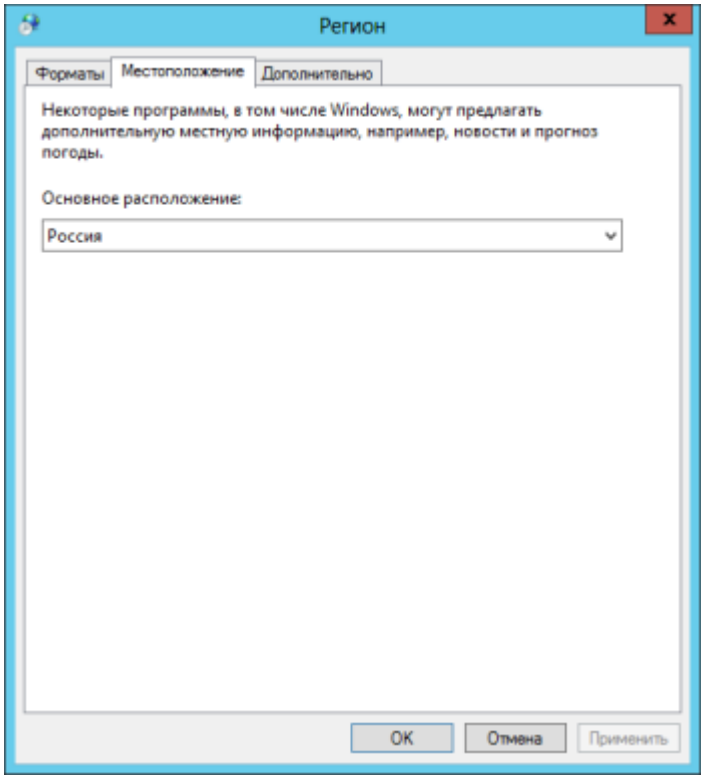


Рисунок 110: Выбор текущего расположения

Региональные настройки в ОС Windows Vista, Server 2008, Windows 7, Server 2008 R2

Для установки поддержки кириллицы на ОС Windows Vista, Server 2008, Windows 7, Server 2008 R2:

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**).

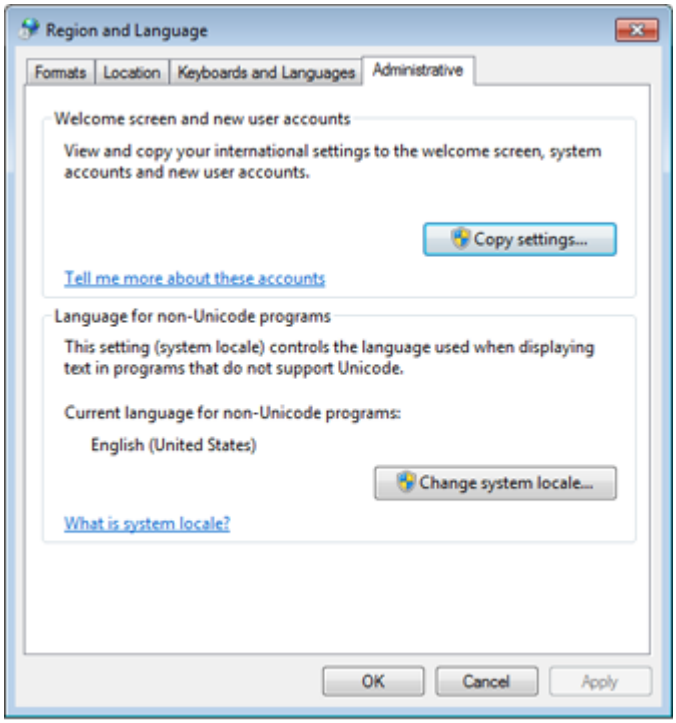


Рисунок 111: Дополнительные языковые параметры

3. На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Изменить язык системы** (**Change system locale**).

4 В появившемся окне в списке выберите **Русский (Россия)** (**Russian (Russia)**).

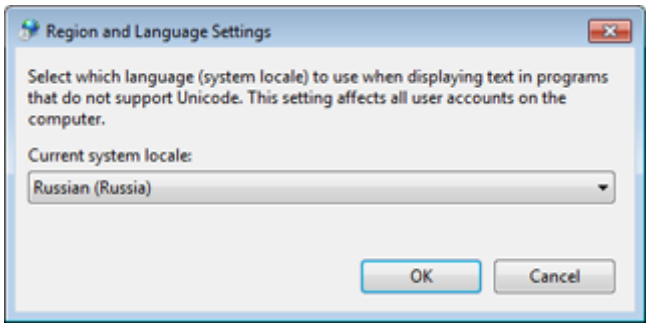


Рисунок 112: Выбор языка системы

5 Нажмите кнопку **OK**. Потребуется перезагрузка.

6 После перезагрузки 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**.

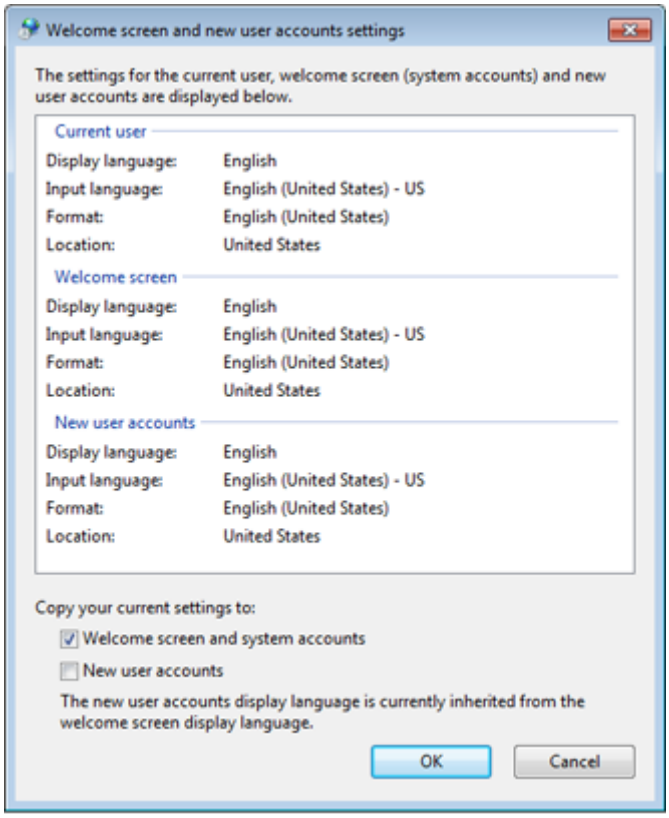


Рисунок 113: Копирование параметров

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)**).

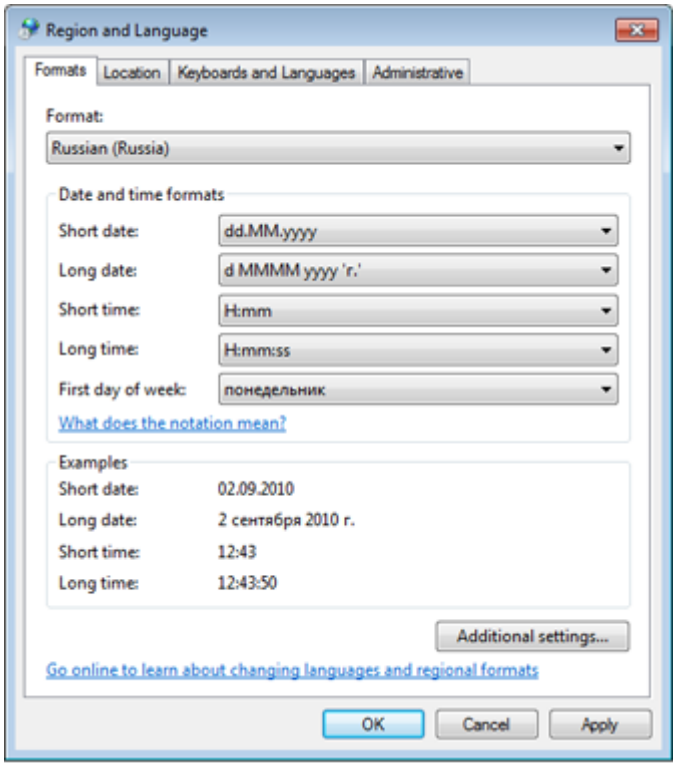


Рисунок 114: Настройка форматов

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

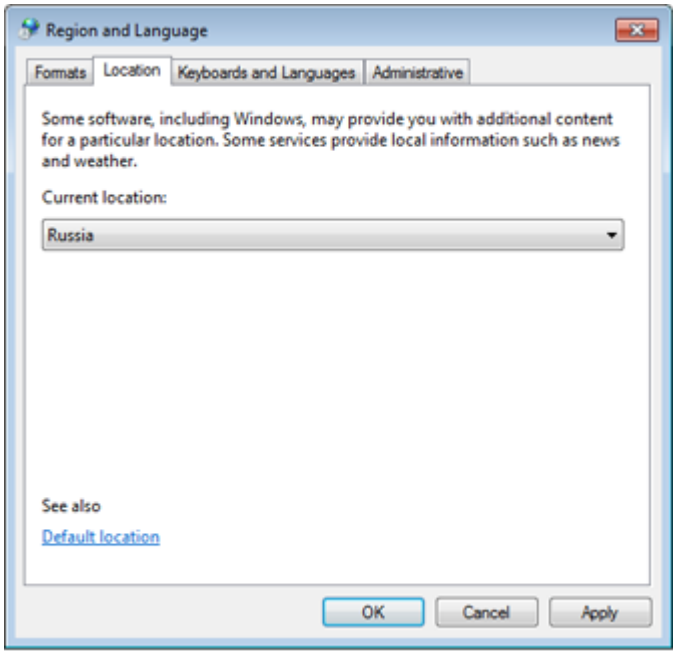


Рисунок 115: Выбор текущего расположения

Региональные настройки в ОС Windows XP, Server 2003

Для установки поддержки кириллицы на ОС Windows XP, Server 2003:

1. Откройте **Панель управления** (**Control Panel**).
2. Щелкните **Язык и региональные стандарты** (**Regional and Language Options**).
3. В окне **Язык и региональные стандарты** (**Regional and Language Options**) перейдите на вкладку **Дополнительно** (**Advanced**).
4. Далее в списке выберите **Русский** (**Russian**).
5. Установите флажок **Применить эти параметры для текущей учетной записи и для стандартного профиля пользователя** (**Apply all settings to the current user account and to the default user profile**).

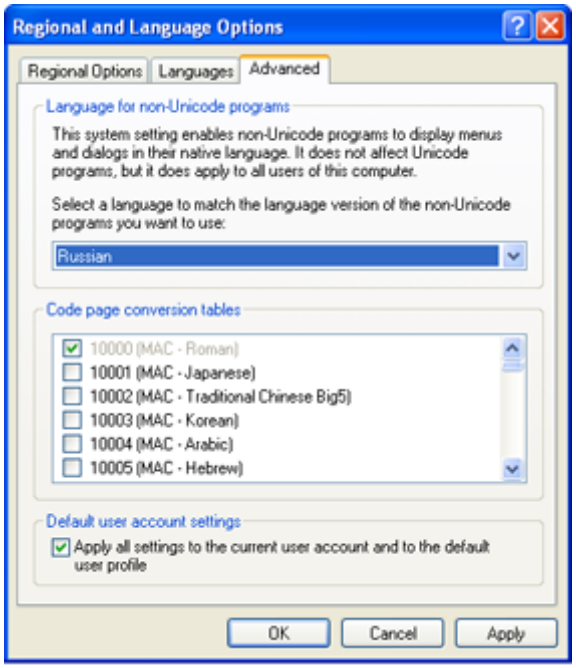


Рисунок 116: Выбор языка для программ, не поддерживающих Юникод, в Windows XP

6. Нажмите кнопку **OK**. Возможно, потребуется перезагрузка.

Глоссарий

P

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 распределенных системах через создание сертификатов открытых ключей и поддержание их жизненного цикла.

См. также: Открытый ключ (на стр. 234).

S

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).

А

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.

См. также: Закрытый ключ (на стр. 233), Открытый ключ (на стр. 234), Симметричное шифрование.

Д

Доверенное лицо (администратор) удостоверяющего центра

Лицо, обладающее правом издавать сертификаты от имени удостоверяющего центра.

См. также: Удостоверяющий центр (на стр. 235).

З

Закрытый ключ

Закрытая (секретная) часть пары асимметричных ключей. Служит для создания электронных подписей, которые можно проверять с помощью парного ему открытого ключа, или для расшифрования сообщений, которые были зашифрованы парным ему открытым ключом.

Ключ электронной подписи (см. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи») является закрытым ключом.

См. также: Асимметричное шифрование (на стр. 232), Открытый ключ (на стр. 234), Электронная подпись (на стр. 236).

Запрос на сертификат

Защищенное электронной подписью сообщение, содержащее имя пользователя, открытый ключ 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).

См. также: Закрытый ключ (на стр. 233), Открытый ключ (на стр. 234), Сертификат открытого ключа подписи пользователя (на стр. 235), Электронная подпись (на стр. 236).

К

Квалифицированный сертификат

Сертификат открытого ключа подписи пользователя, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

См. также: Аккредитованный удостоверяющий центр, Сертификат открытого ключа подписи пользователя (на стр. 235), Электронная подпись (на стр. 236).

Контейнер ключей

Файл, в котором хранятся закрытый ключ и соответствующий ему сертификат открытого ключа.

См. также: Закрытый ключ (на стр. 233), Сертификат открытого ключа подписи пользователя (на стр. 235).

Корневой сертификат

Самоподписанный 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.

См. также: Сертификат издателя (на стр. 234), Сертификат открытого ключа подписи пользователя (на стр. 235), Удостоверяющий центр (на стр. 235).

О

Открытый ключ

Последовательность символов, связанная с закрытым ключом определенным математическим соотношением. Открытый ключ доступен любым пользователям информационной системы и предназначен для подтверждения подлинности электронной подписи (или шифрования).

Ключ проверки электронной подписи (см. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи») является открытым ключом.

См. также: Асимметричное шифрование (на стр. 232), Закрытый ключ (на стр. 233), Электронная подпись (на стр. 236).

С

Сертификат издателя

Сертификат уполномоченного лица удостоверяющего центра, которым заверяются издаваемые сертификаты.

См. также: Сертификат открытого ключа подписи пользователя (на стр. 235).

Сертификат открытого ключа подписи пользователя

Электронный документ определенного формата, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Сертификат содержит информацию о владельце ключа, открытый ключ, сведения о его назначении и области применения, информацию о выпустившем сертификат удостоверяющем центре, период действия сертификата, а также некоторые дополнительные параметры. В программе ViPNet Удостоверяющий и ключевой центр сертификат создается в соответствии со стандартом X.509 v3 и заверяется электронной подписью администратора УКЦ.

В терминологии Федерального закона Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» сертификат открытого ключа подписи пользователя называют «сертификатом ключа проверки электронной подписи».

См. также: Администратор УКЦ, Открытый ключ (на стр. 234), Удостоверяющий центр (на стр. 235), Электронная подпись (на стр. 236), ViPNet Удостоверяющий и ключевой центр (УКЦ).

Список отозванных сертификатов (СОС)

Список сертификатов, которые были отозваны или приостановлены администратором удостоверяющего центра и недействительны на момент, указанный в данном списке отозванных сертификатов.

См. также: Доверенное лицо (администратор) удостоверяющего центра (на стр. 233), Отзыв сертификата, Приостановление действия сертификата.

У

Удостоверяющий центр

В широком смысле, удостоверяющий центр — организация, осуществляющая выпуск сертификатов открытых ключей подписи пользователя, а также сертификатов другого назначения. В сетях ViPNet сертификаты выпускаются в программе ViPNet Удостоверяющий и ключевой центр (УКЦ).

В контексте сети ViPNet, термином «Удостоверяющий центр» также обозначается сетевой узел с установленной программой ViPNet Удостоверяющий и ключевой центр.

См. также: Сертификат открытого ключа подписи пользователя (на стр. 235), Сеть ViPNet, ViPNet Удостоверяющий и ключевой центр (УКЦ).

Э

Электронная подпись

Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата открытого ключа подписи пользователя, а также установить отсутствие искажения информации в электронном документе.

См. также: Закрытый ключ (на стр. 233), Сертификат открытого ключа подписи пользователя (на стр. 235).

Электронная рулетка

Встроенный компонент программного обеспечения ViPNet, который позволяет инициализировать датчик случайных чисел на основе действий пользователя.

Указатель