

Создание рабочего места Администратора ОО

Для начала работы в системе «Единая Точка Доступа» (далее – ЕТД) необходимо придерживаться организационно-технических рекомендаций для рабочего места Администратора на компьютере:

1. Обязательно наличие одного из браузеров, поддерживающих установку защищенных соединений по алгоритмам ГОСТ (**Chromium-Gost** или **Яндекс.Браузер**), не старше последних трех версий.
2. Наличие установленного криптопровайдера КриптоПРО CSP.
3. Наличие установленных сертификатов ФГИС «Моя школа».



Установка браузера.

Для установки браузера **Chromium-Gost** необходимо перейти на портал разработчика: <https://www.cryptopro.ru/products/chromium-gost/>. Далее нажать кнопку «Скачать». В открывшемся окне выбрать нужный дистрибутив, в соответствии с операционной системой. Затем произвести скачивание и установку на компьютер.

Для установки **Яндекс.Браузера** необходимо перейти на портал разработчика: <https://browser.yandex.ru/>. Затем произвести скачивание и установку на компьютер.



Установка криптопровайдера КриптоПРО CSP.

Для установки криптопровайдера КриптоПРО CSP необходимо перейти на портал разработчика: <https://cryptopro.ru/products/csp/downloads/> и пройти авторизацию/регистрацию на портале.

Профиль пользователя

[Вход](#) [Регистрация](#) [Забыли пароль?](#)

Е-mail: *

Enter your e-mail address.

Пароль / Password: *

Enter the password that accompanies your e-mail.

[Вход](#)

В открывшемся окне требуется ознакомиться с лицензионным соглашением КристоПРО и нажать кнопку **Я согласен**.

КристоПро CSP

Срок использования демонстрационной версии КристоПро CSP ограничен 90 днями с момента установки.

Передача прав на использование программного обеспечения производства ООО "КРИПТО-ПРО" осуществляется на основании Лицензионного соглашения.

Лицензии на использование продукта необходимо приобретать в ООО "КРИПТО-ПРО" или у официального дилера.

Лицензии на право использования программного обеспечения оформляются на бумажном носителе формата А4.

Предупреждение.

Для штатной эксплуатации средств криптографической защиты информации (СКЗИ) они должны быть установлены с дистрибутива.

Дистрибутив может быть:

1. Приобретен у производителя или у официального дилера производителя на материальном носителе.
2. Получен с сайта производителя или официального дилера.

Порядок получения дистрибутива с сайта:

Вместе с дистрибутивами СКЗИ на странице загрузки размещаются контрольные суммы установочных модулей и документации. Контрольные суммы рассчитываются в соответствии с ГОСТ Р 34.11-94 с учетом RFC 4357, а так же md5.

Установка СКЗИ на рабочее место пользователя может быть осуществлена только в случае подтверждения целостности полученных установочных модулей СКЗИ и эксплуатационной документации.

Проверка должна быть осуществлена с помощью утилиты `cpverify.exe` (<http://www.cryptopro.ru/sites/default/files/public/cpverify.exe>), входящей в состав СКЗИ «КристоПро CSP» `cpverify -mk -alg GR3411_2012_256 <filename>`, либо иным другим сертифицированным ФСБ России шифровальным (криптографическим) средством, реализующим ГОСТ Р 34.11-94.

Контрольная сумма md5 может быть проверена, например, с помощью `md5sum` (linux) или File Checksum Integrity Verifier (<http://support.microsoft.com/kb/841290>).

Использование программного обеспечения регламентируется приведенным ниже Лицензионным соглашением с ООО "КРИПТО-ПРО":

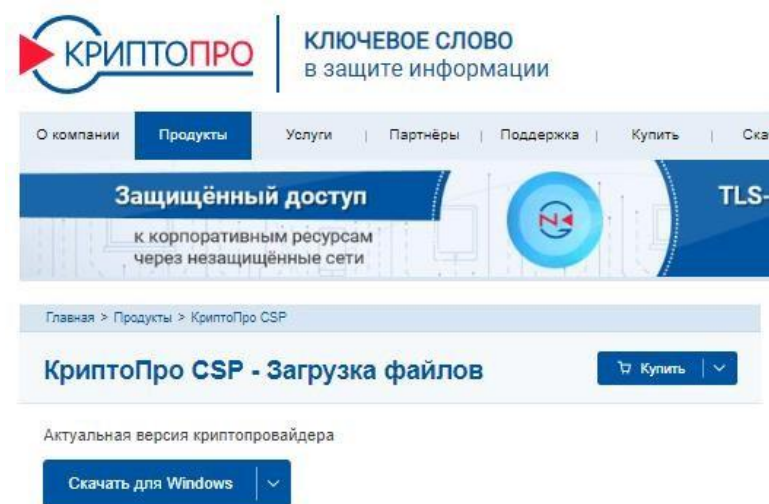
ВНИМАТЕЛЬНО ОЗНАКОМЬТЕСЬ С ЛИЦЕНЗИОННЫМ СОГЛАШЕНИЕМ НА ИСПОЛЬЗОВАНИЕ ИЗДЕЛИЯ

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

1. Исключительные права на программу для ЭВМ, включая документацию в электронном виде, (далее – Изделие) принадлежат ООО «КРИПТО-ПРО», далее – Правообладатель.
2. Настоящее соглашение является офертой ООО «КРИПТО-ПРО» к физическому или юридическому лицу, далее - Пользователь.
3. Пользователь в соответствии с настоящим соглашением получает право использовать Изделие на территории Российской Федерации.
4. Установка Изделия в память ЭВМ рассматривается как безусловное согласие Пользователя с условиями настоящего соглашения.
5. В случае несогласия с каким-либо из условий настоящего соглашения Пользователь не имеет права продолжать установку Изделия в память ЭВМ, а в случае установки Изделия в память ЭВМ обязан удалить Изделие из ЭВМ.

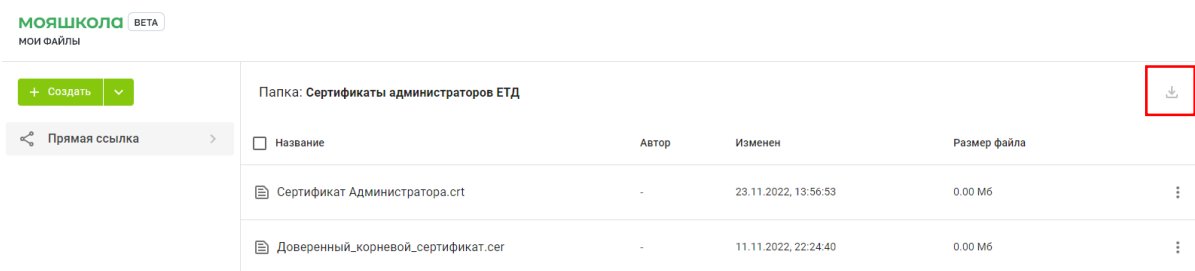
Я согласен с Лицензионным соглашением. Перейти к загрузке.

Далее производим скачивание и установку КристоПРО CSP на компьютер. После установки КристоПРО CSP необходимо **перезагрузить компьютер**.

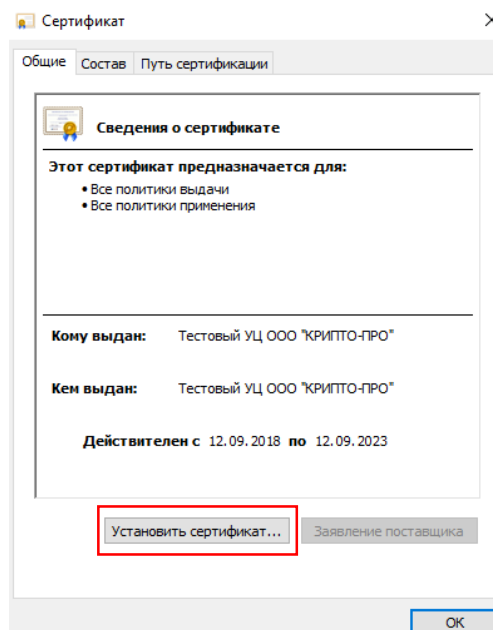


Установка сертификатов.

Для установки **сертификатов** ФГИС «Моя школа» необходимо перейти по ссылке в раздел «Мои Файлы» ФГИС «Моя школа»: <https://docs.myschool.edu.ru/link/A4E886CC16D5B7BF7D4A6F7E2B99D9082A7E798D> и произвести скачивание и установку сертификатов на компьютер.



Для установки **доверенного корневого сертификата** требуется открыть файл с названием «Доверенный_корневой_сертификат.cer», затем нажать кнопку **«Установить сертификат»**.



В окне **«Мастер импорта сертификатов»** выбрать расположение хранилища **«Текущий пользователь»** для установки под текущей учётной записью Windows и нажать кнопку **«Далее»**.

← Мастер импорта сертификатов

Мастер импорта сертификатов

Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.

Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.

Расположение хранилища

☒ Текущий пользователь

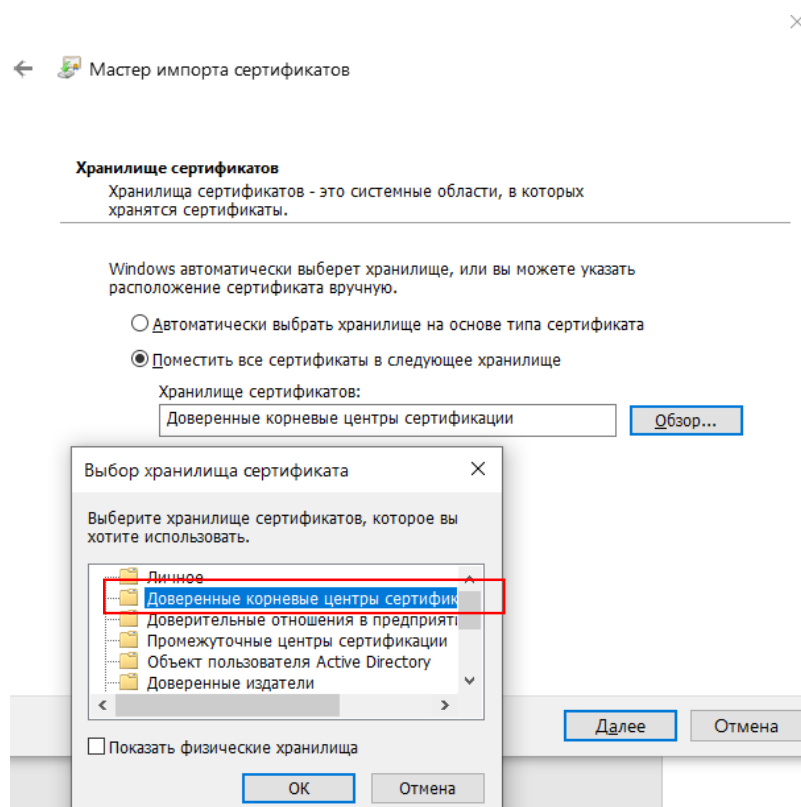
☐ Локальный компьютер

Для продолжения нажмите кнопку "Далее".

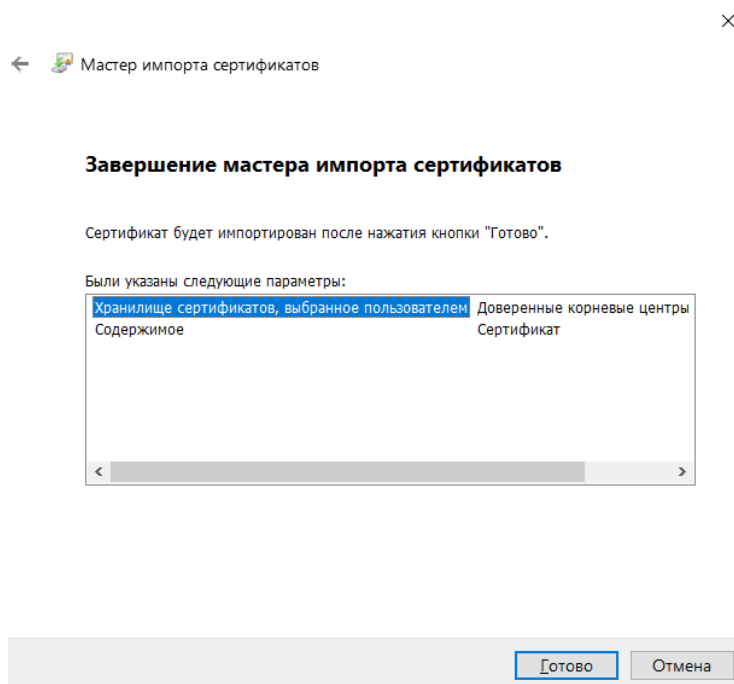
Далее

Отмена

В открывшемся окне выбрать пункт в чекбоксе **«Поместить все сертификаты в следующее хранилище»**, далее нажать **«Обзор»** и выбрать **«Доверенные корневые центры сертификации»**. После выбора хранилища кликнуть кнопку **«ОК»**, затем кнопку **«Далее»**.



В новом окне нажать кнопку «Готово».



Для завершения установки сертификата в окне «Предупреждение системы безопасности» необходимо нажать кнопку «Да».



Будет установлен сертификат от центра сертификации (ЦС), представляющий:

Тестовый УЦ ООО "КРИПТО-ПРО"

Windows не удастся проверить, что сертификат действительно получен от "Тестовый УЦ ООО "КРИПТО-ПРО"". Обратитесь к "Тестовый УЦ ООО "КРИПТО-ПРО"" для подтверждения происхождения сертификата. В ходе этого процесса вам пригодится следующее значение:

Отпечаток (sha1) : 927C1E1E B2B397CB C5D11712 E2E3BBED C876BD7E

Предупреждение:

Если вы установите этот корневой сертификат, Windows будет автоматически доверять любому сертификату, выданному этим ЦС. Установка сертификата с неподтвержденным отпечатком представляет риск для безопасности. Если вы нажмете кнопку "Да", вы принимаете на себя этот риск.

Вы хотите установить этот сертификат?

Да

Нет

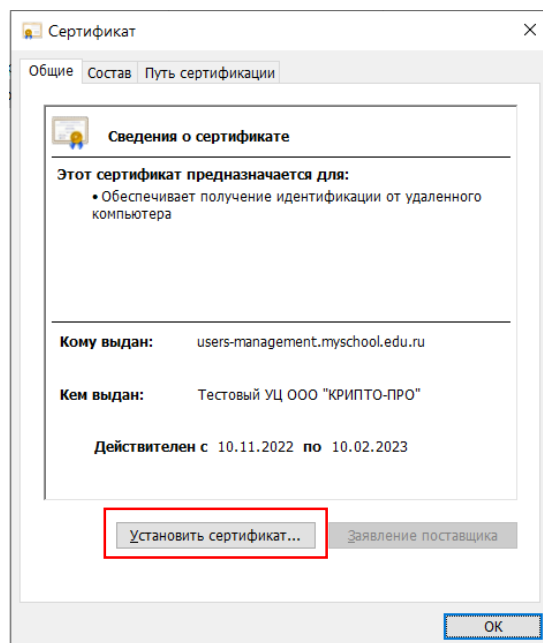
В окне «**Мастер импорта сертификатов**» нажмите кнопку «**ОК**». Сертификат установлен.



Импорт успешно выполнен.

ОК

Для установки **сертификата Администратора** требуется открыть предварительно скачанный на компьютер файл с названием «Сертификат_администратора_Моя_школа.crt». Нажать «**Установить сертификат**».



В окне «**Мастер импорта сертификатов**» выбрать расположение хранилища «**Текущий пользователь**» для установки под текущей учётной записью Windows и нажать кнопку «**Далее**».



Мастер импорта сертификатов

Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.

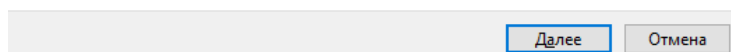
Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.

Расположение хранилища

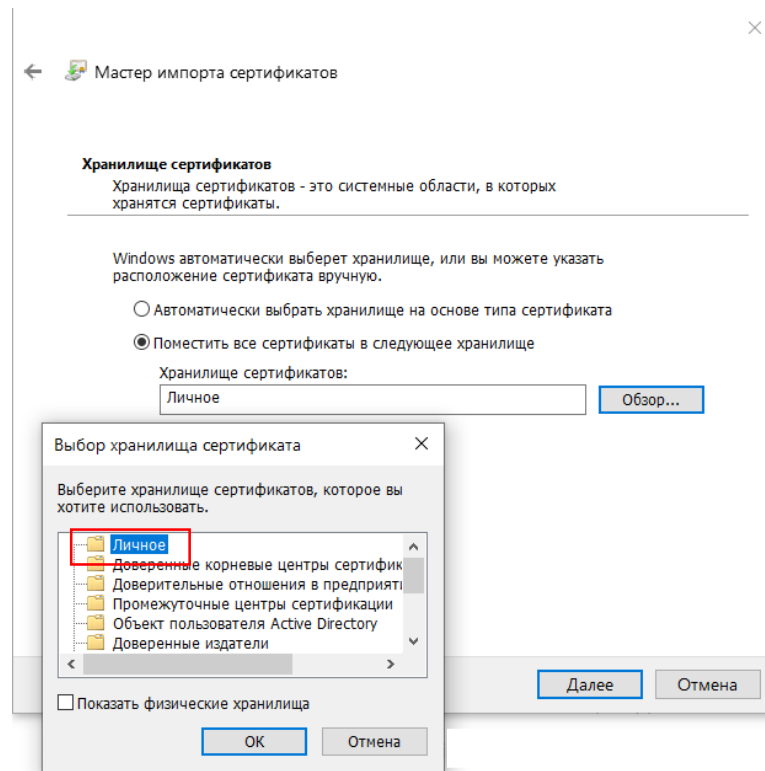
☒ Текущий пользователь

☐ Локальный компьютер

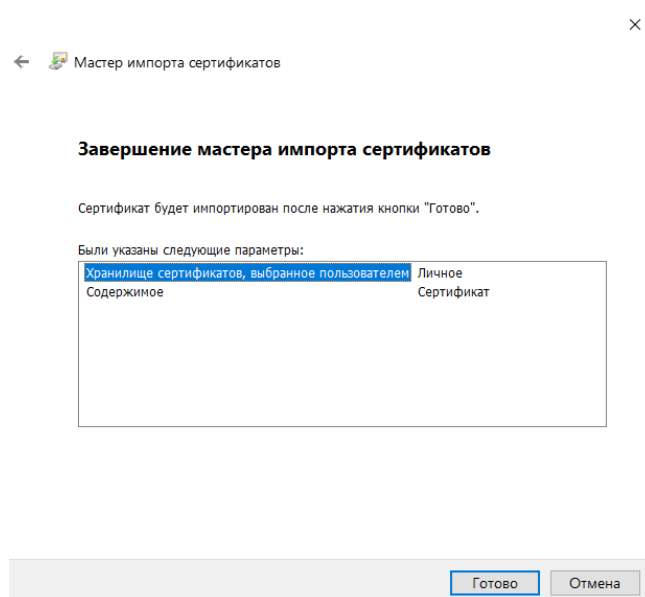
Для продолжения нажмите кнопку "Далее".



В открывшемся окне выбрать пункт в чекбоксе «**Поместить все сертификаты в следующее хранилище**», далее нажать «**Обзор**» и выбрать «**Личные**». После выбора хранилища кликнуть «**ОК**», затем кнопку «**Далее**» и нажать кнопку «**Готово**». В окне «**Мастер импорта сертификатов**» нажмите кнопку «**ОК**». Сертификат установлен.



В новом окне нажать кнопку «Готово».



В окне «Мастер импорта сертификатов» нажмите кнопку «ОК». Сертификат установлен.



Импорт успешно выполнен.

ОК

Для входа в ЕТД необходимо перейти по ссылке: <https://users-management.myschool.edu.ru/> в браузере **Chromium-Gost** или **Яндекс.Браузере**. Чтобы осуществить вход, нажмите кнопку «ESIA (CryptoPRO)» и авторизуйтесь с помощью данных ЕСИА.

Sign in to your account

Имя пользователя или E-mail



Пароль



Вход

Or sign in with

ESIA (CryptoPRO)

госуслуги

Телефон / Email / СНИЛС

Пароль

Восстановить

Войти

Войти другим способом


Эл. подпись

Не удаётся войти?

Зарегистрироваться

Куда ещё можно войти с
паролем от Госуслуг?

После авторизации в системе осуществляется переход на окно выбора профиля пользователя.

 В ЕТД можно работать только под профилем **Администратора**.

Вход

<input type="radio"/>	Профиль педагогического работника	<input checked="" type="radio"/>	Профиль администратора
<div>Войти</div>			