Инструкция по настройке рабочего места для ОС Windows

В документе описан порядок установки и настройки программ, необходимых для работы с системой обмена юридически значимыми документами Synerdocs в ОС Windows.

Содержание

Основные понятия

Закрытый ключ

Ключ, известный только своему владельцу. Сохранение пользователем в тайне своего закрытого ключа гарантирует невозможность подделки злоумышленником документа и цифровой подписи от имени заверяющего.

Ключ электронной подписи

Набор уникальных данных, который используется криптографическим алгоритмом при шифровании и расшифровке сообщений, постановке и проверке цифровой подписи. При ассиметричном алгоритме шифрования различают закрытый и открытый ключ.

Корневой сертификат

Начальный сертификат в цепочке доверия. Как правило, корневым сертификатом является сертификат удостоверяющего центра.

Облачная электронная подпись

Квалифицированная электронная подпись (КЭП), созданная с использованием закрытого ключа и СКЗИ, которые физически установлены на удаленном защищенном сервере.

Открытый ключ

Ключ, который может быть опубликован и используется для проверки подлинности подписанного документа, а также для предупреждения мошенничества со стороны заверяющего лица в виде отказа его от подписи документа. Открытый ключ подписи вычисляется как значение некоторой функции от закрытого ключа, но знание открытого ключа не дает возможности определить закрытый ключ.

Промежуточный сертификат

Сертификат в цепочке доверия, подписанный на другом сертификате УЦ.

Сертификат пользователя (сертификат ключа проверки электронной подписи, сертификат открытого ключа)

Цифровой или бумажный документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Содержит информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название центра сертификации и т.д.

Токен

Уникальный идентификатор сессии, который выдается пользователю после успешной авторизации и обеспечивает доступ к объектам сервиса Synerdocs.

Цепочка доверия

Механизм проверки, при котором происходит построение пути от текущего сертификата до любого из доверенных корневых центров, причем каждый сертификат проверяется последующим.

Электронная подпись (ЭП)

Реквизит электронного документа, удостоверяющий автора подписи и гарантирующий неизменность документа после его подписания.

Системные требования

К компьютеру, на котором будут работать с системой ЭДО Synerdocs, предъявляются требования:

ОС	• Microsoft Windows XP Professional/Service Pack 2/Service Pack 3 • Microsoft Windows 7 Professional/Enterprise/Ultimate 32- или 64-разрядная версия • Microsoft Windows 8/8.1/10 Pro/Enterprise 32- или 64-разрядная версия
Браузер	• Google Chrome • Mozilla Firefox, см. раздел «Настройка Mozilla Firefox» • Internet Explorer 10.0 и выше, см. раздел «Настройка Internet Explorer»
Прочее	• СКЗИ: КриптоПро CSP 3.6 и выше (http://www.cryptopro.ru/products/csp/overview) или VIPNet CSP 4.0 и выше (https://infotecs.ru/downloads/product_full.php?id_product=2096) При использовании облачной электронной подписи СКЗИ не требуется. • КриптоПро ЭЦП Browser Plug-in версии 1.05.0946 и выше При использовании облачной электронной подписи не является обязательным, так как будет доступна авторизация по логину и паролю.

Общие сведения

Для автоматической настройки рабочего места рекомендуется использовать мастер настройки.

Если в процессе выполнения автоматической настройки возникают ошибки, рабочее место можно настроить вручную.

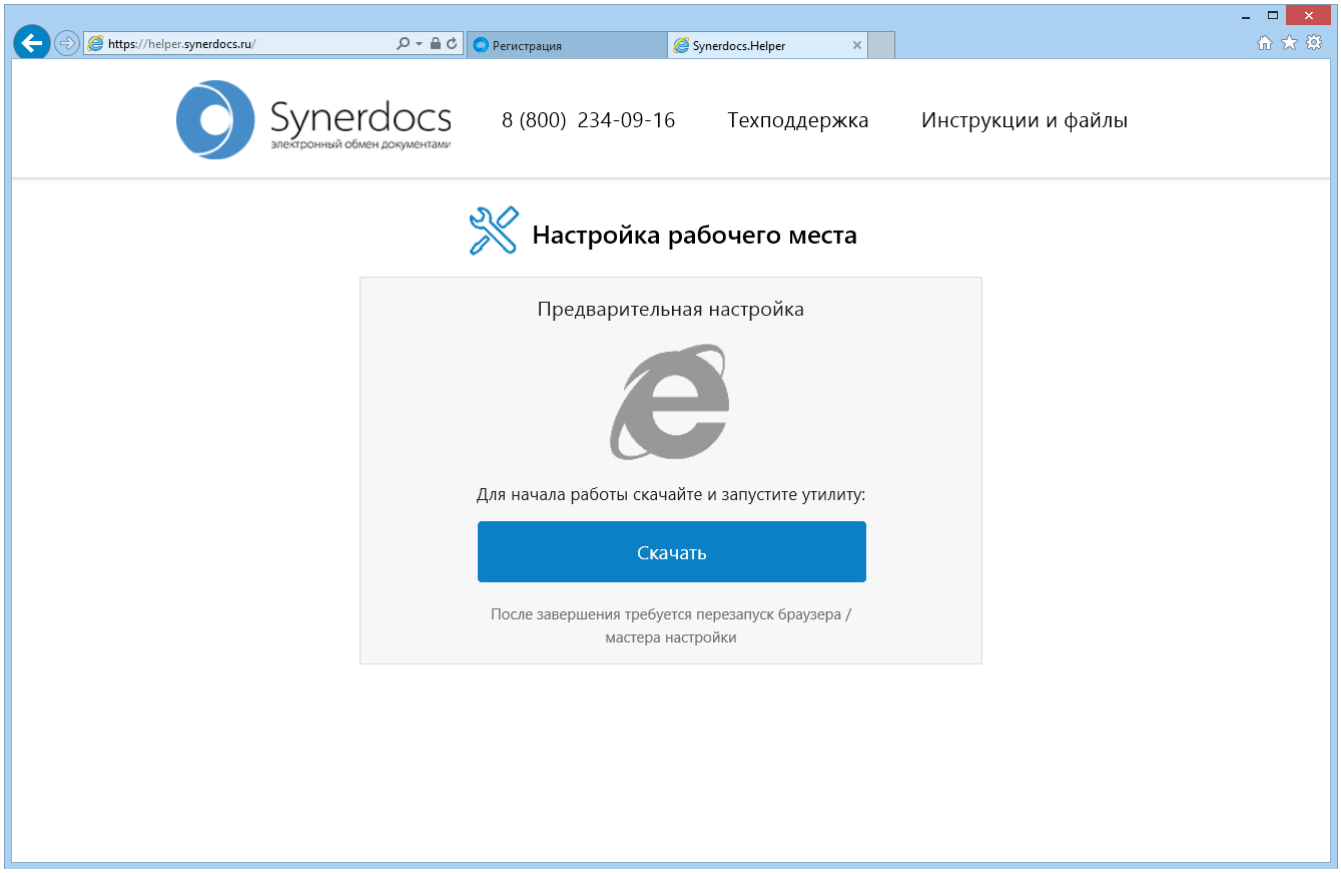
Автоматическая настройка

Порядок автоматической настройки может различаться в зависимости от используемого браузера:

- Internet Explorer
- Google Chrome и Mozilla Firefox

Internet Explorer

1. На странице регистрации нажмите на кнопку **Настроить рабочее место**. Откроется вкладка «Настройка рабочего места», на которой будут выполняться этапы мастера настройки:



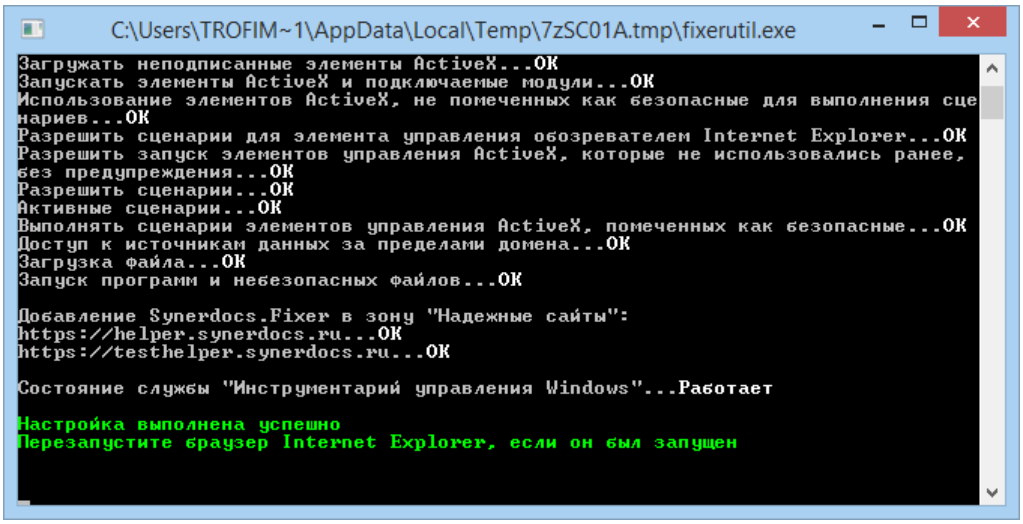
   По вопросам, возникающим в ходе настройки, можно обратиться к специалистам технической поддержки. Например, отправить обращение с приложением файла или заказать звонок. Для этого нажмите на кнопку **Техподдержка**.

   При необходимости можно скачать файлы программ и инструкций по кнопке **Инструкции и файлы**:

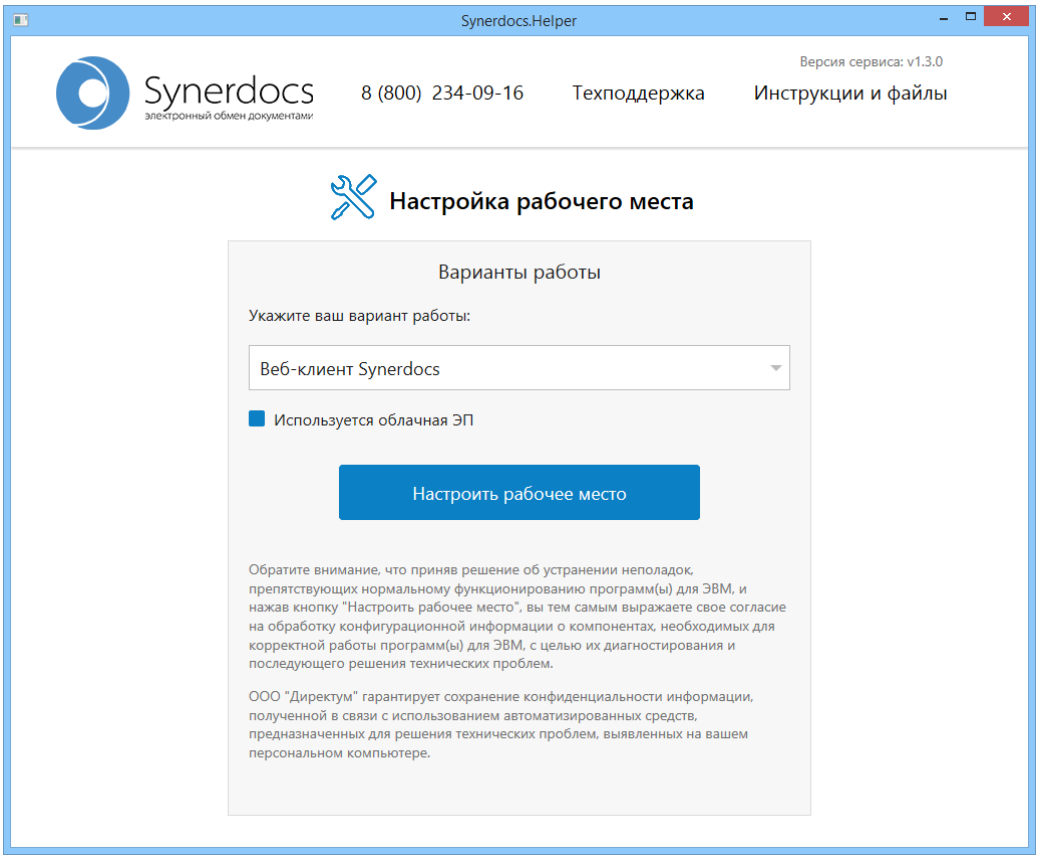
   - для работы в веб-клиенте – файлы для установки КриптоПро CSP и КриптоПро ЭЦП Browser plug-in, руководство пользователя и инструкцию по настройке рабочего места;

- для работы в 1С – файлы для установки КриптоПро CSP и интеграционных решений Synerdocs и 1С, руководства пользователя интеграционных решений.

2. На этапе мастера «Предварительная настройка» нажмите на кнопку **Скачать**, чтобы скачать утилиту для настройки прав доступа и настроек браузера. Если настройки уже были выполнены ранее, мастер перейдет к этапу «Варианты работы», см. п.4.
3. Запустите утилиту. Откроется консольное окно со списком выполненных настроек:



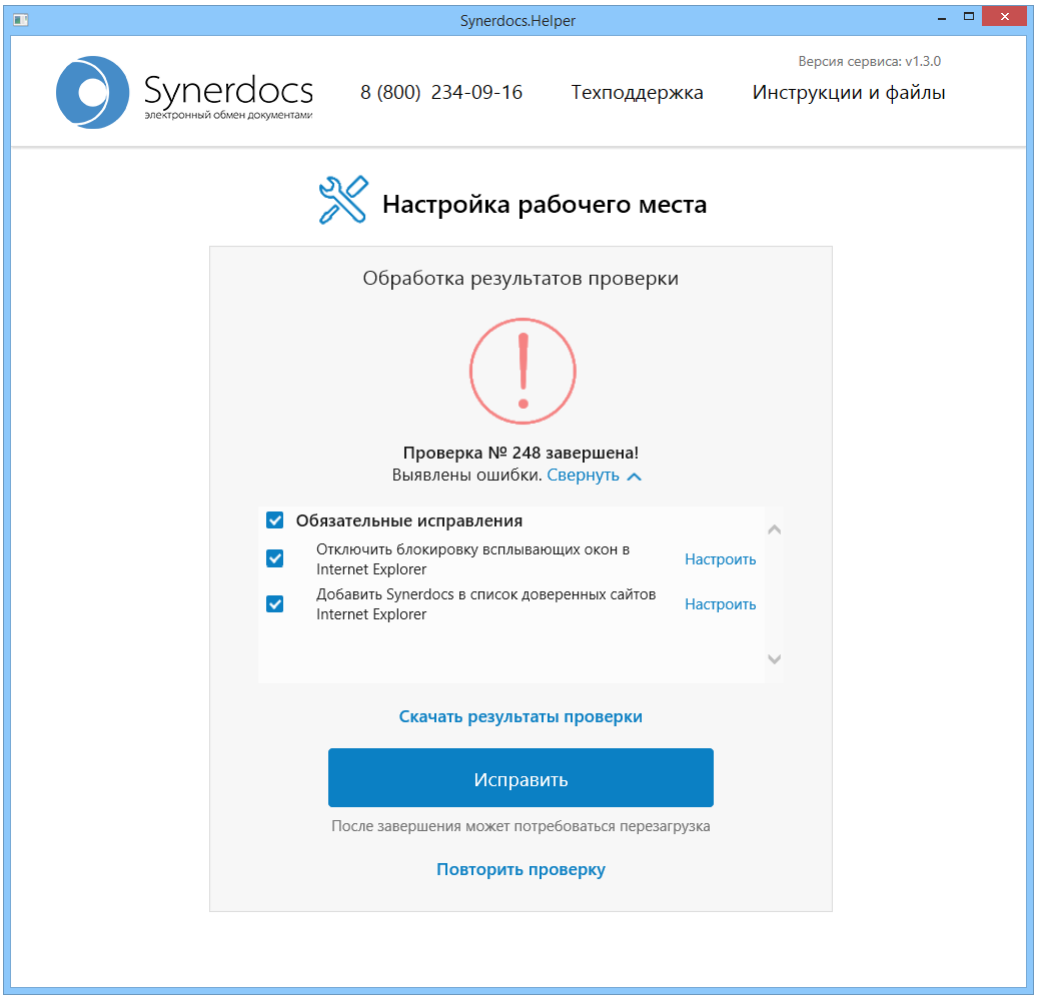
Далее автоматически будет запущена локальная версия мастера настройки на этапе «Варианты работы»:



4. На данном этапе мастера:
   - укажите вариант, через который будете работать: веб-клиент или 1С. Можно указать оба варианта;
   - если в работе будет использоваться облачная ЭП, установите флажок **Используется облачная ЭП**;

- нажмите на кнопку **Настроить рабочее место**.

5. На этапе мастера «Обработка результатов проверки» отображаются результаты настройки:



При обнаружении ошибок:

- перейдите по ссылке **Посмотреть**, чтобы раскрыть список ошибок;
- в случае обнаружения обязательных и необязательных исправлений нажмите на кнопку **Исправить**. Для исправления отдельных обязательных исправлений перейдите по соответствующим ссылкам:
  - **Настроить** – настройка программы;
  - **Скачать** – скачивание и дальнейшая установка программы;
  - **Инструкция** – выполнение прочих настроек по инструкции.

Примечание

Обновление КриптоПро CSP рекомендуется выполнять в случае, если у вас не приобретен лицензионный ключ. После обновления лицензионный ключ может не подойти к новой версии КриптоПро CSP, и продукт станет действителен только в течение пробного периода.

Если какие-либо из обязательных исправлений не удается устранить, сохраните их локально с помощью ссылки **Скачать результаты проверки**. Затем обратитесь к специалистам технической поддержки по кнопке **Техподдержка**, приложив сохраненный файл;

- в случае обнаружения только необязательных исправлений проанализируйте их и при необходимости перейдите по ссылке **Исправить необязательные**;

- выполните проверку повторно с помощью ссылки **Повторить проверку**, если был изменен вариант работы.

6. Если обязательных ошибок нет или все обязательные ошибки исправлены, нажмите на кнопку **Начать работу**.

Google Chrome и Mozilla Firefox

1. На странице регистрации нажмите на кнопку **Настроить рабочее место**. Откроется вкладка «Настройка рабочего места».
2. Скачайте локальную версию мастера настройки с помощью кнопки **Скачать**.
3. Запустите мастер. Если настройки браузера и прав доступа не были настроены ранее, откроется консольное окно со списком выполненных настроек.
4. Мастер автоматически перейдет к этапу «Варианты работы». Выполните действия, аналогичные действиям в браузере Internet Explorer, начиная с п.4.

Ручная настройка

1. Установите СКЗИ и сертификаты
2. Установите и настройте КриптоПро ЭЦП Browser plug-in
3. Настройте браузер

Установка СКЗИ и сертификатов

В качестве средства криптозащиты информации может выступать Крипто ПРО CSP или ViPNet CSP.

КриптоПро CSP

Программа КриптоПро CSP предназначена для интеграции криптографических функций в клиентское приложение. Посредством криптографических функций осуществляется расшифрование токена авторизации и работа с электронной подписью.

По вопросам получения лицензии на КриптоПро CSP обратитесь в отдел продаж Synerdocs: office@synerdocs.ru.

Примечание

При работе с системой через интеграционное решение Synerdocs и 1С в терминальном режиме, КриптоПро CSP необходимо устанавливать на сервер с системой 1С.

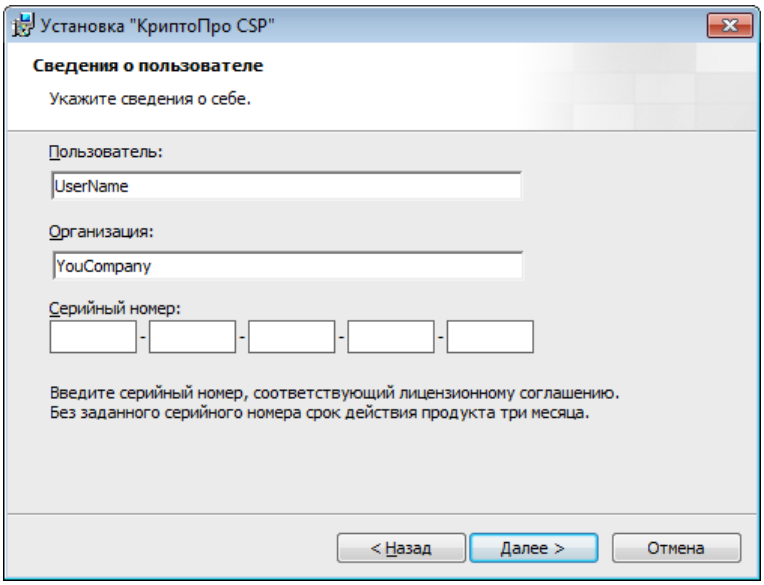
Подробнее об установке программы и сертификатов пользователя см. в разделах «Порядок установки» и «Установка сертификатов».

Порядок установки

1. Скачайте программу установки на сайте http://cryptopro.ru/products/csp/downloads.
2. Запустите файл установки.
3. В окне приветствия нажмите на кнопку **Далее >**.
4. В окне «Лицензионное соглашение»:
   - ознакомьтесь с текстом лицензионного соглашения КриптоПро CSP;

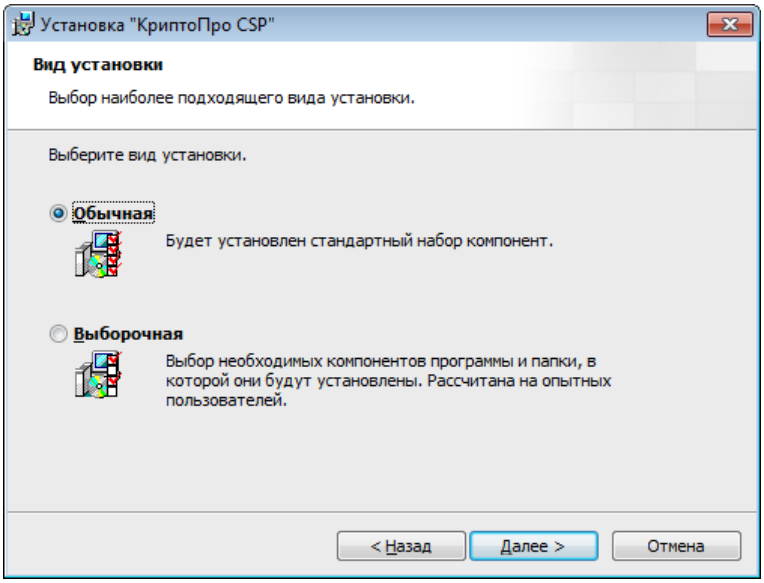
- установите переключатель **Я принимаю условия лицензионного соглашения**, если согласны;
- нажмите на кнопку **Далее >**.

5. В окне «Сведения о пользователе»:



- в поле ***Пользователь** укажите имя пользователя, на компьютер которого устанавливается программа КриптоПро CSP. Значение по умолчанию – имя компьютера;
- в поле ***Организация** укажите название организации;
- в поле ***Серийный номер** укажите серийный номер программы КриптоПро CSP. Без заданного серийного номера срок действия программы составляет три месяца;
- нажмите на кнопку **Далее >**.

6. В окне «Вид установки»:



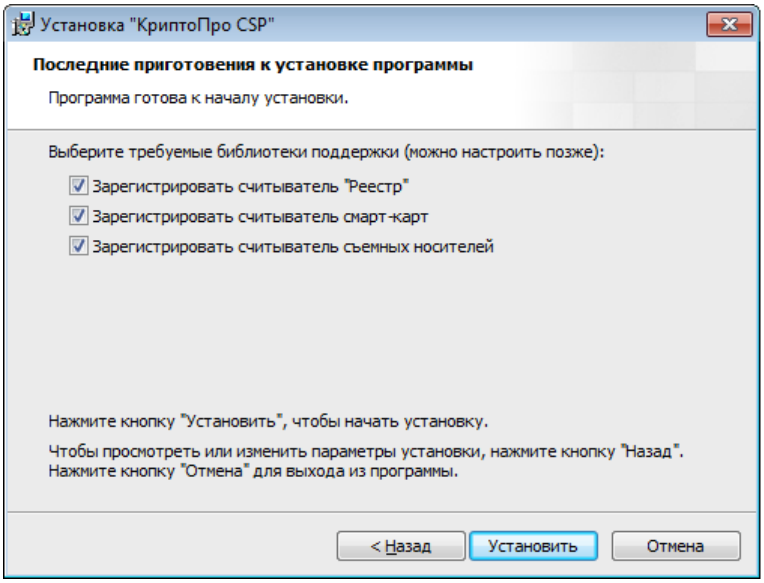
- выберите вид установки программы КриптоПро CSP;

Примечание

Если на компьютере установлена система банк-клиент, рекомендуется выбирать выборочную установку и включать компоненту **Совместимость с КриптоПро CSP 3.0**.

- нажмите на кнопку **Далее >**. Если выбран вид установки **Обычная**, установка перейдет к шагу 8.

7. В окне «Выборочная установка» выберите компоненты, которые необходимо установить и нажмите на кнопку **Далее >**.
8. В окне «Последние приготовления к установке программы»:



   - установите флажок **Зарегистрировать считыватель «Реестр»**, если закрытые ключи хранятся в реестре;
   - установите флажок **Зарегистрировать считыватель смарт-карт** для возможности работы со смарт-картами;
   - установите флажок **Зарегистрировать считыватель съемных носителей** для возможности работы с USB-носителями;
   - нажмите на кнопку **Установить**.
9. В окне «Программа установки «КриптоПро CSP» завершена» нажмите на кнопку **Готово**.
10. В окне предупреждения о перезагрузке нажмите на кнопку **Да**. Перезагрузка необходима для учета изменений в настройках КриптоПРО CSP.

Установка сертификатов

Если у пользователя нет сертификата, выданного аккредитованным удостоверяющим центром, то необходимо оформить заявку на приобретение электронной подписи. Для этого обратитесь в отдел продаж Synerdocs: office@synerdocs.ru.

Существуют варианты установки сертификата:

- Установка сертификата из файла
- Установка сертификата из контейнера закрытого ключа

Установка сертификата из файла

Для установки сертификата пользователя необходим файл с расширением *.crt или*.cer.

Чтобы установить сертификат пользователя:

1. Убедитесь, что съемный носитель с закрытым ключом подключен к компьютеру, если ключ не установлен в реестре.
2. Запустите программу Крипто-Про CSP.

3. Перейдите на вкладку «Сервис» и нажмите на кнопку **Установить личный сертификат**. Запустится мастер установки сертификата.
4. Нажмите на кнопку **Обзор** и выберите сертификат (файл с расширением *.crt или *.cer). Следуйте инструкциям мастера.
5. В диалоге выбора контейнера закрытого ключа установите флажок **Найти контейнер автоматически**. Если контейнер не находится автоматически, выберите его вручную с помощью кнопки **Обзор**.
6. В диалоге выбора хранилища сертификатов выберите параметр **Личное** и установите флажок **Установить сертификат в контейнер**.
7. В окне «Завершение работы мастера установки личного сертификата» проверьте параметры установки и нажмите на кнопку **Готово**.

Установка сертификата из контейнера закрытого ключа

1. Убедитесь, что съемный носитель с закрытым ключом подключен к компьютеру, если ключ не установлен в реестре.
2. Запустите программу Крипто-Про CSP.
3. Перейдите на вкладку «Сервис», нажмите на кнопку **Просмотреть сертификаты в контейнере...**.
4. В окне с выбором контейнера для просмотра убедитесь, что в поле **Введенное имя задает ключевой контейнер** выбран пункт **Пользователя** и нажмите на кнопку **Обзор**.
5. Выберите контейнер на съемном носителе либо в реестре, в зависимости от того, где он установлен, и нажмите на кнопку **ОК**.
6. В окне «Контейнер закрытого ключа» нажмите на кнопку **Далее >**.
7. В окне «Сертификат для просмотра» нажмите на кнопку **Установить**.
8. Нажмите на кнопку **Готово**. Появится сообщение о том, что импорт сертификата успешно выполнен.

ViPNet CSP

Программа ViPNet предназначена для вызова криптографических функций в ОС Windows и обеспечивает хеширование и шифрование данных, работу с ключами электронной подписи и сертификатами пользователей.

Подробнее об установке программы см. в разделе «Порядок установки».

Для длительного использования программу необходимо зарегистрировать, подробнее см. раздел «Регистрация».

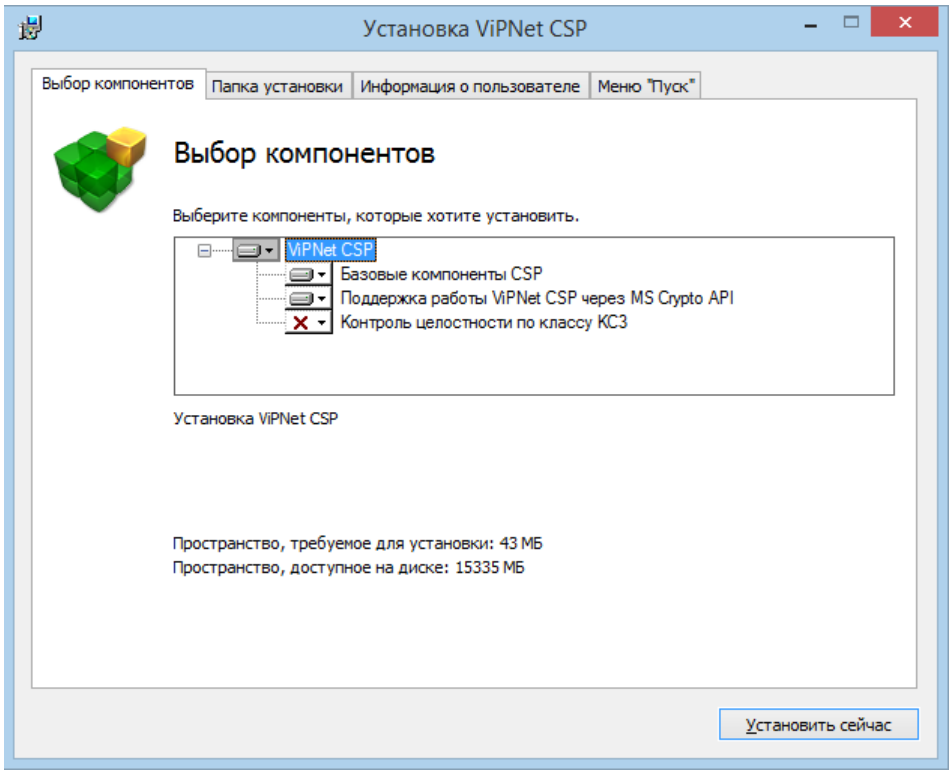
Порядок установки сертификатов пользователей см. в разделе «Установка сертификатов».

Порядок установки

1. Скачайте программу установки на сайте https://infotecs.ru/downloads/product_full.php?id_product=2096.
2. Запустите файл установки.
3. В окне «Лицензионное соглашение»:
   - ознакомьтесь с текстом лицензионного соглашения ViPNet CSP;
   - установите переключатель **Я принимаю это соглашение**, если согласны;

- нажмите на кнопку **Продолжить**.

4. В окне «Способ установки» нажмите на кнопку **Настроить**, чтобы задать параметры установки.
5. В окне задания параметров:



- на вкладке «Выбор компонентов» укажите компоненты, которые необходимо установить;
- на вкладке «Папка установки» укажите путь до папки, в которую будут установлены файлы программы;
- на вкладке «Информация о пользователе» укажите имя и название организации;
- на вкладке «меню «Пуск» укажите название и путь до папки в меню «Пуск»;
- нажмите на кнопку **Установить сейчас**.

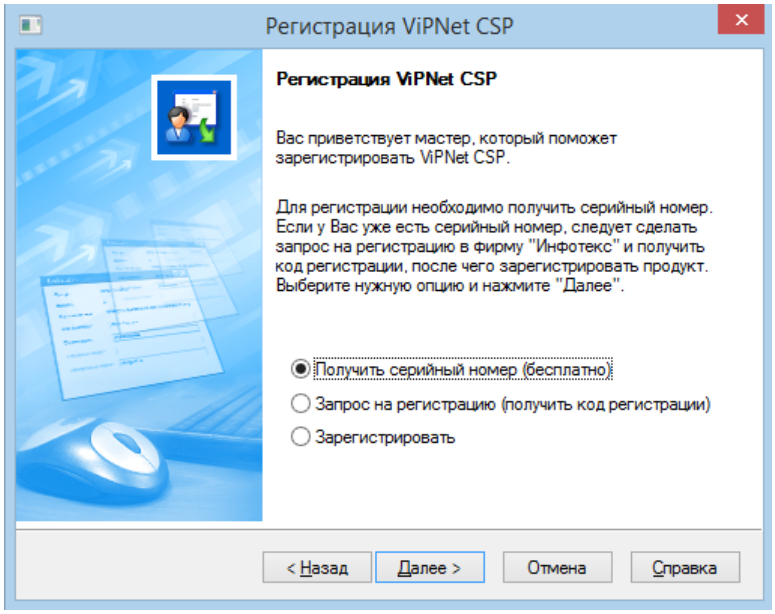
6. В окне о завершении установки нажмите на кнопку **Закрыть**.
7. В окне предупреждения о перезагрузке нажмите на кнопку **Да**. Перезагрузка необходима для вступления в силу изменений в настройках ViPNet CSP.

Регистрация

После установки программа работает в демо-режиме 14 дней. Чтобы использовать ViPNet CSP после истечения срока действия, необходимо ее зарегистрировать. Для этого:

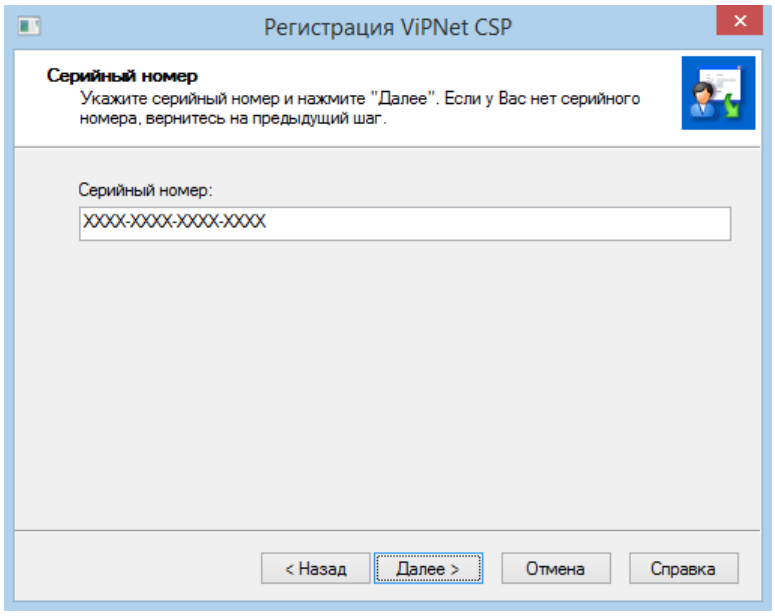
1. Запустите программу ViPNet CSP.
2. В открывшемся окне установите флажок **Зарегистрировать ViPNet CSP** и нажмите на кнопку **Далее**.

3. В окне «Регистриция ViPNet CSP»:



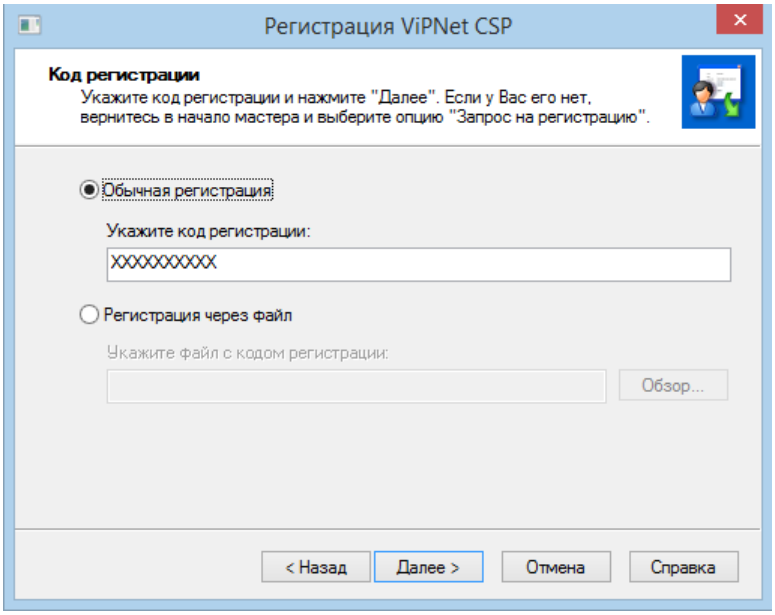
- установите флажок **Получить серийный номер (бесплатно)**, если он не был получен при скачивании дистрибутива. Выполните дальнейшие шаги по получению серийного номера;
- установите флажок **Запрос на регистрацию (получить код регистрации)**, если серийный номер получен, а код регистрации еще нет. Выполните дальнейшие шаги по получению серийного номера;
- установите флажок **Зарегистрировать**, если серийный номер и код регистрации получены;
- нажмите на кнопку **Далее >**.

4. В окне «Серийный номер»:



- укажите полученный серийный номер;
- нажмите на кнопку **Далее >**.

5. В окне «Код регистрации»:



   - укажите полученный код регистрации;
   - нажмите на кнопку **Далее >**.
6. В завершающем окне об успешной регистрации программы нажмите на кнопку **Готово**.

Установка сертификатов

Если у пользователя нет сертификата открытого ключа, выданного аккредитованным удостоверяющим центром, то необходимо оформить заявку на приобретение электронной подписи. Для этого обратитесь в отдел продаж Synerdocs: office@synerdocs.ru.

Если сертификат и закрытый ключ находятся в одном контейнере, размещенном в папке, выполните установку контейнера ключей из папки.

Для возможности использования сертификата, например для формирования электронной подписи, выполните установку сертификата в контейнер с закрытым ключом.

После установки сертификата в контейнер ключей выполните установку сертификата в системное хранилище.

Установка контейнера ключей из папки

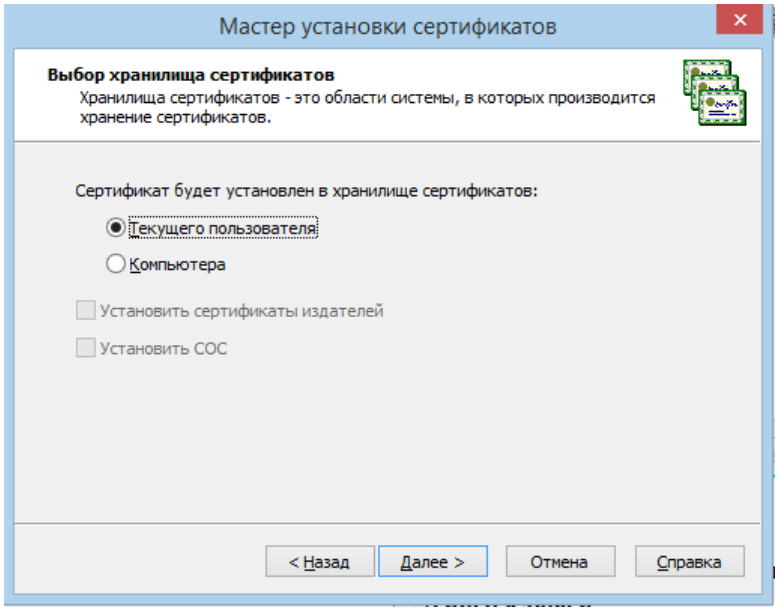
1. Запустите программу ViPNet CSP.
2. Перейдите в раздел **Контейнеры** и нажмите на кнопку **Добавить**.
3. В окне инициализации контейнера ключей:
   a) Нажмите на кнопку **Обзор** и выберите сертификат (файл с расширением *.crt или *.cer).
   b) Нажмите на кнопку **ОК**.
4. В сообщении об успешном добавлении контейнера и добавлении его в системное хранилище пользователя нажмите на кнопку **Да**.

Установка сертификата в контейнер ключей

1. Запустите программу ViPNet CSP.
2. Перейдите в раздел **Контейнеры**.
3. В списке контейнеров выберите тот, в который необходимо установить сертификат и нажмите на кнопку **Свойства**.
4. В окне «Свойства контейнера ключей» в области «Закрытые ключи» нажмите на кнопку **Добавить...**.
5. Укажите сертификат, соответствующий закрытому ключу в контейнере.
6. Нажмите на кнопку **Открыть**.

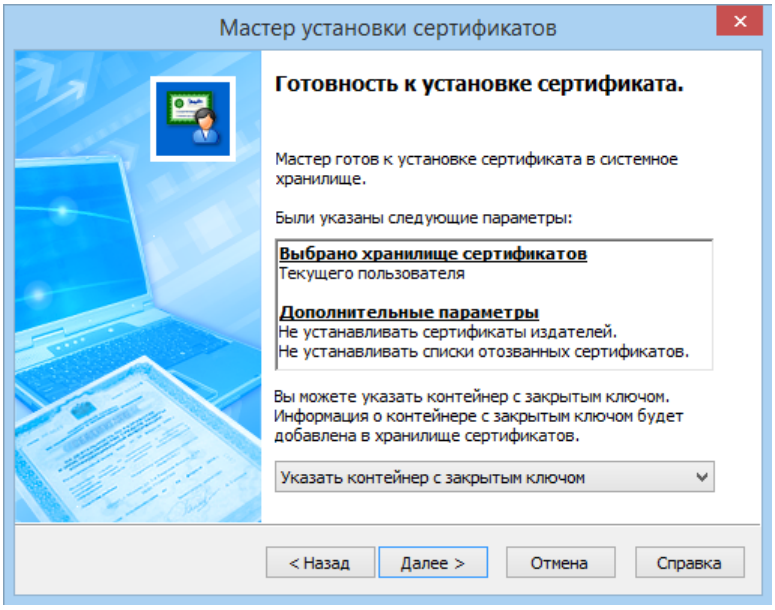
Установка сертификата в системное хранилище

1. Запустите программу ViPNet CSP.
2. Перейдите в раздел **Контейнеры**.
3. В списке контейнеров выберите тот, в который необходимо установить сертификат и нажмите на кнопку **Свойства**.
4. В окне «Свойства контейнера ключей»:
   - в области «Закрытые ключи» выберите необходимый закрытый ключ;
   - нажмите на кнопку **Сертификат**.
5. В окне «Сертификат» на вкладке «Общие» нажмите на кнопку **Установить сертификат**. Запустится мастер установки сертификатов.
6. В окне приветствия нажмите на кнопку **Далее >**.
7. В окне «Выбор хранилища сертификатов»:



   - установите флажок **Текущего пользователя**;
   - нажмите на кнопку **Далее >**.

8. В окне «Готовность к установке сертификата»:



- в выпадающем списке укажите одно из значений:

  Указать контейнер с закрытым ключом – для указания контейнера вручную;

  Найти контейнер с закрытым ключом – для автоматического поиска контейнера.

- нажмите на кнопку **Далее >**.

9. Укажите контейнер с закрытым ключом или выберите найденный системой контейнер в зависимости от указанного значения на предыдущем этапе и нажмите на кнопку **ОК**.
10. В окне завершения работы мастера нажмите на кнопку **Готово**.

Установка и настройка КриптоПро ЭЦП Browser plug-in

Программа КриптоПро ЭЦП Browser plug-in предназначена для создания и проверки электронной подписи на веб-страницах.

Программа необходима независимо от того, какое средство СКЗИ используется: КриптоПро CSP или ViPNet CSP.

Чтобы установить КриптоПро ЭЦП Browser plug-in:

1. Скачайте программу установки на сайте www.cryptopro.ru/products/cades/plugin/get.
2. Запустите файл установки.
3. В сообщении о том, что для корректной работы КриптоПро ЭЦП Browser plug-in необходимо перезапустить браузер, нажмите на кнопку **ОК**.

Чтобы при работе с сертификатами у пользователя не запрашивались подтверждения, необходимо добавить веб-клиент Synerdocs в список надежных узлов. Для этого:

1. Откройте **Настройки ЭЦП Browser plug-in**.

   Если используется ОС Windows 7 и ниже, это можно сделать, последовательно выбрав пункты меню **Пуск**, **Крипто-Про** и **Настройки ЭЦП Browser plug-in**. Откроется форма настройки.

   Настройки рекомендуется открывать через браузер, с разрешением на их изменение.
2. В поле **Добавить узел** введите значение https://client.synerdocs.ru/ и последовательно нажмите на кнопки **Добавить** и **Сохранить**. В поле **Список доверенных узлов** отобразится введенное значение.

Настройка Internet Explorer

При открытии веб-клиента Synerdocs в Internet Explorer в верхней части страницы появится предупреждение о том, что для веб-узла нужна настройка. При этом авторизация по сертификату в сервисе Synerdocs будет недоступна.

Для настройки работы Internet Explorer:

1. Последовательно выберите пункты меню **Сервис** и **Свойства браузера**.
2. Перейдите на вкладку «Безопасность».
3. Перейдите в раздел «Надежные сайты» и нажмите на кнопку **Сайты**.
4. Добавьте в список веб-сайтов узел https://client.synerdocs.ru/.

В результате настройки предупреждение больше не будет открываться в окне браузера и будет доступна авторизация по сертификату.

Настройка Mozilla Firefox

Для настройки работы Mozilla Firefox:

1. На панели инструментов браузера нажмите на кнопку **Дополнения**. Откроется вкладка «Управление дополнениями».
2. Перейдите в раздел **Плагины** и для CryptoPro CAdeS NPAPI Browser Plug-in установите значение **Всегда включать**: