

КриптоПро CSP 4.0

Инструкция по установке

КриптоПро CSP - это криптопровайдер. Криптопровайдером называется независимый модуль в операционной системе, позволяющий осуществлять криптографические операции, такие как, создание электронной подписи, шифрование и имитозащита. Большинство известных программ для подписи и шифрования работают в связке с криптопровайдером и не могут ничего подписать при его отсутствии.

КриптоПро CSP - это СКЗИ (Средство криптографической защиты информации). СКЗИ необходимый программный компонент для сдачи электронной отчетности в государственные органы, участия в электронных торговых площадках, организации юридически значимого электронного документооборота и защиты конфиденциальной информации при передаче их по каналам связи.

Разработчиком КриптоПро CSP является компания "КРИПТО-ПРО", занимающая лидирующее положение на отечественном рынке программных СКЗИ. На сегодняшний день есть сразу три разные версии КриптоПро CSP: 3.6, 3.9 и 4.0. Они различаются между собой по поддерживаемым операционным системам, поддерживаемым криптографическим алгоритмам и срокам действия сертификатов соответствия, выдаваемых ФСБ России. На сайте "КРИПТО-ПРО" размещены таблицы сравнений версий, там также доступна информация о действующих сертификатах соответствия.

Рассмотрим процесс установки КриптоПро CSP на примере 4-й версии. Почему мы выбрали КриптоПро CSP 4.0? Все просто, это последняя из выпущенных версий, она поддерживает новые алгоритмы подписи ГОСТ Р 34.10-2012, которые приходят в замен устаревающим ГОСТ Р 34.10-2001. Работает на Windows 10, что востребовано для тех, кто уже перешел на "десятку" или планирует на будущее. К сожалению, КриптоПро CSP 4-й версии до сих пор не сертифицирована, и для загрузки доступна только предварительная версия. Но в компании утверждают, что сертификация продукта вот-вот будет завершена.

Скачать дистрибутив программы можно на сайте "КРИПТО-ПРО" после предварительной регистрации.



КРИПТО-ПРО

Ключевое слово в защите информации

Поиск

О компании | Продукты | Услуги | Партнёры | Поддержка | Приобретение | Загрузка | Блог | Форум

Главная

Как загрузить дистрибутив?

ДОСТУП ОГРАНИЧЕН: Получение дистрибутивов возможно только после [предварительной регистрации](#). Если вы являетесь зарегистрированным пользователем, [войдите под вашей учётной записью](#) и повторите действие.

Получение дистрибутивов возможно только после [предварительной регистрации](#). Если вы являетесь зарегистрированным пользователем, [войдите под вашей учётной записью](#) и повторите действие.

Для штатной эксплуатации средств криптографической защиты информации (СКЗИ), к которым относятся КристоПро CSP и КристоПро JCP, эти средства должны быть установлены с дистрибутива, полученного у производителя или у [официального дилера](#) на материальном носителе.

Купить



Вход

Имя пользователя: *

Пароль: *

Вход

[Регистрация](#)

[Вход для дилеров](#)

[Забыли пароль?](#)

После регистрации вы увидите страницу с лицензионным соглашением. Ознакомившись с правилами и условиями нажмите внизу экрана кнопку "Я согласен" для перехода в раздел загрузки дистрибутивов.

Главная > Продукты > СКЗИ КристоПро CSP

КристоПро CSP - Загрузка файлов

Предварительные несертифицированные версии (с поддержкой Microsoft Windows 10)

[КристоПро CSP 4.0 для Windows и UNIX \(несертифицированный\)](#)

[КристоПро CSP 3.9 R2 для Windows, UNIX и Apple OS X \(несертифицированный\)](#)

[КристоПро CSP для Google Android \(несертифицированный\)](#)

СКЗИ КристоПро CSP

Использование

КристоПро TLS

Совместимость реализаций TLS

КристоПро EAP-TLS

КристоПро Winlogon

Считыватели

Библиотека считывателей

Загрузка файлов

История версий

Выбрав вариант "КристоПро CSP 4.0 для Windows и UNIX (несертифицированный)" вы увидите ссылку на дистрибутив "КристоПро CSP 4.0 для Windows" над информацией с его контрольной суммой. Нажмите ЛКМ, чтобы начать загрузку.

Для Windows:

> [КристоПро CSP 4.0 для Windows](#)

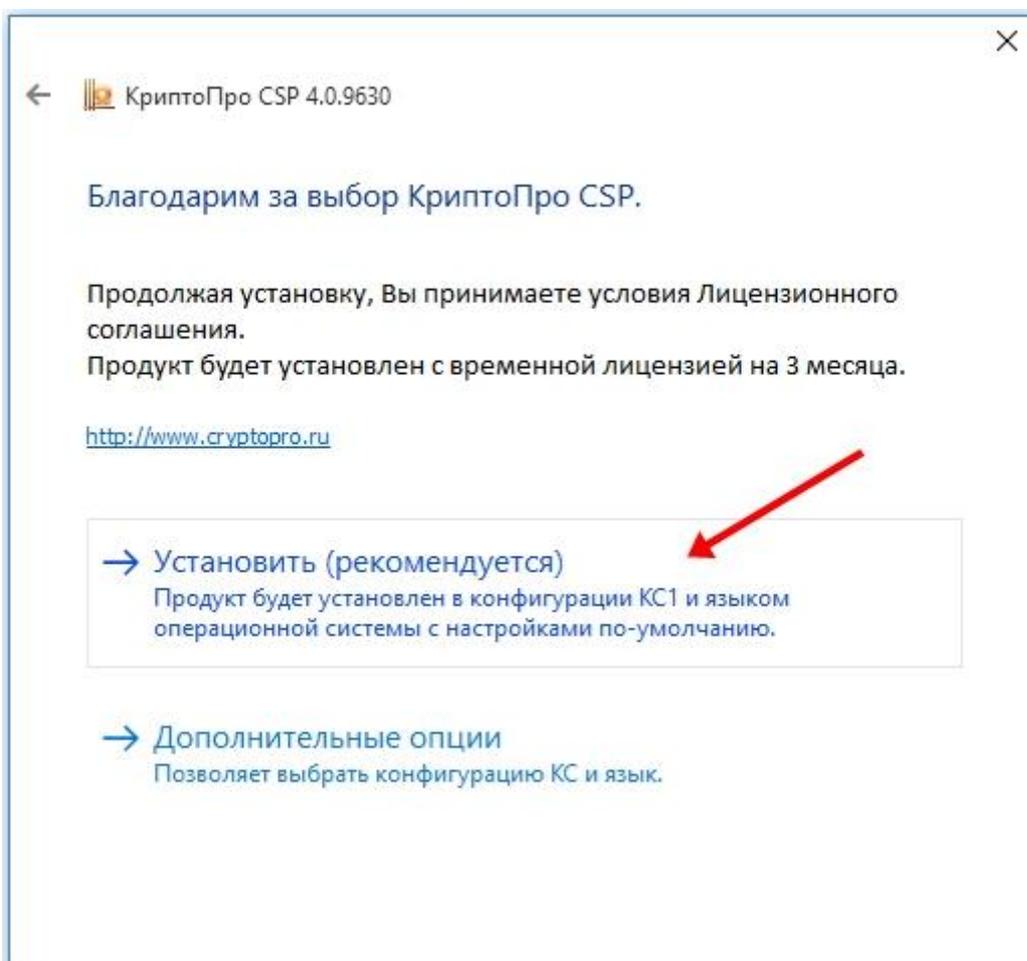
Контрольная сумма
ГОСТ: 60FA86EC16543BD860FBD36AFBAF3768F322CC118CE97C2505283DCA2A376801
MD5: f3b4f2e787279333ec79b05a8a44a0e

универсальный установщик (настройки, ключи и сертификаты при обновлении сохраняются)

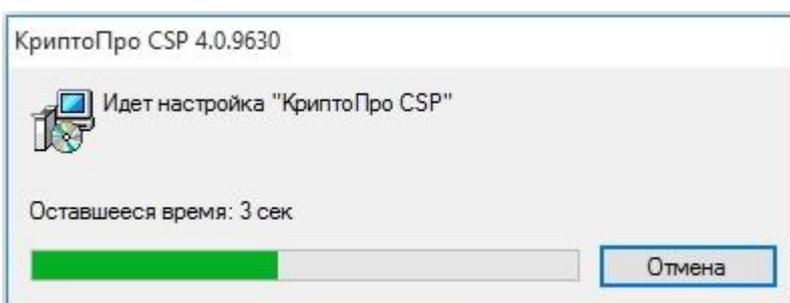
— ▶ Дистрибутивы в формате Windows Installer для автоматизации установки:

Процесс загрузки и установки предельно прост. Кликаем по ссылке на дистрибутив и ждем, загрузка начинается автоматически. При ее завершении запустите загруженный файл CSPSetup.exe.

Во всплывающем окне предупреждения системы безопасности необходимо нажать на кнопку «Да» чтобы разрешить программе внести изменения на компьютере. Далее выбираем установку программы.

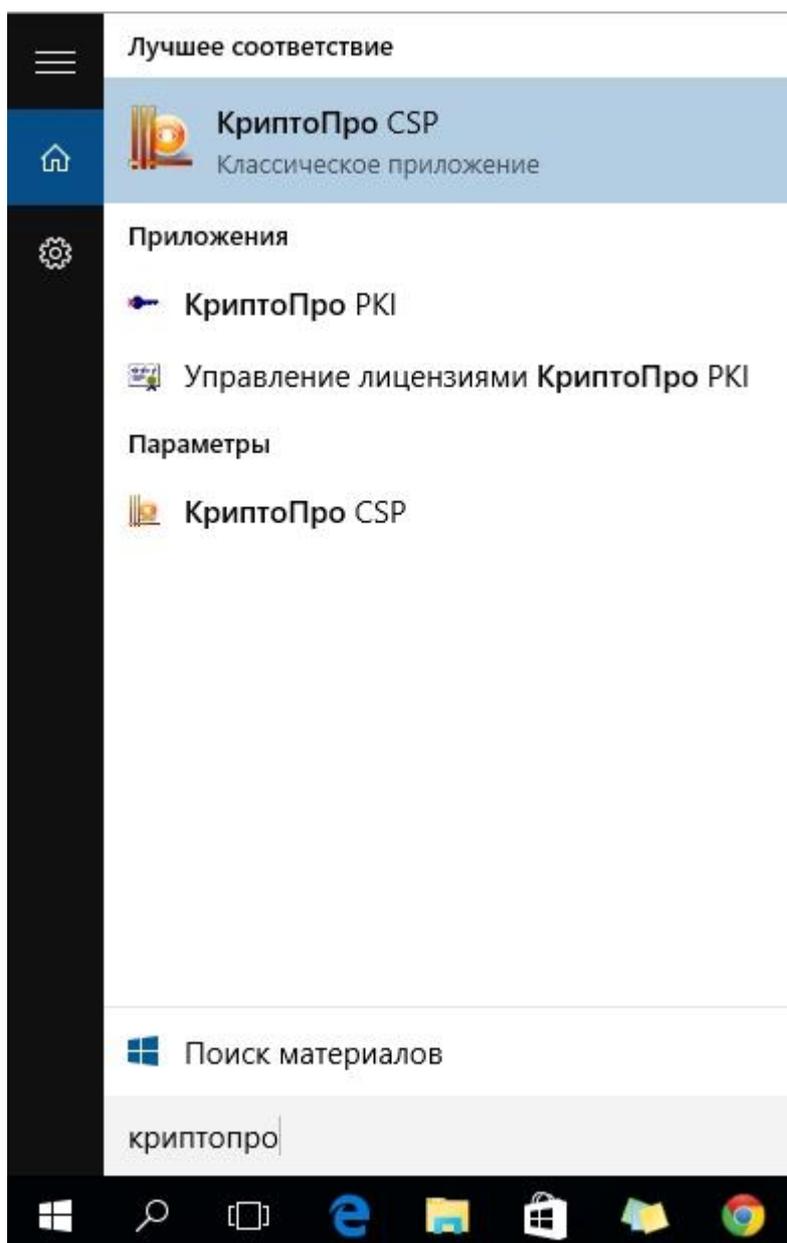


Сама установка проходит меньше чем за 30 секунд и не требует участия пользователя.

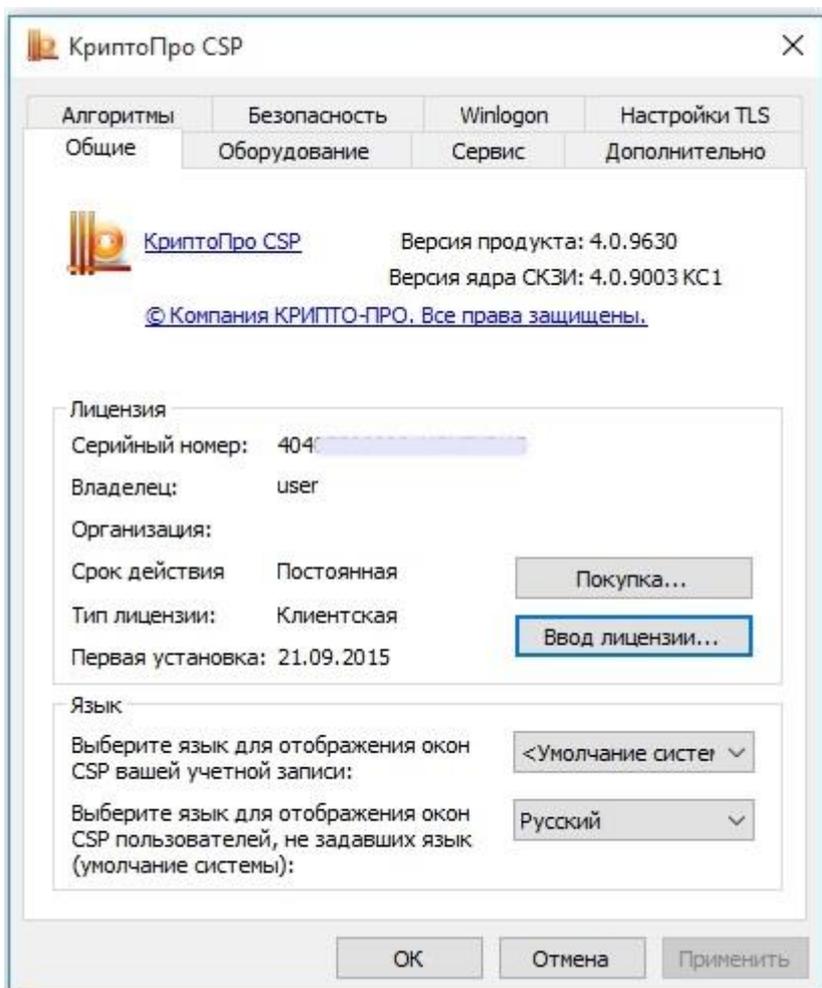


Программа установлена. Можно ли начать с ней работать? По условиям лицензионного соглашения срок использования демонстрационной версии КриптоПро CSP ограничен 90 днями с момента установки. Важное уточнение, демонстрационный период предоставляется лишь при первой установке программы на компьютере, при повторных установках получить его невозможно.

Чтобы посмотреть информацию о типе лицензии и сроке действия, откройте приложение КриптоПро CSP. В Windows 10 удобно воспользоваться поиском приложений (значок "Лупа" справа от кнопки "Пуск"), наберите "криптопро" и выберите КриптоПро CSP.



Во вкладке "Общие" КриптоПро CSP обратите внимание блок "Лицензия". В левой ее части указываются серийный номер (не полностью), имя владельца лицензии, название организации, срок действия, тип лицензии (клиентская либо серверная) и дата первой установки.



Инструкция по установке сертификата

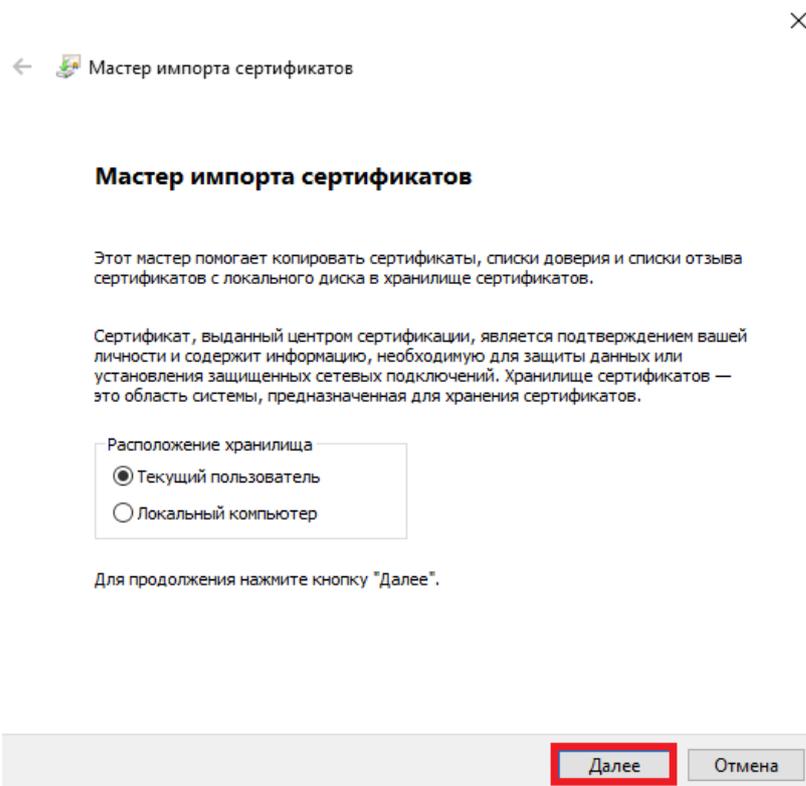
Чтобы установить сертификат, выполните следующие действия:

Нажмите на контейнер сертификата.

Имя	Дата изменения	Тип	Размер
 Сертификат	18.11.2019 13:01	Файл обмена ли...	5 КБ

Тип: Файл обмена личной информацией
Размер: 4,38 КБ
Дата изменения: 18.11.2019 13:01

Откроется «Мастер импорта сертификатов». Выбираем расположение хранилища и нажимаем кнопку «далее».



В следующем окне будет расположен адрес данного сертификата, нажимаем кнопку «далее».

×

←  Мастер импорта сертификатов

Импортируемый файл
Укажите файл, который вы хотите импортировать.

Имя файла:

Замечание: следующие форматы файлов могут содержать более одного сертификата в одном файле:

- Файл обмена личной информацией - PKCS #12 (.PFX, .P12)
- Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)
- Хранилище сериализованных сертификатов (.SST)

Если у закрытого ключа был установлен пароль, вам необходимо ввести его и нажать кнопку «далее».

×

←  Мастер импорта сертификатов

Защита с помощью закрытого ключа
Для обеспечения безопасности закрытый ключ защищен паролем.

Введите пароль для закрытого ключа.

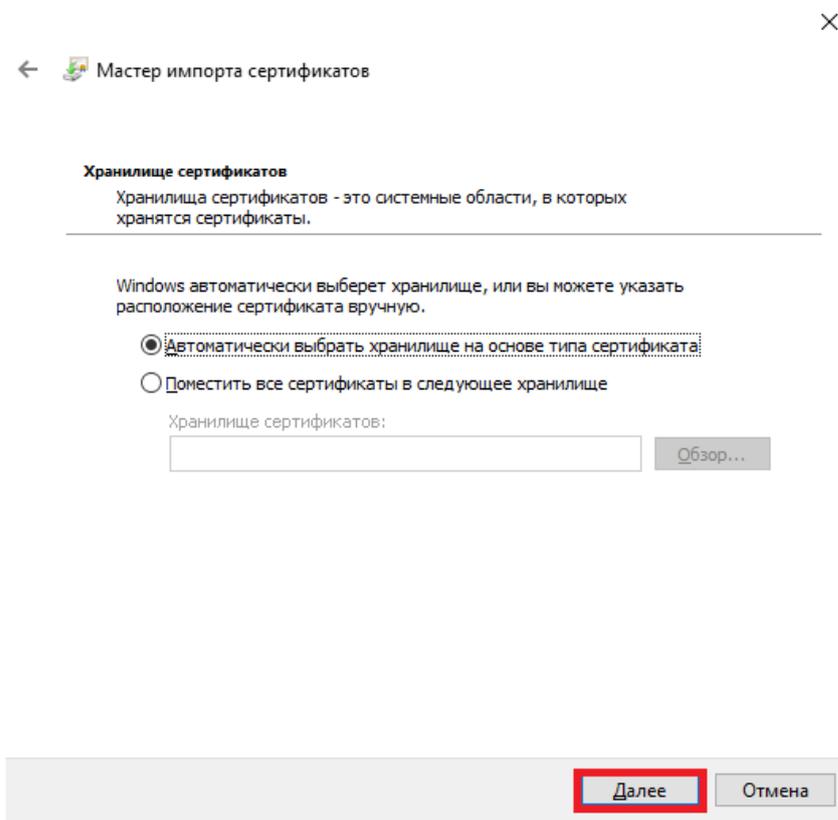
Пароль:

Показывать пароль

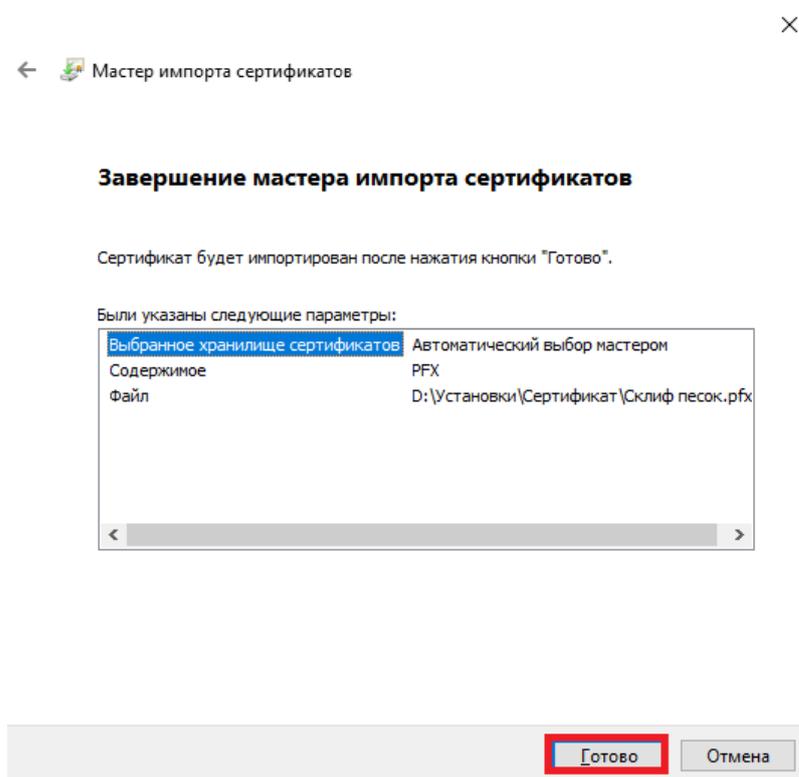
Параметры импорта:

- Включить усиленную защиту закрытого ключа. В этом случае при каждом использовании закрытого ключа приложением будет запрашиваться разрешение.
- Пометить этот ключ как экспортируемый, что позволит сохранять резервную копию ключа и перемещать его.
- Защита закрытого ключа с помощью безопасной виртуализации (неэкспортируемый)
- Включить все расширенные свойства.

В следующем окне оставьте переключатель на пункте «Автоматически выбрать хранилище на основе типа сертификата» и нажмите «Далее». Сертификат будет установлен в хранилище «Личные».



Видим перечень указанных параметров, нажимаем кнопку «Готово»



Импорт успешно выполнен. Нажимаем кнопку «Ок».

