**5.62 Электронная подпись**

Электронная подпись – реквизит электронного документа, с помощью которого можно удостовериться в неизменности электронного документа с момента его подписи. Для установки подписи необходимо иметь ключ электронной подписи с сертификатом ключа, установленным в него. Ключ можно создать с помощью программы электронной подписи и шифрования. Сертификат ключа электронной подписи можно получить в удостоверяющем центре, например, в удостоверяющем центре фирмы 1С (подробнее см. сайт <http://ca.1c.ru/>). Только удостоверяющий центр может выдать юридически значимый (квалифицированный) сертификат.

Контроль неизменности электронного документа осуществляется в результате проверки соответствия электронной подписи документа его текущему содержанию с помощью ключа проверки электронной подписи, копия которого хранится в сертификате ключа. Если электронная подпись соответствует документу, то это является гарантией того, что документ не был изменен кем-либо с момента его подписания. Контроль неизменности электронного документа можно выполнить в любой момент времени.

Результат и дата проверки электронной подписи для файлов и документов сохраняются в программе, поэтому их можно посмотреть в дальнейшем без обязательного выполнения повторной проверки, для которой требуется программа электронной подписи.

Для электронной подписи и шифрования требуется установить специальную программу электронной подписи и шифрования (криптопровайдер).

Можно выполнять следующие операции:

■ Подписывать объекты программы (например, в документе поля **Наименование** и **Краткое содержание**);

■ Подписывать содержимое хранимых файлов;

■ Шифровать содержимое хранимых файлов.

Объекты программы, для которых доступно подписание и шифрование:

Списки:

■ **Файлы**.

Подписание и шифрование предполагает три этапа:

■ Настройка программы (см. раздел [Настройка программы](https://its.1c.ru/db/content/bsp301doc/src/5.62%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F%20%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C.htm?_=1542292879#_настройка_программы_38));

■ Персональные настройки (см. раздел [Персональные настройки](https://its.1c.ru/db/content/bsp301doc/src/5.62%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F%20%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C.htm?_=1542292879#_заявление));

■ Выполнение операций подписания и шифрования.

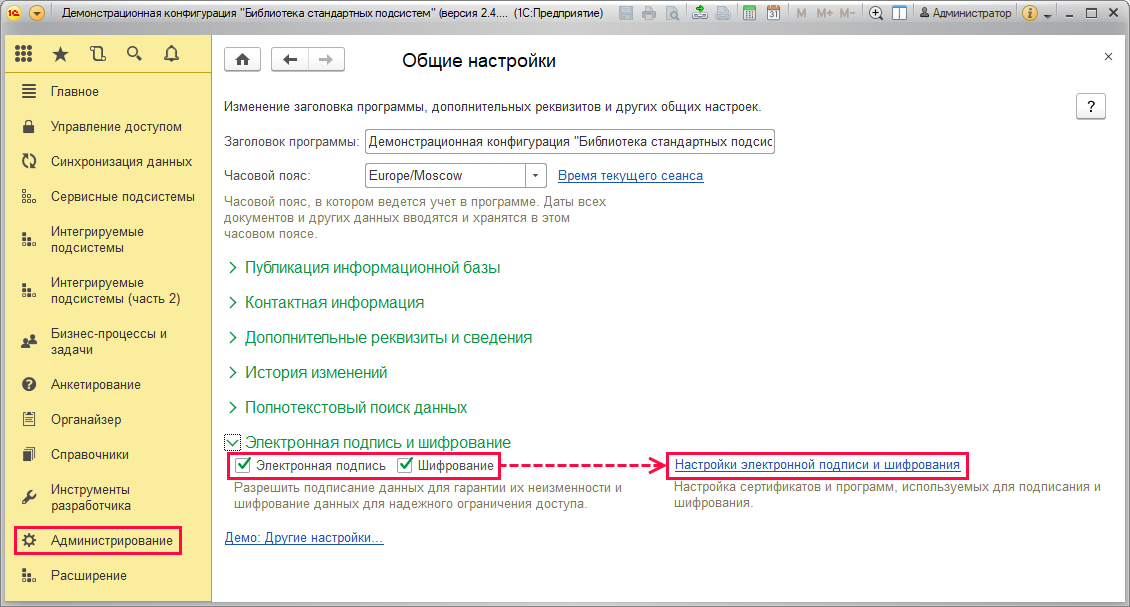
Общая настройка программы производится администратором, персональные настройки выполняются самостоятельно, однако может понадобиться помощь администратора. Для работы с электронной подписью пользователю требуется установить роль Добавление и изменение электронных подписей и шифрование.

**Настройка программы**

Настройка программы для работы с электронной подписью осуществляется вразделе **Администрирование** – Общие настройки – Электронная подпись и шифрование.

Для того чтобы подписывать данные, нужно включить флажок Электронная подпись, а для шифрования нужно включить флажок Шифрование в разделе **Администрирование** – Общие настройки – Электронная подпись и шифрование.

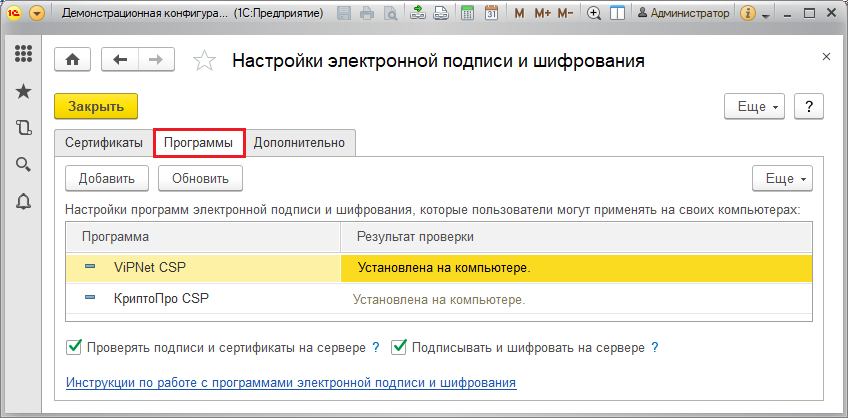
После этого становится доступной ссылка Настройки электронной подписи и шифрования в этом разделе и в персональных настройках программы, с помощью которой можно открыть соответствующий список.



Для создания электронных подписей и шифрования необходимо использовать программу электронной подписи (криптопровайдер).

Вкладка Программы содержит список программ для электронной подписи или шифрования, которые будут использованы в информационной базе (в том числе во всех узлах распределенной ИБ). При первом открытии списка производится поиск программ, установленных на компьютере. Это занимает некоторое время.

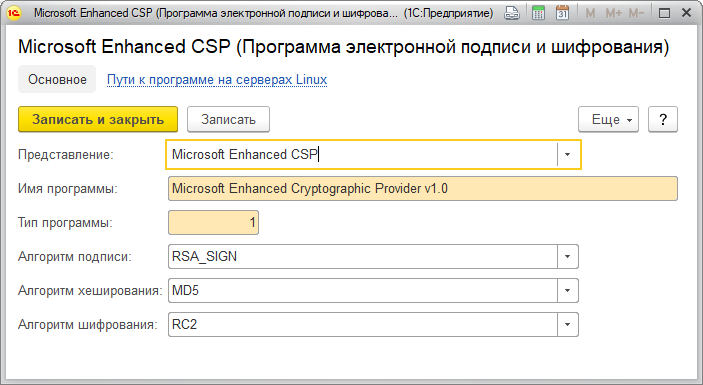
В колонке Программа приводятся представления программ, установленных на компьютере. В колонке Результат проверки отражаются сведения, по которым можно понять, установлена ли программа на компьютере или нет или же установлена, но некорректно.



Для создания юридически значимых электронных подписей необходимо использовать программу, поддерживающую ГОСТ Р 34.10-2001, например, ViPNet CSP или КриптоПро CSP. Эти программы не входят в состав ОС Windows, поэтому их нужно будет установить на компьютеры пользователей вместе с программой 1С:Предприятие. Кроме того, потребуется заключить договор с удостоверяющим центром для получения квалифицированных сертификатов.

Если юридически значимая электронная подпись не нужна (например, для использования электронной подписи только внутри предприятия), то можно использовать любую программу электронной подписи (криптопровайдер), например, Microsoft Enhanced Cryptographic Provider v1.0.

Указанная программа не добавлена в список используемых автоматически, поэтому ее требуется добавить вручную. Для этого нажмите кнопку Добавить.



В поле Представление выберите соответствующее наименование программы с помощью кнопки https://its.1c.ru/db/content/bsp301doc/src/_img/a8ac365292f91872c91b58b5276d597d/image037.png?_=1542292879.

Данные программы заполняются автоматически. Так же просто можно добавить записи о других имеющихся на компьютере программах электронной подписи и шифрования (поставляются готовые настройки для Microsoft Enhanced CSP, ViPNet CSP, КриптоПро CSP, ЛИССИ CSP, Сигнал-КОМ CSP).

Программа Microsoft Enhanced Cryptographic Provider v1.0 входит в состав ОС Windows и ее не нужно устанавливать отдельно. Сертификаты можно получить с помощью контроллера домена Windows Server 2003 или 2008 (с помощью утилиты certmgr.msc, выполнив команду All tasks - Request new certificate, подробное описание утилиты см. в справке к ОС Windows, а так же сайт фирмы Microsoft – [http://technet.microsoft.com/en-us/library/cc754122%28WS.10%29.aspx](http://technet.microsoft.com/en-us/library/cc754122(WS.10).aspx)).

В случае использования распределенной информационной базы рассмотренные выше настройки можно изменить только в главном узле.

В клиент-серверном режиме работы программы, для того чтобы не устанавливать программы электронной подписи на каждом компьютере пользователя, можно использовать сервер 1С:Предприятия или веб-сервер.

На сервер нужно установить используемые программы электронной подписи (лучше выбрать только одну, чтобы избежать конфликтов между ними).

После этого можно включить флажок Проверять электронные подписи и сертификаты на сервере. Если включить флажок Подписывать и шифровать на сервере, то потребуется также установить на сервере секретные ключи пользователей.

Для того чтобы изучить Инструкции по работе с программами электронной подписи и шифрования, перейдите по ссылке в нижней части списка в соответствующий раздел 1С:ИТС, если имеются вопросы.

Внимание! Для использования данной функции необходим договор 1С:ИТС.

Если требуется использовать программу электронной подписи и шифрования (криптопровайдер) отличную от известных, тогда нужно указать ее имя, тип и алгоритмы, как указано в инструкции, поставляемой ее производителем.

Для этого нажмите кнопку Добавить, в поле Представление с помощью кнопки https://its.1c.ru/db/content/bsp301doc/src/_img/a8ac365292f91872c91b58b5276d597d/image037.png?_=1542292879 Выбрать из списка укажите значение Другая программа и заполните вручную ее характеристики:

■ Представление – краткое наименование, которое будет использоваться в программе;

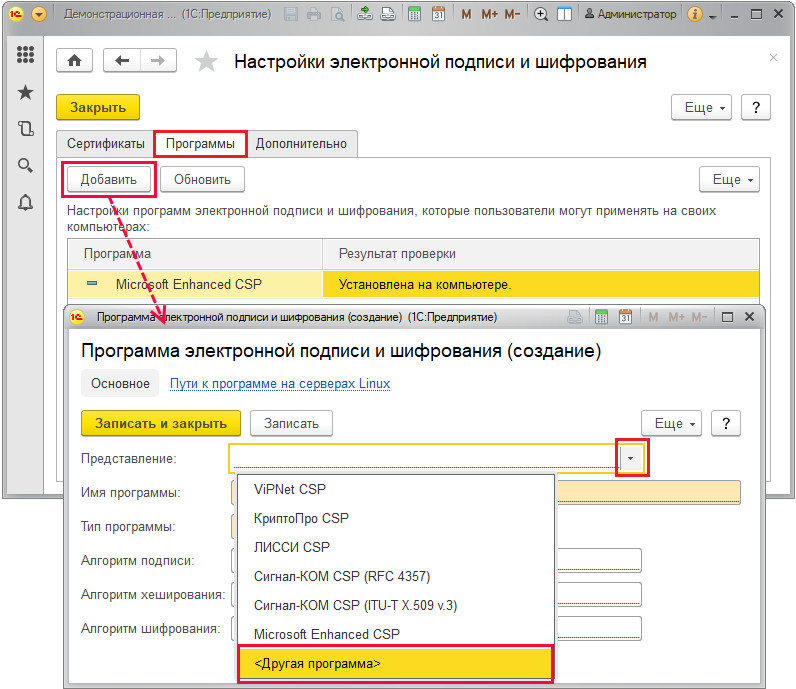
■ Имя программы – официальное название;

■ Тип программы – специальное число, которое описывает тип программы и дополняет имя программы, для известных программ является фиксированным;

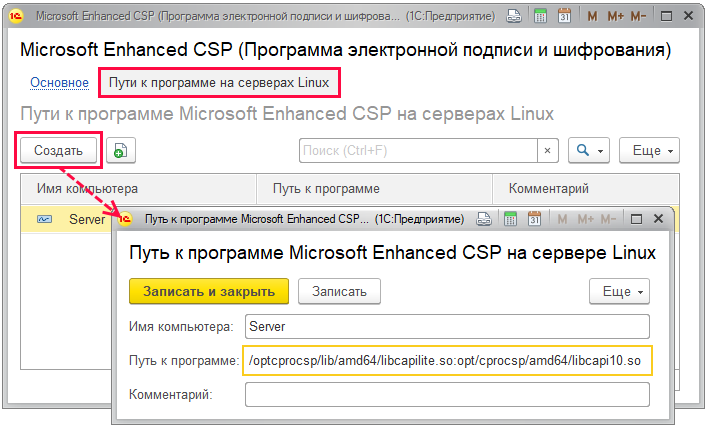
■ Алгоритм подписи;

■ Алгоритм хеширования;

■ Алгоритм шифрования.



Если один из флажков Проверять подписи и сертификаты на сервере или Подписывать и шифровать на сервере включен, то в панели навигации карточки программы становится доступной ссылка Пути к программе на серверах Linux.



При необходимости с помощью соответствующей ссылки панели навигации можно заполнить Пути к программе на серверах Linux:

■ напишите Имя компьютера, например, **Server**;

■ укажите Путь к программе;

■  например, **/opt/cprocsp/lib/amd64/libcapilite.so:/opt/cprocsp/lib/amd64/libcapi10.so:/opt/cprocsp/lib/amd64/libcapi20.so** для обеспечения совместимости и со старой, и с новой версией КриптоПро;

■ напишите Комментарий – дополнительные сведения о программе.

На вкладке Дополнительно автоматически заполняются настройки программы, но их можно изменить при необходимости.

Задайте Расширение для зашифрованных файлов при отправке по почте, при выполнении команды Сохранить и при экспорте папки (по умолчанию .p7m).

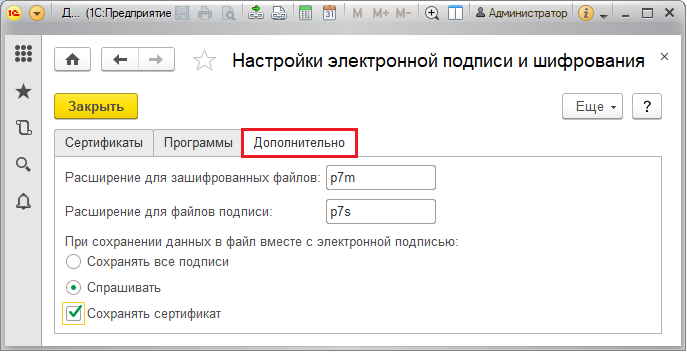
Напишите Расширение для файлов подписи (по умолчанию .p7s).

С помощью переключателя задайте поведение программы При сохранении данных в файл вместе с электронной подписью:

■ Сохранять все подписи – все подписи сохраняются;

■ Спрашивать – выбор сохраняемых подписей осуществляется из списка;

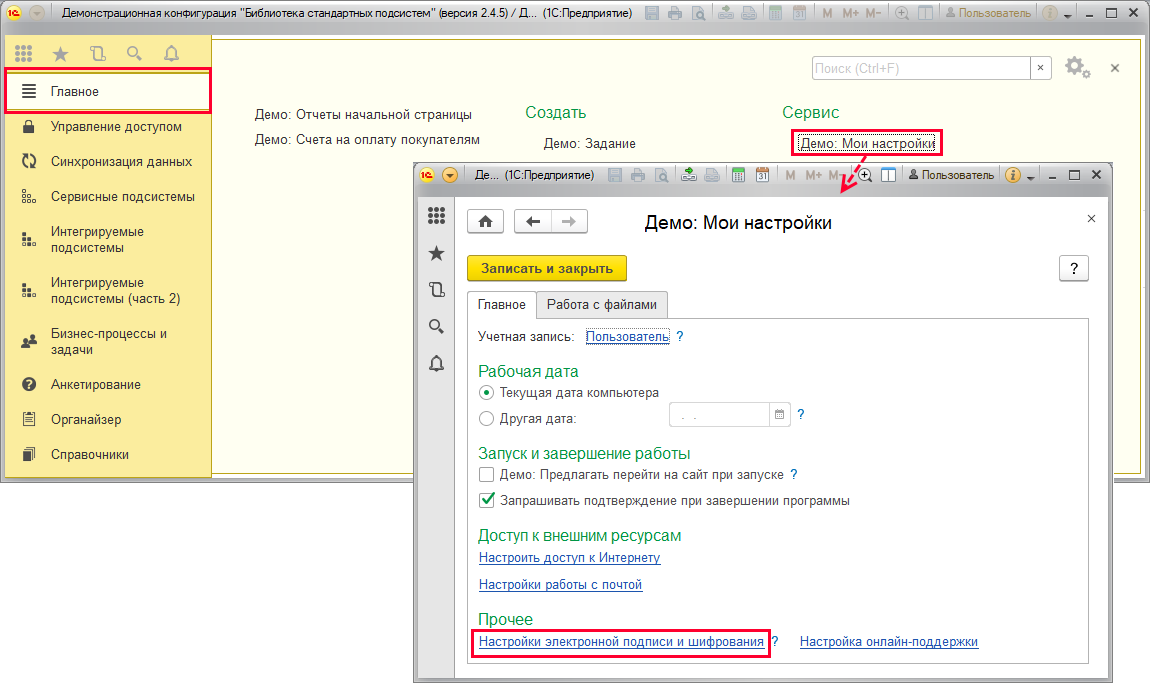
■ Сохранять сертификат – кроме подписи будет сохранен и сертификат электронной подписи.



**Персональные настройки**

Перед началом работы с подписанием и шифрованием необходимо произвести соответствующие настройки.

Персональные настройки электронной подписи и шифрования доступны всем пользователям, у которых есть роль на использование возможностей электронной подписи и шифрования. Персональные настройки программы открываются по команде **Демо: Мои настройки** в панели Сервис раздела **Главное**.



Список настроек состоит из трех вкладок: Сертификаты (подробнее см. разделы [Заявление](https://its.1c.ru/db/content/bsp301doc/src/5.62%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F%20%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C.htm?_=1542292879#_заявление_2) и [Сертификаты](https://its.1c.ru/db/content/bsp301doc/src/5.62%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F%20%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C.htm?_=1542292879#_сертификаты)), Программы и Дополнительно.

Перейдите на вкладку Программы (подробнее см. раздел [Настройка программы](https://its.1c.ru/db/content/bsp301doc/src/5.62%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F%20%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C.htm?_=1542292879#_настройка_программы_38)). Она содержит список программ для электронной подписи и шифрования, настроенный администратором, которые могут быть использованы в информационной базе (в том числе во всех узлах распределенной ИБ).

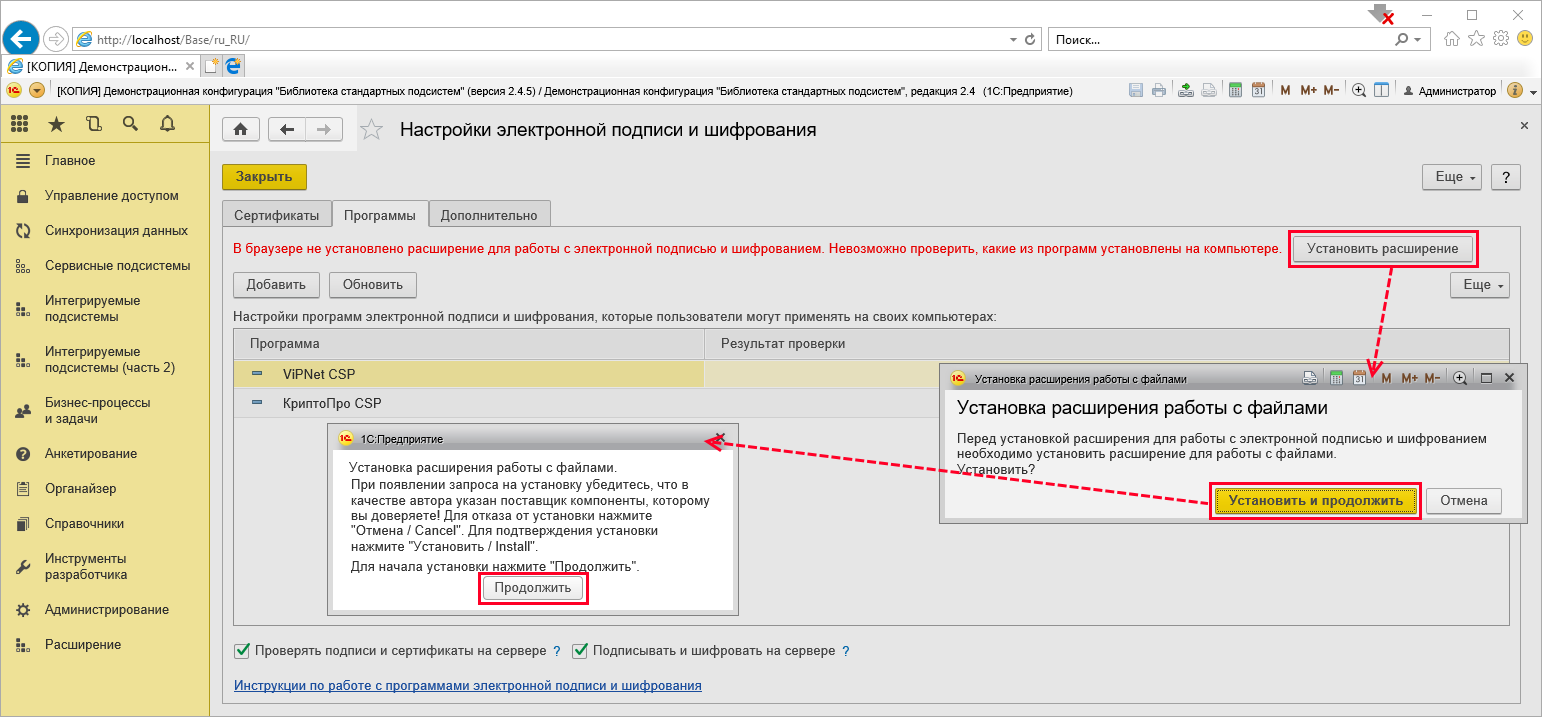
Если нет ни одной установленной программы для подписания и шифрования, то ее придется установить самостоятельно. Исключение составляет случай, когда для создания электронных подписей и шифрования используется сервер (это можно уточнить у администратора).

Для того чтобы самостоятельно выполнить установку, воспользуйтесь инструкцией, которая входит в комплект программы электронной подписи. Для программ VipNet CSP или КриптоПро CSP воспользуйтесь ссылкой Инструкции по работе с программами электронной подписи и шифрования.

**Особенности работы в веб-клиенте**

Для работы с программами электронной подписи и шифрования в веб-клиенте необходимо установить расширение.

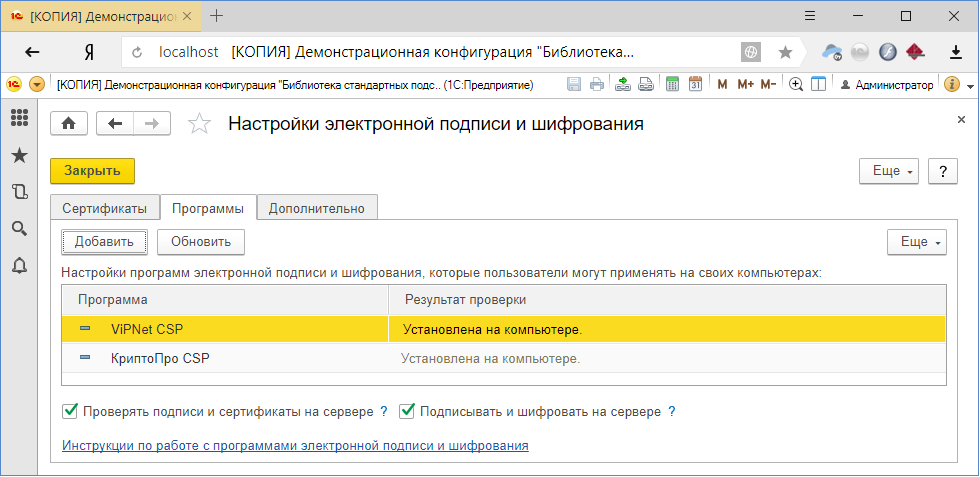
На вкладке Программы имеется кнопка для установки расширения. Для перехода в браузер нажмите кнопку Продолжить. Перед этим может потребоваться установить расширение для работы с файлами. Об этом программа выводит сообщение. Нажмите кнопку Установить и продолжить.



Проверьте издателя программы (1С) и подтвердите для браузера установку программы на компьютер, нажав кнопку Установить.

После окончания установки нажмите Продолжить, для того чтобы приступить к настройкам.

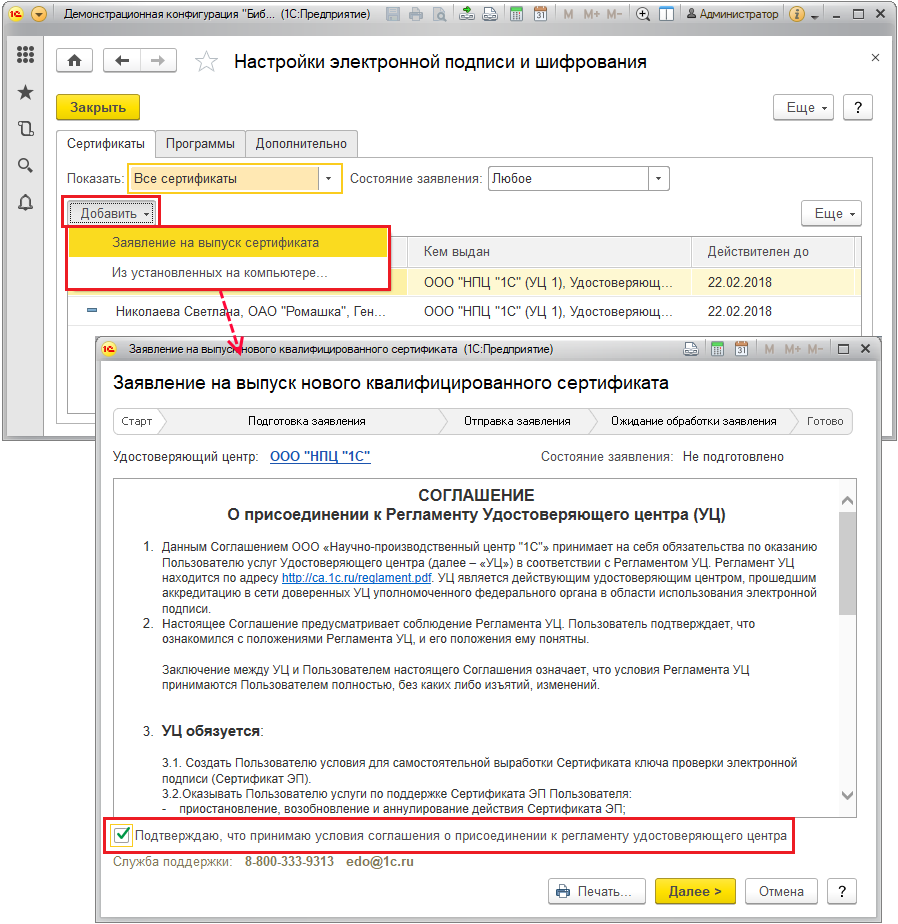
Установка расширения работы с криптографией проходит аналогично. После установки расширения список настроек электронной подписи и шифрования становится доступным для работы.



**Заявление**

В программе есть возможность подготовки заявления на выпуск нового квалифицированного сертификата в удостоверяющий центр 1С.

В списке Настройки электронной подписи и шифрования нажмите кнопку Добавить, выберите Заявление на выпуск сертификата.



На первой странице помощника подготовки заявления прочтите соглашение о присоединении к регламенту удостоверяющего центра (УЦ). По гиперссылке в тексте соглашения можно перейти к просмотру информации об УЦ.

Если вы принимаете условие Соглашения о присоединении к Регламенту Удостоверяющего центра, включите флажок. После этого становится доступной кнопка Далее для дальнейшего оформления заявления.

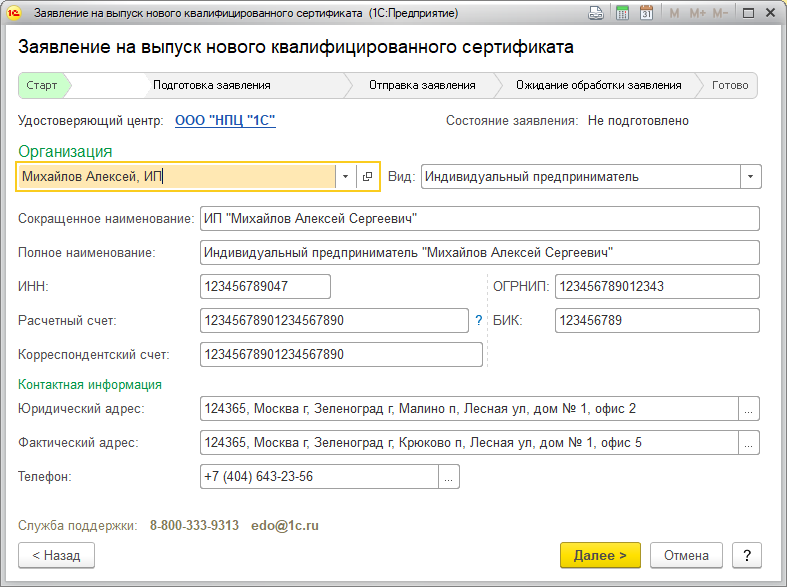
На странице Организация выберите организацию из списка. Если данные организации были заполнены ранее, то поля заполняются программой автоматически.

Программа проверяет правильность заполнения реквизитов.

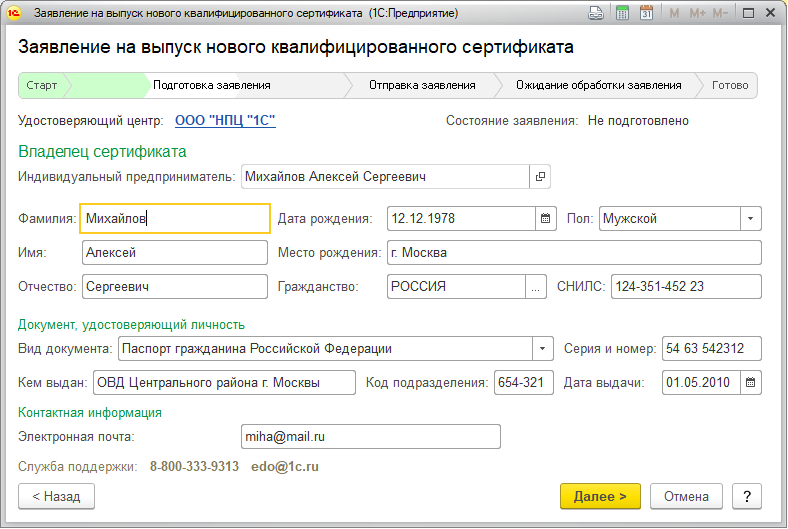
Нажмите Далее для перехода к заполнению данных владельца сертификата.

Заявление сохраняется автоматически на стадии подготовки и хранится в списке сертификатов. В любой момент к нему можно вернуться и продолжить работу.

Аналогично заполняются данные индивидуального предпринимателя. Выберите его из списка. Данные заполняются автоматически.



На странице Владелец сертификата данные для индивидуального предпринимателя заполняются автоматически, если они имеются в программе.



Программа проверяет правильность заполнения полей СНИЛС и Адрес электронной почты.

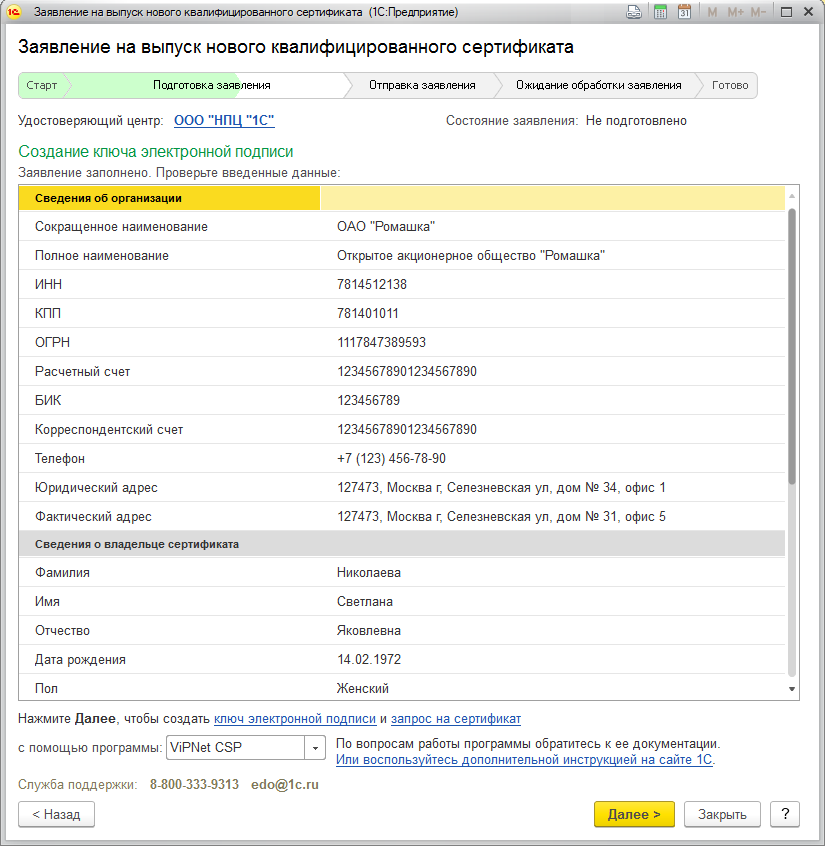
Если заявление на сертификат создается для организации, то поле Владелец также заполняется автоматически, но можно выбрать другого сотрудника. Для этого нажмите кнопку Выбрать из списка, выберите список, затем выберите сотрудника из списка. Если данные физического лица, связанного с организацией, были введены в программу, то они будут автоматически заполнены.

Нажмите Далее, для того чтобы перейти к созданию ключа электронной подписи и запроса на сертификат.

На странице Создание ключа электронной подписи данные владельца электронной подписи выводятся для проверки.

С помощью ссылок можно получить справку о том, что такое Ключ электронной подписи и Запрос на сертификат. Также можно перейти по гиперссылке и изучить подробную инструкцию на сайте 1С.

В поле С помощью программы автоматически проставляется криптопровайдер из списка установленных на компьютере. Если их несколько, выберите нужную программу из списка.



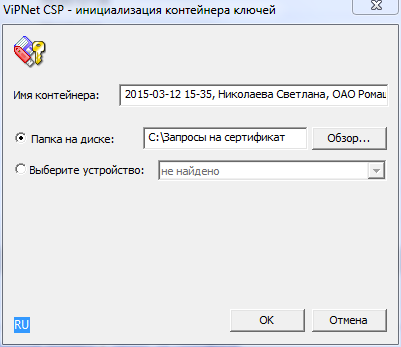
Нажмите Далее для создания ключа электронной подписи и запроса на сертификат.

Ключ электронной подписи – это секретная информация, которая сохраняется на компьютер, USB-накопитель, дискету или другой носитель информации и используется в дальнейшем для создания электронных подписей.

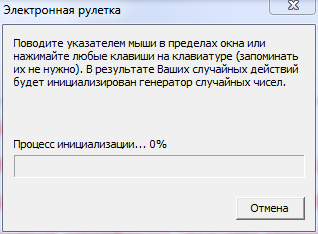
Запрос на сертификат – это не секретная информация, которая создается на основе ключа электронной подписи, отправляется вместе с заявление на выпуск сертификата и требуется для выпуска сертификата.

Для подготовки ключа (контейнера ключей) и запроса нужно установить дополнительную компоненту. В ответ на сообщение программы нажмите Установить. После установки компоненты нажмите кнопку ОК.

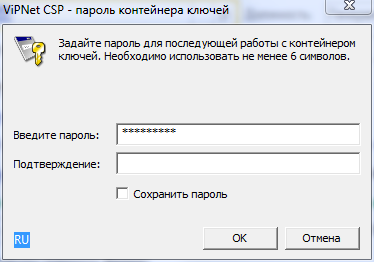
С помощью выбранной программы электронной подписи и шифрования (криптопровайдера) проводится инициализация контейнера ключей. С помощью кнопки Обзор укажите папку на компьютере или выберите специальное устройство для его хранения, нажмите кнопку ОК для начала инициализации.



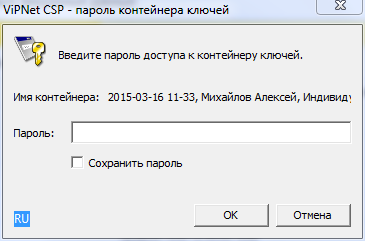
Программа выводит сообщение с указанием произвести случайные действия мышью или на клавиатуре.



Введите Пароль и Подтверждение пароля для контейнера ключей (не менее 6 символов). При необходимости включите флажок Сохранить пароль. Нажмите кнопку ОК.



Введите пароль доступа к контейнеру ключей для проверки, нажмите кнопку ОК.



Состояние подготовки заявления меняется на Подготовлено.

Для организации на странице Отправка заявления необходимо заполнить сведения о руководителе для печати заявления.

Для индивидуального предпринимателя никаких дополнительных сведений о нем не требуется.

Заполните Данные обслуживающей организации (партнера 1С). Для заполнения с помощью кнопки https://its.1c.ru/db/content/bsp301doc/src/_img/a8ac365292f91872c91b58b5276d597d/image031.png?_=1542292879 Выбрать из списка укажите организацию из списка **Демо: Контрагенты**.

Нажмите кнопку Печать для отправки подготовленного заявления на принтер.

Необходимо подготовить комплект документов (для того чтобы узнать, какие документы входят в комплект, перейдите по соответствующей ссылке):

Для организации заявление и все копии документов должны быть заверены подписью руководителя и печатью организации:

■ Заявление на выпуск сертификата;

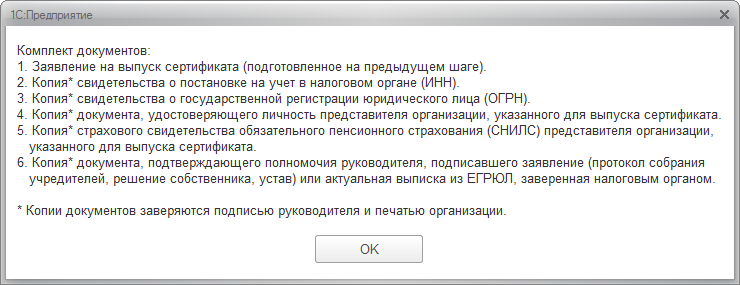
■ Копия свидетельства о постановке на учет в налоговом органе (ИНН);

■ Копия свидетельства о государственной регистрации юридического лица (ОГРН);

■ Копия документа, удостоверяющего личность представителя организации, указанного для выпуска сертификата;

■ Копия страхового свидетельства пенсионного страхования (СНИЛС) представителя организации, указанного для выпуска сертификата;

■ Копия документа, подтверждающего полномочия руководителя, подписавшего заявление (протокол собрания учредителей и т.п.) или актуальная выписка из ЕГРЮЛ, заверенная налоговым органом.



Для индивидуального предпринимателя требуется следующий комплект документов:

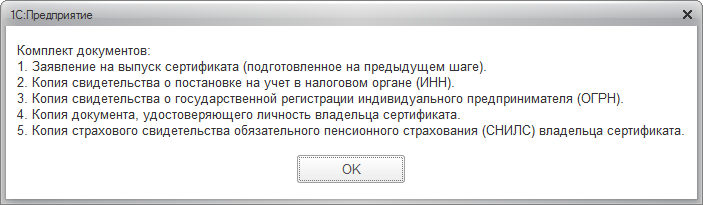
■ Заявление на выпуск сертификата (для индивидуального предпринимателя на заявлении нужна только подпись Заявителя);

■ Копия свидетельства о постановке на учет в налоговом органе (ИНН);

■ Копия свидетельства о государственной регистрации индивидуального предпринимателя (ОГРН);

■ Копия документа, удостоверяющего личность владельца сертификата;

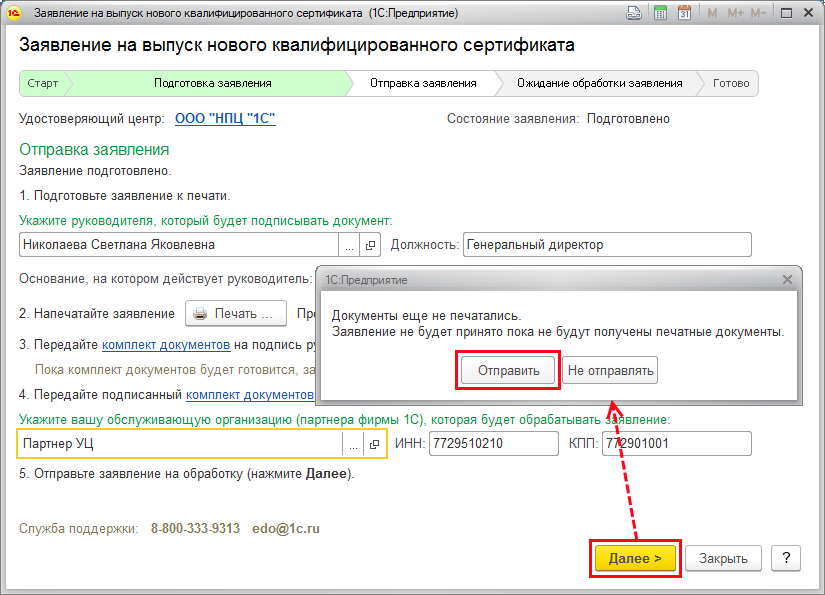
■ Копия страхового свидетельства обязательного пенсионного страхования (СНИЛС) владельца сертификата.



Подготовленный комплект документов необходимо передать уполномоченному представителю обслуживающей организации.

После этого для отправки заявления на обработку нажмите кнопку Далее.

Внимание! Заявление не будет принято, пока не будут получены печатные документы. При попытке отправить заявление программа выводит об этом напоминание.



Для отправки заявления необходимо ввести логин и пароль на сайте поддержки пользователей. Если регистрации на сайте еще нет, нажмите ссылку Перейти к регистрации на сайте поддержки пользователей.

После отправки заявления открывается страница Ожидание обработки заявления.

Для проверки состояния заявления или получения готового сертификата нажмите кнопку Обновить состояние.

После получения сертификата установите его на компьютер с помощью кнопки Установить сертификат. Сертификат помещается в контейнер ключей, который был создан ранее (см. выше). Потребуется ввести пароль контейнера ключей, который был установлен при его создании.

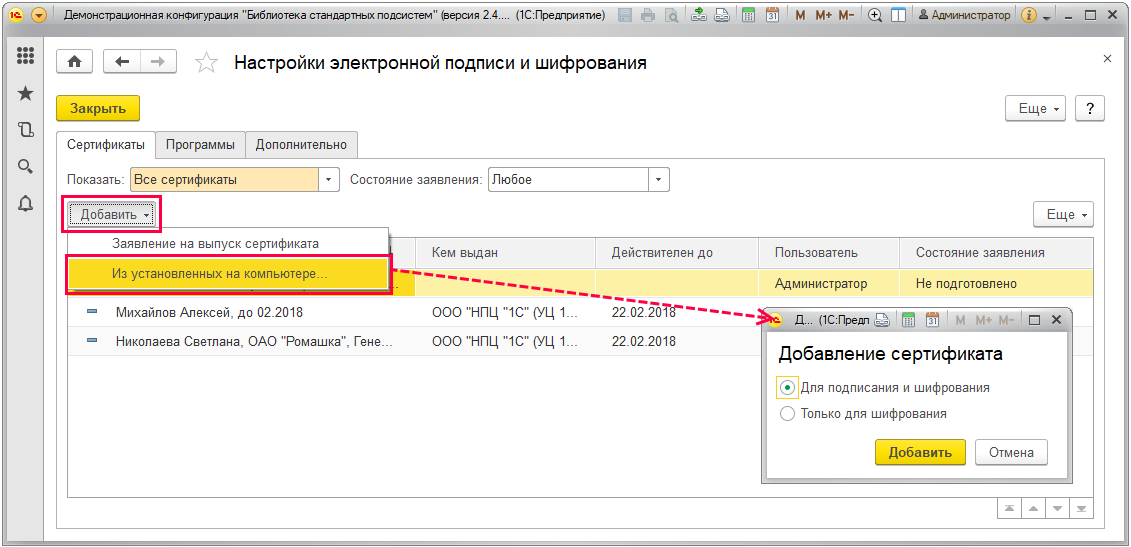
Воспользуйтесь соответствующей ссылкой, для того чтобы Выгрузить сертификат. Это может потребоваться, если установить автоматически сертификат не удалось.

**Сертификаты**

Вкладка показывает все сертификаты, которые используются для подписания и шифрования данных, а также заявления на выпуск нового сертификата.

Сертификат можно Добавить из числа установленных на компьютере. Также это можно сделать в процессе подписания или шифрования данных.

С помощью кнопки Добавить можно также подготовить Заявление на выпуск нового сертификата. Подробнее см. раздел [Заявление](https://its.1c.ru/db/content/bsp301doc/src/5.62%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F%20%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C.htm?_=1542292879#_заявление_2).



С помощью переключателя выберите, для чего будет использоваться сертификат:

■ Для подписания и шифрования;

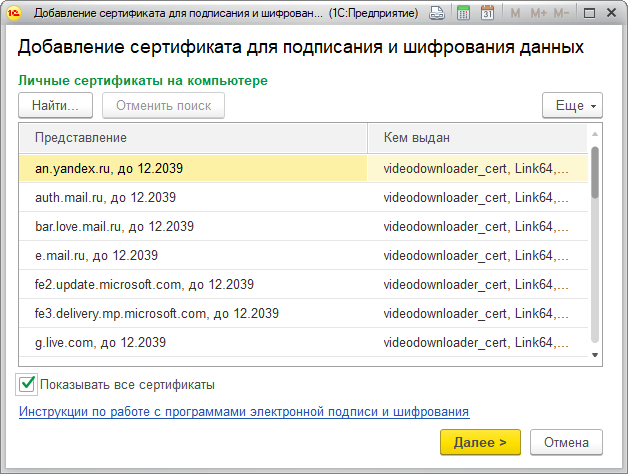
■ Только для шифрования.

Нажмите кнопку Добавить. Сертификаты для подписания и шифрования программа подбирает автоматически. Если список пуст, то на компьютере нет подходящих сертификатов.

Включите флажок, для того чтобы Показывать все сертификаты.

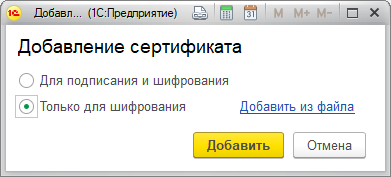
Для того чтобы изучить Инструкции по работе с программами электронной подписи и шифрования, перейдите по ссылке. Внимание! Для использования данной функции необходим договор 1С:ИТС.

Если сертификаты найдены, выделите нужный, нажмите кнопку Далее.



После этого открывается карточка сертификата, необходимо заполнить некоторые поля. См. ниже.

Добавить сертификат только для шифрования можно самостоятельно из файла на компьютере. Выберите с помощью переключателя Только для шифрования, затем нажмите ссылку Добавить из файла, укажите путь к файлу на компьютере.



Открывается карточка сертификата.

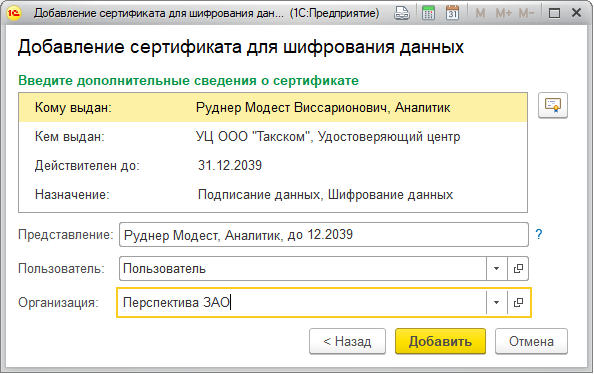
Поля Кому выдан, Кем выдан, Действителен до, Назначение и Представление программа заполняет автоматически.

Введите сведения о сертификате:

■ Пользователь – выберите из списка пользователя программы, который будет подписывать или шифровать документы с помощью этого сертификата электронной подписи;

■ Организация – выберите из списка организацию, от лица которой будут подписываться или шифроваться документы.

Нажмите кнопку Добавить для помещения сертификата в список.



После добавления сертификатов управлять ими можно в списке. Срок действия сертификатов программой проверяется автоматически. Устаревшие сертификаты становятся неактивными.

В поле Показать можно изменить настройку отбора сертификатов. Администратору по умолчанию показываются Все сертификаты, пользователю – «свои» сертификаты.

Обычно сертификат персональный, но выбрать можно и любой другой, если соответствующий закрытый ключ электронной подписи установлен на компьютере и известен пароль к ключу.

Для работы с заявлениями на выпуск нового сертификата предусмотрен отбор по полю Состояние заявления:

■ Любое;

■ Не подготовлено;

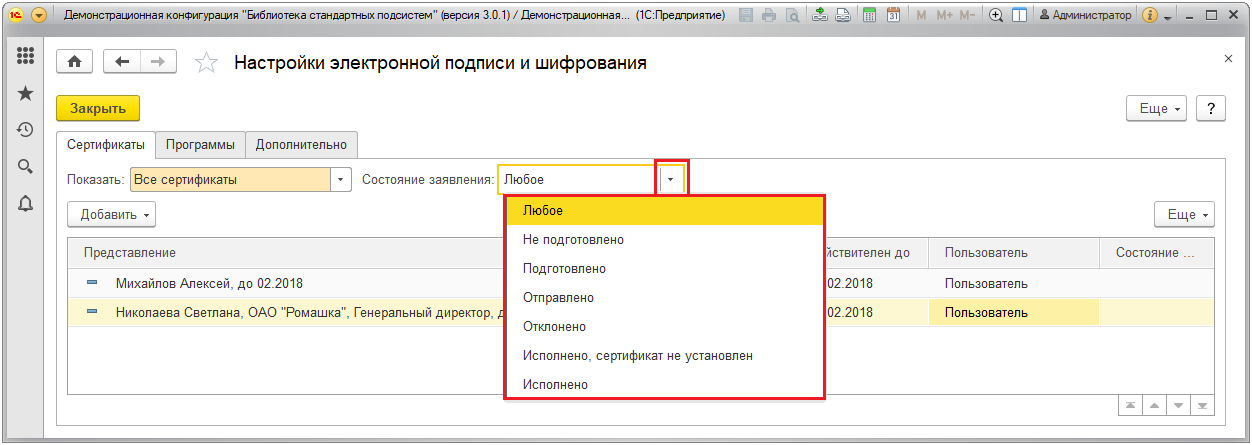
■ Подготовлено;

■ Отправлено;

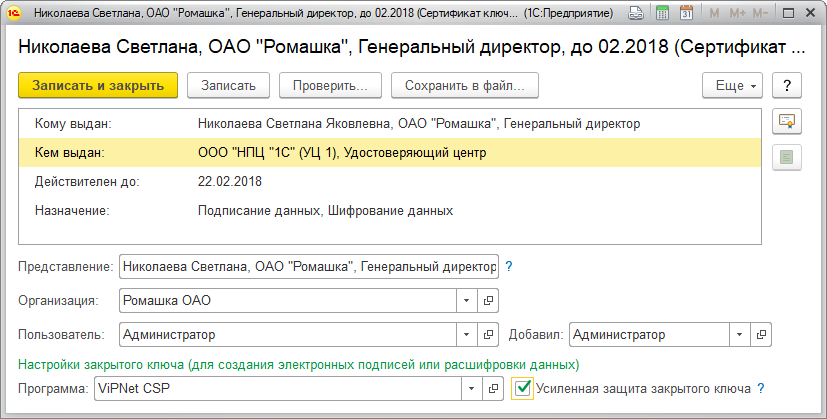
■ Отклонено;

■ Исполнено, сертификат не установлен;

■ Исполнено.

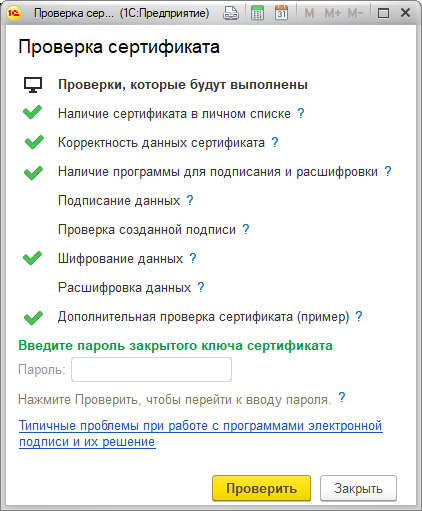


Просмотреть информацию о сертификате или [заявление](https://its.1c.ru/db/content/bsp301doc/src/5.62%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F%20%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C.htm?_=1542292879#_заявление_2) на выпуск нового сертификата можно, дважды щелкнув мышью по нужной строке. Также можно это сделать с помощью команды Изменить контекстного меню по правой кнопке мыши или меню Еще. Для подписания и расшифровки данных должно быть заполнено поле Программа в соответствии с закрытым ключом сертификата. При добавлении сертификата с проверкой возможности подписания поле заполняется автоматически. Для приложения в Интернете (только на сайте [https://1cfresh.com](https://1cfresh.com/)) доступна программа Электронная подпись в облачном сервисе. Подробнее см. раздел [Особенности работы с электронной подписью и шифрованием в разных моделях использования программы](https://its.1c.ru/db/content/bsp301doc/src/5.62%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F%20%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C.htm?_=1542292879#_особенности_работы_с).



Для того чтобы сохранить данные сертификата на компьютер, нажмите кнопку Сохранить в файл и укажите папку на компьютере.

Нажмите соответствующую кнопку, для того чтобы Проверить действительность сертификата. Проверка квалифицированного сертификата занимает некоторое время, проводится по нескольким параметрам.



Для просмотра подробных сведений о сертификате нажмите кнопку https://its.1c.ru/db/content/bsp301doc/src/_img/a8ac365292f91872c91b58b5276d597d/image2816.png?_=1542292879. Изменить данные о сертификате невозможно.

В верхней части окна выводятся основные сведения о сертификате:

■ Кому выдан – личные данные владельца сертификата;

■ Кем выдан – данные об Удостоверяющем центре, который выдал сертификат;

■ Действителен до – дата, до которой действует сертификат.

На вкладках размещается дополнительная информация о сертификате.

Вкладка Назначение содержит виды и коды назначений сертификата:

■ Подписание – флажок включен, если сертификат предназначен для подписания;

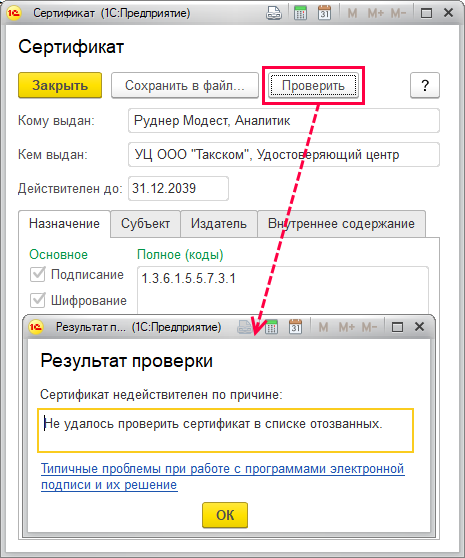
■ Шифрование – флажок включен, если сертификат предназначен для шифрования.

Вкладка Субъект содержит список свойств субъекта сертификата в привычных названиях, которые удалось распознать.

Вкладка Издатель содержит список свойств издателя сертификата в привычных названиях, которые удалось распознать.

Вкладка Внутреннее содержание содержит состав и значения свойств, как они указаны в данных сертификата.

Сертификат можно Сохранить в файл, укажите путь для сохранения сертификата на компьютере. Для более детальной проверки сертификата нажмите кнопку Проверить. Если сертификат действителен, программа выводит об этом сообщение.



Если сертификат недействителен, то программа выводит подробное сообщение о возможных причинах его недействительности.

В программе предусмотрена автоматическая проверка срока действия сертификатов. Выводится сообщение, если срок действия сертификата подходит к концу. В сообщении предусмотрен флажок Больше не напоминать для прекращения его вывода. Не рекомендуется выключать флажок, т.к. в этом случае придется самостоятельно контролировать срок действия сертификата.

**Создание электронной подписи и шифрование**

Возможности подписания и шифрования в программе наиболее полно реализованы при работе с хранимыми файлами. Если в программе включено использование подписания и шифрования, то для хранимых файлов становится доступным ряд команд в списке **Файлы**. Редактируемый файл недоступен для подписания или шифрования.

К файлам можно применить следующие команды, которые можно найти в выпадающем меню по кнопке https://its.1c.ru/db/content/bsp301doc/src/_img/a8ac365292f91872c91b58b5276d597d/image2820.png?_=1542292879 **Электронная подпись и шифрование**:

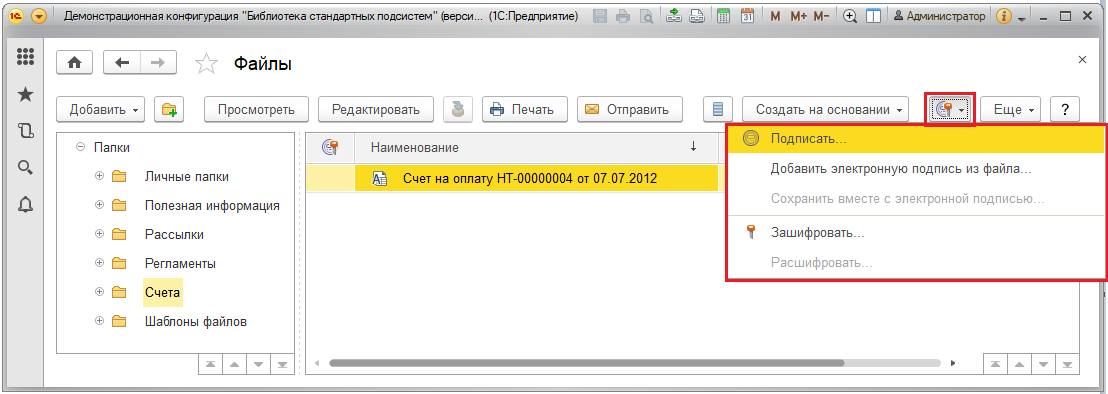
■ **Подписать** — создает для файла электронную подпись. Перед созданием электронной подписи программа предлагает выбрать сертификат ключа электронной подписи из имеющихся на компьютере. Сертификат, которого еще нет в списке сертификатов, автоматически в него добавляется. Добавить сертификат в список сертификатов из имеющихся на компьютере можно и на вкладке **Сертификаты** персональных настроек программы, см. раздел [Сертификаты](https://its.1c.ru/db/content/bsp301doc/src/5.62%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F%20%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C.htm?_=1542292879#_сертификаты). Для подписания нужно выбрать один сертификат, а также ввести пароль к закрытому ключу (вводится пользователем в процессе создания сертификата). Созданная электронная подпись хранится вместе с файлом. Подписанный файл становится недоступным для редактирования и отображается в списках со значком https://its.1c.ru/db/content/bsp301doc/src/_img/a8ac365292f91872c91b58b5276d597d/image2822.png?_=1542292879. Подписанный файл можно скопировать, при этом программа задаст вопрос – копировать файл с подписью или без. Подписывать файл могут разные пользователи, при этом для каждого будет создана своя подпись;

■ **Добавить электронную подпись из файла** – добавляет подпись к файлу. Команду можно использовать, например, если подпись (файл подписи) была получена позже, чем подписанный файл;

■ **Сохранить вместе с электронной подписью** – команда сохраняет подпись в файл на диске. Команду можно использовать, например, если необходимо передать подписанный файл другому лицу;

■ **Зашифровать** — по команде происходит шифрование файла. В отличие от подписания могут использоваться несколько сертификатов, например, если необходимо зашифровать файл для нескольких пользователей. Перед шифрованием необходимо выбрать сертификаты пользователей, которым будет разрешено расшифровывать файл. Зашифрованный файл в списках отображается с особенным значком https://its.1c.ru/db/content/bsp301doc/src/_img/a8ac365292f91872c91b58b5276d597d/image2824.png?_=1542292879. В отличие от подписания пароль к закрытому ключу в процессе шифрования вводить не нужно (пароль необходим при расшифровке). Однако при выборе личного сертификата из имеющихся на компьютере пароль запрашивается в процессе выбора, для того чтобы пользователь, который выполнил шифрование, смог расшифровать файл после того, как он будет зашифрован. Зашифрованный файл доступен для редактирования. Шифруются все версии файла. Для зашифрованных файлов не работает полнотекстовый поиск. Зашифрованный файл можно скопировать. При этом новый, скопированный файл останется зашифрованным. Зашифрованный файл нельзя подписать. Подписанный файл зашифровать можно, при этом перед проверкой электронной подписи у зашифрованного файла программа запросит пароль для предварительной расшифровки файла;

■ **Расшифровать** — по команде происходит расшифровка файла. Для расшифровки нужно ввести пароль к закрытому ключу.



При добавлении подписи сразу выполняется проверка подписи с сохранением результата.

Если в программе включено использование подписания и шифрования, в карточке файла доступны две вкладки:

■  **Электронные подписи** – на вкладке размещена информация об электронных подписях;

■ **Разрешено расшифровывать** – в списке на этой вкладке отображаются сертификаты, с помощью которых зашифрован файл.

В списке на вкладке **Электронные подписи** отображаются электронные подписи, с помощью которых подписан файл, в заголовке вкладки указывается, сколько подписей у файла.

Программа предоставляет возможность видеть результат последней проверки электронных подписей без необходимости перепроверки. Результат и дата проверки электронной подписи для файлов и документов теперь сохраняются в программе, поэтому их можно посмотреть в дальнейшем без обязательного выполнения повторной проверки, для которой требуется программа электронной подписи.

На вкладке можно:

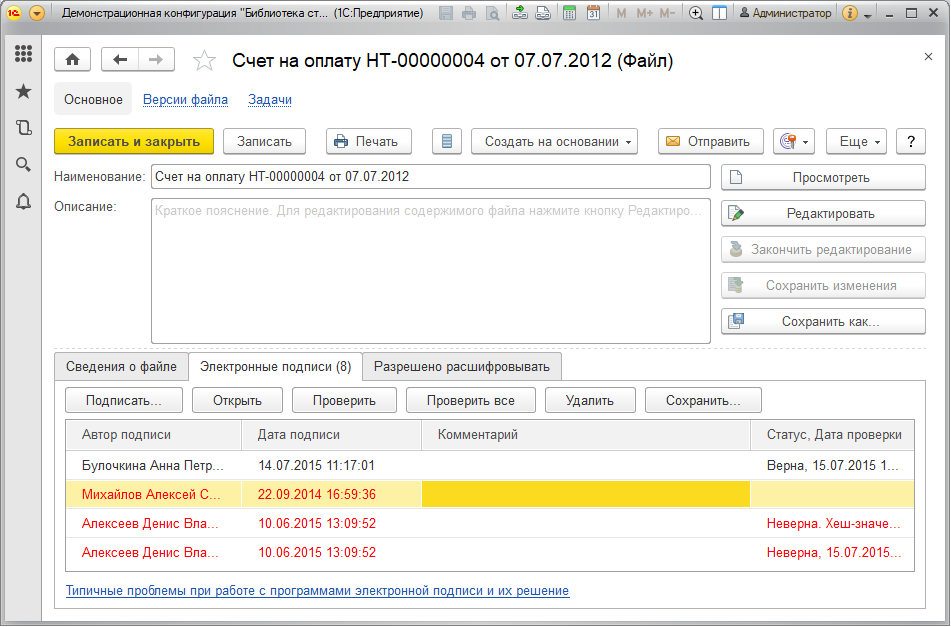
■ **Подписать** файл (аналогична команде **Подписать** в списке **Файлы**, см. выше);

■ **Открыть сертификат** – открыть окно с основными свойствами сертификата электронной подписи выделенного файла: кому и кем выдан, назначение и срок действия сертификата, на основе которого создана подпись;

■ **Проверить**, изменялся ли кем-либо подписанный файл, с помощью одного или всех сертификатов электронной подписи. Если электронная подпись хранимого файла не соответствует какому либо сертификату электронной подписи, то такая электронная подпись после проверки будет выделена в списке красным цветом, а в колонке **Статус, Дата проверки** у такой электронной подписи будет указано **Не верна**, также будет указана дата проверки;

■ **Сохранить** электронную подпись на диск в файл;

■ **Удалить** у файла электронную подпись.



Текст ошибки электронной подписи в колонке **Статус, Дата проверки** не сохраняется, но выводится при нажатии кнопки **Проверить**.

В списке на вкладке **Разрешено расшифровывать** с помощью кнопки **Открыть сертификат** или двойным щелчком мыши можно просмотреть основные свойства сертификата электронной подписи: кому и кем выдан, назначение и срок действия сертификата. Подробнее см. раздел [Сертификаты](https://its.1c.ru/db/content/bsp301doc/src/5.62%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F%20%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C.htm?_=1542292879#_сертификаты).

**Особенности работы с электронной подписью и шифрованием в разных моделях использования программы**

Работа в приложении в интернете аналогична работе в веб-клиенте. См. раздел [Особенности работы в веб-клиенте](https://its.1c.ru/db/content/bsp301doc/src/5.62%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F%20%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C.htm?_=1542292879#_особенности_работы_в).

Для приложения в Интернете (только на сайте [https://1cfresh.com](https://1cfresh.com/)) предусмотрена программа Электронная подпись в облачном сервисе, которая используется для сертификатов ключей, созданных с помощью программы 1С:Отчетность. Параметры программы электронной подписи для работы в приложении в интернете указывать не требуется, ее параметры определяются автоматически.

Для подписания и расшифровки данных в карточке сертификата должна быть указана программа. Для проверки подписи и шифрования данных программа может быть не заполнена.

**Роли для работы с электронными подписями и шифрованием**

Для работы с электронными подписями и шифрованием необходимо назначить следующие роли:

|  |  |
| --- | --- |
| Роль | Краткое описание |
| Полные права | Дает право доступа к настройкам параметров программы. |
| Добавление и изменение электронных подписей и шифрование | Дает право использовать электронную подпись и шифрование. Дает право доступа к персональным настройкам, дает право открытия окна подписи объектов программы и хранимых файлов, позволяет просматривать сведения о сертификате электронной подписи. |