

Инструкция по установке криптографического программного обеспечения и сертификатов

Версия инструкции 1.11

Москва
2021

Оглавление

Глава 1	Изменения в текущей версии (1.11) инструкции	3
Глава 2	Быстрый старт: краткое руководство по установке криптографического ПО и сертификатов	4
Глава 3	Подготовка к установке криптографического ПО	7
Глава 4	Установка криптографического ПО	8
Глава 5	Установка сертификатов	31
Глава 6	Установка "CryptoEnergyPro"	57
Глава 7	Элементы первичной диагностики проблем	64
Глава 8	Приложение	81

- Изменения в текущей версии (1.11) инструкции
- [Быстрый старт: краткое руководство по установке криптографического ПО и сертификатов](#)
- [Подготовка к установке криптографического ПО](#)
- ✚ [Установка криптографического ПО](#)
- ✚ [Установка сертификатов](#)
- [Установка "CryptoEnergyPro"](#)
- ✚ [Элементы первичной диагностики проблем](#)
- ✚ [Приложение](#)

Прочтите! [Указания по чтению этой инструкции](#)

1. В связи с прекращением с 01.01.2020 технической поддержки коммерческим оператором ОРЭМ (АО "АТС") криптографических сервисов с применением носителей ключей всех моделей eToken, из инструкции исключены все сведения о работе с ключевыми носителями eToken.
2. В раздел "Быстрый старт" добавлен пункт: "Оплатить доступ к ПАК на основании Приложения № 1 к Договору на ПО".



- [Изменения в текущей версии \(1.11\) инструкции](#)

- Быстрый старт: краткое руководство по установке криптографического ПО и сертификатов

- [Подготовка к установке криптографического ПО](#)

- [Установка криптографического ПО](#)

- [Установка сертификатов](#)

- [Установка "CryptoEnergyPro"](#)

- [Элементы первичной диагностики проблем](#)

- [Приложение](#)

Прочтите! [Указания по чтению этой инструкции](#)

Введение.

В данном разделе руководства приводится описание установки криптографического ПО и сертификатов "с нуля", то есть установки на компьютер, на котором отсутствует криптографическое ПО и сертификаты. Однако, в ситуации, когда вы (сотрудник Участника) получили новый сертификат в ключевом носителе "Рутокен", вам понадобится только [установить новый сертификат в хранилище "Личное"](#) на своем компьютере. В дальнейшем вам понадобится [установить в соответствующие хранилища актуальные корневые сертификаты из полученного в УЦ АО "АТС" ключевого носителя Рутокен](#). Поэтому необходимо [установить утилиту "Панель управления Рутокен"](#) (утилиту поддержки ключевых носителей "Рутокен"). Кроме того, "Панель управления Рутокен" предоставляет вам дополнительные возможности: присваивание [ключевому носителю индивидуального имени и изменение pin-кода ключевого контейнера](#).

Замечание: при установке утилиты "Панель управления Рутокен" не требуется удалять ранее установленное криптографическое ПО.

Установка криптографического ПО и сертификатов "с нуля".

Чтобы приступить к работе с программами АО "АТС":

- АРМ Участника,
- CryptoSendMail,
- АРМ КУ,
- Криптораздел сайта АО "АТС",

Участник должен выполнить следующие действия, предшествующие установке криптографического ПО и сертификатов:

1. Заключить с АО "АТС" Договор оказания услуг удостоверяющего центра (УЦ) и приобрести в УЦ АО "АТС" необходимое Участнику количество ключей электронно-цифровой подписи (ЭЦП) на носителях USB Рутокен. Перечень документов, необходимый для заключения Договора и получения ключей, доступен на сайте АО "АТС" в разделе "Удостоверяющий центр": Главная -> Электронный документооборот -> Удостоверяющий центр -> [Регламентирующие документы УЦ АО "АТС"](#).

2. Оплатить доступ к ПАК на основании Приложения № 1 к Договору на ПО.

3. Получить в Департаменте допуска АО "АТС" логин и пароль для доступа в раздел "Программные продукты сайта АО "АТС": [Вход в раздел "Программные продукты"](#).

4. Скачать из раздела "Программные продукты" сайта АО "АТС" дистрибутивы программ АО "АТС":

Главная -> Электронный документооборот -> [Программные продукты](#).

Примечание: по этой ссылке вы попадете на страницу "Авторизация". Вы можете использовать для входа на страницу "Программные продукты" как логин и пароль, так и свой личный сертификат, полученный в УЦ АО "АТС".

5. На компьютере, на котором установлена ОС Windows 7 или Windows 10, установить криптографическое ПО и сертификаты (в последовательности, указанной ниже).



- [Изменения в текущей версии \(1.11\) инструкции](#)
- Быстрый старт: краткое руководство по установке криптографического ПО и сертификатов
- [Подготовка к установке криптографического ПО](#)
- ✚ [Установка криптографического ПО](#)
- ✚ [Установка сертификатов](#)
- Установка "CryptoEnergyPro"
- ✚ [Элементы первичной диагностики проблем](#)
- ✚ [Приложение](#)

Установка криптографического ПО и сертификатов.

Замечание: ниже приводится краткое описание [первичной установки](#) криптографического ПО и сертификатов. Если требуется выполнить обновление модулей криптографического ПО, то сначала [удалите уже установленное ПО](#).

1. Установите утилиту поддержки (драйвер) USB ключевого носителя "Рутокен" ("[Панель управления Рутокен](#)") для всех версий ОС Windows.

2. Установите систему криптографической защиты информации (СКЗИ) "КриптоПро CSP 4.0":

Внимание! Коммерческий оператор ОПЭМ (АО "АТС") не предоставляет Участникам лицензионное ПО "КриптоПро CSP".

Скачайте дистрибутив "КриптоПро CSP 4.0" с [сайта производителя](#) или официального дилера производителя.

Описание скачивания дистрибутива "КриптоПро CSP 4.0" и установки "КриптоПро CSP 4.0" смотрите в разделах "[Получение файла дистрибутива КриптоПро CSP 4.0](#)" и "[Установка "КриптоПро CSP" из файла](#)".

3. Выполните настройку "КриптоПро CSP" для работы с ключевым носителем "Рутокен".

Описание настройки смотрите в разделе "[Настройка "КриптоПро CSP"](#)".

При настройке рекомендуется [изменить pin-код контейнера ключевого носителя](#), полученного в АО "АТС".

4. Установите в хранилище сертификатов "Доверенные корневые центры сертификации" ("Trusted Root Certification Authorities")

корневые сертификаты Головной удостоверяющий центр и Минкомсвязь России за 2017-2019 годы, и корневые сертификаты УЦ АО "АТС" за 2011-2015 годы,

а также в хранилище "Промежуточные центры сертификации" ("Intermediate Certification Authorities") корневые сертификаты

АО АТС за 2017-2018 годы, УЦ 1 ИС ГУЦ и УЦ ОАО АТС за 2016 год одним из двух способов:

а) Из ключевого носителя "Рутокен" (рекомендуется для актуальных сертификатов за 2018-2019 годы).

Смотрите раздел "Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "[Панель управления Рутокен](#)" (все версии Windows)".

б) Из файлов, скачанных с сайта [АО "АТС"](#)

("Главная -> [Электронный документооборот](#) -> Удостоверяющий центр -> [Корневые сертификаты удостоверяющих центров](#)").

Смотрите раздел "[Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)".

- [Изменения в текущей версии \(1.11\) инструкции](#)
- Быстрый старт: краткое руководство по установке криптографического ПО и сертификатов
- [Подготовка к установке криптографического ПО](#)
- + [Установка криптографического ПО](#)
- + [Установка сертификатов](#)
- Установка "CryptoEnergyPro"
- + [Элементы первичной диагностики проблем](#)
- + [Приложение](#)

5. Установите в локальное хранилище сертификатов "Личные" на компьютере пользователя личный сертификат Участника (из контейнера в ключевом носителе "Рутокен").
Смотрите описание установки личного сертификата Участника в разделе "[Установка личного сертификата закрытого ключа пользователя](#)".
6. Установите в локальное хранилище сертификатов "Другие пользователи" на компьютере пользователя сертификаты открытых ключей АО "АТС" (скачайте файлы сертификатов с сайта [АО "АТС"](#)).
Пошаговое описание установки сертификатов открытых ключей АО "АТС" смотрите в разделе "[Установка сертификатов открытых ключей АО "АТС"](#)".
7. Скачайте файл установки "CryptoEnergyPro" из раздела "Программные продукты" ("Главная->Электронный документооборот->[Программные продукты](#)") сайта АО "АТС" и установите "CryptoEnergyPro" в соответствии с описанием установки в разделе "[Установка "CryptoEnergyPro"](#)".
8. Установите нужные вам программы АО "АТС" в соответствии с инструкциями по установке этих программ.
Инструкции по установке программ АО "АТС" содержатся в руководствах пользователя по этим программам (для АРМ КУ в руководстве администратора).
9. Проверьте наличие необходимых "своих" и "чужих" сертификатов в списках выбора сертификатов в программах АО "АТС".
Если нужный вам сертификат (например, сертификат контрагента) отсутствует, установите его в соответствующее типу сертификата хранилище.

- [Изменения в текущей версии \(1.11\) инструкции](#)
- [Быстрый старт: краткое руководство по установке криптографического ПО и сертификатов](#)
- Подготовка к установке криптографического ПО
- + [Установка криптографического ПО](#)
- + [Установка сертификатов](#)
- [Установка "CryptoEnergyPro"](#)
- + [Элементы первичной диагностики проблем](#)
- + [Приложение](#)

Виды установки: первичная и обновление.

Первичная установка

Первичной установкой называется установка криптографического ПО на компьютер, на котором такого ПО никогда не было или оно было корректно удалено. Первичная установка описывается в разделах:

- "Быстрый старт: краткое руководство по установке криптографического ПО и сертификатов",
- "Первичная установка" (пошаговое описание процедур установки модулей ПО и сертификатов).

Обновление

Обновлением называется замена версии модуля криптографического ПО на другую версию.

ПО "КриптоПро CSP 4.0" можно устанавливать поверх (без предварительного удаления) текущей версии этого модуля.

Замена модуля поддержки (драйвера) eToken на модуль поддержки Рутокен и обновление модуля "CryptoEnergyPro" выполняется в следующей последовательности:

1. Удаление текущих версий модулей криптографического ПО

Удаление модулей выполняется через "Панель управления": "Панель управления->Установка и удаление программ":

Примечание: значки  и  расположены в левом нижнем углу экрана.

Windows 7



-> **Панель управления** -> **Программы и компоненты** -> выберите модуль криптографического ПО ->

нажмите кнопку **Удалить** в верхней части списка программ или правой кнопкой мыши откройте контекстное меню -> выберите **"Удалить"**.

Windows 10



-> правой кнопкой мыши откройте меню -> выберите **Control Panel** ("Панель управления") -> откройте раздел



Programs and Features («Программы и компоненты») -> выберите модуль криптографического ПО ->

нажмите кнопку **"Uninstall"** ("Удалить") или правой кнопкой мыши откройте меню и выберите в нем **"Uninstall"** ("Удалить").

После удаления модулей перезагрузите компьютер.

2. Установка новых версий модулей криптографического ПО

Перед обновлением "CryptoEnergyPro" может потребоваться переустановить корневые сертификаты, входящие в "цепочку доверия" личных сертификатов, выданных сотрудникам Участника удостоверяющим центром АО "АТС". После обновления версии "КриптоПро CSP" необходимо выполнить его настройку (смотрите раздел "[Настройка "КриптоПро CSP"](#)").

Смотрите раздел "[Установка криптографического ПО](#)"

• Установка драйвера РУТОКЕН для Windows

Установите утилиту (системную программу) "Панель управления ключевыми носителями РУТОКЕН":



для Windows, установленной на вашем компьютере (поддерживаются версии Windows 10/8.1/2012R2/8/2012/7/2008R2/Vista/2008/XP/2003). Смотрите в конце этого раздела руководства [краткий обзор возможностей утилиты "Панель управления ключевыми носителями РУТОКЕН"](#). Перед началом установки драйвера закройте все запущенные приложения. Убедитесь, что вы обладаете достаточными правами для установки ПО и записи информации в реестр (рекомендуется выполнять установку с правами локального администратора, пароль локального администратора должен быть непустой). Выполняйте установку локально на компьютере, а не через клиента удаленного доступа.

Получение файла установки комплекта драйверов для Windows.

Файл установки комплекта драйверов для Windows содержит:

- набор драйверов для ключевых носителей "Рутокен S" для всех версий Windows (32- и 64-разрядные Microsoft Windows 10/8.1/2012R2/8/2012/7/2008R2/Vista/2008/XP/2003).

- утилиту поддержки всех типов носителей "Рутокен" (панель управления "Рутокен").

Замечание: Для работы в СКЗИ КриптоПро CSP 4.0 с ключевыми носителями "Рутокен" всех типов, кроме "Рутокен S", установка комплекта драйверов не является обязательной. Тем не менее, установить панель управления "Рутокен" необходимо, так как эта утилита позволяет пользователю УЦ АО "АТС" установить корневые сертификаты из ключевого носителя, полученного в УЦ "АО АТС", в хранилища "Доверенные корневые центры сертификации" и "Промежуточные центры сертификации". Несмотря на то, что существует альтернативный способ установки корневых сертификатов путем скачивания с сайта АО "АТС" файлов с корневыми сертификатами, и последующей установки этих сертификатов из файлов, рекомендуется установка актуальных корневых сертификатов из ключевого носителя, как более безопасный для пользователя способ.

Программа установки драйверов автоматически определяет архитектуру и версию Windows, под которой выполняется установка драйверов, и устанавливает нужные версии драйверов. Поэтому в данной инструкции не описывается отдельно установка драйверов для каждой версии Windows.

Файл установки драйверов для Windows можно скачать с сайта ["https://www.rutoken.ru"](https://www.rutoken.ru) (главная страница сайта) компании "Актив".

Для этого выполните следующую последовательность шагов:

1 На главной странице сайта щелкните мышью ссылку "Центр загрузки" (рис. 1):

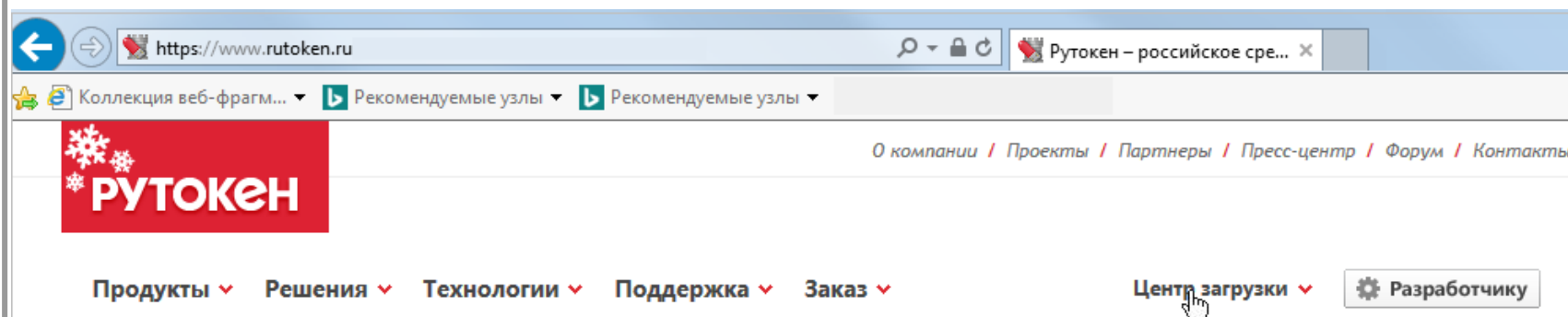


Рис. 1

- Установка драйвера РУТОКЕН для Windows

Откроется раздел сайта "Центр загрузки" (рис. 2):

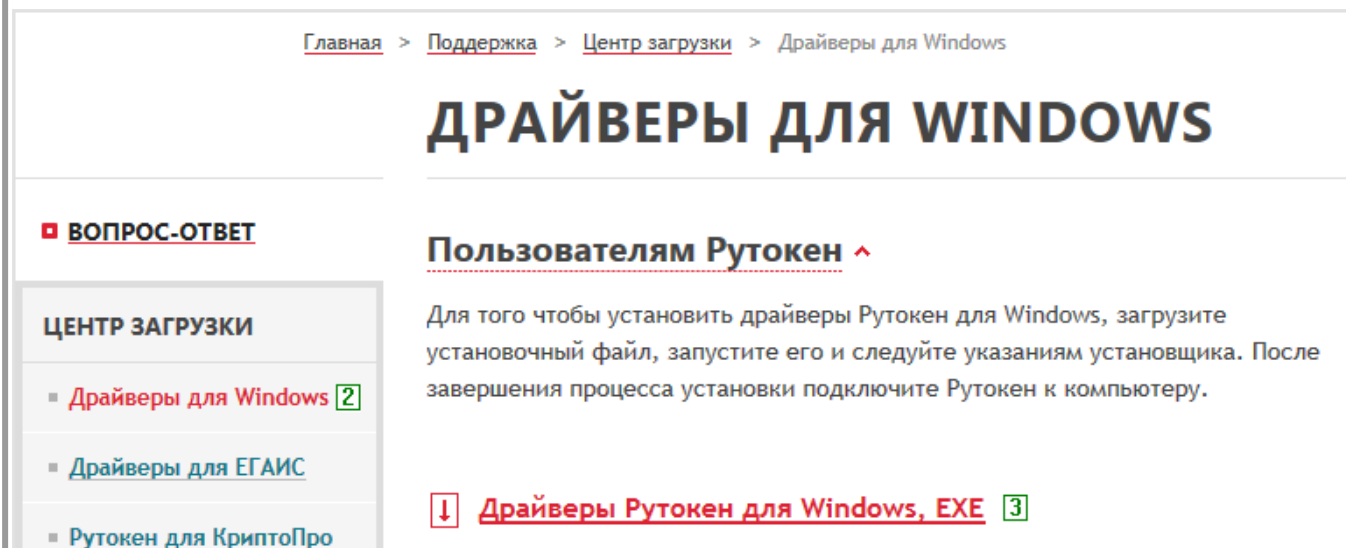


Рис. 2

² Если в этом разделе не открыта по умолчанию страница "Драйверы для Windows" (открытая страница выделена на панели "ЦЕНТР ЗАГРУЗКИ" красным цветом), то выберите эту страницу на панели "ЦЕНТР ЗАГРУЗКИ".

³ Щелкните мышью ссылку "Драйверы Рутокен для Windows, EXE".

• Установка драйвера
РУТОКЕН
для Windows

Откроется страница "Лицензионное соглашение". Ваши действия на этой странице показаны на рис. 3:

Главная > Поддержка > Центр загрузки > Лицензионное соглашение

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

ВОПРОС-ОТВЕТ

ЦЕНТР ЗАГРУЗКИ

- Драйверы для Windows
- Драйверы для ЕГАИС
- Рутокен для КriptoПро
- Рутокен для Signal-COM
- Рутокен Плагин
- Библиотека PKCS#11
- Рутокен Логон
- Рутокен Коннект
- Драйверы для *nix

Перед использованием программных продуктов и/или онлайн-сервисов Рутокен (Rutoken), ознакомьтесь с условиями Лицензионного соглашения. Любое использование программных продуктов и/или онлайн-сервисов Рутокен (Rutoken) означает полное и безоговорочное принятие его условий.

[Загрузить Лицензионное соглашение в виде отдельного PDF-документа](#)

Утверждено
Приказом генерального директора
АО «Актив-софт»
№ 01-ЛС от 31.08.2012 г.

1 Прочтите лицензионное соглашение

**Лицензионное соглашение
на использование программных продуктов
и/или онлайн-сервисов Рутокен (Rutoken)
Редакция №1 от 31.08.2012 г.**

Настоящий документ представляет собой предложение Акционерного общества «Актив-софт» (далее — «Правообладатель») заключить соглашение на изложенных ниже условиях.

2 Отметьте флажок (кнопка "Условия приняты" станет активной)

☐ Условия Лицензионного соглашения прочитаны и приняты в полном объеме.

3 Нажмите кнопку "Условия приняты"

УСЛОВИЯ ПРИНЯТЫ

Рис. 3

• Установка драйвера
РУТОКЕН
для Windows

Откроется страница "Загрузка файла". Ваши действия на этой странице показаны на рис. 4:

Главная > Поддержка > Центр загрузки > Загрузка файла > Драйверы Рутокен для Windows, EXE

ЗАГРУЗКА ФАЙЛА

ВОПРОС-ОТВЕТ

Загружается файл **Драйверы Рутокен для Windows, EXE**.

Загрузка начнется автоматически через **0 секунды**. Если загрузка не началась, [используйте прямую ссылку](#) для принудительной загрузки файла. **Откроется окно:**

Открытие «rtDrivers.exe»

Вы собираетесь открыть:

rtDrivers.exe
являющийся: Binary File (26,2 МБ)
из <https://download.rutoken.ru>

Вы хотите сохранить этот файл?

1 Если загрузка не началась, щелкните мышью эту ссылку

2 Нажмите кнопку "Сохранить файл".
Файл установки драйвера **rtDrivers.exe** будет сохранен в папке "Загрузки".
Ниже показан путь к папке "Загрузки" для русскоязычной версии Windows:

Вернуться в раздел «Драйверы для Windows»

Компьютер: [имя компьютера] ► Локальный диск (C:) ► Пользователи ► [имя текущ. пользователя] ► Загрузки

Рис. 4

• Установка драйвера
РУТОКЕН
для Windows

1 Запустите файл установки драйвера  rtDrivers.exe.

Откроется окно с предупреждением системы безопасности Windows и требованием подтвердить ваше намерение:

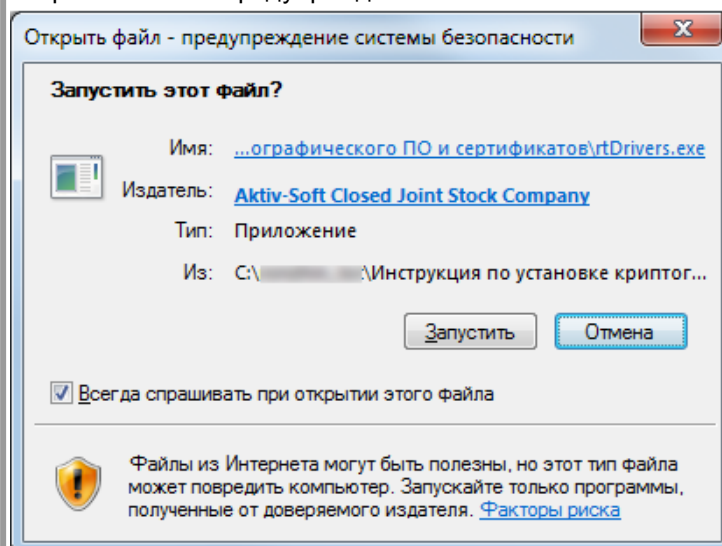


Рис. 5

2 Нажмите кнопку "Запустить". Откроется окно "Начало установки":

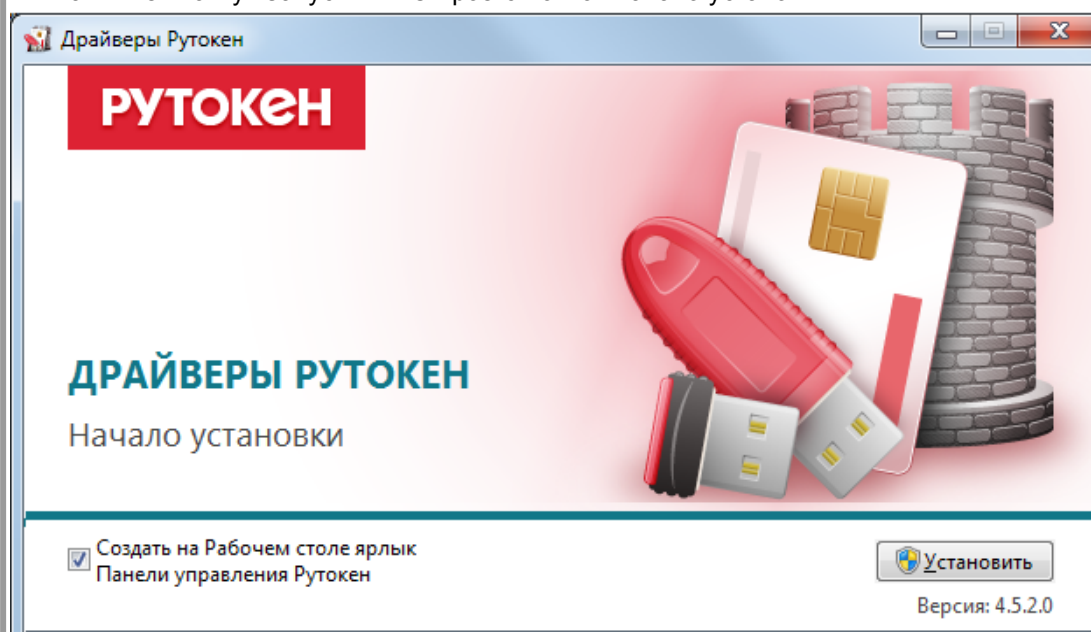


Рис. 6

• Установка драйвера РУТОКЕН для Windows

Нажмите кнопку "Установить".

Программа установки драйвера запросит разрешение на внесение изменений в системную информацию на вашем компьютере:

"Разрешить следующей программе (имя программы: "Rutoken drivers package") внести изменения на этом компьютере?".

Нажмите кнопку "Да".

В процессе установки программа установки выдаст несколько сообщений, в том числе сообщение об определении версии ОС Windows и сообщение об установке считывателей. Действия, выполняемые программой установки, протоколируются в журнале установки (путь к файлу журнала: "C:\Users\[текущий пользователь ОС]\AppData\Local\Temp\Rutoken_Drivers_yуууmmddhnn").

Если установка завершается успешно, то выдается сообщение об этом.

Если в процессе установки возникли ошибки, то вы можете посмотреть информацию о них в журнале установки:

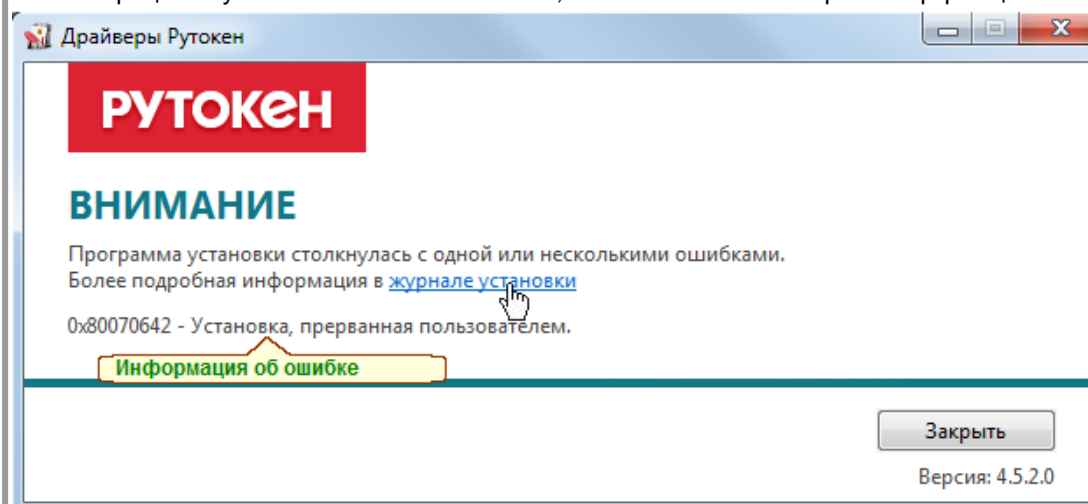


Рис. 7

Если что-то помешало программе установки создать файл журнала (например, она не выполнила никаких действий, так как вы прервали ее), то вы получите сообщение:

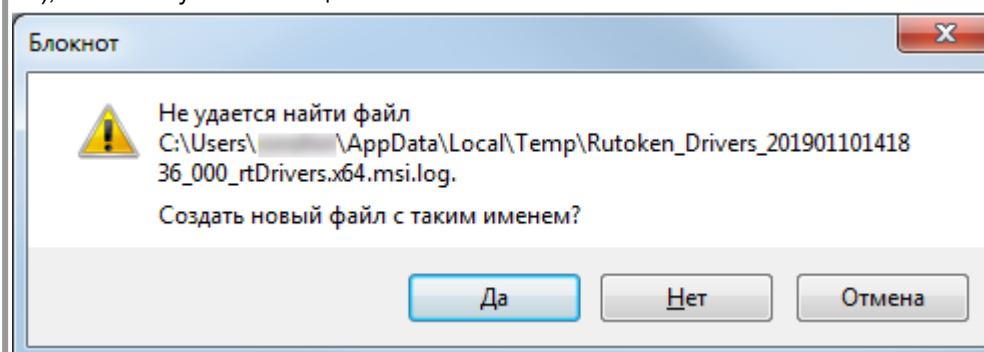


Рис. 8

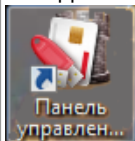
Вы можете нажать кнопку "Да", и записать в файл журнала вручную полезную на ваш взгляд информацию об этой попытке установки.

Замечание: в некоторых случаях (например, в случае, показанном на рис. 7) информация об ошибке не заносится в журнал.

• Установка драйвера
РУТОКЕН
для Windows

Результат установки драйвера.

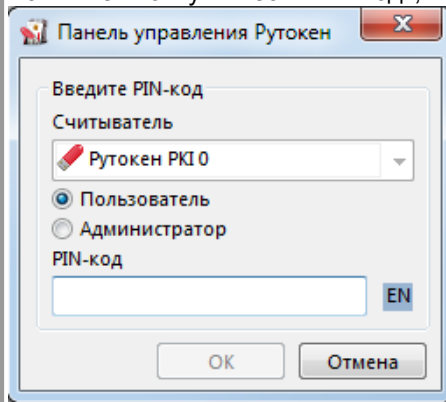
Если вы в процессе установки драйвера не сбросили (по каким-то своим соображениям) установленный по умолчанию флажок "Создать на рабочем столе ярлык Панели управления Рутокен", то этот ярлык появится на рабочем столе вашего компьютера:



Краткий обзор возможностей утилиты "Панель управления Рутокен"

Вкладка "Администрирование"

Нажмите кнопку "Ввести PIN-код", в открывшемся окне:



установите переключатель "Пользователь"/"Администратор" в положение "Пользователь", отметив радиокнопку "Пользователь" (если она не отмечена по умолчанию), введите pin-код пользователя, нажмите "ОК".

Замечание: pin-код пользователя, который вы вводите - это pin-код ключевого контейнера, который вы можете изменить как в панели управления Рутокен, так и средствами панели управления "КриптоПро CSP" (🔑). Смотрите раздел "[Изменение pin-кода ключевого контейнера](#)".

• Установка драйвера РУТОКЕН для Windows

После ввода pin-кода станут доступными кнопки:

- "Изменить" (изменить pin-код пользователя),
- "Изменить" (изменить имя токена - ключевого носителя).

На рис.1 красными стрелками показаны ваши действия при изменении pin-кода пользователя и имени токена. Зелеными стрелками показаны результаты действий пользователя:

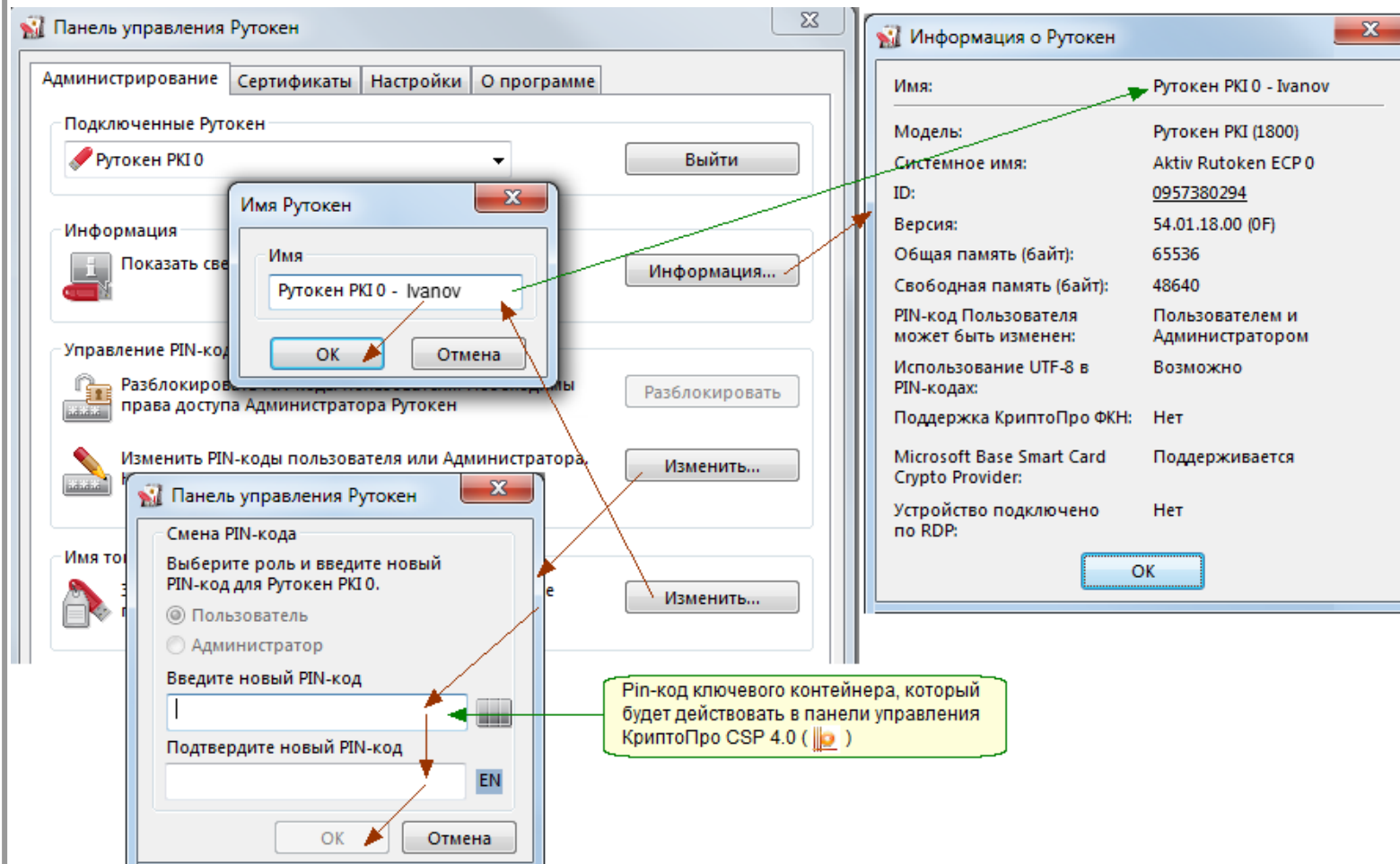


Рис. 1

Описание работы пользователя на вкладке "Сертификаты" приведено в разделе ["Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#).



+ [Установка драйвера](#)

[ключевого носителя](#)

- [Получение файла дистрибутива КриптоПро CSP 4.0](#)

- [Установка "КриптоПро CSP" из файла](#)

+ [Настройка КриптоПро CSP 4.0](#)

Возможны два способа получения файла дистрибутива КриптоПро CSP 4.0:

- а) на компакт-диске, полученном у производителя или у официального дилера производителя,
- б) скачать файл дистрибутива на сайте компании "КРИПТО-ПРО".

Ниже приводится описание второго способа:

1. Зайдите на сайт компании КРИПТО-ПРО (<http://www.cryptopro.ru>):



КриптоПро
Ключевое слово в защите информации

Поиск

▼ [О компании](#)

► [Контакты](#)

Ключевое слово в защите информации

С чего начать?

Клиентам

Правовая информация

Разработчикам



- › Продукты
- › [Загрузка файлов](#)
- › Приобретение
- › Поддержка
- › Обслуживание в УЦ
- › Вход для дилеров (информация)
- › Контактная информация

Новости КриптоПро

Купить



Вход

E-mail: *

Пароль / Password: *

Вход

[Регистрация](#)

[Забыли пароль?](#)

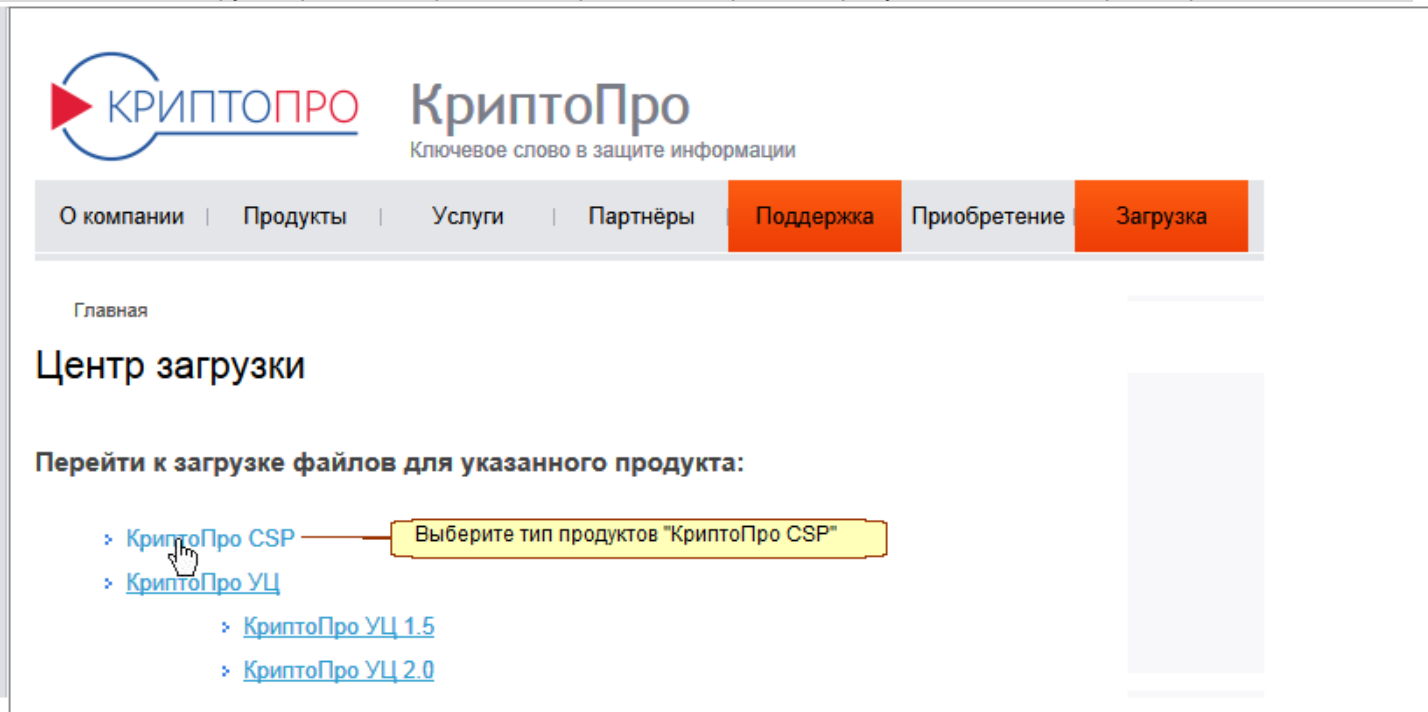
Возможны два варианта действий на этой странице:
Вариант 1 (рекомендуется):
а) выполнить вход на сайт по своей учетной записи (e-mail, который вы указали при регистрации и пароль), или выполнить регистрацию, а затем вход;
б) пройти по ссылке "Загрузка файлов".
Вариант 2:
Сразу пройти по ссылке "Загрузка файлов".
В этом случае вход или регистрацию придется выполнить позже - при попытке скачать файл

+ [Установка драйвера](#)[ключевого носителя](#)

- Получение файла дистрибутива КристоПро CSP 4.0
- [Установка "КристоПро CSP" из файла](#)

+ [Настройка КристоПро CSP 4.0](#)

2. По ссылке "Загрузка файлов" открывается страница выбора типа продуктов компании "КристоПро"



+ [Установка драйвера](#)

[ключевого носителя](#)

- Получение файла дистрибутива КристоПро CSP 4.0

- [Установка "КристоПро CSP" из файла](#)

+ [Настройка КристоПро CSP 4.0](#)

3. Откроется лицензионное соглашение:



КристоПро
Ключевое слово в защите информации

[О компании](#) | [Продукты](#) | [Услуги](#) | [Партнёры](#) | [Поддержка](#) | [Приобретение](#) | [Загрузка](#)

[Главная](#)

Лицензионное соглашение

КристоПро CSP

[Текст лицензионного соглашения]

Ознакомьтесь с лицензионным соглашением и нажмите кнопку "Я согласен с лицензионным соглашением. Перейти к загрузке". Если вы после установки КристоПро CSP 4.0 намерены использовать сертификаты подписи с ограниченной лицензией, то при ознакомлении с лицензионным соглашением, примите во внимание, что пункт 7 и пункт 10 («Пользователь не вправе использовать Изделие без активации Изделия путем ввода ключа установки Изделия (серийного номера лицензии)....») этого соглашения вы можете игнорировать, так как вы имеете право при наличии ограниченной лицензии использовать ПО «КристоПро CSP» без его активации для подписывания и расшифровки документов в течение периода действия закрытого ключа сертификата подписи в вашем ключевом носителе, полученном в УЦ АО «АТС».

[Я согласен с Лицензионным соглашением. Перейти к загрузке.](#)

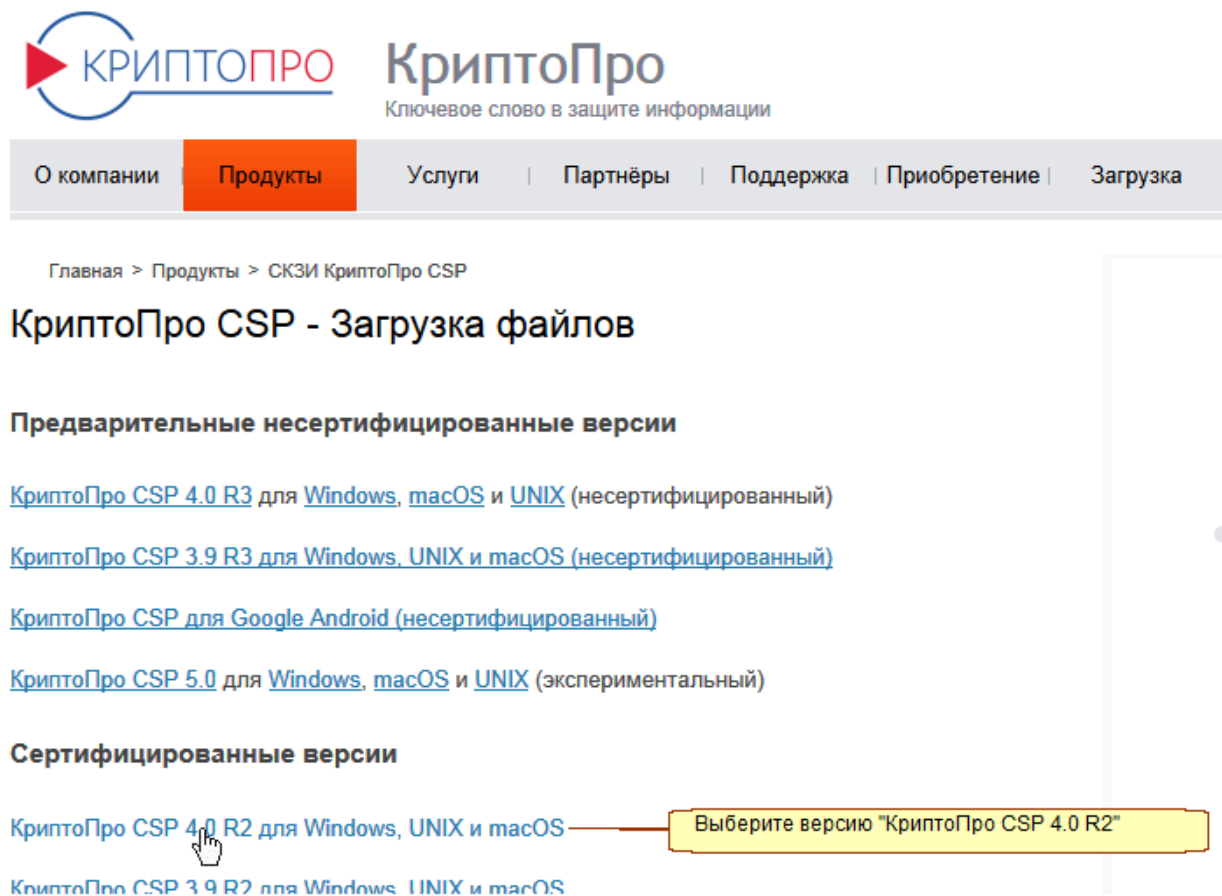
+ [Установка драйвера](#)[ключевого носителя](#)

- Получение файла дистрибутива КристоПро CSP 4.0

- [Установка "КристоПро CSP" из файла](#)

+ [Настройка КристоПро CSP 4.0](#)

4. Откроется страница выбора версии "КристоПро CSP":



КРИПТОПРО КристоПро
Ключевое слово в защите информации

О компании | **Продукты** | Услуги | Партнёры | Поддержка | Приобретение | Загрузка

Главная > Продукты > СКЗИ КристоПро CSP

КристоПро CSP - Загрузка файлов

Предварительные несертифицированные версии

[КристоПро CSP 4.0 R3 для Windows, macOS и UNIX](#) (несертифицированный)

[КристоПро CSP 3.9 R3 для Windows, UNIX и macOS](#) (несертифицированный)

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

[КристоПро CSP 5.0 для Windows, macOS и UNIX](#) (экспериментальный)

Сертифицированные версии

[КристоПро CSP 4.0 R2 для Windows, UNIX и macOS](#)

[КристоПро CSP 3.9 R2 для Windows, UNIX и macOS](#)

Выберите версию "КристоПро CSP 4.0 R2"



+ [Установка драйвера](#)

[ключевого носителя](#)

- [Получение файла дистрибутива КриптоПро CSP 4.0](#)

- [Установка "КриптоПро CSP" из файла](#)

+ [Настройка КриптоПро CSP 4.0](#)

5. После выбора версии страница сайта будет автоматически "прокручена" до заголовка "КриптоПро CSP 4.0 R2":

КриптоПро CSP 4.0 R2

Сертифицированная версия КриптоПро CSP 4.0.9842 (Riemann) от 15.11.2016.

Сертификаты соответствия: СФ/114-3009, СФ/124-3010 от "30" декабря 2016 г.

Действительны до "31" декабря 2018 г.

Извещения об изменениях: ЖТЯИ.00087-01.1-2016, ЖТЯИ.00088-01.1-2016.

Внимание:

- › Все дистрибутивы подписаны цифровой подписью - её можно проверить с помощью обновленной утилиты [cspverify](#), [команды для проверки](#)
- › Вопросы можно задать в нашем форуме в ветке [КриптоПро CSP 4.0](#)
- › и на [портале технической поддержки](#).

Документация:

- › [Список изменений \(changelog\)](#)
- › [Документация по установке и использованию КриптоПро CSP 4.0 \(ZIP\)](#)
- › [Документация для разработчиков и примеры \(SDK\)](#)

Для Windows:

- › [КриптоПро CSP 4.0 для Windows](#)

Контрольная сумма

ГОСТ: 86A2828B818135102723A88E97891CF919981CBA8035A12207C98A1ED36AD357
MD5: 0b028b6ef14d0dd5be71068bb6d98b1f

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

- ▶ [Дистрибутивы в формате Windows Installer для автоматизации установки:](#)

Выберите формат файла дистрибутива:

1) Ехе-файл.

Рекомендуется сотрудникам Участника, самостоятельно устанавливающим "КриптоПро CSP 4.0" на свой компьютер.

2) msi-файл.

Рекомендуется системным администраторам для автоматизации установки. Запускается из командной строки с ключами (параметрами).

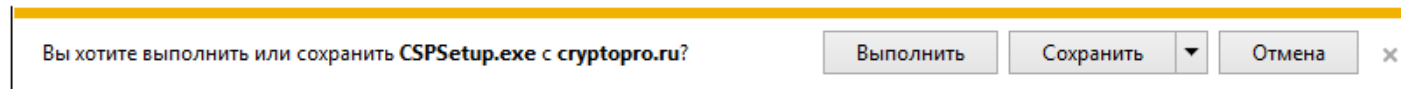
Установка криптографического ПО ► Получение файла дистрибутива КриптоПро CSP 4.0

6 из 6

+ Установка драйвера ключевого носителя

- Получение файла дистрибутива КриптоПро CSP 4.0
- Установка "КриптоПро CSP" из файла
- + Настройка КриптоПро CSP 4.0

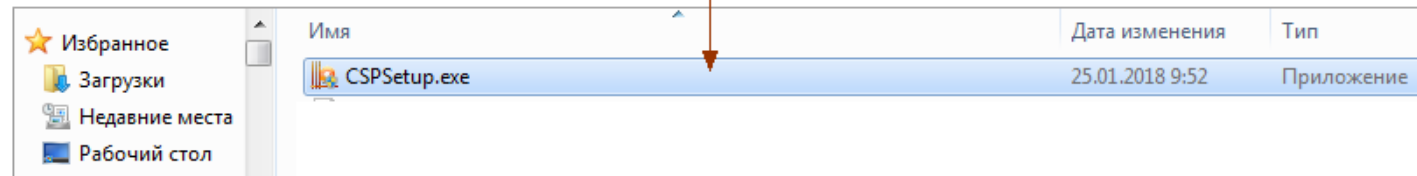
6. После выбора формата файла (далее рассматривается вариант выбора exe-файла) щелчком мыши по ссылке "КриптоПро CSP 4.0 для Windows" откроется окно загрузки файла:



Нажмите кнопку "Сохранить".
Через некоторое время вместо кнопок "Сохранить" и "Отмена" появятся кнопки "Открыть папку" и "Просмотреть загрузки":



Нажмите кнопку "Открыть папку".
Откроется папка загрузки, в которой загруженный файл будет выделен:



Скопируйте (Ctrl+C) или переместите (Ctrl+X) файл в удобную для вас папку (Ctrl+V).

Перед установкой "КриптоПро CSP 4.0" рекомендуется проверить целостность файла дистрибутива (убедиться в том, что загруженный файл - это именно тот файл, который вам нужен, и что он не поврежден).
Смотрите раздел инструкции "[Проверка контрольной суммы файла дистрибутива](#)".

После проверки контрольной суммы выполните установку "КриптоПро CSP 4.0" из файла дистрибутива.
Смотрите раздел инструкции "[Установка КриптоПро CSP 4.0 из файла дистрибутива](#)".

+ Установка драйвера

[ключевого носителя](#)

• [Получение файла](#)

[дистрибутива КриптоПро CSP 4.0](#)

• Установка "КриптоПро CSP" из файла

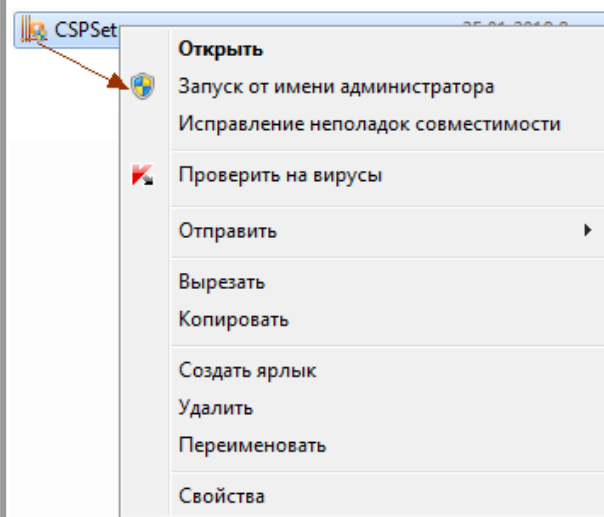
+ [Настройка КриптоПро CSP 4.0](#)

Перед началом установки "КриптоПро CSP" закройте все запущенные приложения. Убедитесь, что вы обладаете достаточными правами для установки ПО и записи информации в реестр (рекомендуется выполнять установку и настройку от имени администратора). Выполняйте установку и настройку "КриптоПро CSP" локально на компьютере, а не через клиента удаленного доступа.

Примечание: "КриптоПро CSP 4.0" - это универсальное ПО, способное работать с любой версией Windows, в том числе с Windows 7.

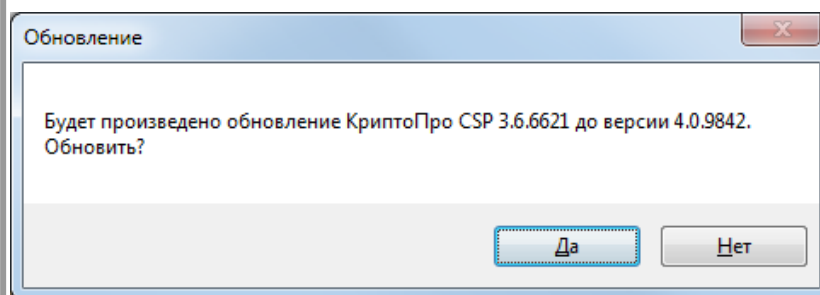
Выполните следующие шаги:

1. Запустите программу установки "КриптоПро CSP 4.0" (файл CSPSetup) от имени администратора. Для этого откройте правой кнопкой мыши контекстное меню этого файла, в котором выберите пункт Запуск от имени администратора ("Выполнить от имени администратора"):



Откроется окно с вопросом (не показано здесь): "Разрешить следующей программе внести изменения на этом компьютере?"
Нажмите кнопку "Да".

2. Программа установки определит текущую установленную версию КриптоПро CSP и запросит разрешение на замену текущей версии КриптоПро CSP на "КриптоПро CSP 4.0":



+ Установка драйвера

ключевого носителя

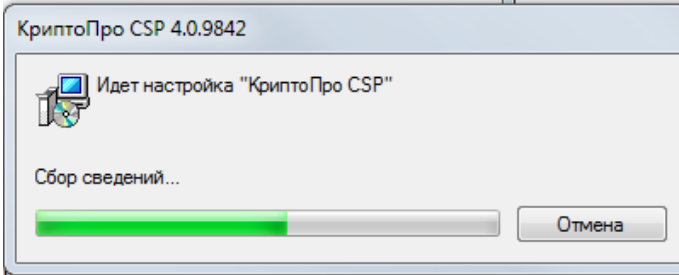
• Получение файла

[дистрибутива КриптоПро CSP 4.0](#)

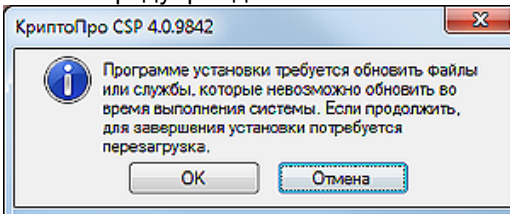
• Установка "КриптоПро CSP" из файла

+ Настройка КриптоПро CSP 4.0

3. Программа начнет установку КриптоПро CSP 4.0. Будет выдано несколько информационных сообщений о ходе установки, не требующих от пользователя каких либо действий, например:

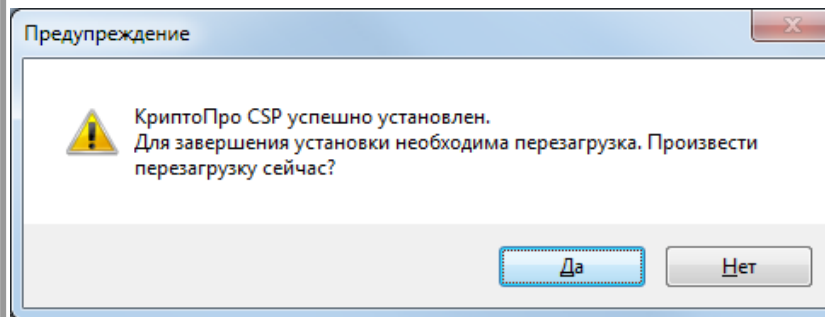


а также предупреждение:



Нажмите кнопку "ОК" чтобы продолжить установку.

4. После завершения установки откроется окно:



Нажмите кнопку "Да" и перезагрузите компьютер.

Далее, если вы **не планируете** использовать сертификат со [ограниченной лицензией](#), то должны приобрести лицензию у компании «КриптоПро» и ввести номер лицензии в окно настройки КриптоПро CSP (смотрите раздел данной инструкции [«Активация КриптоПро CSP 4.0 \(ввод лицензии\)»](#)).

- Активация КриптоПро CSP 4.0 (ввод лицензии)
- [Проверка/Настройка конфигурации считывателей](#)
- [Задание места хранения ключей и включение/выключение кэширования](#)
- [Отключение КриптоПро WinLogon \(рекомендуется\)](#)
- [Изменение pin-кода ключевого контейнера](#)

Если вы планируете использовать только сертификаты подписи со **ограниченной лицензией**, то пропустите этот шаг настройки КриптоПро CSP, иначе [откройте панель управления](#). Далее последовательность ваших действий показана на рис.1 стрелками и цифрами:

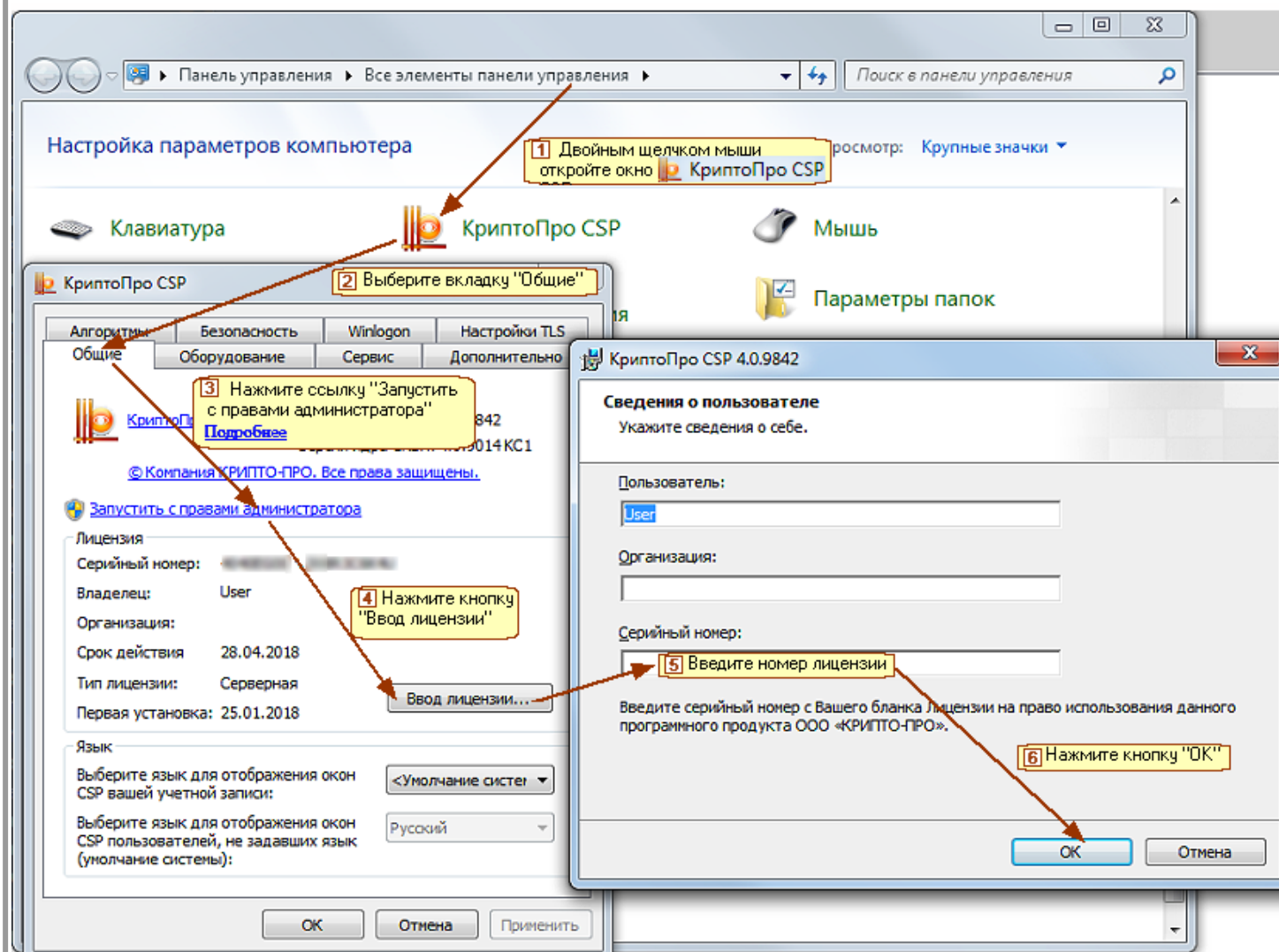


Рис. 1

- [Активация КриптоПро CSP 4.0 \(ввод лицензии\)](#)
- Проверка/Настройка конфигурации считывателей
- [Задание места хранения ключей и включение/выключение кэширования](#)
- [Отключение КриптоПро WinLogon \(рекомендуется\)](#)
- [Изменение pin-кода ключевого контейнера](#)

Откройте панель управления. Далее последовательность действий пользователя показана на рис.1 стрелками и цифрами:
Проверка конфигурации считывателей

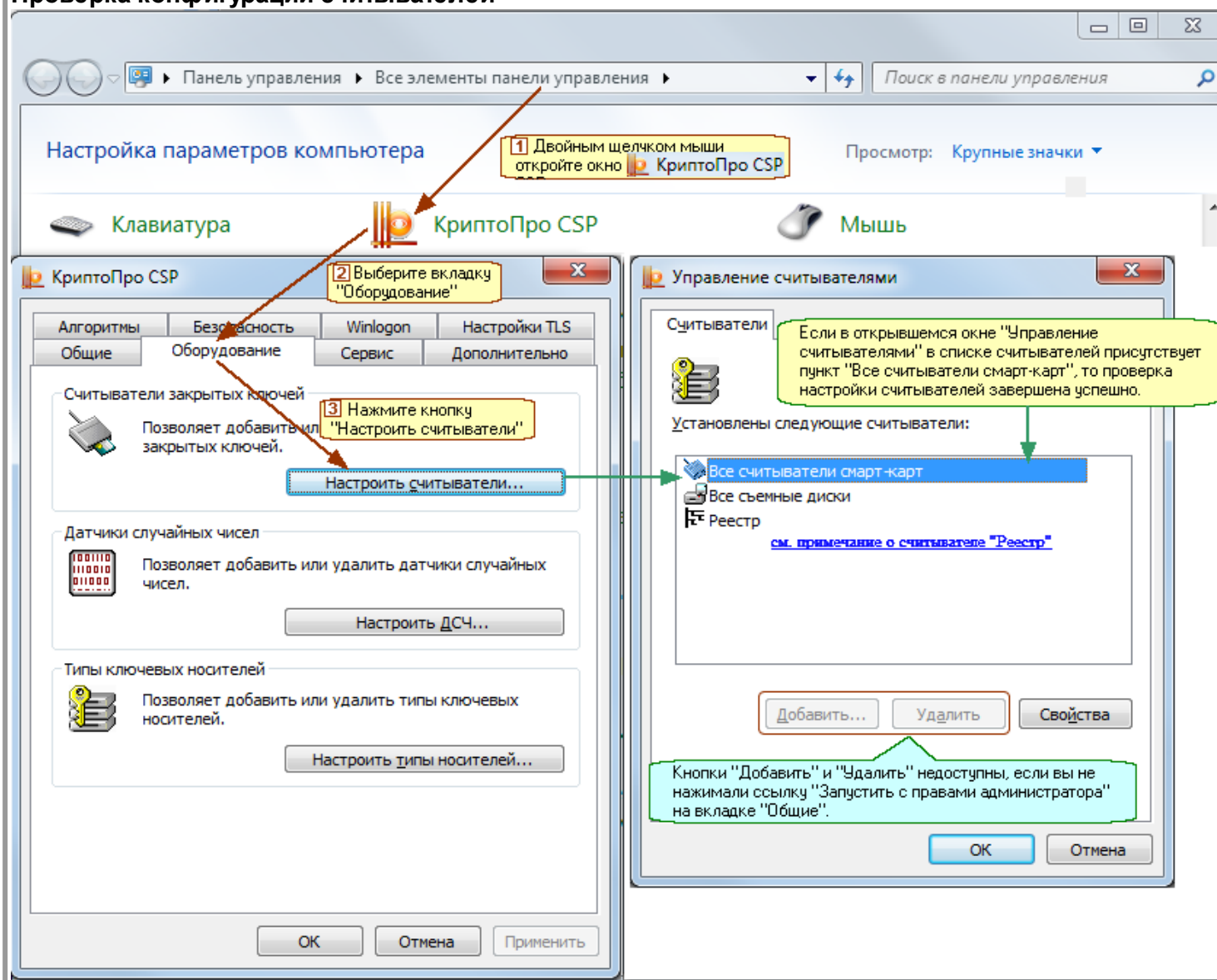


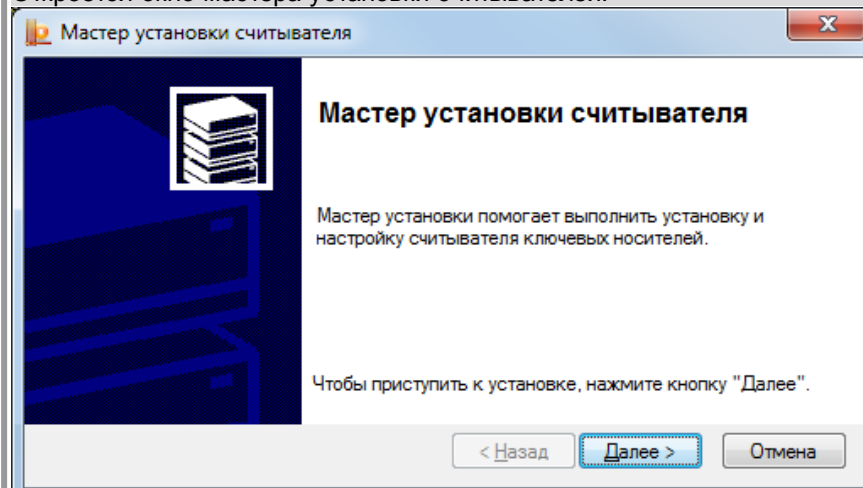
Рис. 1

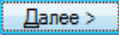
- [Активация КриптоПро CSP 4.0 \(ввод лицензии\)](#)
- Проверка/Настройка конфигурации считывателей
- [Задание места хранения ключей и включение/выключение кэширования](#)
- [Отключение КриптоПро WinLogon \(рекомендуется\)](#)
- [Изменение pin-кода ключевого контейнера](#)

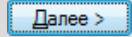
Настройка конфигурации считывателей.

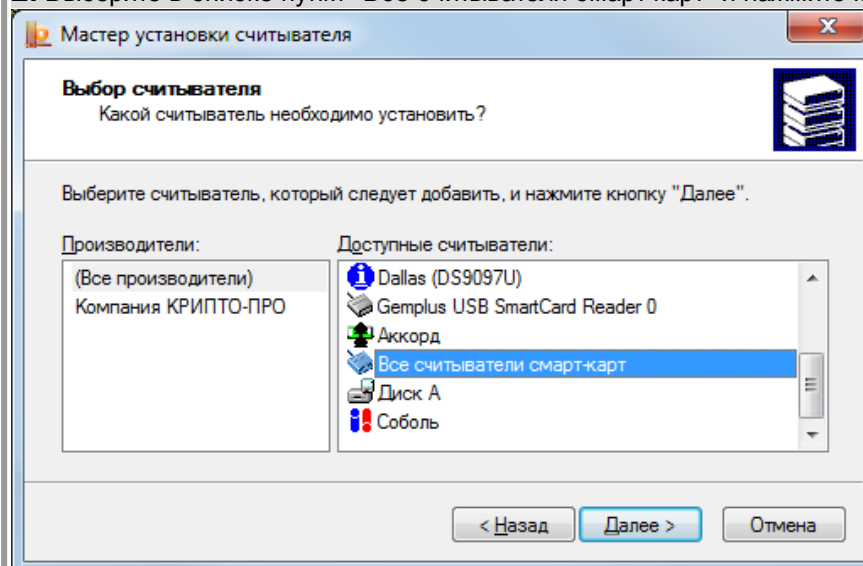
1. Если в списке установленных считывателей отсутствует пункт "Все считыватели смарт-карт", то его необходимо добавить в список. Для этого выполните шаги **1**, **2**, **3**, показанные на рис. 1, но (!) перед шагом **2** нажмите ссылку "[Запустить с правами администратора](#)". Затем в окне  **Управление считывателями** нажмите кнопку "Добавить".

Откроется окно мастера установки считывателей:



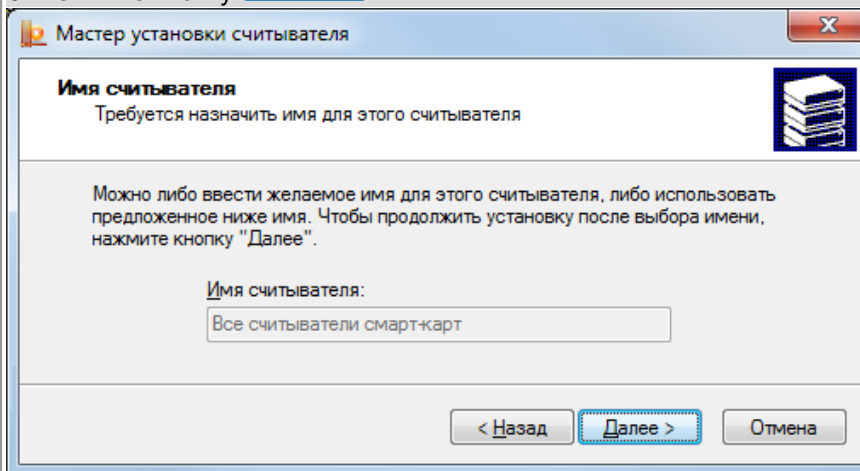
Нажмите кнопку .

2. Выберите в списке пункт "Все считыватели смарт карт" и нажмите кнопку .

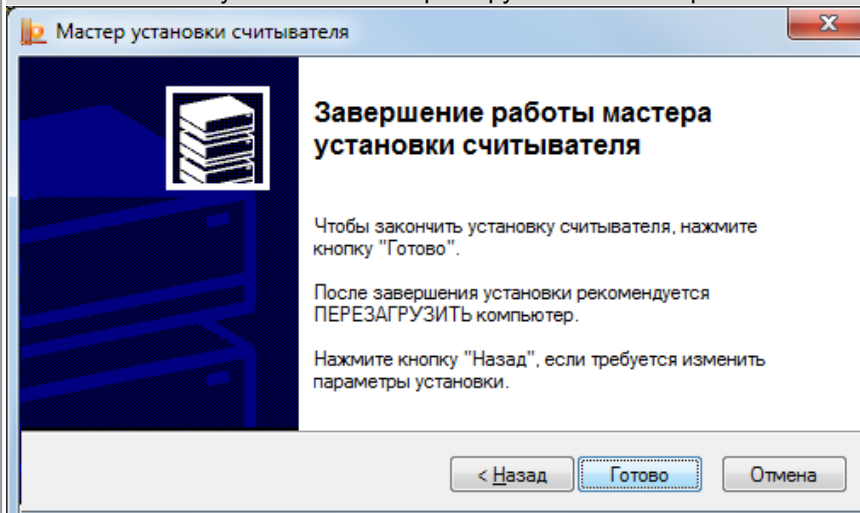


- [Активация КриптоПро CSP 4.0 \(ввод лицензии\)](#)
- Проверка/Настройка конфигурации считывателей
- [Задание места хранения ключей и включение/выключение кэширования](#)
- [Отключение КриптоПро WinLogon \(рекомендуется\)](#)
- [Изменение pin-кода ключевого контейнера](#)

3. Нажмите кнопку **Далее >**.



4. Нажмите кнопку **Готово** и перезагрузите компьютер:



Закройте окно  **Управление считывателями** нажатием кнопки "ОК".

Закройте окно  **КриптоПро CSP** нажатием кнопки "ОК".

Примечание: наличие в списке установленных считывателей элемента "Все считыватели смарт-карт" обеспечивает работу КриптоПро CSP 4.0 с ключевыми носителями "Рутокен".

- [Активация КриптоПро CSP 4.0 \(ввод лицензии\)](#)
- [Проверка/Настройка конфигурации считывателей](#)
- [Задание места хранения ключей и включение/выключение кэширования](#)
- [Отключение КриптоПро WinLogon \(рекомендуется\)](#)
- [Изменение pin-кода ключевого контейнера](#)

[Откройте панель управления.](#)

Далее последовательность действий пользователя показана на рис.1 стрелками и цифрами:

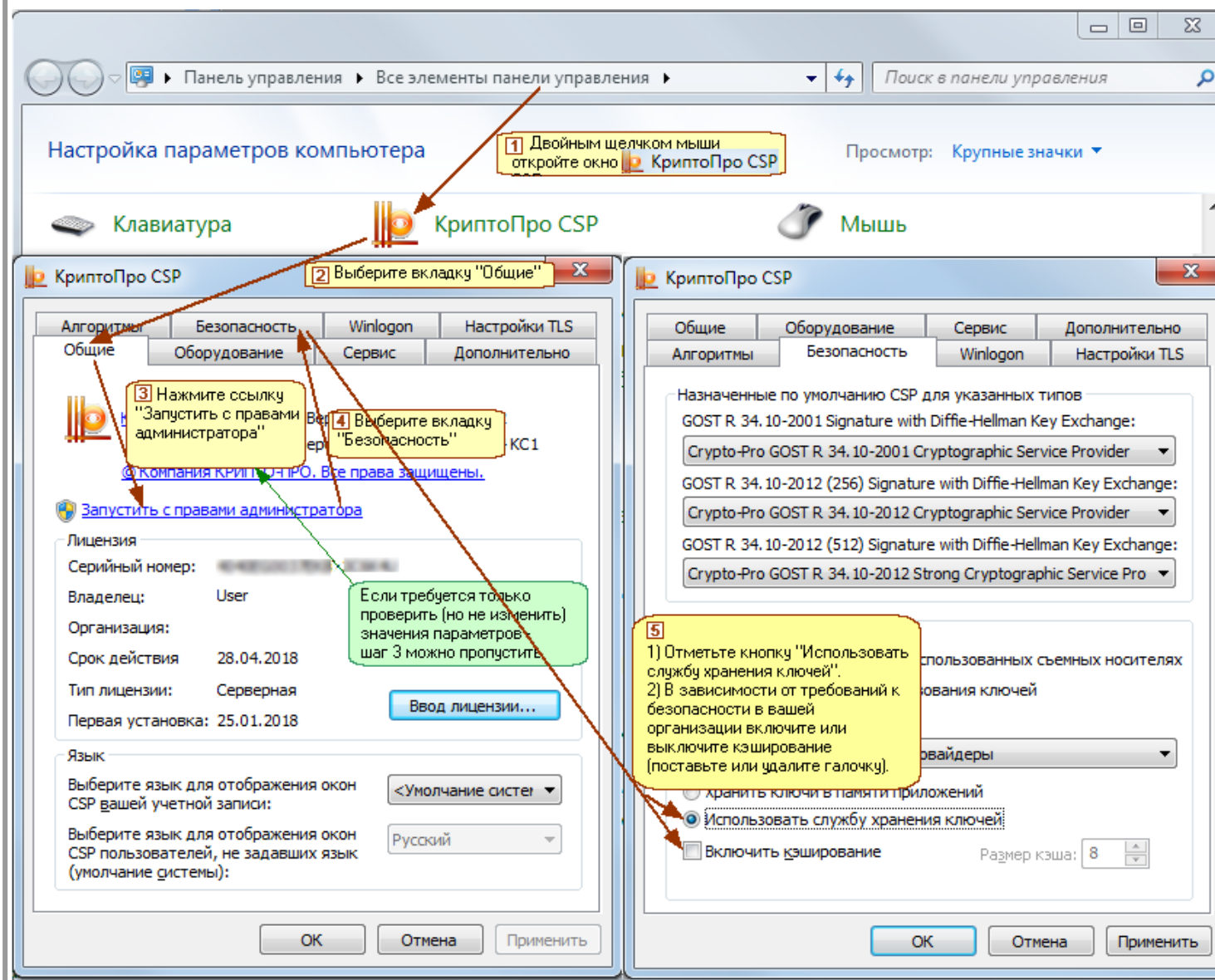
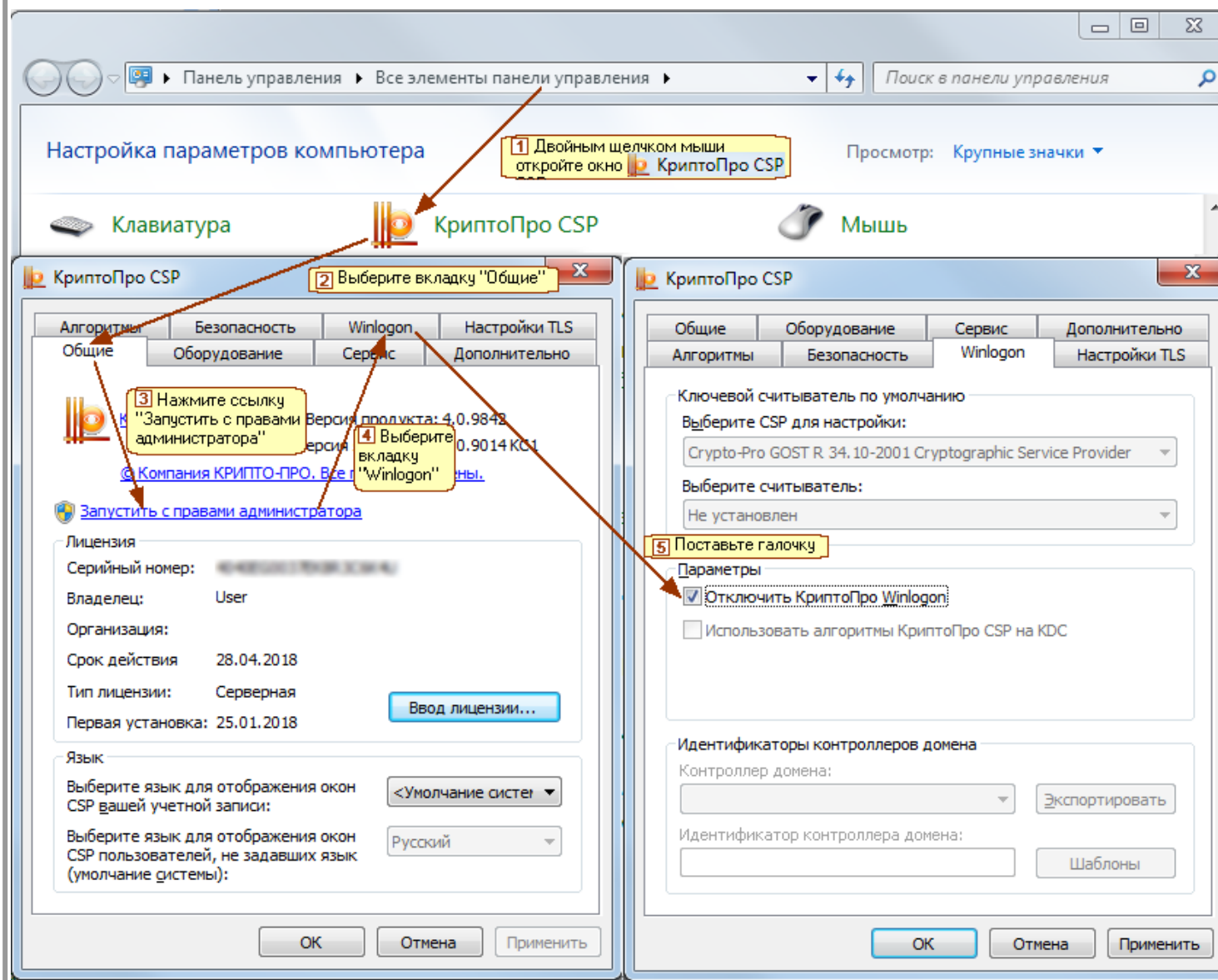


Рис. 1

- [Активация КриптоПро CSP 4.0 \(ввод лицензии\)](#)
- [Проверка/Настройка конфигурации считывателей](#)
- [Задание места хранения ключей и включение/выключение кэширования](#)
- [Отключение КриптоПро WinLogon \(рекомендуется\)](#)
- [Изменение pin-кода ключевого контейнера](#)

Откройте панель управления.

Далее последовательность действий пользователя показана на рис.1 стрелками и цифрами



- [Активация КриптоПро CSP 4.0 \(ввод лицензии\)](#)
- [Проверка/Настройка конфигурации считывателей](#)
- [Задание места хранения ключей и включение/выключение кэширования](#)
- [Отключение КриптоПро WinLogon \(рекомендуется\)](#)
- **Изменение pin-кода ключевого контейнера**

Откройте панель управления и на вкладке "Общие" нажмите ссылку "Запустить с правами администратора".

Далее последовательность ваших действий показана на рис.1 стрелками и цифрами:

- 1 На вкладке "Сервис" нажмите кнопку "Изменить пароль".
- 2 В открывшемся окне "Изменение пароля контейнера закрытого ключа":
 - а) нажмите кнопку "Обзор",
 - б) в открывшемся окне "Выбор ключевого контейнера" (не показано на рис.1) выберите ключевой контейнер и нажмите кнопку "ОК",
- 3 В окне "Изменение пароля контейнера закрытого ключа" нажмите кнопку "Готово".
- 4 В открывшемся окне "Введите pin-код для контейнера [имя контейнера]" введите текущий pin-код и нажмите кнопку "ОК".
- 5 Введите два раза новый pin-код и 6 нажмите кнопку "ОК".

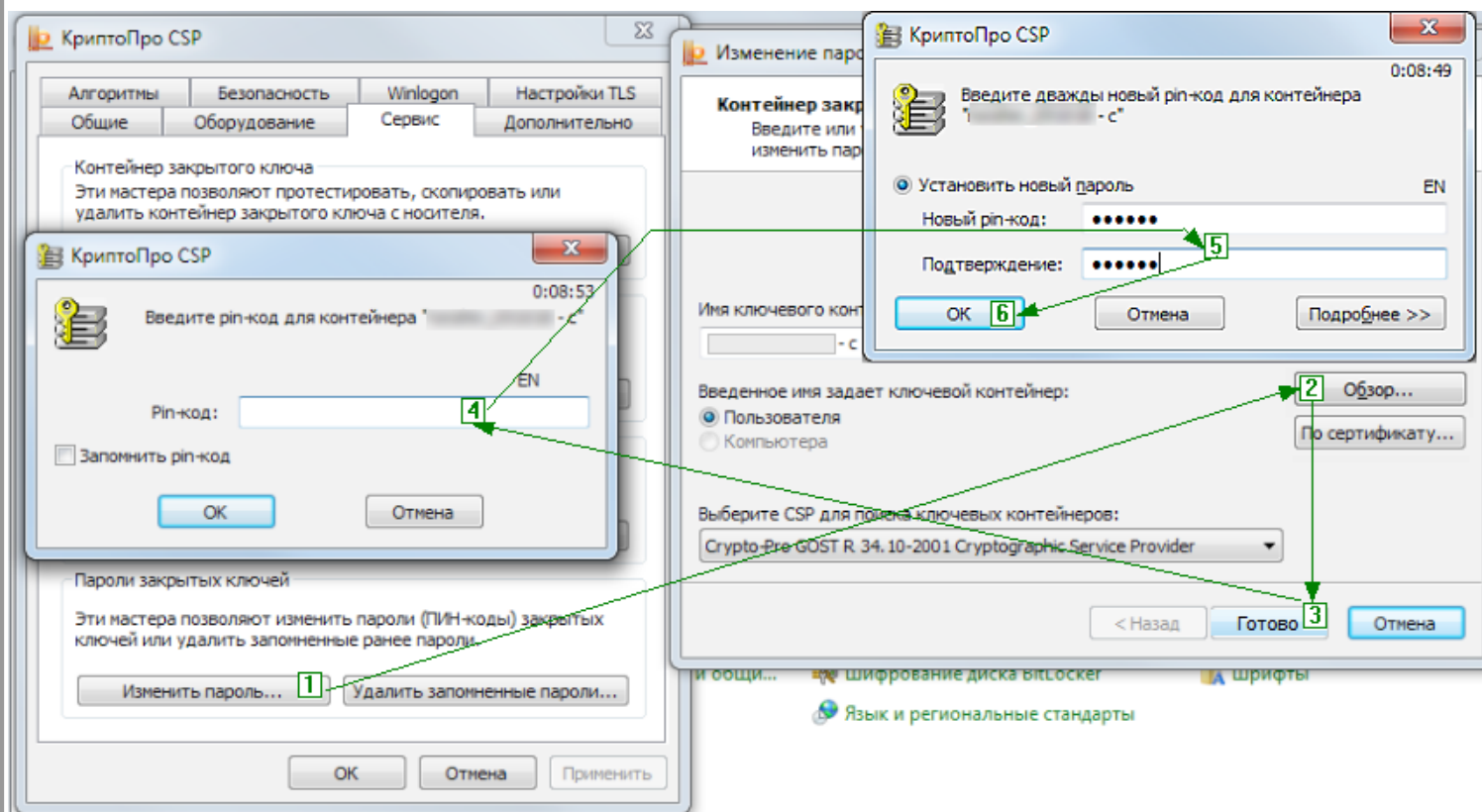


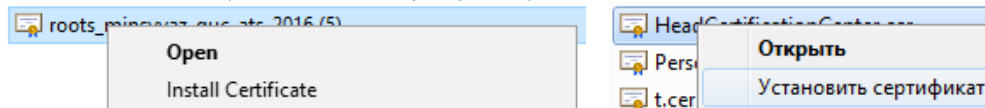
Рис. 1



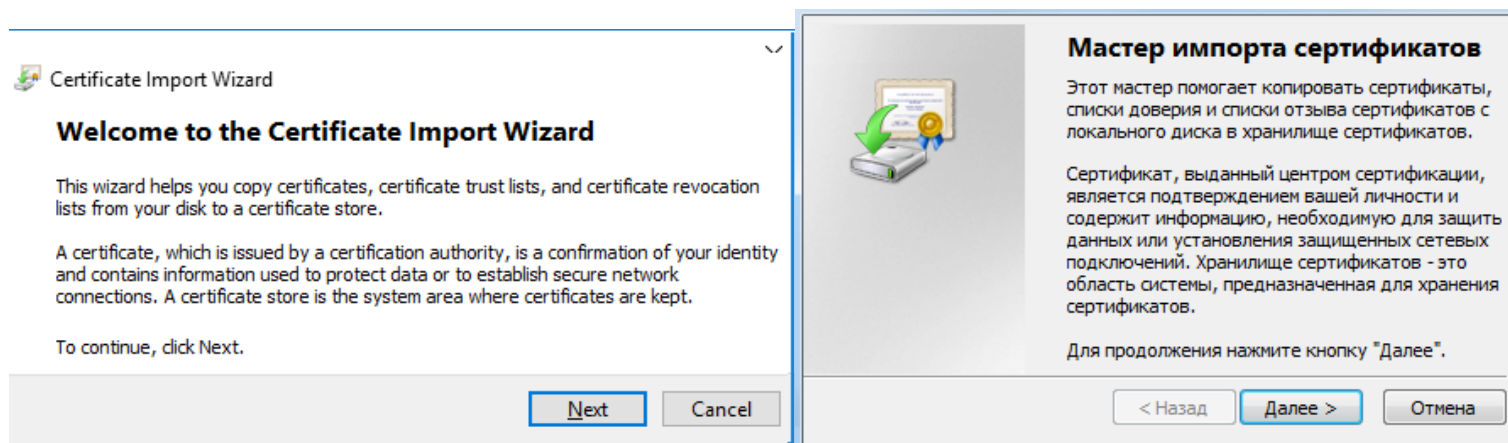
- Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

В данном разделе руководства приведено описание установки в хранилища "Доверенные корневые центры сертификации" и "Промежуточные центры сертификации" сертификатов, [скачанных с сайта АО "АТС"](#), и сертификатов, экспортированных из ключевого носителя с использованием утилиты "[Панель управления Рутокен](#)".

1. Щелчком правой кнопки мыши по файлу с сертификатами откройте контекстное меню для этого файла и выберите в нем пункт "Install Certificate" ("Установить сертификат").



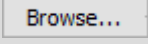
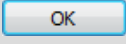
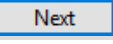
2. Откроется первое окно мастера установки (импорта) сертификатов. Нажмите в нем кнопку **Next** ("Далее").

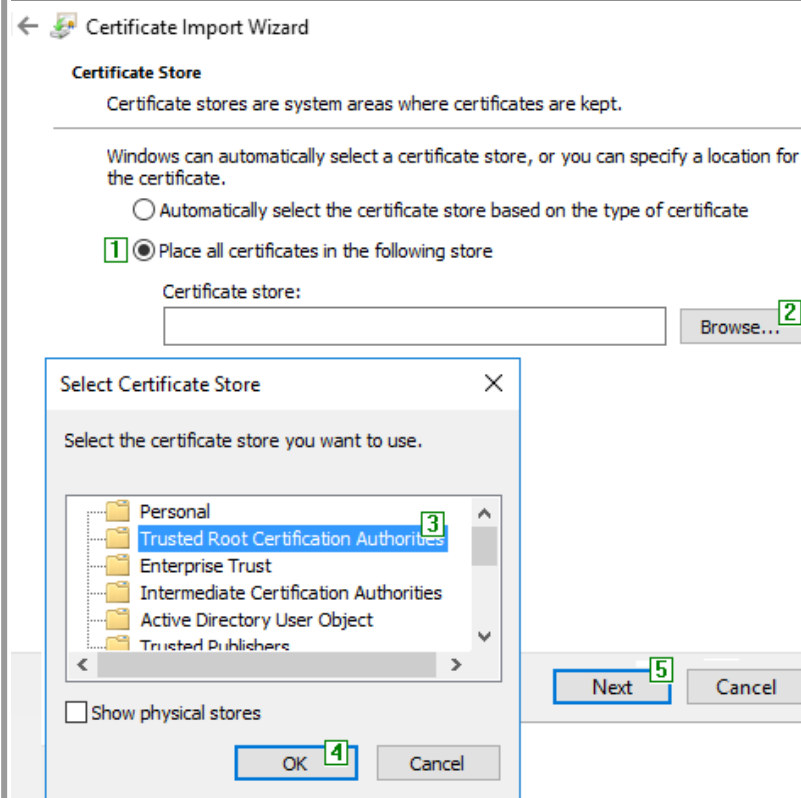




- Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

3. Откроется окно "Certificate Store" ("Хранилище сертификатов"). Выполните следующие действия:

- 1 Отметьте кнопку  Place all certificates in the following store ("Поместить все сертификаты в следующее хранилище").
- 2 Нажмите кнопку  ("Обзор").
Откроется окно "Select Certificate Store" ("Выбор хранилища сертификатов").
- 3 Выберите хранилище.
 - Если вы устанавливаете корневые сертификаты из файла, скачанного с сайта АО "АТС", то выберите хранилище  Trusted Root Certification Authorities ("Доверенные корневые центры сертификации"). Смотрите [комментарий к шагу 4](#).
 - Если вы устанавливаете корневой сертификат из файла, экспортированного из ключевого носителя при помощи утилиты "Панель управления Рутокен", то для сертификатов  Головной удостоверяющий центр и  Минкомсвязь России выбирайте хранилище "Доверенные корневые центры сертификации", для остальных корневых сертификатов выбирайте хранилище "Промежуточные центры сертификации".
- 4 Нажмите кнопку .
Окно "Select Certificate Store" закроется.
Выбранное хранилище появится в поле "Certificate Store" в окне "Certificate Store" ("Хранилище сертификатов").
- 5 Нажмите кнопку  ("Далее") в окне "Certificate Store".



Хранилище сертификатов

Хранилища сертификатов - это системные области, в которых хранятся сертификаты.

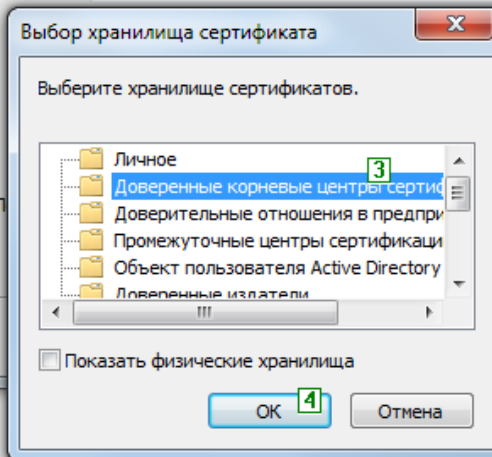
Выбор хранилища может быть произведен Windows автоматически, или же можно указать размещение сертификата вручную.

☐ Автоматически выбрать хранилище на основе типа сертификата

1 ☒ Поместить все сертификаты в следующее хранилище

Хранилище сертификатов:

2 Обзор...



5 Далее >

Отмена



- Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

4. Откроется окно "Completing the Certificate Import Wizard" ("Завершение работы мастера импорта сертификата").

В этом окне мастер установки сертификатов сообщает, что сертификаты, содержащиеся в файле, будут установлены в выбранное пользователем хранилище.

Если вы устанавливаете корневые сертификаты из файла, скачанного с сайта АО "АТС" по ссылке [Корневые сертификаты Минкомсвязи России и УЦ АО «АТС» 2017-2018 \(включая ГОСТ-2012\)](#)

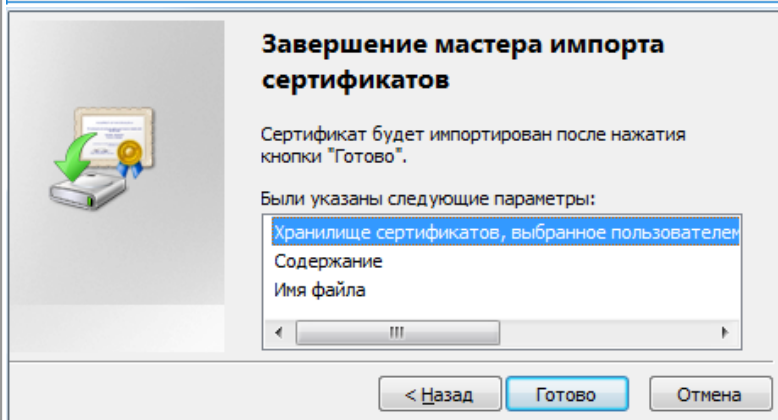
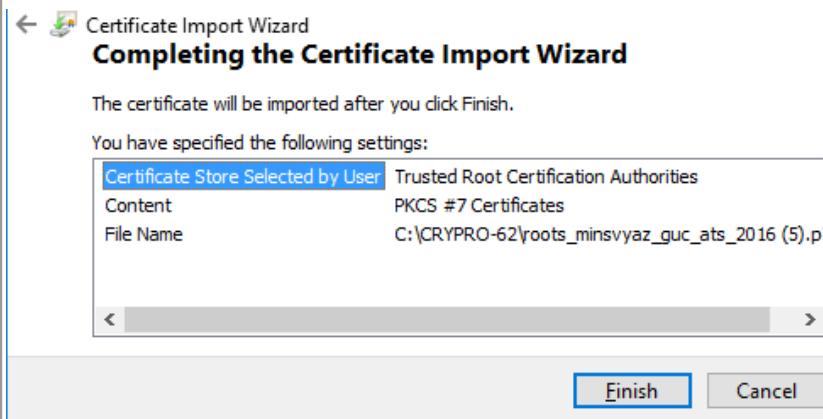
или по ссылке:

[Корневые сертификаты Минкомсвязи России, ГУЦ и УЦ АО «АТС» 2016](#)

то, поскольку эти файлы содержат сертификаты, которые должны быть установлены в разные хранилища, но данный мастер "умеет" устанавливать сертификаты только в одно хранилище, то мы на шаге 3 выбираем хранилище:

Trusted Root Certification Authorities ("Доверенные корневые центры сертификации"), а после завершения работы этого мастера перемещаем сертификаты УЦ 1 ИС ГУЦ и АО АТС в хранилище "Промежуточные центры сертификации" (смотрите шаги 9 - 11 данной процедуры).

Нажмите кнопку Finish (Готово).

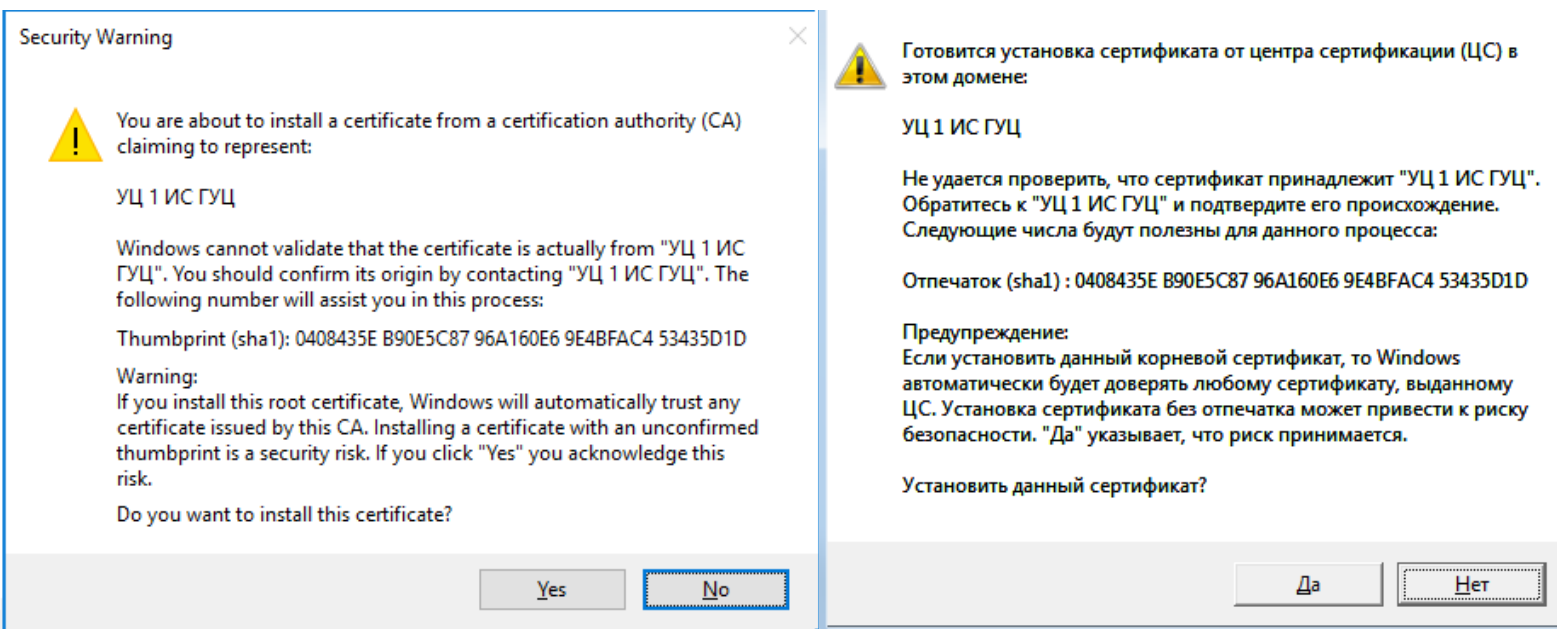




- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

5. Если вы устанавливаете сертификат из файла "Корневые сертификаты Минкомсвязи России, ГУЦ и УЦ АО «АТС» 2016", то получите предупреждение от Системы безопасности Windows в отношении сертификата "УЦ 1 ИС ГУЦ".

Нажмите кнопку ("Да") в окне предупреждения.





- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

6. Вы получите предупреждение от Системы безопасности Windows в отношении сертификата "Головной удостоверяющий центр".

Если вы уже установили сертификат  Головной удостоверяющий центр из файла [Корневые сертификаты Минкомсвязи России и УЦ АО «АТС» 2017-2018 \(включая ГОСТ-2012\)](#),

то нажмите кнопку (Нет), так как нет необходимости устанавливать его второй раз), иначе нажмите кнопку ("Да").

Security Warning



You are about to install a certificate from a certification authority (CA) claiming to represent:

Головной удостоверяющий центр

Windows cannot validate that the certificate is actually from "Головной удостоверяющий центр". You should confirm its origin by contacting "Головной удостоверяющий центр". The following number will assist you in this process:

Thumbprint (sha1): 8CAE88BB FD404A7A 53630864 F9033606 E1DC45E2

Warning:

If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Yes

No



Готовится установка сертификата от центра сертификации (ЦС) в этом домене:

Головной удостоверяющий центр

Не удастся проверить, что сертификат принадлежит "Головной удостоверяющий центр". Обратитесь к "Головной удостоверяющий центр" и подтвердите его происхождение. Следующие числа будут полезны для данного процесса:

Отпечаток (sha1) : 8CAE88BB FD404A7A 53630864 F9033606 E1DC45E2

Предупреждение:

Если установить данный корневой сертификат, то Windows автоматически будет доверять любому сертификату, выданному ЦС. Установка сертификата без отпечатка может привести к риску безопасности. "Да" указывает, что риск принимается.

Установить данный сертификат?

Да

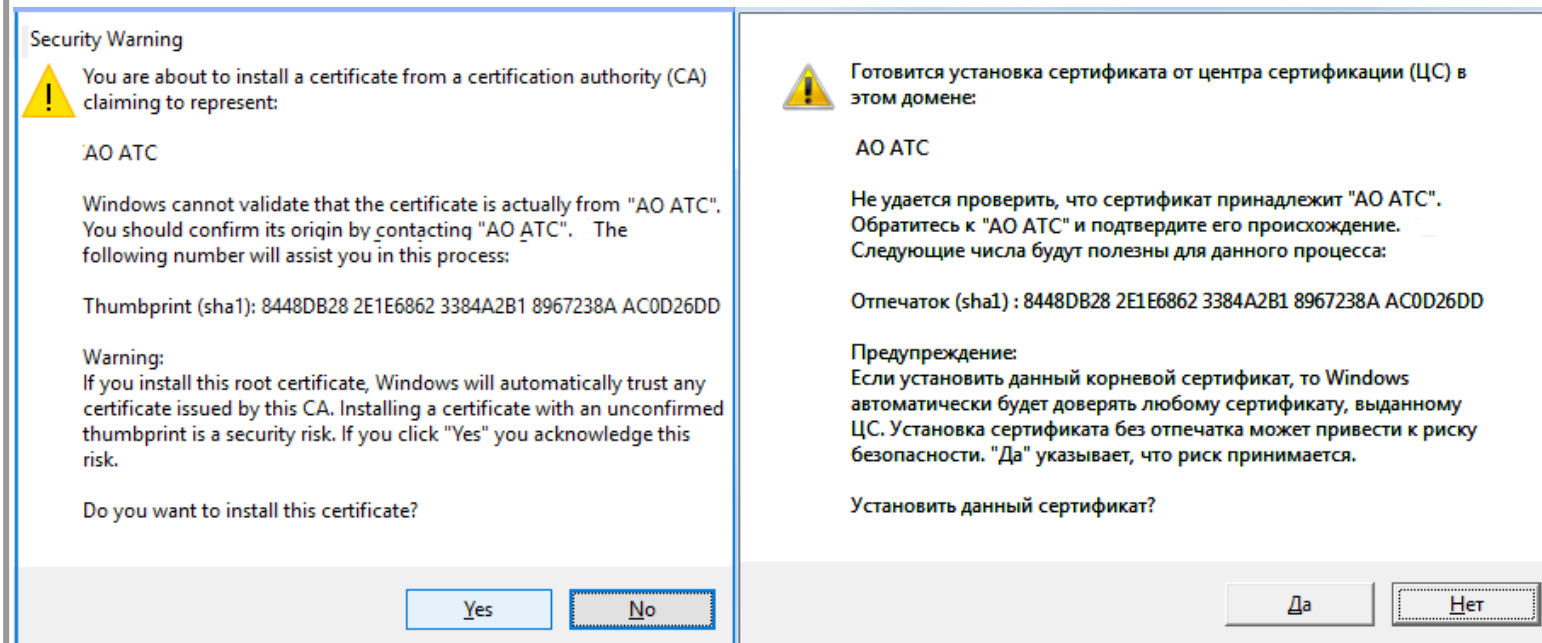
Нет



- Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

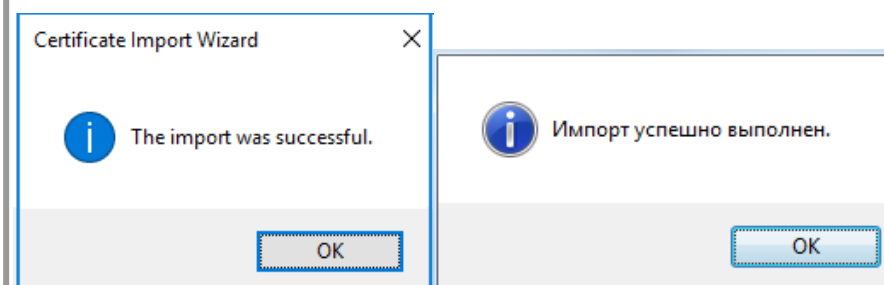
7. Вы получите аналогичное предупреждение в отношении сертификата АО АТС.

Нажмите кнопку ("Да") в окне предупреждения.



8. Вы получите сообщение о завершении установки сертификатов ("The import was successful").

Нажмите кнопку .





- Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

Внимание!

Шаги 9 - 11 выполняются только в том случае, если вы устанавливаете корневые сертификаты из файла, скачанного с сайта АО "АТС" по ссылке

[Корневые сертификаты Минкомсвязи России и УЦ АО «АТС» 2017-2018 \(включая ГОСТ-2012\)](#)

или по ссылке:

[Корневые сертификаты Минкомсвязи России, ГУЦ и УЦ АО «АТС» 2016](#)

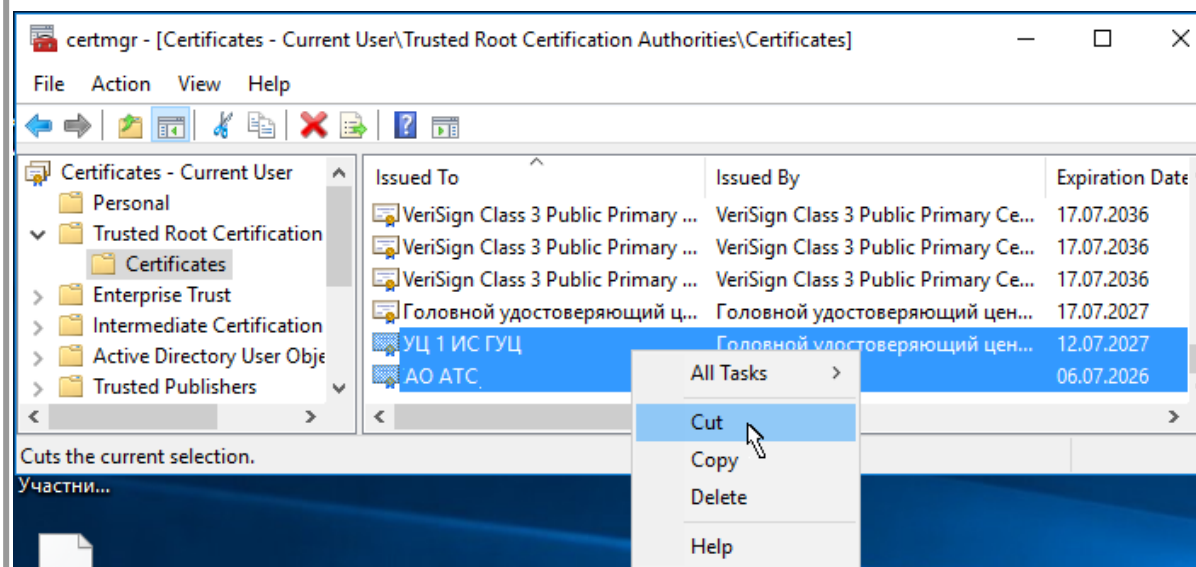
В этом случае сертификаты  УЦ 1 ИС ГУЦ и  АО АТС необходимо переместить из хранилища "Trusted Root Certification Authorities" ("Доверенные корневые центры сертификации") в хранилище "Intermediate Certification Authorities" ("Промежуточные центры сертификации").

Если вы устанавливаете корневые сертификаты из файла, скачанного с сайта АО "АТС" по ссылке

[Корневые сертификаты УЦ АО «АТС» за 2011-2015 годы](#),

или если вы устанавливаете корневой сертификат из файла, экспортированного из ключевого носителя с использованием утилиты "Панель управления Рутокен", то выполнять пункты 9 - 11 **не нужно!**

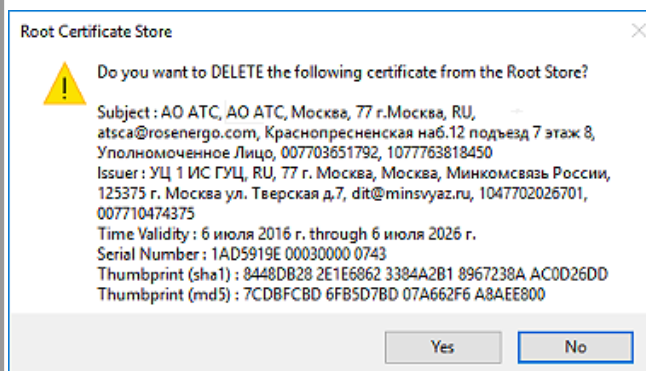
9. Чтобы переместить сертификаты в хранилище "Промежуточные центры сертификации", выделите сертификаты  УЦ 1 ИС ГУЦ и  АО АТС в списке (нажмите клавишу "Ctrl" и, удерживая ее, щелкните мышью эти сертификаты), затем правой кнопкой мыши откройте контекстное меню и выберите в нем пункт "Cut" ("Вырезать").



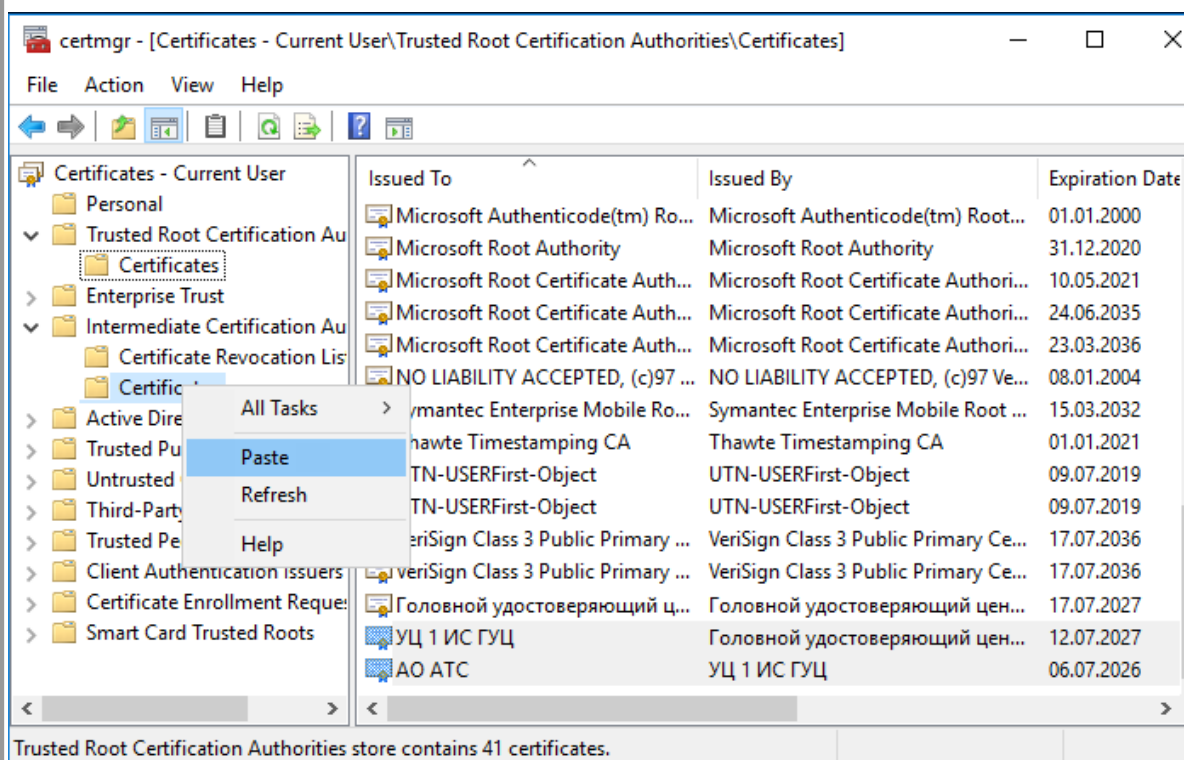


- Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов
- Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"
- Установка личного сертификата закрытого ключа пользователя
- Проверка контейнера закрытого ключа личного сертификата подписи
- Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"

10. Так как при перемещении сертификатов они удаляются из исходного хранилища (вы выбрали команду "Вырезать"), Windows потребует от вас подтвердить удаление. Нажмите кнопку



11. Выделите щелчком мыши папку "Intermediate Certification Authorities -> Certification", правой кнопкой мыши откройте контекстное меню для этой папки и выберите в нем пункт "Paste" ("Вставить").



- Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов
- Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"
- Установка личного сертификата закрытого ключа пользователя
- Проверка контейнера закрытого ключа личного сертификата подписи
- Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"

Скачивание корневых сертификатов с сайта АО "АТС"

Зайдите на сайт АО "АТС" в раздел "Корневые сертификаты удостоверяющих центров":

"Главная" -> **Электронный документооборот** -> Удостоверяющий центр -> **Корневые сертификаты удостоверяющих центров**"

Вы увидите ссылки для скачивания сертификатов:

Корневые сертификаты удостоверяющих центров

- Корневые сертификаты Минкомсвязи России и УЦ АО «АТС» 2017-2018 (включая ГОСТ-2012)
- Корневые сертификаты Минкомсвязи России, ГУЦ и УЦ АО «АТС» 2016
- Корневые сертификаты УЦ АО «АТС» за 2011-2015 годы

Примечание: наличие в хранилище "Доверенные корневые центры сертификации" корневых сертификатов УЦАО "АТС" за 2011 - 2015 годы, а также корневых сертификатов Минкомсвязи России, ГУЦи УЦАО "АТС" за 2016 год необходимо для работы со старыми документами, а также для корректной установки ПО "CryptoEnergyPro".

Внимание! Сертификаты УЦ АО "АТС" за 2011 - 2015 годы не нужно перемещать в другие хранилища (не нужно выполнять шаги 5.9 - 5.11) в процедуре, описание которой приводится ниже.

Сертификаты, которые можно скачать по ссылке "

Корневые сертификаты Минкомсвязи России и УЦ АО «АТС» 2017-2018 (включая ГОСТ-2012)" рекомендуется устанавливать из файлов, экспортированных из ключевых носителей "Рутокен" при помощи утилиты "Панель управления Рутокен".

Установка сертификатов из ключевых носителей обеспечивает Участнику ОРЭМ более высокий уровень безопасности, так как при этом не используется Интернет.

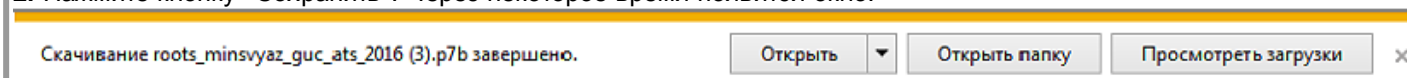
Для двух последних ссылок (или для каждой из трех ссылок) выполните шаги с 1 по 4:

1. Пройдите по ссылке.

Откроется окно загрузки файла, содержащего корневые сертификаты удостоверяющих центров:



2. Нажмите кнопку "Сохранить". Через некоторое время появится окно:



3. Нажмите кнопку "Открыть папку".

Появится окно, содержащее раскрытую папку "Загрузки", в которой загруженный файл с сертификатами выделен.

4. Скопируйте или переместите этот файл из папки "Загрузки" в удобную для вас папку.

Установка сертификатов ► Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен" (все версии Windows)

1 из 1

- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"
- [Установка личного сертификата закрытого ключа пользователя](#)
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

Корневые сертификаты удостоверяющих центров сначала экспортируются из ключевого носителя Рутокен в файлы, а затем устанавливаются в хранилища "Доверенные корневые центры сертификации" и "Промежуточные центры сертификации" из файлов в соответствии с описанием в разделе ["Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов"](#).

Откройте окно утилиты "Панель управления Рутокен" двойным щелчком мыши по ее ярлыку . Далее последовательность ваших действий показана на рис. 1 зелеными цифрами:

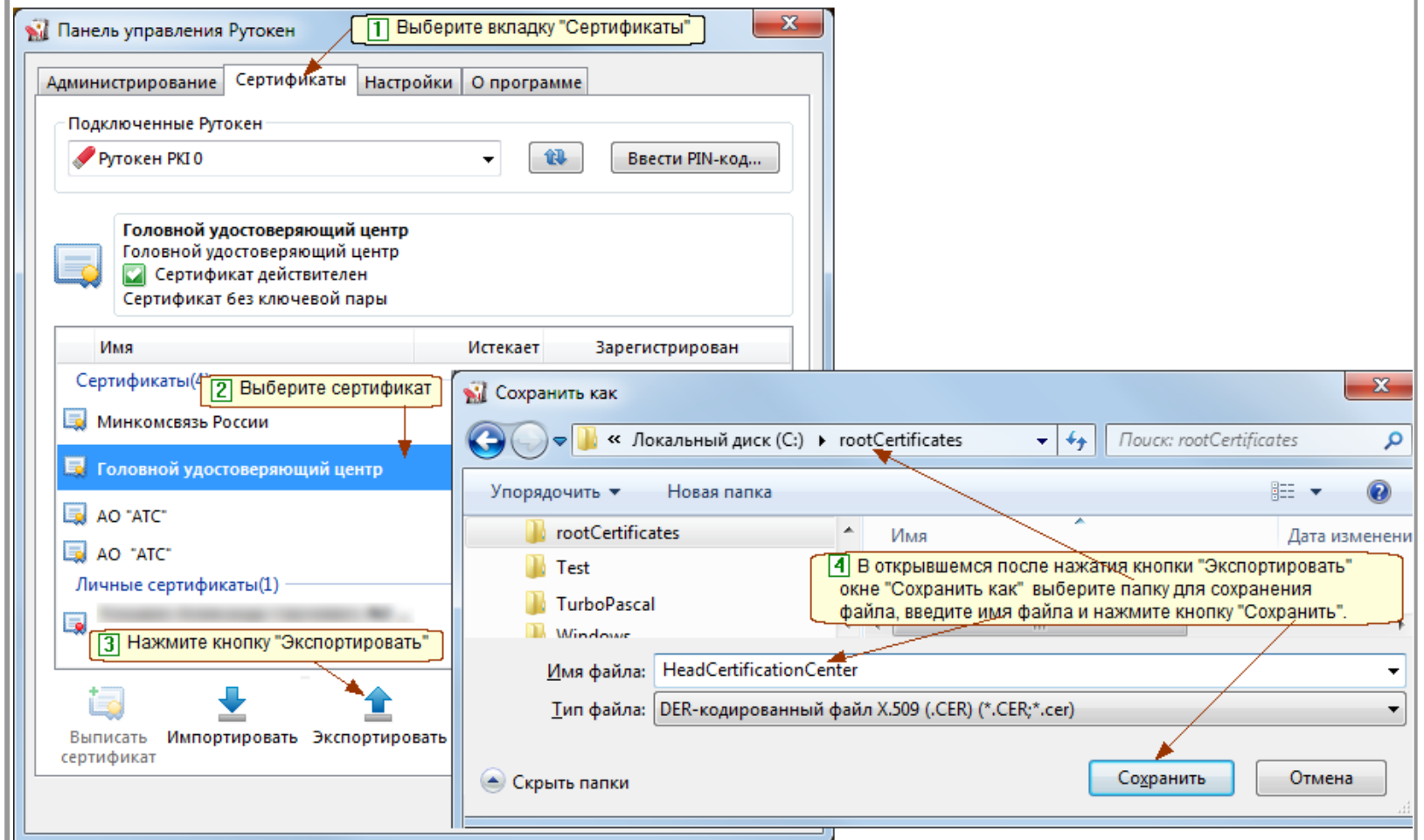


Рис. 1

Далее установите из полученных файлов сертификаты "Головной удостоверяющий центр" и "Минкомсвязь России" в хранилище "Доверенные корневые центры сертификации", и другие сертификаты (кроме личных) в хранилище "Промежуточные центры сертификации", в соответствии с описанием в разделе ["Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов"](#).

- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

Для того чтобы сотрудник Участника мог использовать ключевой носитель **Рутокен** для подписывания исходящих сообщений или для расшифровки входящих сообщений, он должен установить на своем компьютере в хранилище Personal (Личные) свой закрытый (личный, секретный) сертификат, который содержится в ключевом носителе.

Ключевой носитель содержит ключевой контейнер, в котором находится личный (закрытый) ключ Пользователя и парный к нему открытый ключ Пользователя. Ключевой контейнер может содержать не более одного ключа подписи и не более одного ключа шифрования. Дополнительно ключевой контейнер содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей, их целостности и т. п.

АО "АТС" генерирует ключевую пару, записывает ее на электронный носитель "Рутокен", записывает также корневые сертификаты удостоверяющих центров, входящие в путь сертификации личного сертификата Участника ОПЭМ,

Установка личного сертификата в "КриптоПро CSP 3.9" под Windows 10 выполняется так же, как в "КриптоПро CSP 3.6" под Windows 7 (открываются одни и те же окна, в которых выполняются одни и те же действия). На рисунках в этом разделе изображения (снимки с экрана) англоязычных окон получены при установке личного сертификата в "КриптоПро CSP 3.9" под Windows 10, изображения русскоязычных окон получены при установке личного сертификата "КриптоПро CSP 3.6" под Windows 7.

В данном разделе выполняется:

1. Проверка наличия личного (закрытого) ключа в контейнере ключевого носителя Рутокен,
2. Установка личного сертификата представителя Участника в хранилище "Личные" на компьютере Участника.

Шаг 1. Присоединение к компьютеру ключевого носителя

Вставьте в USB порт полученный в УЦ АО "АТС" ключевой носитель "Рутокен".

Шаг 2. Запуск программы настройки ПО "КриптоПро CSP"

Откройте панель управления:

1 Для Windows 7:  -> **Панель управления**.

2 Для Windows 10:

 -> правой кнопкой мыши откройте меню -> выберите **Control Panel** ("Панель управления").
Если в раскрывающемся списке "View by" ("Просмотр") выбран пункт "Категория",

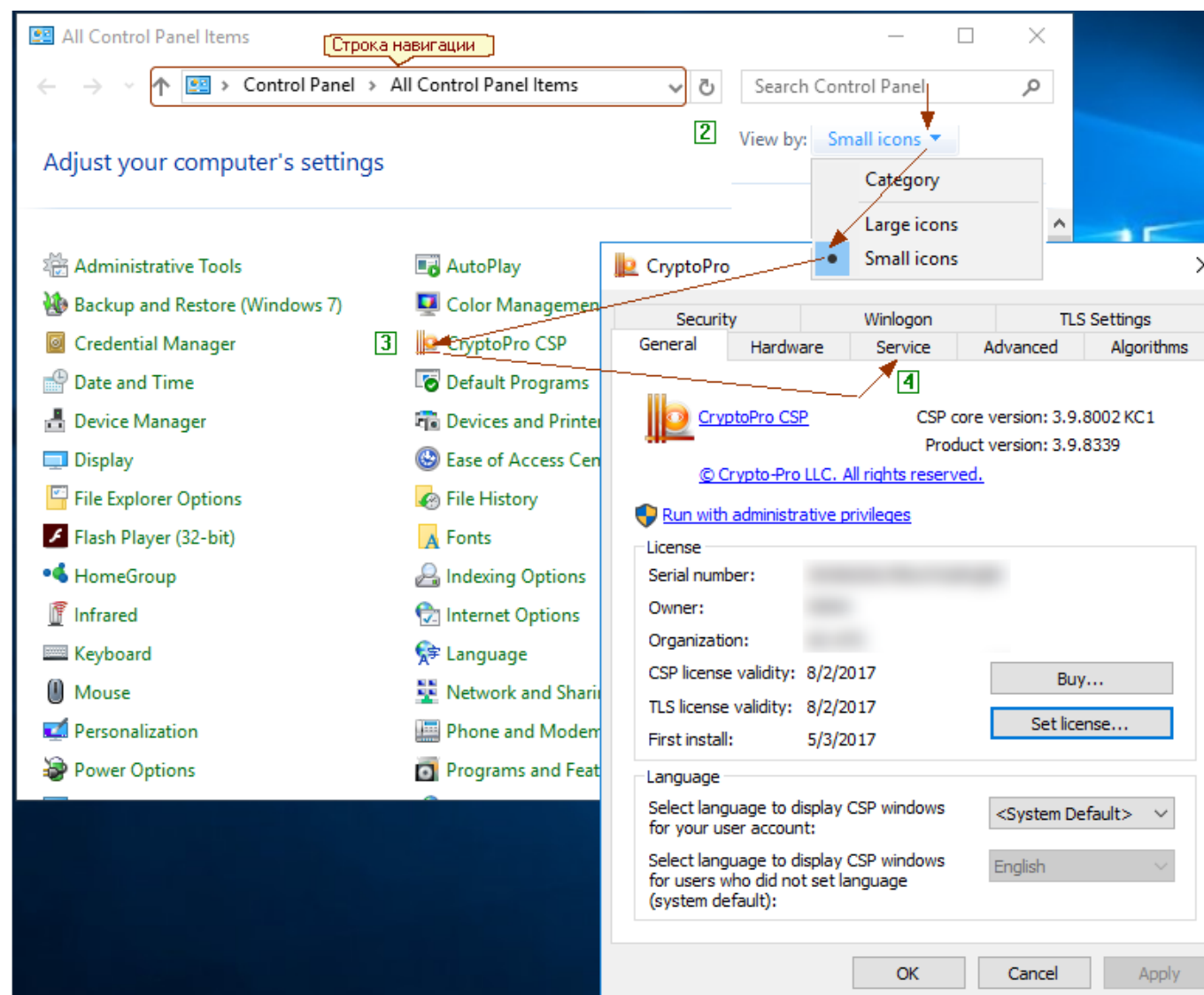
то выберите категорию  **Security and Maintenance** ( **Система и безопасность**),
Если выбран пункт "Small icons" ("Мелкие значки") или "Large icons" ("Крупные значки"),
то сразу переходите к пункту **3**.

3 Двойным щелчком мыши откройте окно "CryptoPro CSP" ("КриптоПРО CSP").

Важно! На вкладке "Общие" ("General") нажмите ссылку "[Запустить с правами администратора](#)".

- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- Установка личного сертификата закрытого ключа пользователя
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

4 В окне "КриптоПРО CSP" выберите вкладку "Service" ("Сервис"):



- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- **Установка личного сертификата закрытого ключа пользователя**
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

Шаг 3. Выбор контейнера ключевого носителя.

На вкладке "Service" ("Сервис") нажмите кнопку "View certificates in container ..." ("Просмотреть сертификаты в контейнере..."):

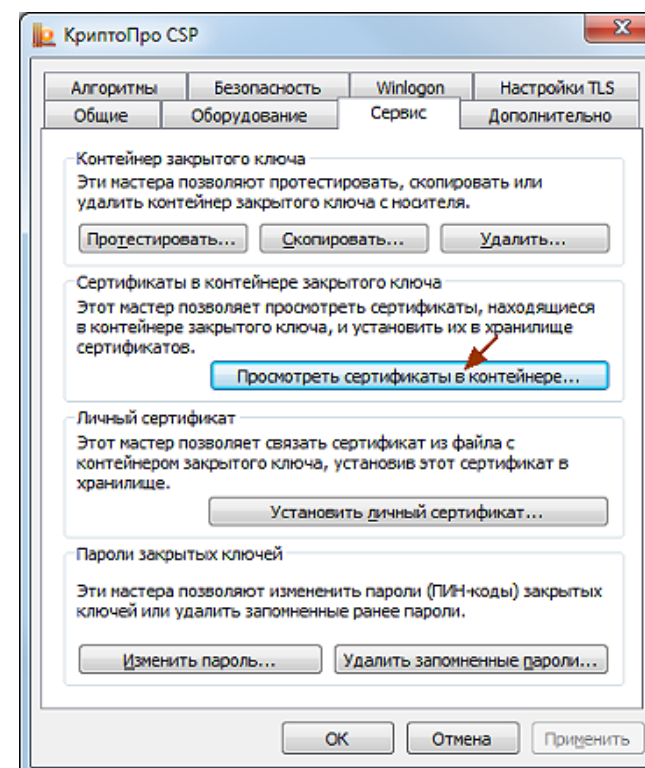
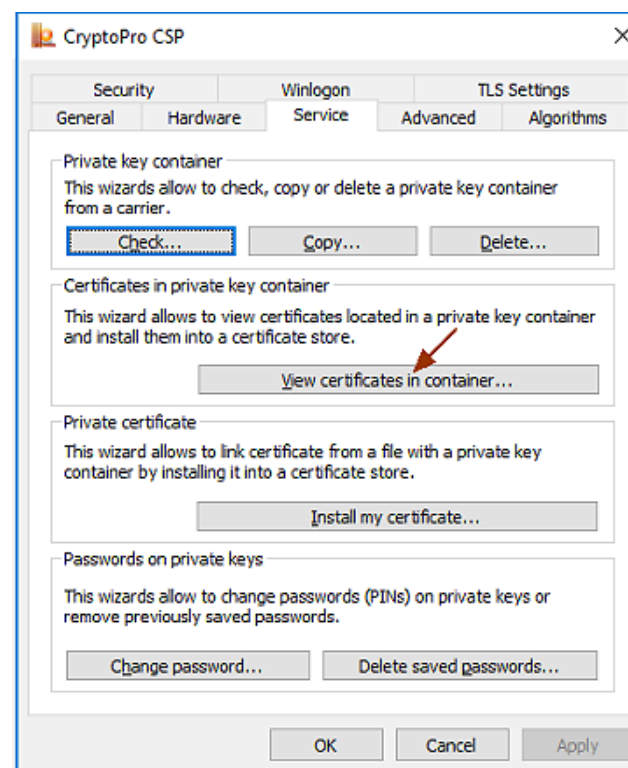


Рис. 3-1

- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- Установка личного сертификата закрытого ключа пользователя
- Проверка контейнера закрытого ключа личного сертификата подписи
- Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"

что приведет к появлению окна "Certificates in private key container" ("Сертификаты в контейнере секретного ключа"):

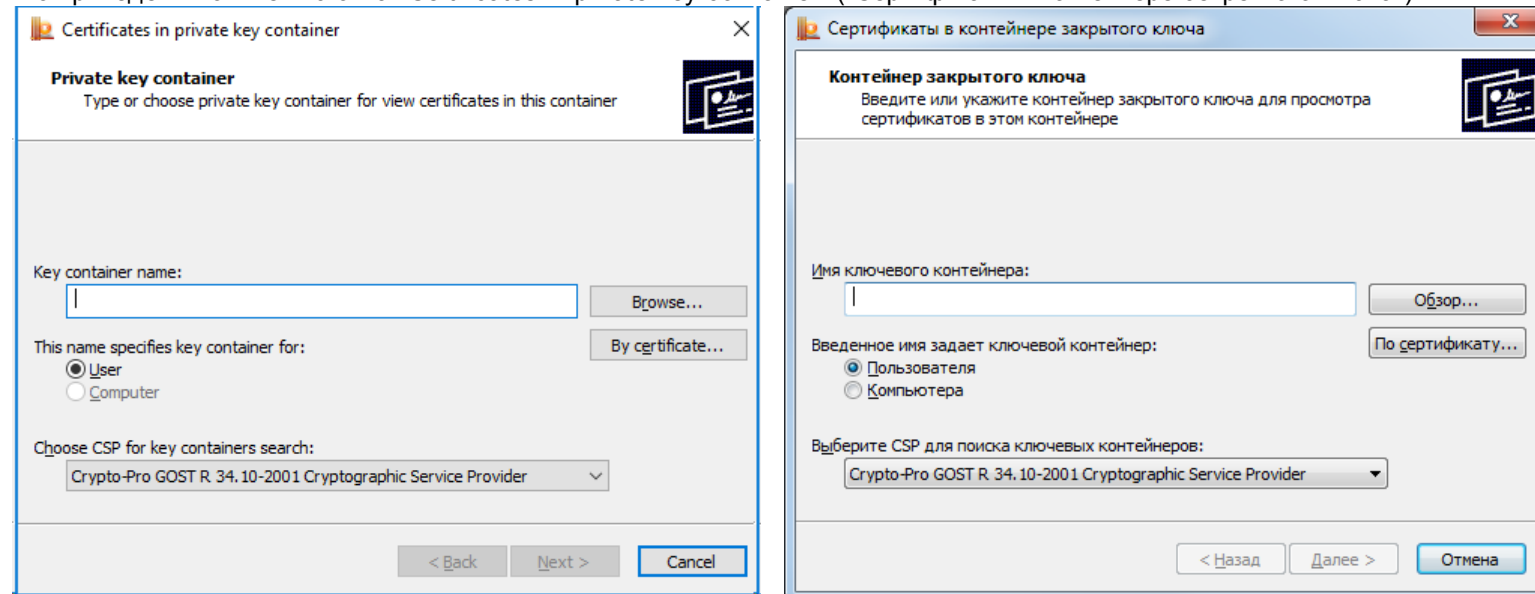


Рис. 3-2

В окне "Certificates in private key container" ("Сертификаты в контейнере секретного ключа"):

выберите ключевой носитель одним из двух способов:

а) нажмите кнопку "Browse..." ("Обзор..."), в появившемся окне "Select key container" ("Выбор ключевого носителя") выделите щелчком мыши контейнер с выбранным ключом пользователя и нажмите кнопку "OK":

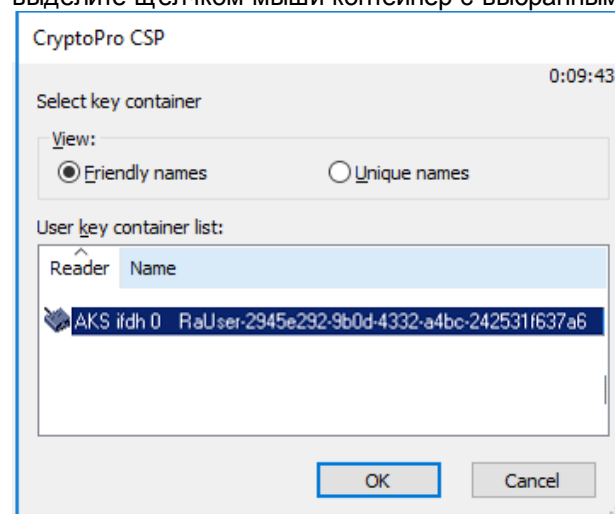
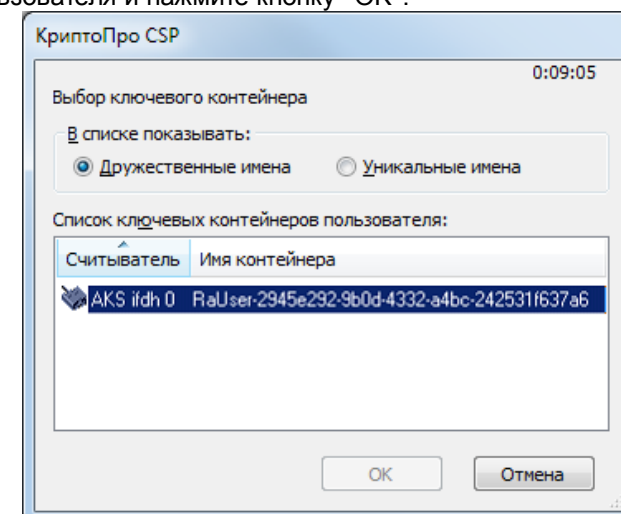


Рис. 3-3



- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- Установка личного сертификата закрытого ключа пользователя
- Проверка контейнера закрытого ключа личного сертификата подписи
- Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"

б) нажмите кнопку "By certificate" ("По сертификату").

В открывшемся окне "Select a Certificate" ("Выбор сертификата") выберите ваш личный сертификат, находящийся в ключевом носителе, присоединенном в данный момент времени к компьютеру.

Выбранное имя ключевого контейнера появится в поле "Key container name" ("Имя ключевого контейнера"):

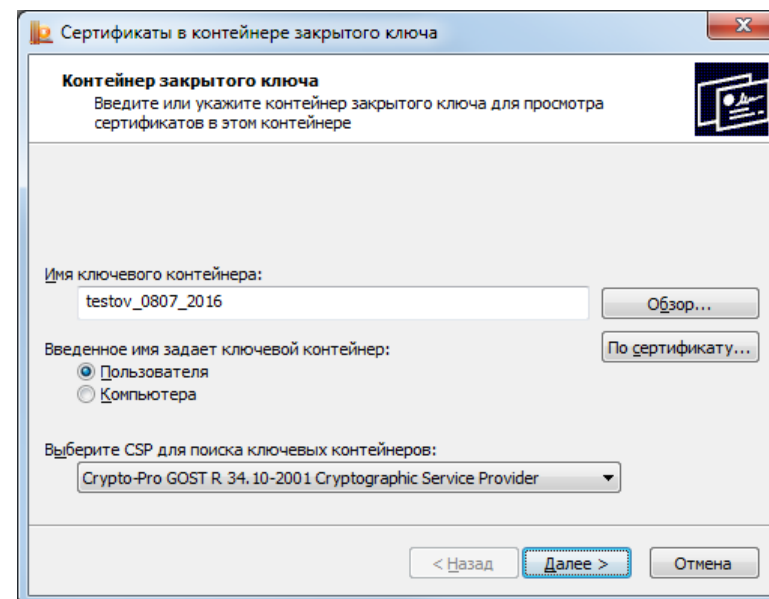
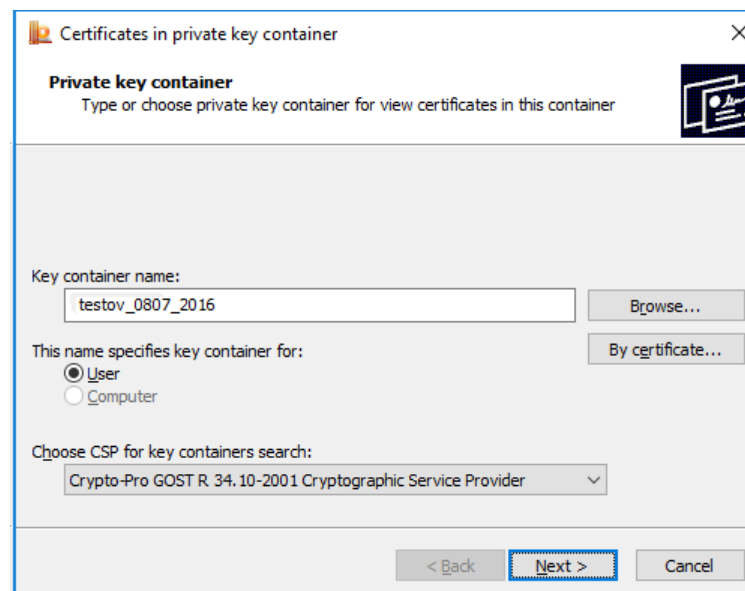


Рис. 3-4

Нажмите кнопку ().

- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- Установка личного сертификата закрытого ключа пользователя
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

Шаг 4. Считывание информации из ключевого носителя и установка в хранилище "Личные".

Если после нажатия кнопки "[Далее >](#)" ("[Next >](#)") появится окно:

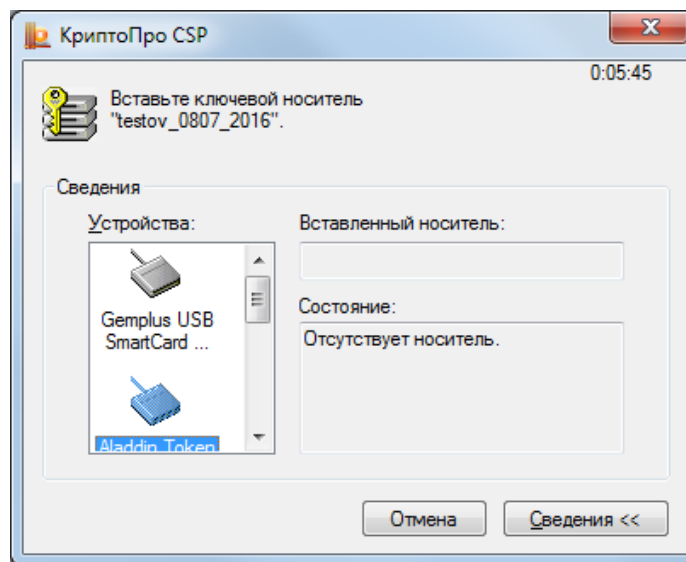


Рис. 4-1

а ключевой носитель, тем не менее, вставлен, то выньте ключевой носитель и снова вставьте его.

После нажатия кнопки "[Далее >](#)" ("[Next >](#)"), возможно, откроется окно для ввода пароля доступа к носителю с закрытым ключом (PIN код) (окно откроется, если пароль еще не был установлен):

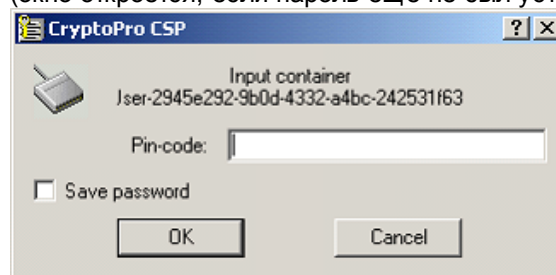
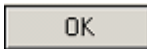


Рис. 4-2

В это окно введите PIN код и нажмите кнопку .

Замечание

Поскольку на данном шаге процедуры запускается процесс обмена информацией с контейнером и с одновременной расшифровкой считанной информации, то до появления следующего окна может пройти достаточно много времени (около 10-30 сек), в течение которого рекомендуется ничего не предпринимать.

- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

После окончания процесса считывания сертификата и его расшифровки, будет открыто окно с его параметрами:

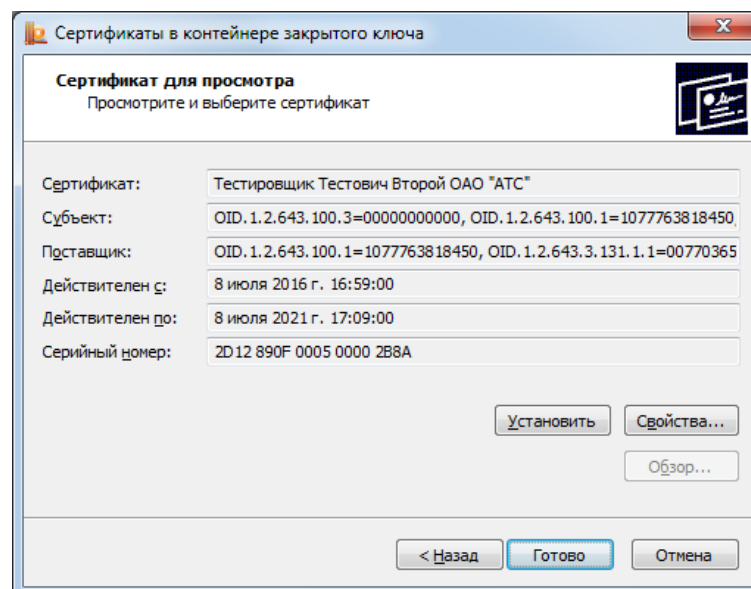
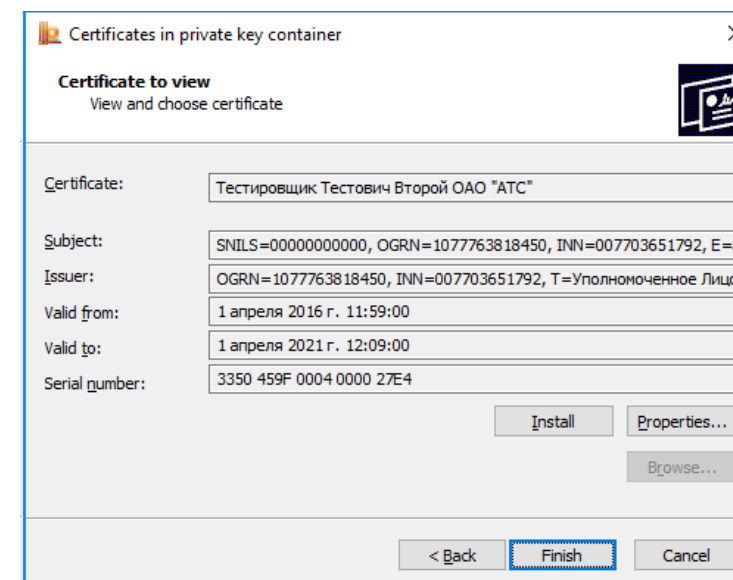


Рис. 4-3



2. Нажмите кнопку **Install** (**Установить**).

Вы получите сообщение:

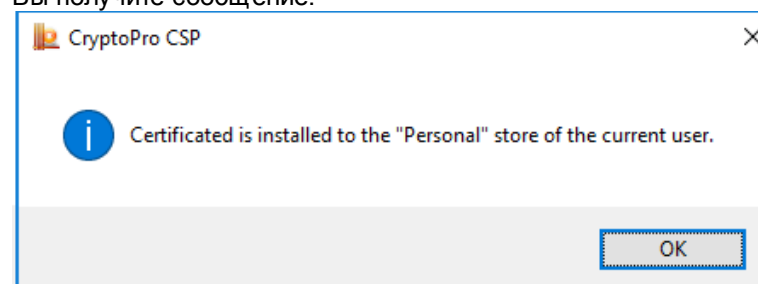


Рис. 4-4

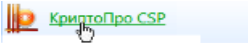
("Сертификат установлен в хранилище "Личные" текущего пользователя").

Нажмите кнопку **OK** в окне , затем кнопку **Finish** в окне "Certificate to view" ("Сертификат для просмотра").

- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- Проверка контейнера закрытого ключа личного сертификата подписи
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

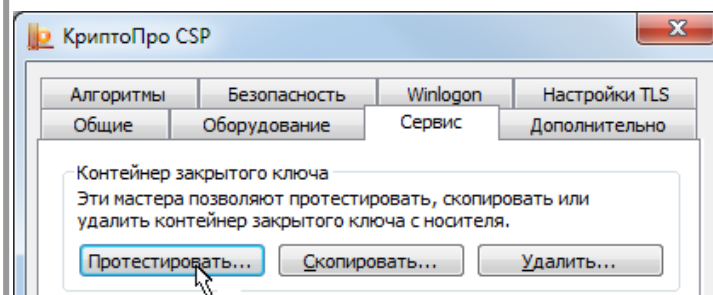
Вставьте в usb - порт компьютера ключевой носитель, содержащий контейнер с вашим личным сертификатом.

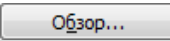
[Откройте панель управления](#)

На панели управления выберите щелчком мыши элемент . Откроется окно свойств "КриптоПро CSP" на вкладке "Общие", в котором: Нажмите [ссылку "Запустить с правами администратора"](#). Выберите вкладку "Сервис".

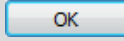
Далее:

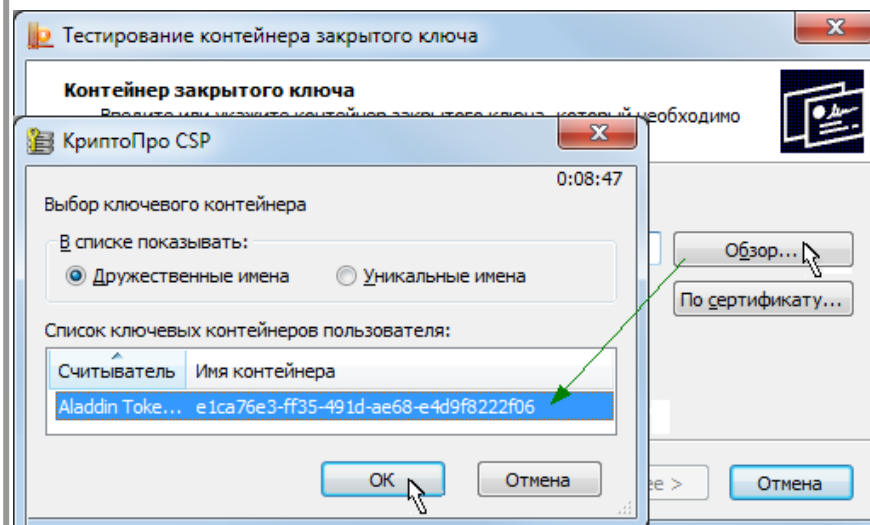
1. Нажмите кнопку "Протестировать..."



2. В открывшемся окне "Контейнер закрытого ключа" нажмите кнопку .

Откроется окно "Выбор ключевого контейнера",

в котором выберите ключевой контейнер (если он не один), и нажмите кнопку .

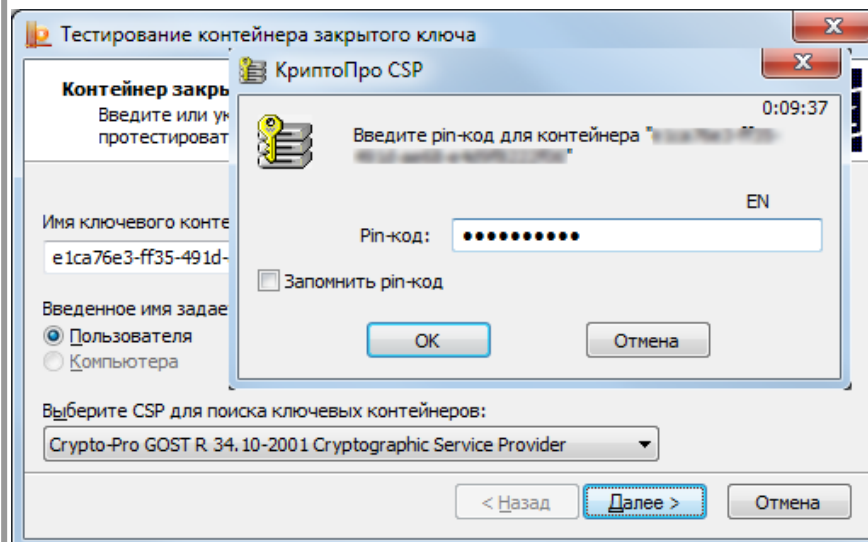


Окно "Выбор ключевого контейнера" закрывается.

- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- Проверка контейнера закрытого ключа личного сертификата подписи
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

3. В окне "Контейнер закрытого ключа" нажмите кнопку **Далее >**.

В открывшемся окне введите pin-код контейнера и нажмите кнопку **OK**.



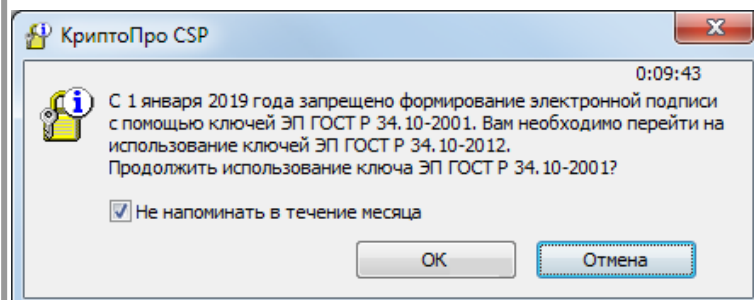
Окно "Введите pin-код для контейнера..." закроется, откроется окно с предупреждением: "С 1 января 2019 года..."

4. В окне с предупреждением

"С 1 января 2019 года запрещено формирование электронной подписи с помощью ключей ЭП ГОСТ Р 34.10-2001..."

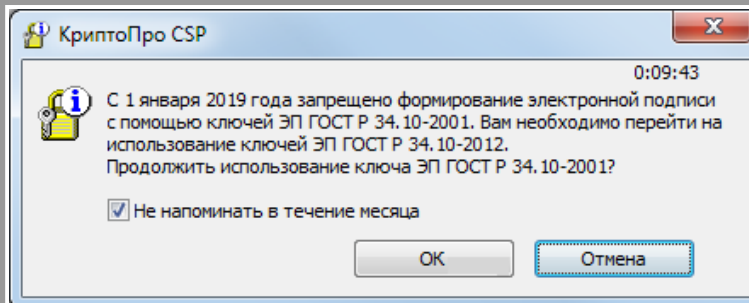
нажмите кнопку **OK**.

Замечание: это предупреждение перестанет появляться после перехода УЦ АО "АТС" на ключи ЭП ГОСТ Р 34.10-2012.



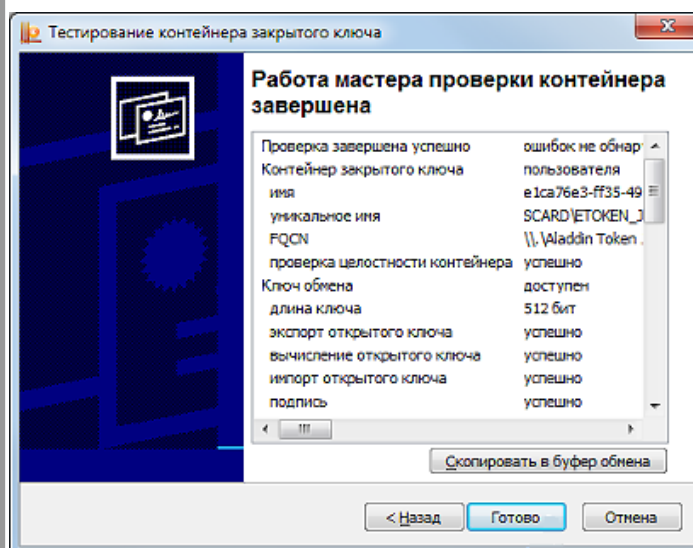
Окно с предупреждением закроется.

- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- Проверка контейнера закрытого ключа личного сертификата подписи
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)



Окно с предупреждением закроется.

5. Просмотрите список результатов проверок. Если есть ошибки, обратитесь в службу поддержки компании "КриптоПро". Нажмите кнопку "Готово":



- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

Наличие сертификатов открытых ключей (сертификатов криптосерверов АО "АТС" и АО "ЦФР") в хранилище Other People (▶ Другие пользователи) необходимо при отправке зашифрованных сообщений в АО "АТС" и АО "ЦФР". В данном разделе инструкции описывается установка сертификатов открытых ключей АО "АТС". Установка сертификатов открытых ключей АО "ЦФР" выполняется аналогично в то же хранилище.

Замечание: непосредственно после установки ОС Windows хранилище Другие пользователи отсутствует. Оно автоматически создается операционной системой, когда возникает необходимость поместить в него сертификат (при получении подписанного сообщения, в частности сообщения, которое вы послали самому себе).

Скачивание файлов сертификатов открытых ключей с сайта АО "АТС"

1. Зайдите на сайт АО "АТС" в раздел "Сертификаты открытых ключей АО "АТС":

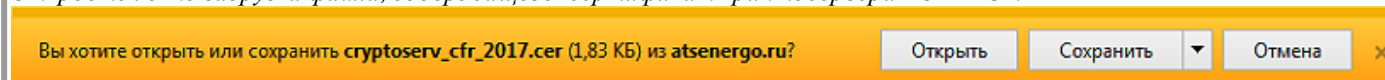
"Главная" -> [Электронный документооборот](#) -> Удостоверяющий центр -> ["Сертификаты открытых ключей АО "АТС"](#)
Откроется страница "Сертификаты открытых ключей АО "АТС", на которой можно скачать следующие сертификаты:

Сертификат	Область применения
■ Сертификат Криптосервера АО "АТС"	Шифрование документов, направляемых в АО "АТС" в рамках проведения конкурентного отбора ценовых заявок на сутки вперед и документов, связанных с торговлей мощностью.
■ Сертификат Тестового Криптосервера АО "АТС"	Шифрование документов по коммерческому учету электроэнергии, направляемых в АО "АТС" в тестовом режиме.
■ Сертификат Криптосервера коммерческого учета АО "АТС"	Шифрование документов, направляемых в АО "АТС" в процессе сбора данных по коммерческому учету электроэнергии.

Чтобы скачать один из указанных выше сертификатов АО "АТС", щелкните левой кнопкой мыши по нужной ссылке на странице "Сертификаты открытых ключей АО "АТС" и сохраните файл сертификата на свой компьютер. Например, чтобы скачать сертификат криптосервера АО "АТС":

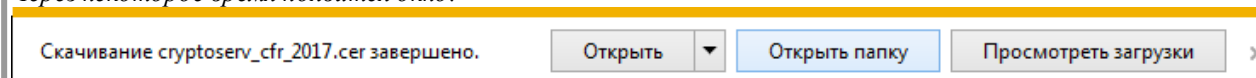
2. Пройдите по ссылке "■ [Сертификат Криптосервера АО "АТС"](#)".

Откроется окно загрузки файла, содержащего сертификат криптосервера АО "АТС":



3. Нажмите кнопку "Сохранить".

Через некоторое время появится окно:



4. Нажмите кнопку "Открыть папку".

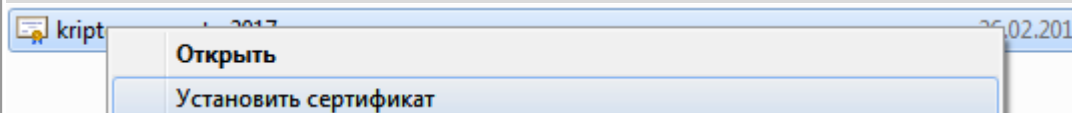
Появится окно, содержащее раскрытую папку "Загрузки", в которой загруженный файл с сертификатами выделен.

5. Правой кнопкой мыши откройте контекстное меню для этого файла, скопируйте (пункт "Копировать") или переместите (пункт "Вырезать") этот файл в удобную для вас папку. (откройте эту папку, откройте контекстное меню и выберите пункт "Вставить").

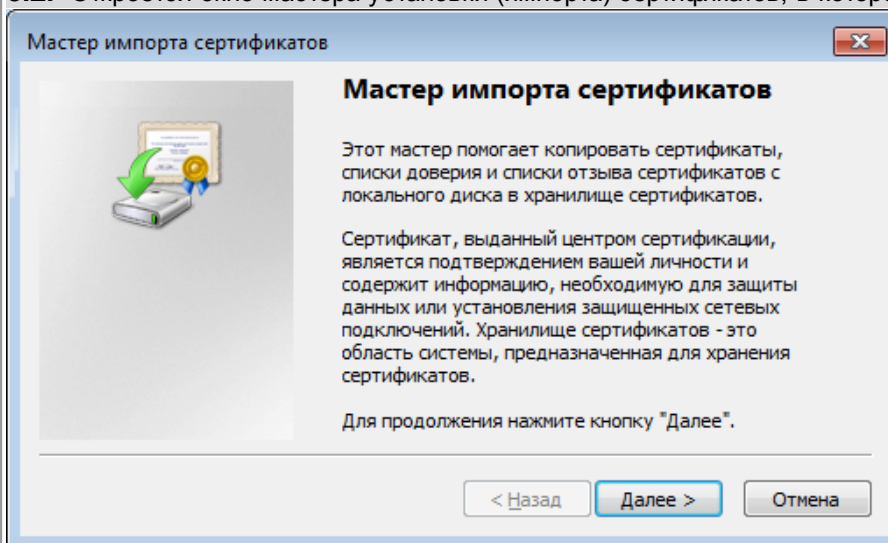
- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

Установка сертификата криптосервера из файла в хранилище сертификатов

5.1. Щелчком правой кнопкой мыши по файлу с сертификатами откройте контекстное меню для этого файла и выберите в нем пункт "Установить сертификат".



5.2. Откроется окно мастера установки (импорта) сертификатов, в котором нажмите кнопку [Далее >](#).

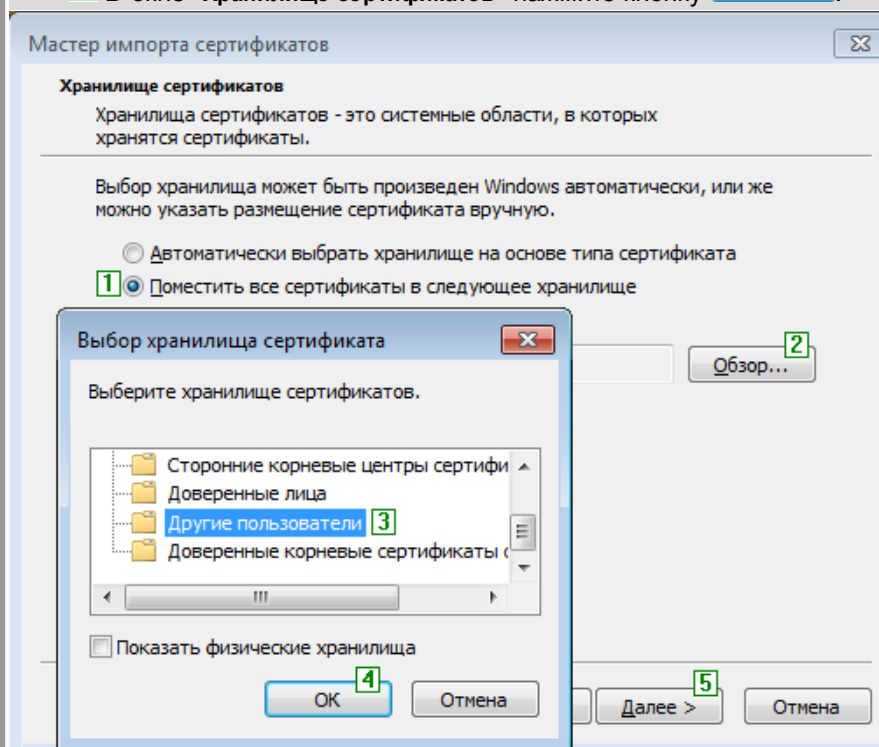


- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- [Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"](#)

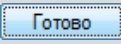
5.3. Открывается окно "Хранилище сертификатов".

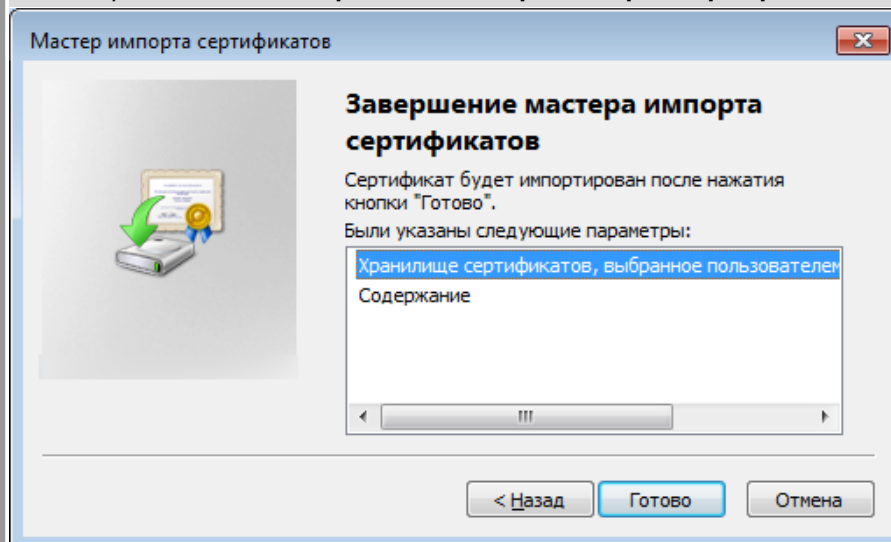
В этом окне :

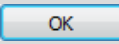
- 1 Отметьте кнопку ☒ Поместить все сертификаты в следующее хранилище
- 2 Нажмите кнопку . Откроется окно "Выбор хранилища сертификатов".
- 3 Выберите хранилище Другие пользователи.
- 4 Нажмите кнопку . Окно "Выбор хранилища сертификатов" закроется.
- 5 В окне "Хранилище сертификатов" нажмите кнопку .

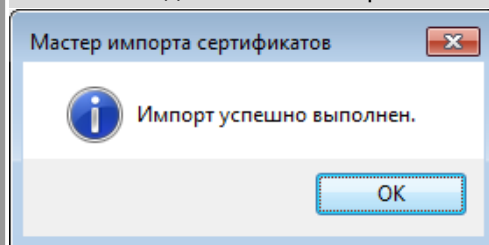


- [Установка корневых сертификатов удостоверяющих центров в хранилища сертификатов из файлов](#)
- [Установка корневых сертификатов удостоверяющих центров из ключевого носителя Рутокен с использованием утилиты "Панель управления Рутокен"](#)
- [Установка личного сертификата закрытого ключа пользователя](#)
- [Проверка контейнера закрытого ключа личного сертификата подписи](#)
- Установка сертификатов открытых ключей АО "АТС" и АО "ЦФР"

5.4. Откроется окно "Завершение мастера импорта сертификатов", в котором нажмите кнопку .



5.5. В последнем окне мастера нажмите кнопку .



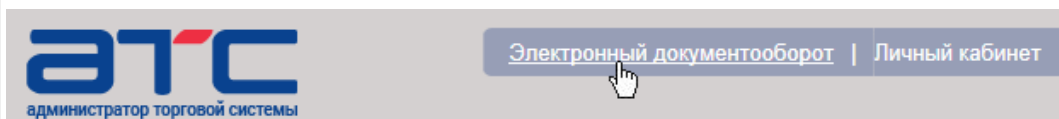
Аналогично установите сертификаты других необходимых вам криптосерверов.

- [Изменения в текущей версии \(1.11\) инструкции](#)
- [Быстрый старт: краткое руководство по установке криптографического ПО и сертификатов](#)
- [Подготовка к установке криптографического ПО](#)
- + [Установка криптографического ПО](#)
- + [Установка сертификатов](#)
- Установка "CryptoEnergyPro"
- + [Элементы первичной диагностики проблем](#)
- + [Приложение](#)

CryptoEnergyPro это универсальное ПО, способное работать с любой версией Windows, в том числе, с Windows 7 и Windows 10.
Установка CryptoEnergyPro выполняется одинаково под Windows 7 и под Windows 10.

Переход на страницу "Программные продукты" сайта АО "АТС".

С главной страницы сайта АО "АТС" перейдите по ссылке "Электронный документооборот" на страницу "Электронный документооборот":



Авторизация.

На странице "Электронный документооборот" нажмите ссылку "Программные продукты".

Откроется страница "Авторизация":

Авторизация

Для доступа необходима авторизация!

Вход по логину

Доступ осуществляется с использованием идентификаторов пользователя и пароля.

Код участника *

Пользователь *

Пароль *

Войти

Вход по сертификату

Доступ производится с использованием ключей, выпущенных Удостоверяющим центром АО "АТС"

Вход по сертификату

Вставьте ключевой носитель с вашим личным сертификатом и нажмите эту кнопку. В открывшемся окне выберите ваш сертификат

ПО "КриптоПро TLS" устанавливается автоматически при установке "КриптоПро CSP", но лицензия приобретается отдельно.

Для доступа в "Персональный раздел" или "ПАК" на компьютере должно быть установлено ПО КриптоПро TLS.

[Инструкция по установке криптографического ПО и сертификатов](#)

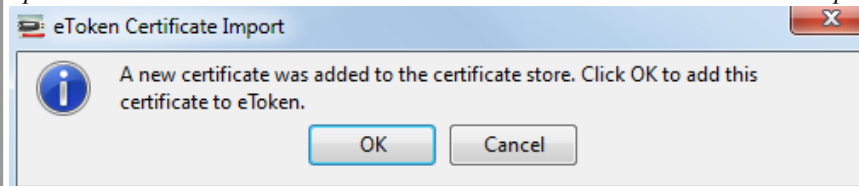
Инструкция, которую вы читаете в данный момент времени.

Выполните авторизацию одним из двух способов:

- Введите код Участника, от имени которого вы выполняете авторизацию, ваш логин и пароль, нажмите кнопку **Войти**.
- Вставьте ключевой носитель, содержащий закрытый ключ вашего личного сертификата, нажмите кнопку **Вход по сертификату**, в открывшемся окне "Выбор сертификата" выберите ваш личный сертификат, нажмите кнопку **Войти**.

- [Изменения в текущей версии \(1.11\) инструкции](#)
- [Быстрый старт: краткое руководство по установке криптографического ПО и сертификатов](#)
- [Подготовка к установке криптографического ПО](#)
- + [Установка криптографического ПО](#)
- + [Установка сертификатов](#)
- Установка "CryptoEnergyPro"
- + [Элементы первичной диагностики проблем](#)
- + [Приложение](#)

Примечание: если после нажатия кнопки **Вход по сертификату** открылось окно:



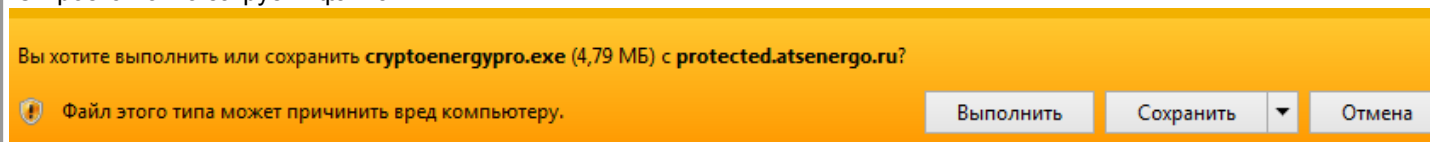
то нажмите кнопку "Cancel".

Скачивание файла программы установки "CryptoEnergyPro".

В открывшемся разделе сайта "Программные продукты" нажмите ссылку **Программа установки CryptoEnergyPro v. 1.2.10 : НОРЭМ**

- Сертификаты УЦ АО "АТС"
- Инструкция по установке криптографического ПО и сертификатов
- Инструкция по установке криптографического ПО и сертификатов (chm)
- Программа установки АРМ Участника ОРЭМ
- Руководство пользователя ПО АРМ Участника ОРЭ
- Руководство пользователя ПО АРМ Участника ОРЭМ v.2.44.0 РП (chm)
- **Программа установки CryptoEnergyPro v. 1.2.10**
- Инструкция по переходу на КриптоПро CSP 4.0

Откроется окно загрузки файла:



Нажмите кнопку "Сохранить" и сохраните файл в удобной для вас папке.

Установка CryptoEnergyPro.

Важно!:

Перед передачей пользователям (перед публикацией на сайте), дистрибутив программы CryptoEnergyPro подписывается сертификатом АО "АТС" и при его открытии проверяется ЭЦП. Поэтому, если **Программа установки CryptoEnergyPro v. 1.2.10** не может выполнить установку, то это может быть по следующим причинам:

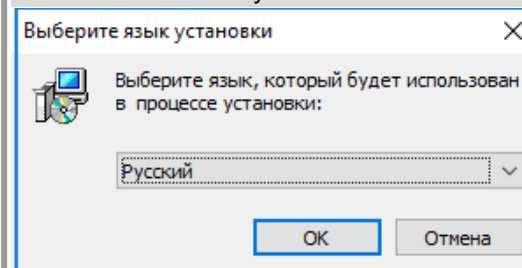
- Корневые сертификаты удостоверяющих центров, указанные в сертификате, которым был подписан файл установки CryptoEnergyPro, отсутствуют в хранилищах "Доверенные корневые центры сертификации" и "Промежуточные центры сертификации".

Решение проблемы: установите корневые сертификаты удостоверяющих центров (актуальные - желательно из ключевого носителя, за прошлые годы - из файла, скачанного с сайта АО "АТС").

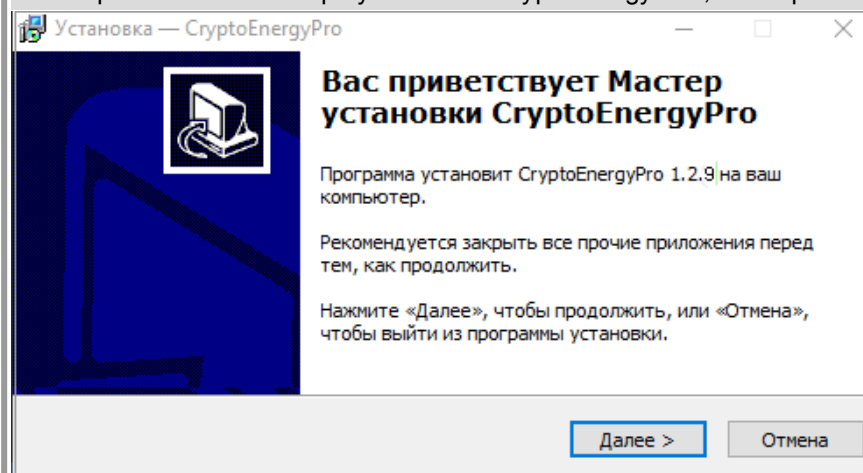
- Не была произведена перезагрузка компьютера после установки сертификатов,
- Дистрибутив CryptoEnergyPro повреждён .

- [Изменения в текущей версии \(1.11\) инструкции](#)
- [Быстрый старт: краткое руководство по установке криптографического ПО и сертификатов](#)
- [Подготовка к установке криптографического ПО](#)
- + [Установка криптографического ПО](#)
- + [Установка сертификатов](#)
- Установка "CryptoEnergyPro"
- + [Элементы первичной диагностики проблем](#)
- + [Приложение](#)

1. Запустите программу установки "CryptoEnergyPro". Откроется окно выбора языка установки. Выберите язык, на котором будут представлены надписи в окнах, которые будет открывать программа установки, и нажмите кнопку .



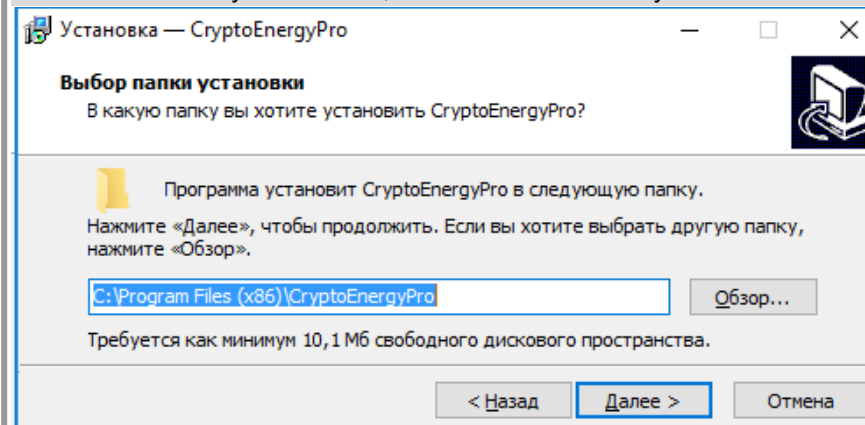
2. Откроется окно Мастера установки "CryptoEnergyPro", в котором нажмите кнопку .



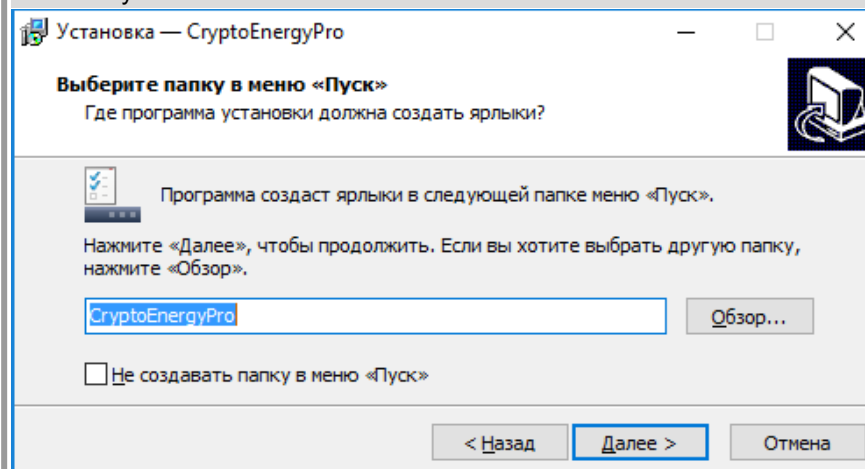
- [Изменения в текущей версии \(1.11\) инструкции](#)
- [Быстрый старт: краткое руководство по установке криптографического ПО и сертификатов](#)
- [Подготовка к установке криптографического ПО](#)
- + [Установка криптографического ПО](#)
- + [Установка сертификатов](#)
- Установка "CryptoEnergyPro"
- + [Элементы первичной диагностики проблем](#)
- + [Приложение](#)

3. Откроется окно "Выбор папки установки".

Если папка по умолчанию (предлагаемая мастером установки), устраивает вас (рекомендуется использовать ее), нажмите кнопку **Далее >**, иначе нажмите кнопку **Обзор...** и выберите другую папку, затем нажмите кнопку **Далее >**.



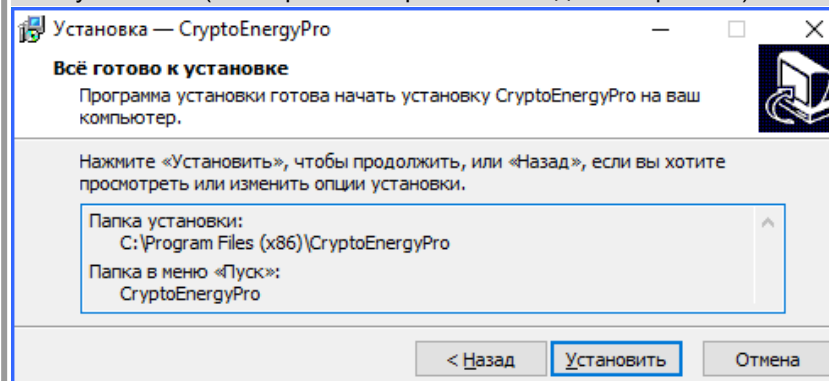
4. Откроется окно выбора папки "CryptoEnergyPro" в меню "Пуск", в которой будут созданы ярлыки программы настройки клиента COM-сервера CryptoGUI и документов, связанных с ней. Если папка по умолчанию (предлагаемая мастером установки), устраивает вас (рекомендуется использовать ее), нажмите кнопку **Далее >**, иначе нажмите кнопку **Обзор...** и выберите другую папку, затем нажмите кнопку **Далее >**.



- [Изменения в текущей версии \(1.11\) инструкции](#)
- [Быстрый старт: краткое руководство по установке криптографического ПО и сертификатов](#)
- [Подготовка к установке криптографического ПО](#)
- + [Установка криптографического ПО](#)
- + [Установка сертификатов](#)
- [Установка "CryptoEnergyPro"](#)
- + [Элементы первичной диагностики проблем](#)
- + [Приложение](#)

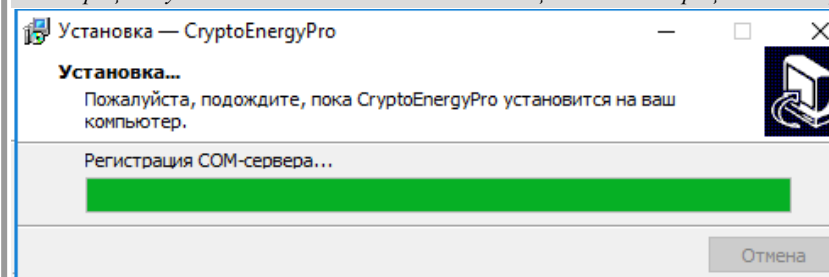
5. Откроется окно "Все готово к установке" в котором Мастер показывает выбранные вами опции установки и сообщает о готовности

к установке (к копированию файлов и созданию ярлыков). Нажмите кнопку [Установить](#).

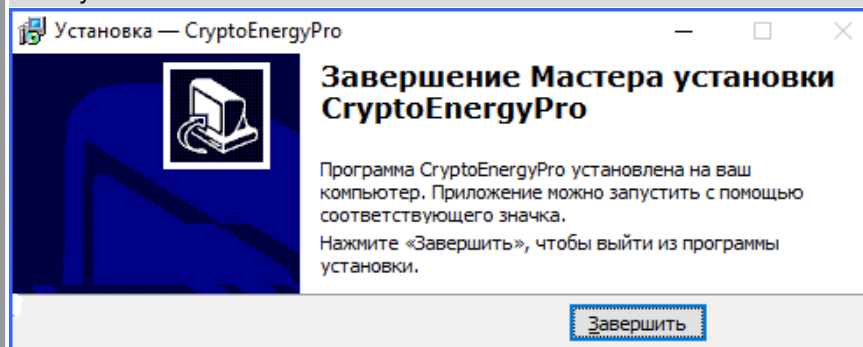


6. Откроется окно "Установка...", в котором будет отображаться индикатор прогресса установки.

В процессе установки должно появиться сообщение "Регистрация COM-сервера"



7. После завершения установки появится окно "Завершение Мастера установки CryptoEnergyPro", в котором нажмите кнопку **Завершить**.



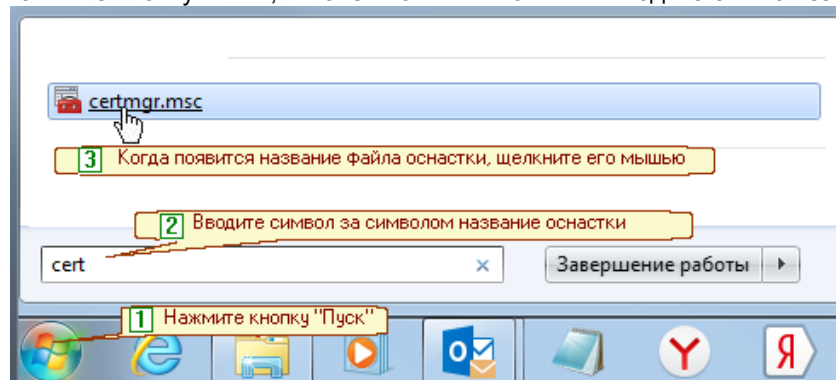
- Проверка наличия сертификатов в хранилищах
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- [Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии](#)
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- [Тестирование установленного криптографического ПО и сертификатов](#)

Если в одной из Программ вы не видите нужного сертификата в списке сертификатов для ЭЦП или в списке сертификатов для шифрования, проверьте, установлен ли он в соответствующее виду этого сертификата ("свой (личный)"/"чужой") хранилище на компьютере пользователя, а также, если вы не видите ни одного сертификата, установлены ли корневые сертификаты удостоверяющих центров, входящие в путь сертификации личного сертификата Участника ОПЭМ. Ниже описывается последовательность шагов, позволяющая открыть и просмотреть папки - хранилища сертификатов.

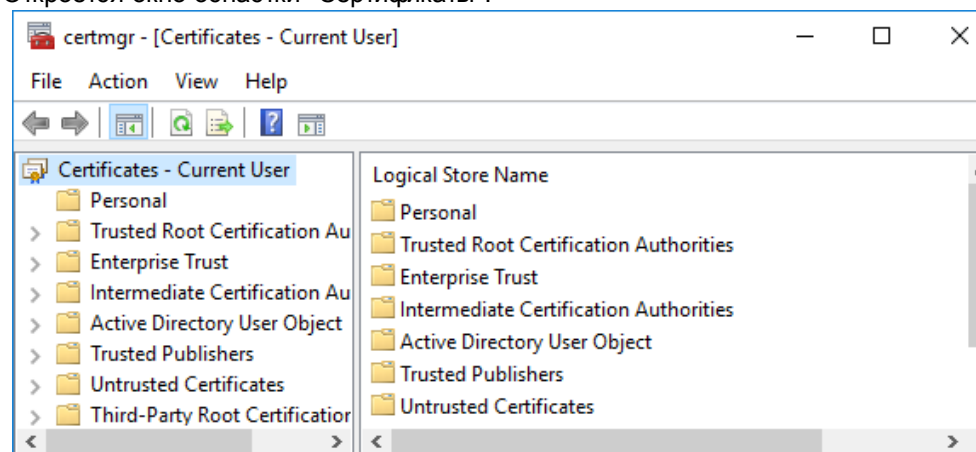
Предполагается, что на компьютере пользователя установлена оснастка "Сертификаты" с названием "certmgr". Если это не так, обратитесь к своему системному администратору, чтобы вам ее создали или сообщили ее название.

Windows 7:

Нажмите кнопку , в поле "Найти/Выполнить" вводите символ за символом название оснастки "Сертификаты":



Когда появится название файла оснастки, запустите его щелчком мыши. Откроется окно оснастки "Сертификаты":



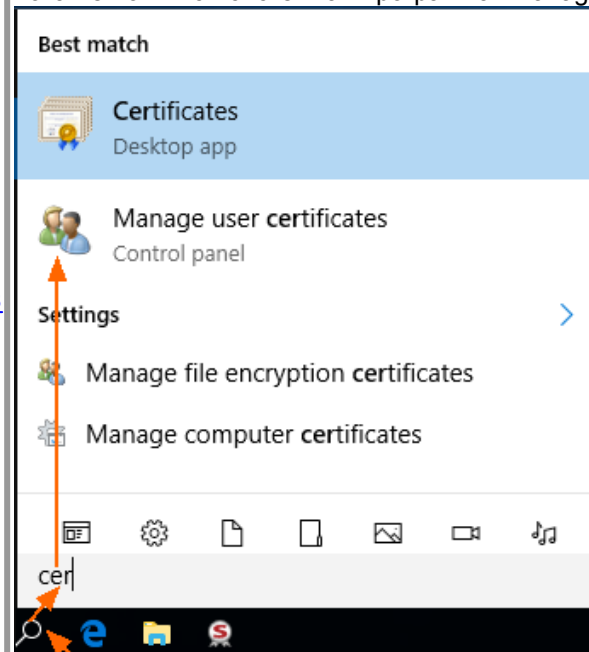
- Проверка наличия сертификатов в хранилищах
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- [Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии](#)
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- [Тестирование установленного криптографического ПО и сертификатов](#)

Windows 10:

Откройте оснастку "Сертификаты" одним из двух способов:

Способ 1:

Нажмите кнопку  ("Лупа") в нижней части экрана, Откроется окно "Search Windows" ("Поиск Windows"), в котором вводите символ за символом, название оснастки "Сертификаты" пока не появится системная программа "Manage user certificates" ("Управление сертификатами пользователя"):



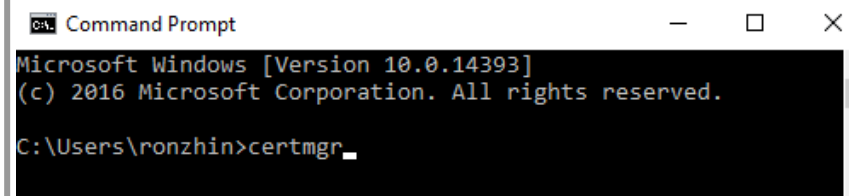
Запустите эту программу щелчком мыши.

Способ 2:

а) Откройте окно командной строки:

 -> правой кнопкой мыши откройте меню "Пуск" -> выберите **Command Prompt** ("Командная строка").

б) вызовите оснастку "Сертификаты" (введите "certmgr" и нажмите "Enter"):





- [Проверка наличия сертификатов в хранилищах](#)
- **Получение и установка списка отзыва сертификатов**
- [Установка личного сертификата открытого ключа пользователя](#)
- [Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии](#)
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- [Тестирование установленного криптографического ПО и сертификатов](#)

Возможны следующие режимы проверки статуса отзыва сертификатов: онлайн/оффлайн/выключена. Управление режимом проверки осуществляется в Программах АО "АТС".

Например, если в АРМ Участника ("Сервис|Настройка...|Криптография") следующие значения флажков:

- ☒ Проверять статус отзыва сертификата подписчика
☐ Проверять статус отзыва сертификата в режиме "он-лайн"

соответствуют режиму проверки статуса отзыва "офф-лайн".

- С учетом того, что список отзыва сертификатов обновляется удостоверяющим центром АО "АТС" каждый час, режим "онлайн" является основным.
В режиме "онлайн" система сама скачивает свежий список отзыва (CRL), при этом он временно сохраняется в виде файла в разных местах, в зависимости от версии ОС и/или браузера Internet Explorer, **но не устанавливается в хранилище**.
- Режим "оффлайн" используется в тех случаях, когда требуется проверять статус отзыва сертификатов, но доступ к онлайн-овому списку (адресу из точки распространения списков отзыва) невозможен (недоступен Интернет, либо недоступен именно этот адрес) - в этом случае файл со списком отзыва получается каким-то другим способом и устанавливается в хранилище так, как это описано в настоящем разделе.

Например, ниже описывается способ получения файла со списком отзыва, использующий другой компьютер, на котором, возможно, не установлены Программы АО "АТС", но который имеет доступ к адресам точек распространения списка отзыва в Интернете (этот компьютер может находиться рядом с компьютером Участника, но при этом иметь другое подключение к Интернету).

URL списка отозванных сертификатов содержится в любом сертификате, выдаваемом УЦ АО "АТС", например, в личном сертификате закрытого ключа:

В окне "Сертификат" URL списка отозванных сертификатов называется точкой распространения (распределения) списка отзыва сертификатов.

Чтобы получить адреса точек распространения списков отзыва, выполните последовательность действий, описанную в разделе "[Установка личного сертификата закрытого ключа пользователя](#)", но на шаге 4 в окне "Сертификат для просмотра" нажмите не кнопку "Установить", а кнопку "Свойства...".

- [Проверка наличия сертификатов в хранилищах](#)
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- [Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии](#)
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- [Тестирование установленного криптографического ПО и сертификатов](#)

Откроется окно "Сертификат", в котором выберите вкладку "Состав":

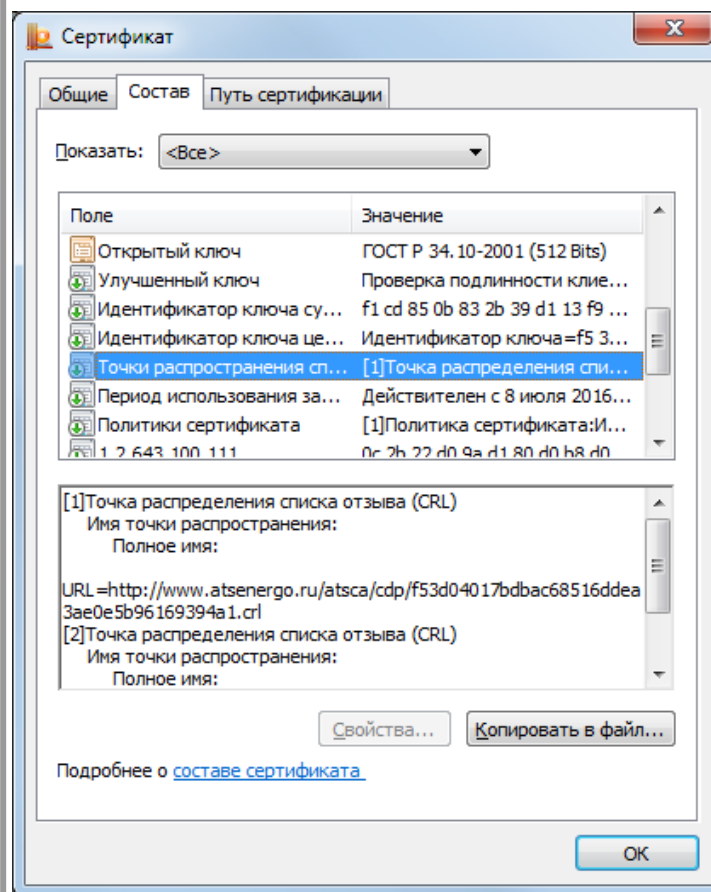


Рис. 1

На рис.1 в нижней области окна "Сертификат" показаны значения двух точек распространения.

Далее:

- выделите в списке "Состав" пункт "Точки распространения...", в нижней части окна появятся URL этих точек,
- выделите URL точки распространения и скопируйте в буфер обмена (Ctrl+C),
- вставьте этот URL (Ctrl+V) в строку адреса браузера и сделайте переход по этому URL,
- скачайте crl-файл со списком отозванных сертификатов,
- каким-либо способом перешлите или перенесите, используя съемное устройство памяти, файл со списком отзыва на компьютер Участника,
- установите список отзыва в хранилище, используя мастер импорта сертификатов из файла.

Для запуска мастера установки сертификата:

- щелкните правой кнопкой мыши по файлу со списком отозванных сертификатов,
- выберите в раскрывшемся меню команду "Установить список отзыва (CRL)" (Install CRL).

- [Проверка наличия сертификатов в хранилищах](#)
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- [Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии](#)
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- [Тестирование установленного криптографического ПО и сертификатов](#)

Откроется начальное окно мастера импорта сертификатов

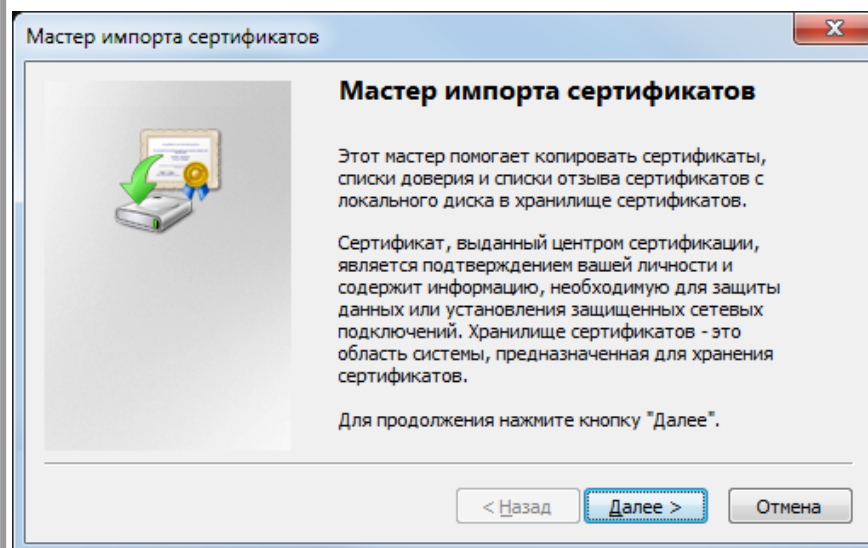


Рис. 2

Нажмите кнопку .
Откроется окно "Хранилище сертификатов":

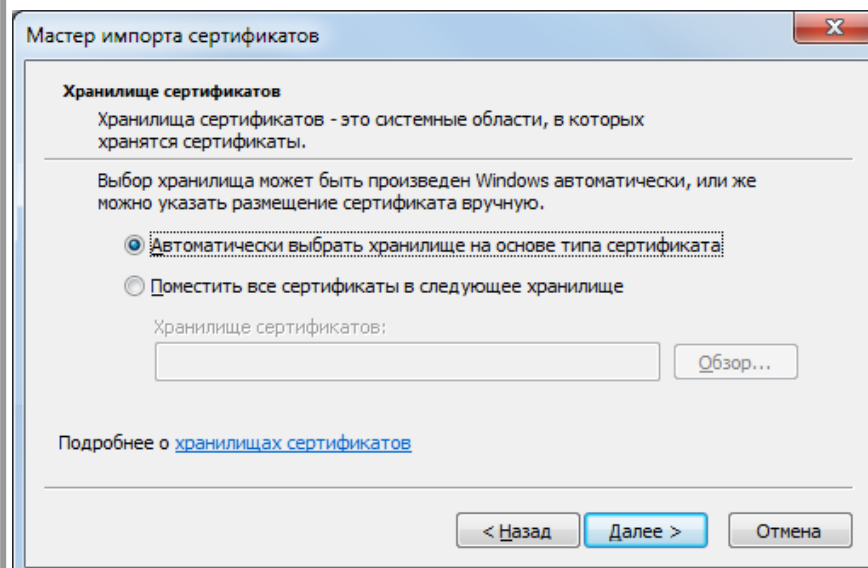


Рис. 3

- [Проверка наличия сертификатов в хранилищах](#)
- **Получение и установка списка отзыва сертификатов**
- [Установка личного сертификата открытого ключа пользователя](#)
- [Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии](#)
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- [Тестирование установленного криптографического ПО и сертификатов](#)

В окне "Хранилище сертификатов" отметьте кнопку ☒ **Автоматически выбрать хранилище на основе типа сертификата** и нажмите кнопку **Далее >**.
Откроется окно "Завершение мастера импорта сертификатов":

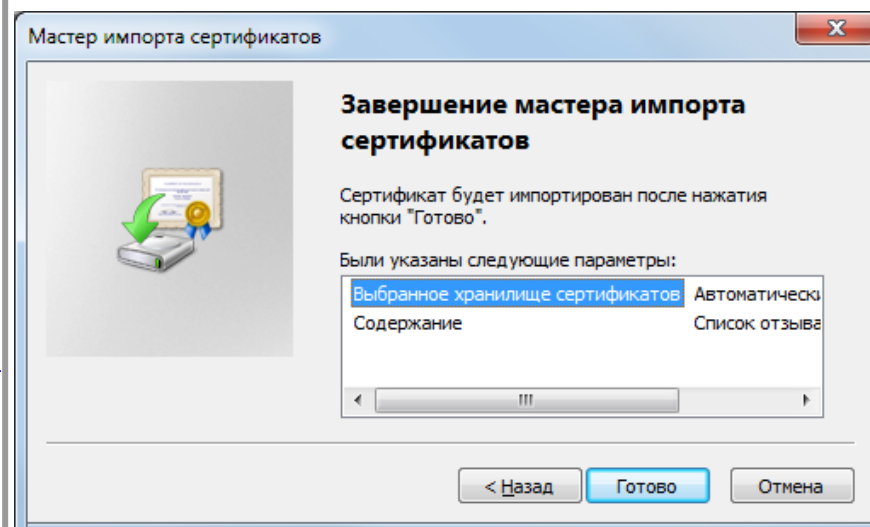


Рис. 4

В окне "Завершение мастера импорта сертификатов" нажмите кнопку **Готово**.

— [Элементы первичной диагностики проблем](#) ► Установка личного сертификата открытого ключа пользователя для отправки сообщений самому себе

1 из 1

- [Проверка наличия сертификатов в хранилищах](#)
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- [Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии](#)
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- [Тестирование установленного криптографического ПО и сертификатов](#)

Наличие открытого ключа пользователя в хранилище "Другие пользователи" (Other people) необходимо только для автономной проверки отправки и получения подписанных и зашифрованных сообщений, когда пользователь посылает сообщение самому себе.

Открытый ключ пользователя автоматически устанавливается в хранилище "Другие пользователи" (Other people), если пользователь проверит ЭЦП сообщения, которое он подписал и сам себе послал. Чтобы выполнить проверку ЭЦП, в Microsoft Outlook достаточно открыть сообщение, подписанное этой ЭЦП. В "АРМ Участника" проверка ЭЦП выполняется в ходе

обработки сообщения (кнопкой  (Обработать сообщение (Ctrl-P)) в окне "Сообщения", либо автоматически после приема/импорта).

- [Проверка наличия сертификатов в хранилищах](#)
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- [Тестирование установленного криптографического ПО и сертификатов](#)

Проверка для Windows 7:

1 Откройте окно «Выполнить» ("Run") комбинацией клавиш "Win + R"

2 Введите "control panel"

3 Нажмите "OK"

4 Откройте окно свойств КриптоПро CSP двойным щелчком мыши по этому значку

5 Проверьте версию

КриптоПро CSP

Алгоритмы	Безопасность	Winlogon	Настройки TLS
Общие	Оборудование	Сервис	Дополнительно

КриптоПро CSP

Версия ядра СКЗИ: 3.6.5359 KC1

Версия продукта: 3.6.6621

Copyright (C) Крипто-Про, 2000-2010

Запустить с правами администратора

Лицензия

Серийный номер: [blurred]

Владелец: [blurred]

Организация: [blurred]

Тип лицензии: CSP

Срок действия: Постоянная

Первая установка: 10.08.2015

Ввод лицензии

Язык

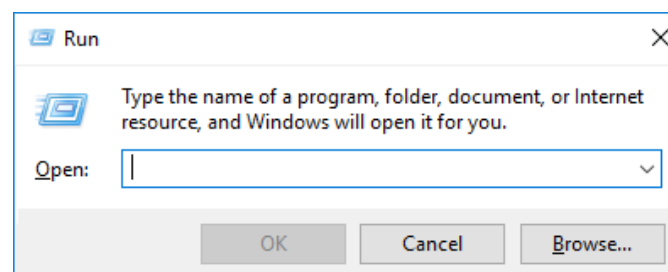
Выберите язык для отображения окон CSP вашей учетной записи: <Умолчание системы>

Выберите язык для отображения окон CSP пользователей, не задавших язык (умолчание системы): Русский

OK Отмена Применить

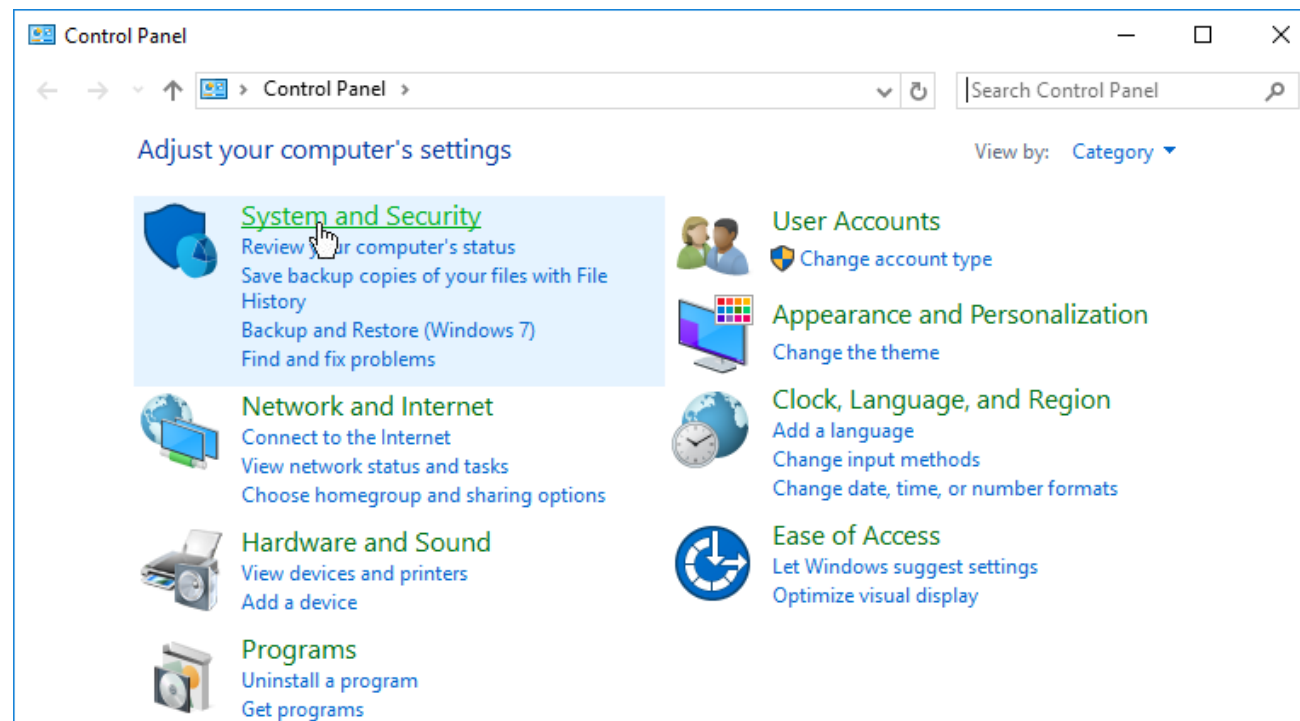
Проверка для Windows 10:

- 1 Откройте окно «Выполнить» ("Run") комбинацией клавиш «Win + R»:



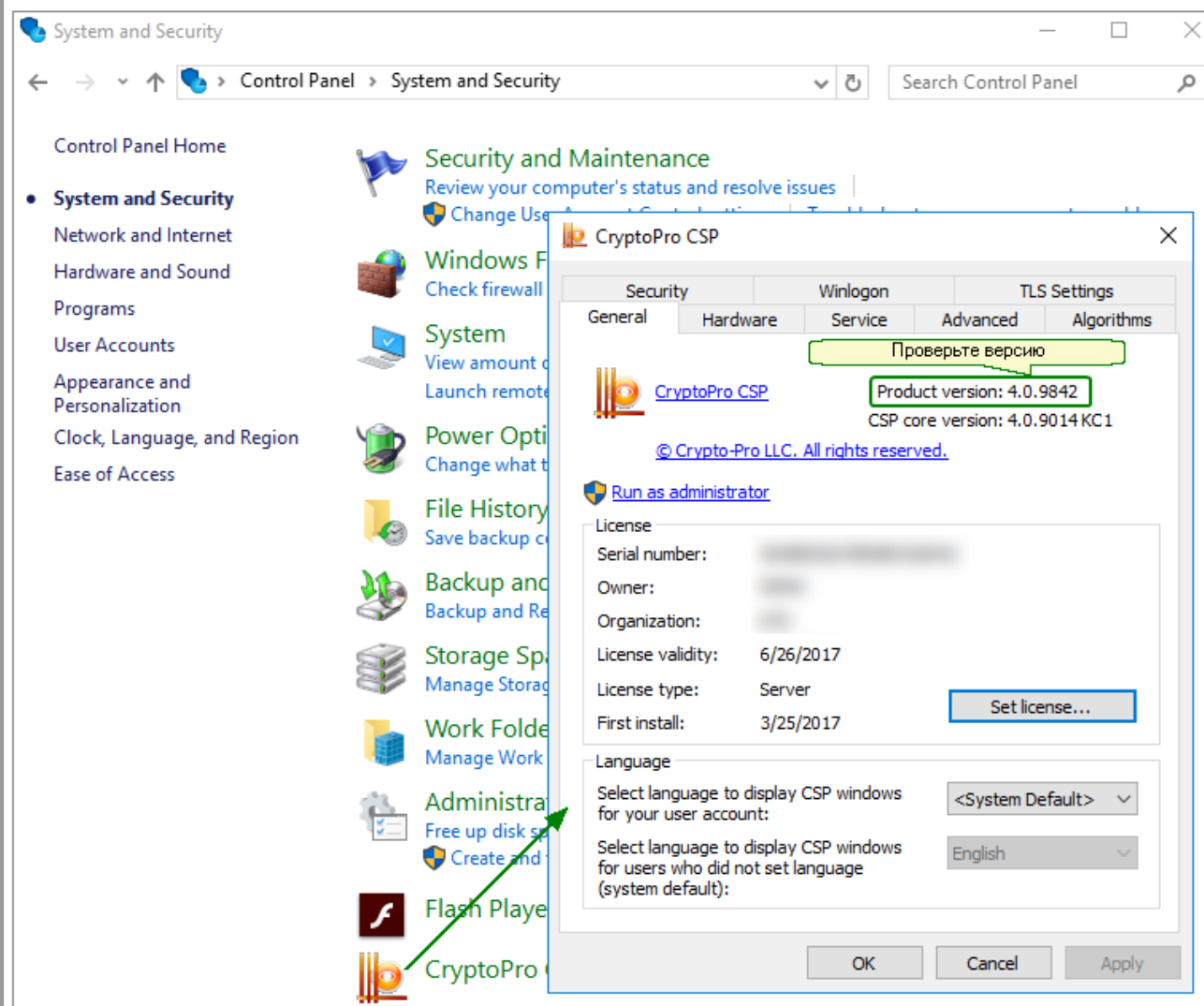
- [Проверка наличия сертификатов в хранилищах](#)
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- [Тестирование установленного криптографического ПО и сертификатов](#)

- 2 Введите "control panel" в поле "Open" и нажмите "OK".
Откроется панель управления, в которой выберите раздел **System and Security**:



- [Проверка наличия сертификатов в хранилищах](#)
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- [Тестирование установленного криптографического ПО и сертификатов](#)

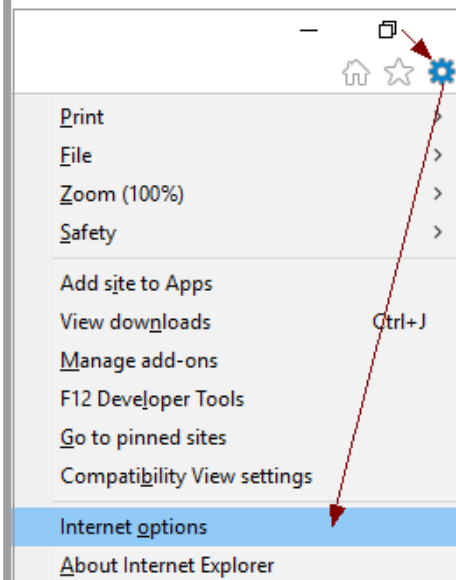
3 Откроется раздел **System and Security** в котором двойным щелчком мыши по значку  откройте окно свойств "КриптоПро CSP":



- [Проверка наличия сертификатов в хранилищах](#)
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- [Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии](#)
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- [Тестирование установленного криптографического ПО и сертификатов](#)

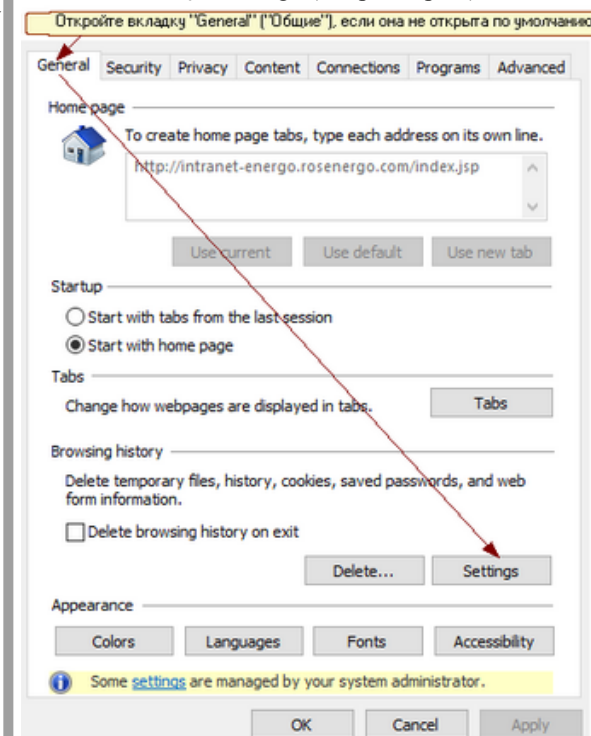
Выполните последовательность шагов 1,... 7.

- 1.** Запустите браузер MS IE11, нажатием кнопки  в правом верхнем углу окна браузера или комбинации клавиш "Alt+X" откройте меню и выберите в нем пункт "Internet options" ("Свойства браузера"):



Откроется форма "Internet option" ("Свойства браузера") →

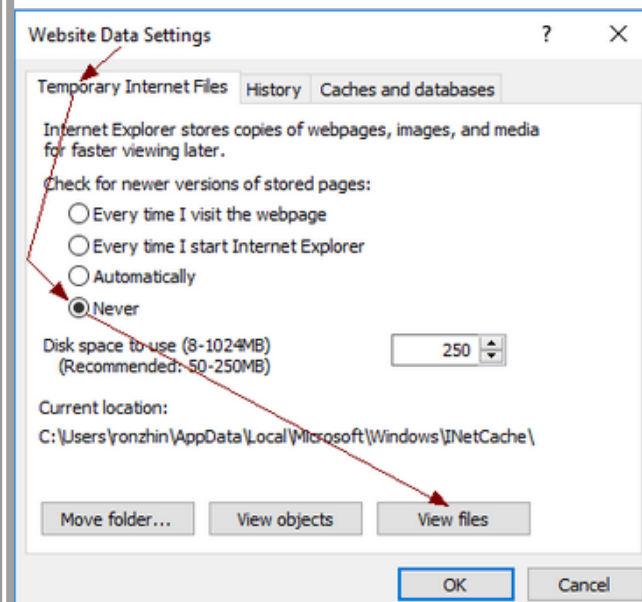
- 2.** В окне "Internet option" ("Свойства браузера"), на вкладке "General" ("Общие") в разделе "Browsing history" ("Журнал браузера") нажмите кнопку "Setting" ("Параметры"):



Откроется окно "Website Data Setting" ("Параметры данных веб-сайта") на вкладке "Temporary Internet Files" ("Временные файлы интернета") **(3)**.

- [Проверка наличия сертификатов в хранилищах](#)
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- [Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии](#)
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- [Тестирование установленного криптографического ПО и сертификатов](#)

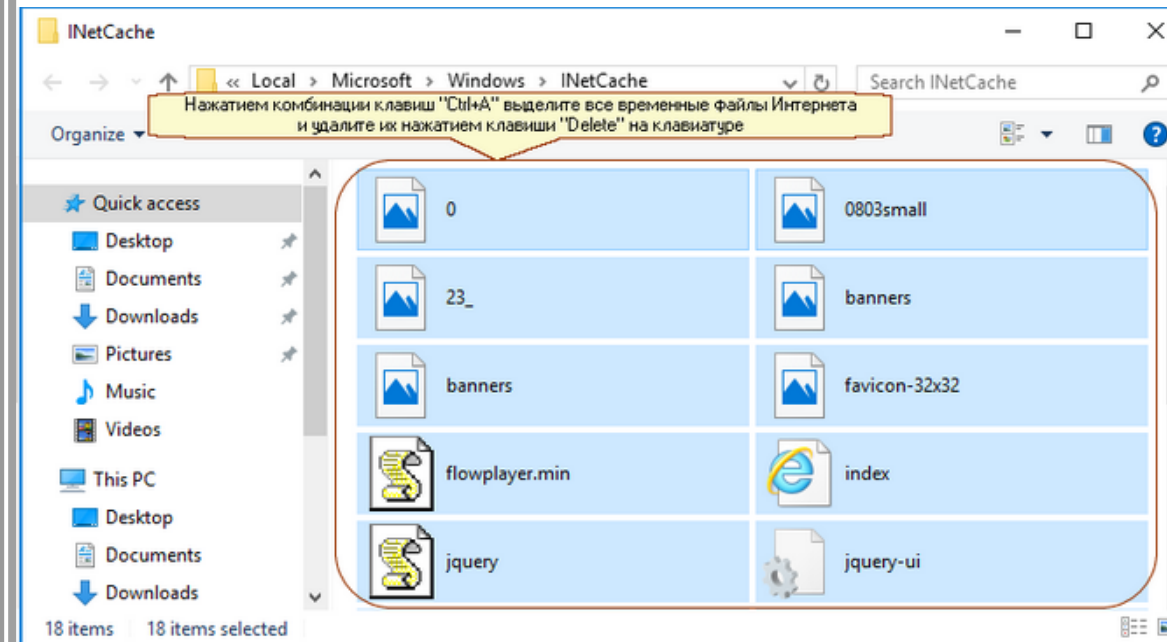
3. В окне "Website Data Setting" (вкладка "Temporary Internet Files") в разделе "Check for newer versions of stored pages" ("Проверять наличие новых версий сохраненных страниц") отметьте кнопку "☒ Never" ("Никогда"), затем нажмите кнопку "View Files" ("Просмотреть файлы"):



Откроется окно "INetCache" ("Временные файлы Интернета").

- [Проверка наличия сертификатов в хранилищах](#)
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- [Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии](#)
- Настройка браузера MS IE11 с целью профилактики ошибок
- [Тестирование установленного криптографического ПО и сертификатов](#)

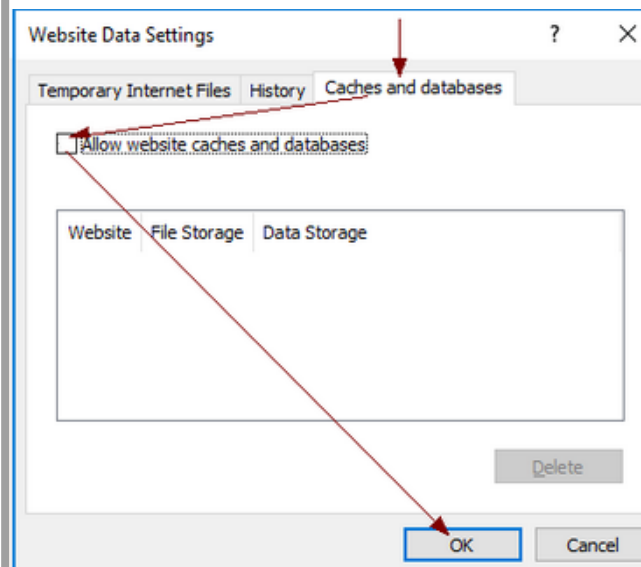
4. В окне "INetCache" ("Временные файлы Интернета") удалите временные файлы Интернета:



Закройте окно нажатием кнопки "X" в правом верхнем углу окна.

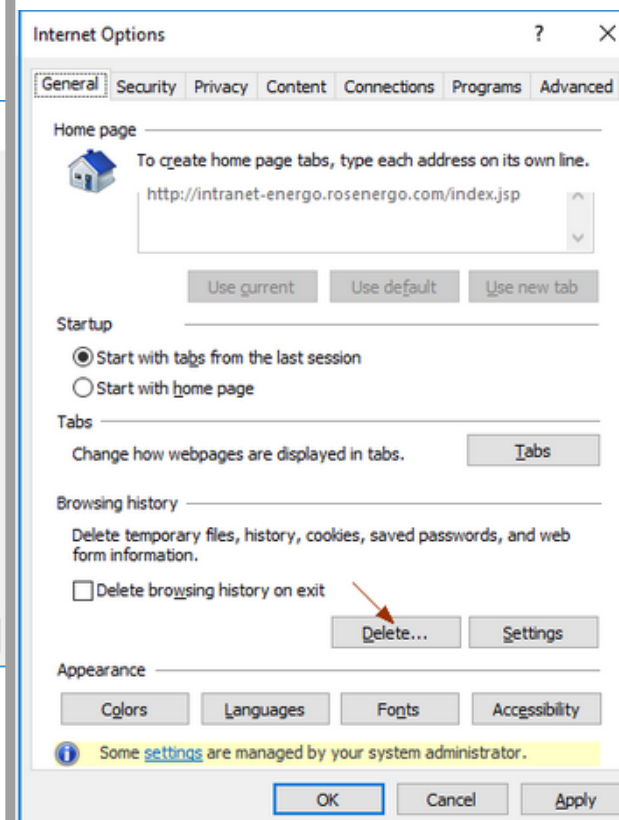
- [Проверка наличия сертификатов в хранилищах](#)
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- [Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии](#)
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- [Тестирование установленного криптографического ПО и сертификатов](#)

5. В окне "Website Data Setting" ("Параметры данных веб-сайта") выберите вкладку "Caches and database" ("Кэш и базы данных"), уберите галочку "Allow website Caches and database" ("Разрешить кэш и базы данных веб-сайта"), нажмите "OK":



Форма закрывается, сделанные настройки будут сохранены.

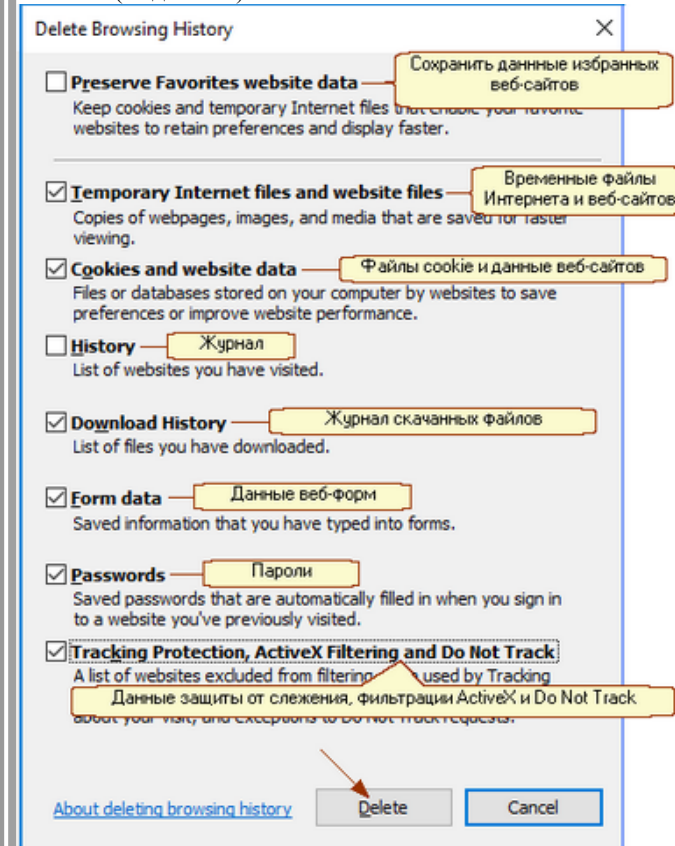
6. В окне "Internet option" ("Свойства браузера") в разделе "Browsing history" ("Журнал браузера") нажмите кнопку "Delete" ("Удалить")



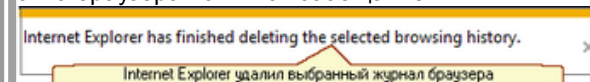
Откроется окно "Удаление истории обзора" (7).

- [Проверка наличия сертификатов в хранилищах](#)
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- [Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии](#)
- Настройка браузера MS IE11 с целью профилактики ошибок
- [Тестирование установленного криптографического ПО и сертификатов](#)

7. В окне "Delete Browsing History" проставьте галочки так, как показано на рисунке и нажмите кнопку "Delete" ("Удалить"):



Окно "Delete Browsing History" закроется, в нижней части окна браузера появится сообщение:



В окне "Internet options" ("Свойства браузера") нажмите кнопку "ОК".

Закройте сообщение нажатием кнопки .

- [Проверка наличия сертификатов в хранилищах](#)
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- [Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии](#)
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- Тестирование установленного криптографического ПО и сертификатов

Наиболее простой способ проверить установленное криптографическое ПО и сертификаты заключается в том, чтобы послать самому себе подписанное и зашифрованное сообщение, используя для этого почтовый клиент программы "АРМ Участника".

Замечания:

1. Программу "АРМ Участника" и руководство пользователя этой программы можно скачать на странице "Программные продукты" сайта АО "АТС".

В этом руководстве смотрите разделы "Установка "АРМ Участника" и "Настройка параметров программы".

2. Перед тем, как посылать самому себе подписанное и зашифрованное сообщение, пошлите самому себе подписанное, но не зашифрованное сообщение (это нужно для того, чтобы открытый ключ вашего личного сертификата появился в хранилище "Другие пользователи").

Последовательность ваших действий при отправке подписанного и зашифрованного сообщения самому себе показана на рис. 1 зелеными цифрами:

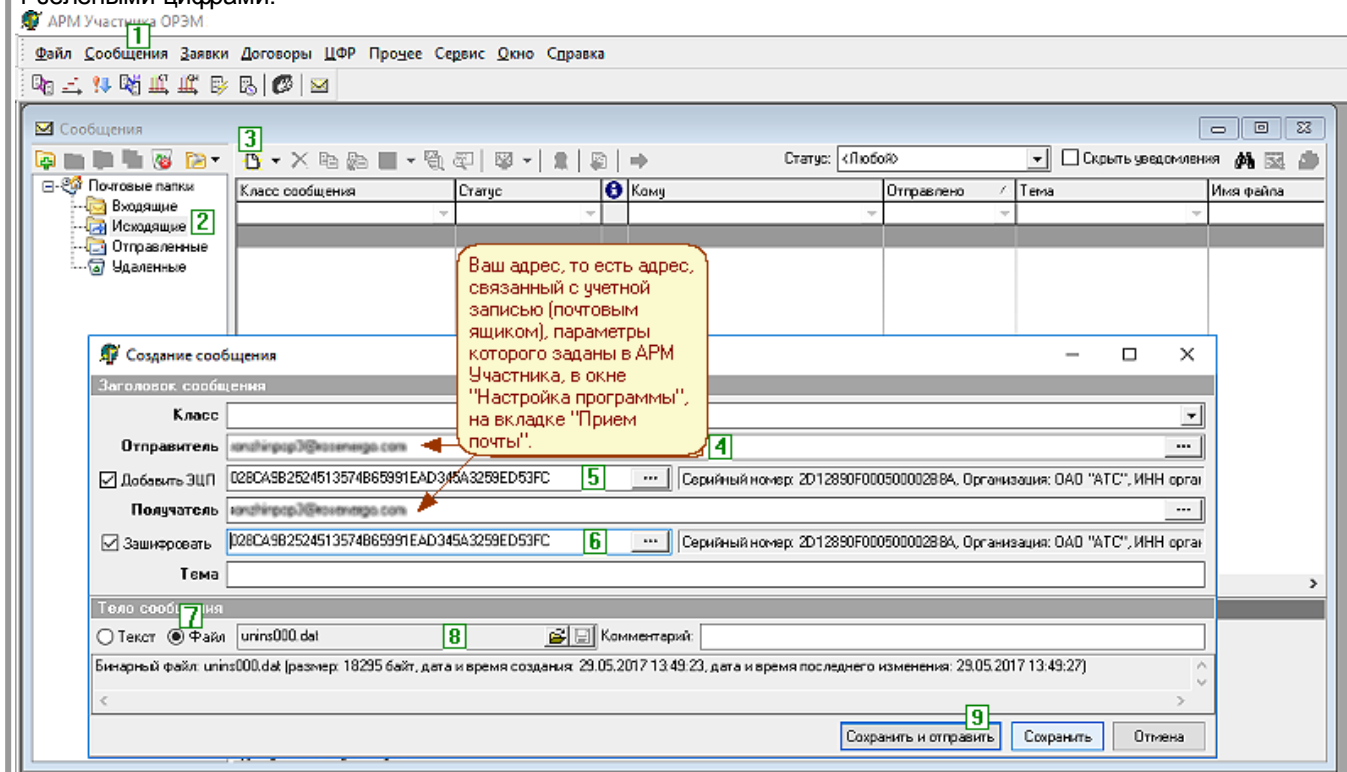


Рис. 1

- 1 В главном меню "АРМ Участника" выберите пункт "Сообщения", в открывшемся меню второго уровня выберите "Список сообщений".
- 2 Откройте почтовую папку "Исходящие".
- 3 Нажмите кнопку . Откроется окно "Создание сообщения".
- 4 Введите в поля "Отправитель" и "Получатель" ваш адрес.
- 5 Установите флажок "Добавить ЭЦП", нажмите кнопку , в открывшемся окне "Выбор своего сертификата" выберите свой личный сертификат.

- [Проверка наличия сертификатов в хранилищах](#)
- [Получение и установка списка отзыва сертификатов](#)
- [Установка личного сертификата открытого ключа пользователя](#)
- [Проверка: установлено ли ПО "КриптоПро CSP" и если установлено, то какой версии](#)
- [Настройка браузера MS IE11 с целью профилактики ошибок](#)
- Тестирование установленного криптографического ПО и сертификатов

6 Установите флажок "Зашифровать", нажмите кнопку , в открывшемся окне "Выбор чужого сертификата" выберите свой личный сертификат.

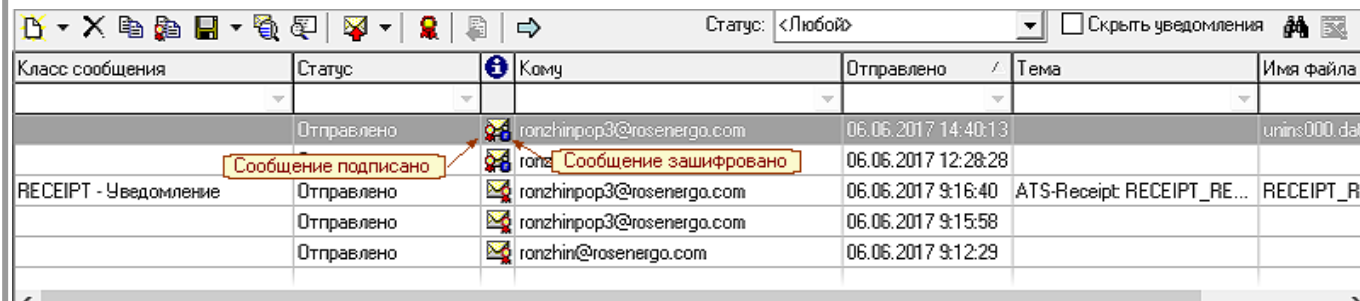
Замечание: так как вы посылаете сообщение самому себе, ваш личный сертификат является одновременно "своим" и "чужим".

7 Отметьте кнопку "Файл", .

8 В открывшемся окне "Загрузить вложение" выберите файл, который будет вложен в сообщение.

9 Нажмите кнопку "Сохранить и отправить".

Результат: сообщение с признаками "Отправлено" и "Зашифровано" должно появиться в папке "Отправленные":



Информация о сообщении

Класс:	Тема сообщения:
Статус: Отправлено	Имя файла: unins000.dat
Отправитель: ronzhinpop3@rosenergo.com	Криптография: Подписано и зашифровано
Получатель: ronzhinpop3@rosenergo.com	Отправлено: 06.06.2017 14:40:13
Обратный адрес: ronzhin@rosenergo.com	Получено:

Сообщение об ошибке:

- Указания по чтению этой инструкции
- [Основные понятия системы криптографической защиты информации](#)
- [Приложение к разделу "Установка криптографического ПО"](#)
- [Ограниченная лицензия на "КриптоПро CSP" для использования с закрытым ключом только одного сертификата](#)

- Используйте ссылки для ускорения получения информации.
- Чтобы вернуться в то место инструкции, откуда вы ушли по ссылке, нажмите комбинацию клавиш  + . Если вы после перехода по ссылке на другую страницу руководства "пролистали" несколько страниц, то, чтобы вернуться на страницу, с которой вы ушли по ссылке, вам может понадобиться нажать эту комбинацию клавиш несколько раз.
- Используйте комбинацию клавиш "Ctrl+N", чтобы развернуть окно руководства на всю ширину экрана.
- Присутствие кнопки  в верхней части страницы руководства (зеленая полоса) означает, что данная страница руководства - не последняя в текущем разделе. По нажатию этой кнопки (или по нажатию клавиши "Page Down" на клавиатуре) выполняется переход на следующую страницу. По нажатию клавиши "Page Up" выполняется переход на предыдущую страницу.
- Работа с оглавлением:
Оглавление представляет собой дерево разделов, где каждый раздел - это либо простой раздел (содержит текст и картинки - снимки с экрана), либо узел (содержит названия других разделов). В левой части каждой страницы руководства показаны разделы, входящие в текущий раскрытый узел оглавления. В правой части страницы руководства показано содержимое простого раздела, выбранного в левой части страницы.
В верхней части каждой страницы руководства (зеленая полоса) указан путь к текущему (выбранному) простому разделу руководства (аналогично тому, как в файловой системе Windows указывается путь к текущей открытой папке). Развернутый узел оглавления отображается как , свернутый узел - как . Чтобы свернуть узел и отобразить содержимое узла более высокого уровня, щелкните мышью либо символ этого узла () , либо ссылку справа от него. Чтобы развернуть узел и отобразить содержимое, щелкните мышью либо символ этого узла () , либо ссылку справа от него.

- [Указания по чтению этой инструкции](#)
- Основные понятия системы криптографической защиты информации
- [Приложение к разделу "Установка криптографического ПО"](#)
- [Ограниченная лицензия на "КриптоПро CSP" для использования с закрытым ключом только одного сертификата](#)

Термин	Значение
Сертификат	Цифровой документ (файл), подтверждающий соответствие между ключом и информацией, идентифицирующим владельца ключа.
Структура сертификата	Сертификат содержит: • имя владельца сертификата (имя пользователя, которому принадлежит сертификат) • один или несколько открытых ключей владельца сертификата • имя удостоверяющего центра • серийный номер сертификата, присвоенный удостоверяющим центром • срок действия сертификата (дата начала действия и дата окончания действия) • информацию об использованных криптографических алгоритмах • электронную цифровую подпись, сгенерированную с использованием секретного ключа удостоверяющего центра (подписывается результат хэширования всей информации, хранящейся в сертификате), • список областей действия (стандартных и расширенных), которые указывают, для каких целей может использоваться данный сертификат (например: защита электронной почты, аутентификация пользователя, подписывание других сертификатов при их издании УЦ, подписывание исполняемых файлов; при этом расширенные области могут задаваться в рамках конкретного УЦ).
"Свой" сертификат	Сертификат, для которого пользователь владеет секретным ключом (на электронном носителе), парным к открытому ключу, указанному в сертификате. Секретный ключ этой пары пользователь применяет для подписывания своих сообщений.
"Чужой " сертификат	Сертификат, для которого пользователь не владеет секретным ключом, парным к открытому ключу, указанному в сертификате. Открытый ключ этой пары пользователь применяет для шифрования своих сообщений. Секретный ключ этой пары хозяин сертификата (тот, кто владеет секретным ключом) - для пользователя в данном сообщении - получатель сообщения - применяет для расшифровки сообщения.
Сертификат открытого ключа и сертификат закрытого ключа	Сертификат открытого ключа и сертификат закрытого ключа - это один и тот же сертификат, но который в зависимости от: • доступности для Участника закрытого ключа этого сертификата (свой или чужой), • целей, для которых используется сертификат (ЭЦП исходящих сообщений, расшифровка входящих сообщений и т.д.), • от хранилища, в которое помещается сертификат - называется так или иначе. Например, "свой" сертификат, который используется для подписи исходящего сообщения называется сертификатом закрытого ключа.
Ключ	Секретная информация, используемая криптографическим алгоритмом при шифровании/расшифровке сообщений, постановке и проверке цифровой подписи. При использовании одного и того же алгоритма результат шифрования зависит от ключа. Для современных алгоритмов сильной криптографии утрата ключа приводит к практической невозможности расшифровать информацию.
Схема использования ключевой пары при обмене сообщениями	АО "АТС" генерирует ключевую пару, записывает ее на электронный носитель Рутокен и выдает вместе с распечаткой сертификата на бумаге. Закрытый ключ на Рутокен применяется для подписывания сообщений, посылаемых в АО "АТС" или АО "ЦФР". Пользователь скачивает сертификаты "чужих" ключей с сайта АО "АТС" и использует их для шифрования сообщений, посылаемых в АО "АТС" и АО "ЦФР".
Хэш	Специальным образом полученный образ сообщения ("отпечаток") в виде битовой строки фиксированной длины, полученной в результате хэширования массива данных. Хэширование — однонаправленное преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины (хэш) таким образом, что разным входным массивам соответствуют разные значения хэша, но по значению хэша нельзя восстановить входной массив.

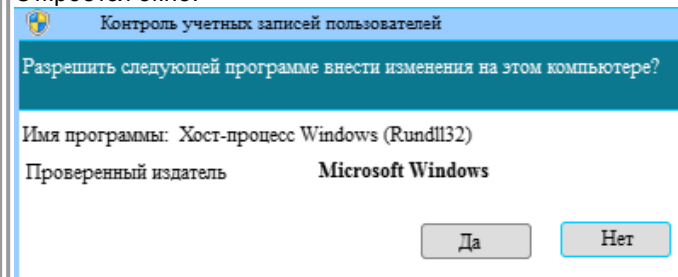
- Система криптографической защиты сообщений, применяемая программами АО "АТС", использует алгоритмы шифрования и ЭЦП по ГОСТ Р 34.10-2001.

- [Указания по чтению этой инструкции](#)
- [Основные понятия системы криптографической защиты информации](#)
- Приложение к разделу "Установка криптографического ПО"
- [Ограниченная лицензия на "КриптоПро CSP" для использования с закрытым ключом только одного сертификата](#)

Вход от имени администратора:

Нажмите ссылку [Запустить с правами администратора](#).

Откроется окно:



Нажмите кнопку "Да".

Нажмите комбинацию клавиш " + ", чтобы вернуться в то место инструкции, откуда вы ушли по ссылке.

Отключение считывателя "Реестр".

Если вы используете программы АО "АТС" (например, "АРМ Участника"), то имейте в виду, что эти программы не допускают использования считывателя "Реестр". Например, при попытке подготовить к отправке документ в "АРМ Участника", вы можете получить сообщение: "Ошибка при выполнении функции get_certificate_info (200): Использование системного реестра в качестве ключевого носителя запрещено". В этом случае, считыватель "Реестр" потребуется удалить.

Переход в "Панель управления".

Windows 7: -> Панель управления.

Windows 10: -> правой кнопкой мыши откройте меню -> выберите ("Панель управления")

Чтобы вернуться в то место инструкции, откуда вы ушли по ссылке, нажмите комбинацию клавиш " + ",

- [Указания по чтению этой инструкции](#)
- [Основные понятия системы криптографической защиты информации](#)
- Приложение к разделу "Установка криптографического ПО"
- [Ограниченная лицензия на "КриптоПро CSP" для использования с закрытым ключом только одного сертификата](#)

Проверка контрольной суммы файла дистрибутива

Перед установкой "КриптоПро CSP 4.0" рекомендуется проверить целостность файла дистрибутива (убедится в том, что загруженный файл - это именно тот файл, который вам нужен, и что он не поврежден).

Для этого:

1. Откройте страницу сайта компании "КРИПТО-ПРО", с которой можно [скачать утилиту проверки контрольной суммы](#) и прочтите на этой странице информацию о контрольных суммах.
2. Пройдите по ссылке <http://www.cryptopro.ru/sites/default/files/public/cpverify.exe>.

Откроется окно загрузки файла:



Рис. 1

3. Нажмите кнопку "Сохранить"

Откроется окно, в котором вместо кнопки "Сохранить" будет кнопка "Открыть папку":

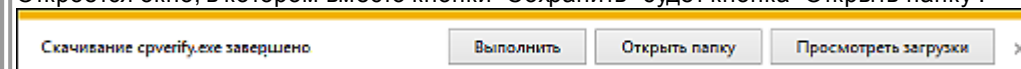


Рис. 2

4. Нажмите кнопку "Открыть папку".

Откроется папка загрузки, в которой загруженный файл будет выделен. Скопируйте его или переместите в удобную для вас папку, например, в папку "C:\Test". В эту же папку скопируйте файл дистрибутива "CSPSetup.exe".

5. Откройте окно командной строки, перейдите в папку, в которой находятся файлы "cpverify.exe" и "CSPSetup.exe", и запустите файл "cpverify.exe" с параметрами "-mk" и "CSPSetup.exe" в командной строке (показано на рис. 3):

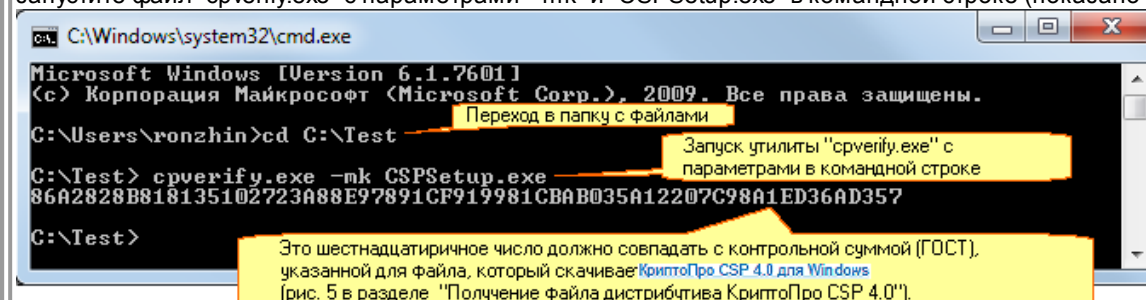


Рис. 3



- [Указания по чтению этой инструкции](#)
- [Основные понятия системы криптографической защиты информации](#)
- [Приложение к разделу "Установка криптографического ПО"](#)
- Ограниченная лицензия на "КриптоПро CSP" для использования с закрытым ключом только одного сертификата]

В данном разделе инструкции используется термин «стандартная лицензия»:

Стандартная лицензия - лицензионное соглашение, с условиями которого вы обязаны согласиться для того, чтобы скачать файл дистрибутива ПО «КриптоПро CSP» с сайта компании «КриптоПро». Стандартная лицензия не ограничена во времени каким-либо сроком (бессрочная).

Примечание: Если вы после установки КриптоПро CSP 4.0 намерены использовать сертификаты подписи с ограниченной лицензией, то при ознакомлении с лицензионным соглашением, примите во внимание, что пункт 7 и пункт 10 («Пользователь не вправе использовать Изделие без активации Изделия путем ввода ключа установки Изделия (серийного номера лицензии)...)» этого соглашения вы можете игнорировать, так как вы имеете право в этом случае использовать ПО «КриптоПро CSP» без его активации для подписывания и расшифровки документов в течение периода действия закрытого ключа сертификата подписи в вашем ключевом носителе, полученном в УЦ АО «АТС».

Ограниченная (распространяющая свое действие только на один сертификат) лицензия на ПО "КриптоПро CSP" для использования с закрытым ключом этого сертификата предоставляется Участникам ОРЭМ на основании договора между АО "АТС" и компанией "КриптоПро". Участник ОРЭМ в заявлении на получение ключей и сертификатов ключей подписи может отказаться от приобретения ограниченной лицензии по разным причинам (например, он уже имеет стандартную лицензию от компании "КриптоПро" (не привязанную к сертификату), или намерен приобрести такую лицензию).

Особенности работы с КриптоПро CSP 4.0 при использовании ограниченной лицензии:

- После установки КриптоПро CSP 4.0 не требуется приобретать лицензию у компании «КриптоПро» и активировать ПО «КриптоПро CSP» путем ввода номера лицензии.
- Вы (пользователь УЦ АО «АТС») приобретаете не стандартную (бессрочную) лицензию у компании «КриптоПро», позволяющую вам работать с сертификатами, выпущенными различными удостоверяющими центрами, а лицензию, действие которой распространяется только на один сертификат, выпущенный по вашему заявлению удостоверяющим центром АО "АТС".

Период действия ограниченной лицензии равен периоду действия (использования) закрытого ключа этого сертификата.

Замечание: сертификат, у которого закончился период действия закрытого ключа (и, как следствие, закончился период действия ограниченной лицензии), остается пригодным для использования в целях, указанных в пункте 8 стандартной лицензии (проверка электронной подписи, вычисление значения функции хеширования, использования протокола TLS при односторонней аутентификации (проверка подлинности сервера)).

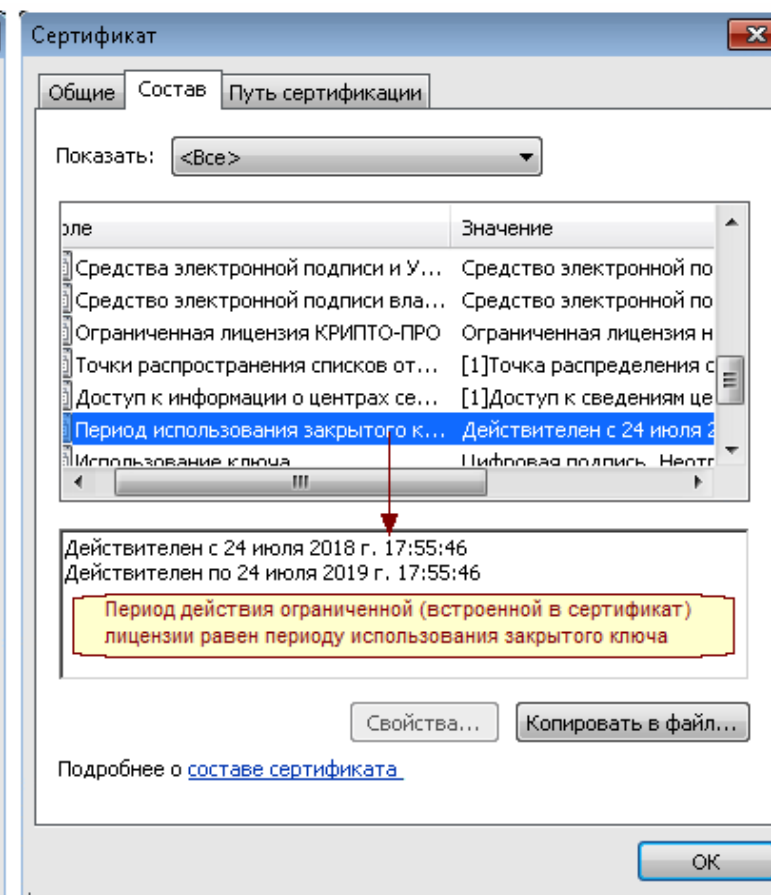
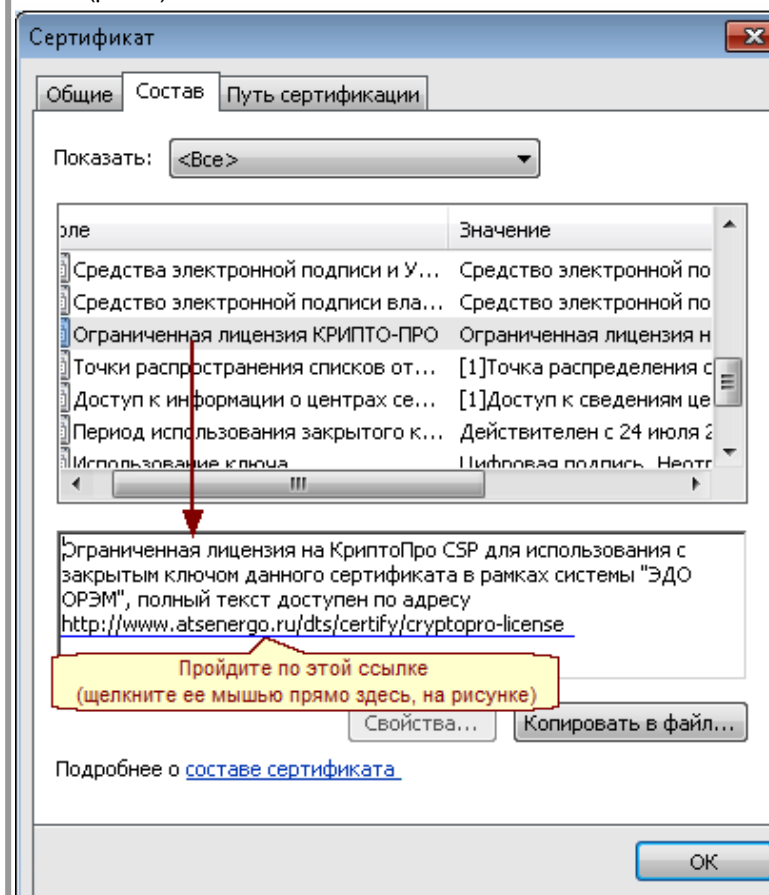
- Стандартная лицензия, которую вы приобретаете у компании «КриптоПро», позволяет установить это ПО на один компьютер. Если вы хотите (например) использовать ПО «КриптоПро CSP» на 5 компьютерах, вам нужно приобрести 5 лицензий. С другой стороны, если вы приобрели один ключевой носитель со встроенной лицензией и бесплатно установили КриптоПро CSP на любое количество компьютеров, вы можете пользоваться этим ключевым носителем на любом из этих компьютеров.
- Стандартная лицензия позволяет использовать сертификат подписи для расшифровки сообщений после окончания периода действия закрытого ключа этого сертификата. Ограниченная лицензия не позволяет этого, так как окончание периода действия закрытого ключа сертификата означает окончание периода действия ограниченной лицензии.

Замечание: указанное различие ограниченной и стандартной лицензий в отношении возможности расшифровывать сообщения после окончания периода действия закрытого ключа сертификата, отсутствует в отношении возможности доступа по сертификату в персональные разделы сайта АО «АТС» после окончания периода действия закрытого ключа сертификата. Это объясняется тем, что при считывании данных из сертификата выполняется операция подписывания данных этим сертификатом.

- [Указания по чтению этой инструкции](#)
- [Основные понятия системы криптографической защиты информации](#)
- [Приложение к разделу "Установка криптографического ПО"](#)
- Ограниченная лицензия на "КриптоПро CSP" для использования с закрытым ключом только одного сертификата

Признак наличия в сертификате ограниченной лицензии

Признаком того, что вашему сертификату предоставлена лицензия на использование ПО «КриптоПро CSP», является наличие в списке свойств этого сертификата (в окне "Сертификат" на вкладке "Состав") поля "Ограниченная лицензия КриптоПро CSP" (рис. 1):



Примечание: чтобы открыть окно "Сертификат", выполните последовательность шагов, описание которой приведено в разделе "Установка личного сертификата закрытого ключа пользователя", но на шаге 3 не изменяйте алгоритм формирования и проверки ЭЦП, а на шаге 4 нажмите не кнопку "Установить", а кнопку "Свойства".

- [Указания по чтению этой инструкции](#)
- [Основные понятия системы криптографической защиты информации](#)
- [Приложение к разделу "Установка криптографического ПО"](#)
- Ограниченная лицензия на "КриптоПро CSP" для использования с закрытым ключом только одного сертификата

Сообщения от "КриптоПро CSP" об ошибках, возникающих при наступлении критических для ПО «КриптоПро CSP» и сертификата подписи дат

Критическая дата для «КриптоПро CSP» - дата окончания пробной лицензии (после установки «КриптоПро CSP» из файла дистрибутива вам автоматически предоставляется на 90 дней пробная лицензия на использование этого ПО для подписывания и расшифровки документов).

Критические даты для сертификата подписи - даты начала и окончания периода действия закрытого ключа этого сертификата. В табл. 1 приведено описание ошибок, зависящих от положения даты попытки подписывания документа относительно этих критических дат.

Табл. 1.

№	Условие возникновения ошибки на дату попытки подписывания документа	Сообщение об ошибке	Комментарий
1	(Период действия пробной лицензии закончился) И (лицензия в сертификате отсутствует).	Сообщение CryptoPro CSP: "Срок действия этой версии КриптоПро CSP истек или еще не наступил, либо серийный номер лицензии не был введен". После его закрытия: "Ошибка 255: Ошибка при выполнении функции sign_data (255): Известная ошибка (0x8007065B, Ошибка исполнения функции).	«0x8007065B, Ошибка исполнения функции» - означает отсутствие лицензии на дату попытки подписывания документа (как пробной лицензии, так и лицензии в сертификате).
2	Период действия закрытого ключа сертификата закончился, либо еще не начинался (независимо от наличия или отсутствия лицензии в сертификате).	Ошибка 255: Ошибка при выполнении функции sign_data (255): Известная ошибка (0x80090010, Отказано в доступе).	"0x80090010, Отказано в доступе" - означает блокировку доступа к ключевому контейнеру в ключевом носителе из-за не попадания даты попытки подписывания документа в период действия закрытого ключа сертификата (появилось в CryptoPro CSP 4.0).
3	Период действия сертификата закончился.	Ошибка при выполнении функции sign_data (255): Известная ошибка (0x80880253, The signer's certificate is not valid for signing).	