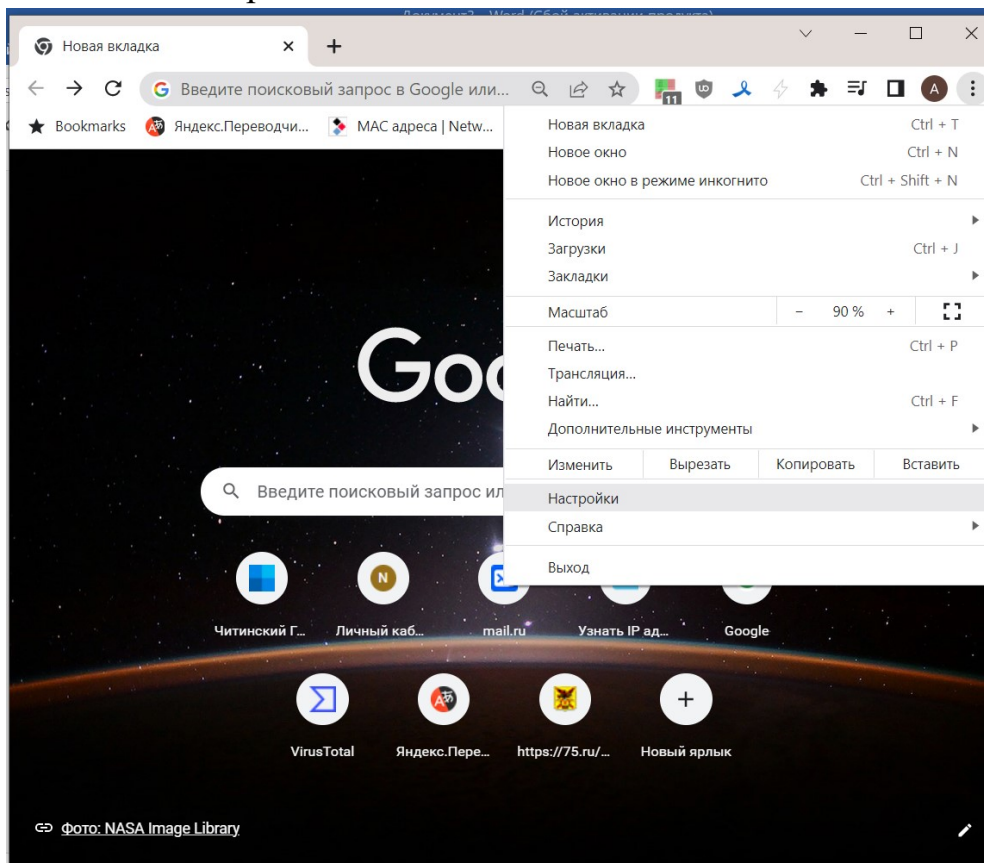


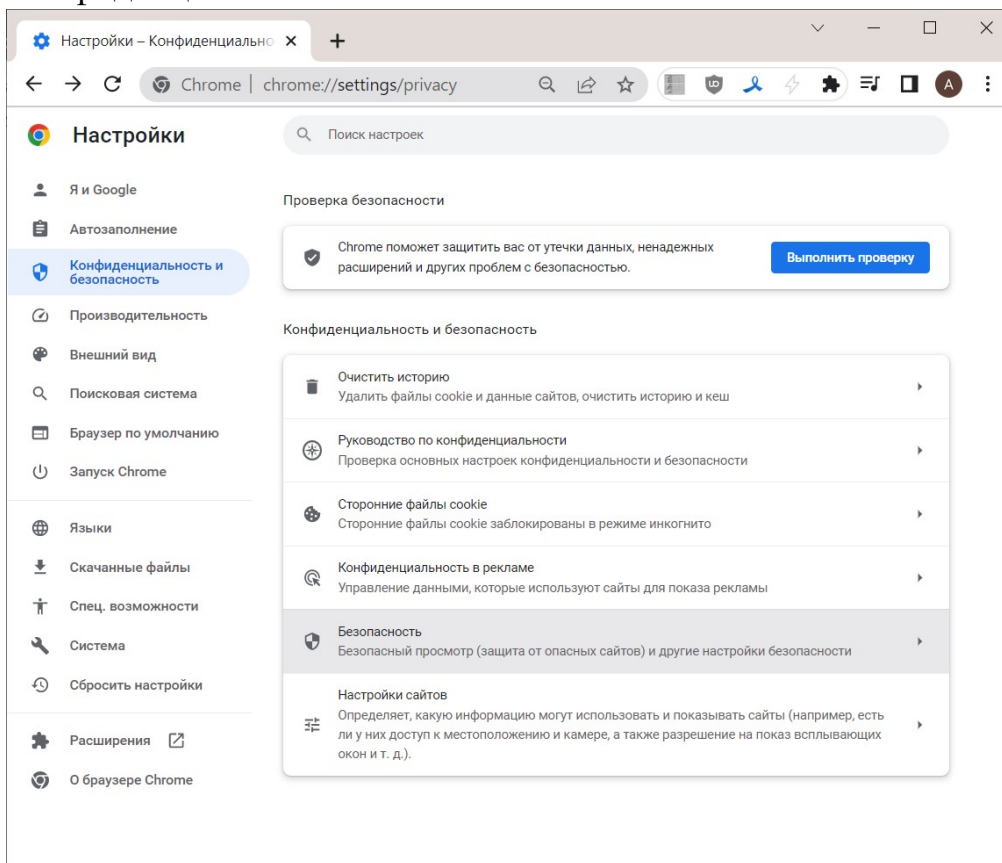
Добавление корневого сертификата в Windows.

Добавление корневого сертификата в браузер Chrome.

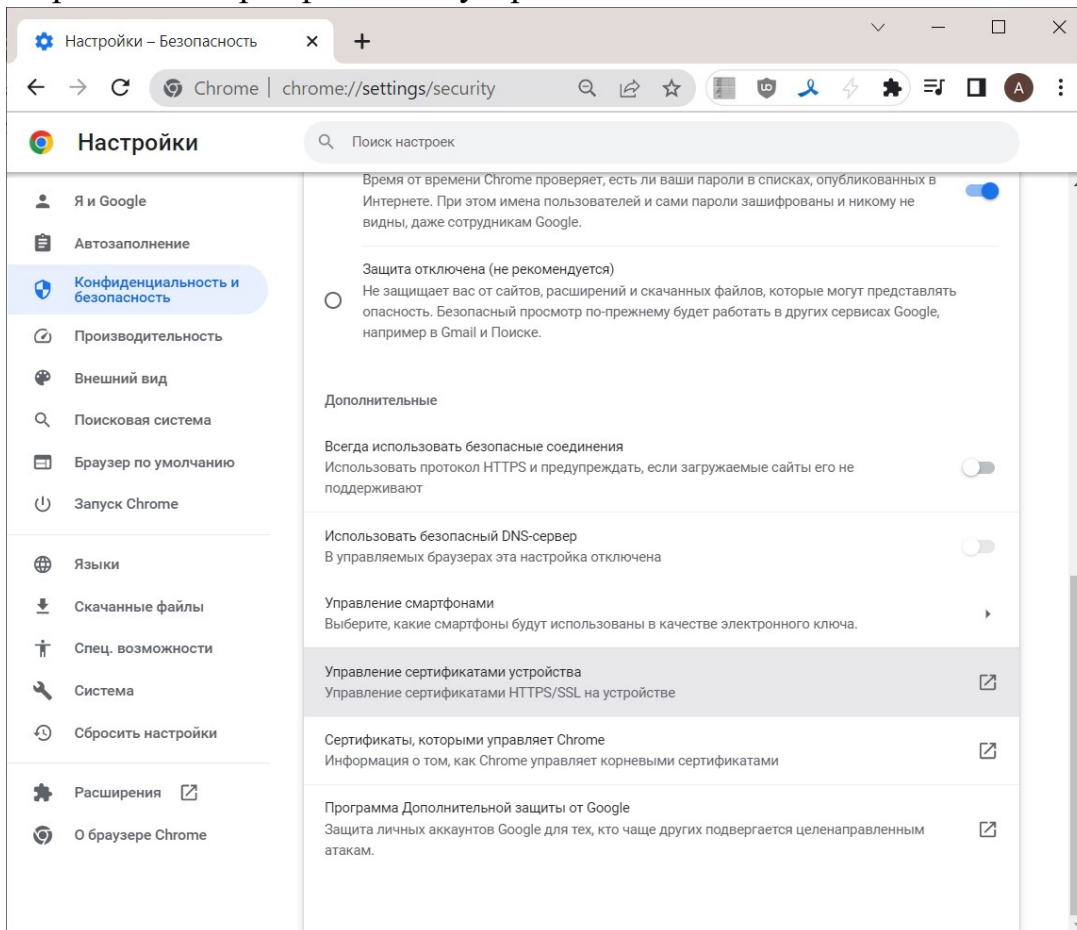
1) Заходим в настройки:



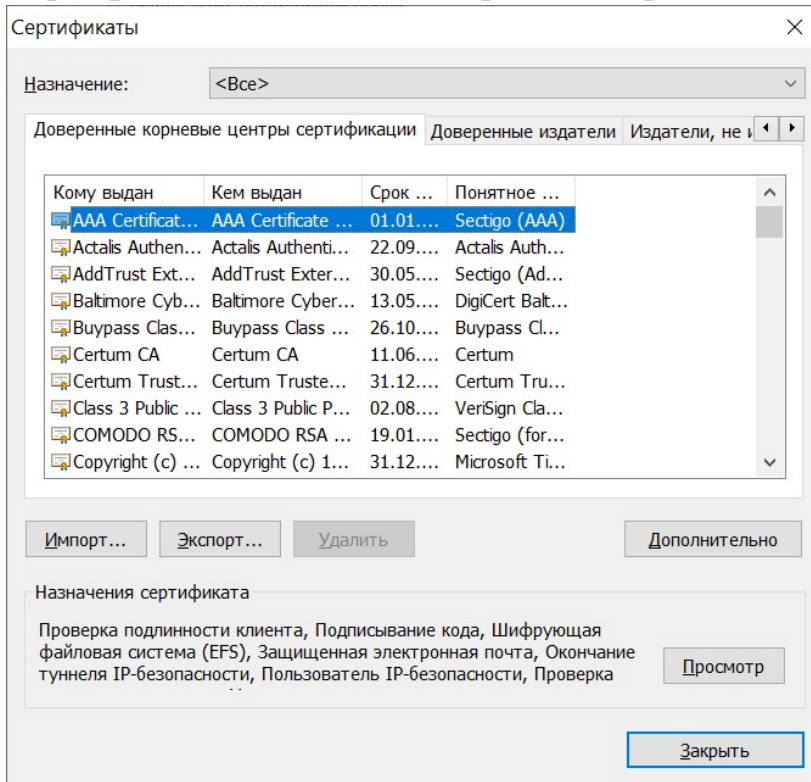
2) Конфиденциальность и безопасность - Безопасность:



3) Управление сертификатами устройства:



4) Сертификаты, вкладка – Доверенные корневые центры сертификации:



5) Импорт:

←  Мастер импорта сертификатов



Мастер импорта сертификатов

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

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

Для продолжения нажмите кнопку "Далее".

Далее

Отмена

6) Выбираем файл сертификата root_ca.crt:

←  Мастер импорта сертификатов



Импортируемый файл

Укажите файл, который вы хотите импортировать.

Имя файла:

Обзор...

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

Файл обмена личной информацией - PKCS #12 (.PFX,.P12)

Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)

Хранилище сериализованных сертификатов (.SST)

Далее

Отмена

7) Далее:

←  Мастер импорта сертификатов



Хранилище сертификатов

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

Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.

- ☐ Автоматически выбрать хранилище на основе типа сертификата
- ☒ Поместить все сертификаты в следующее хранилище

Хранилище сертификатов:

Доверенные корневые центры сертификации

Обзор...

Далее

Отмена



←  Мастер импорта сертификатов

Завершение мастера импорта сертификатов

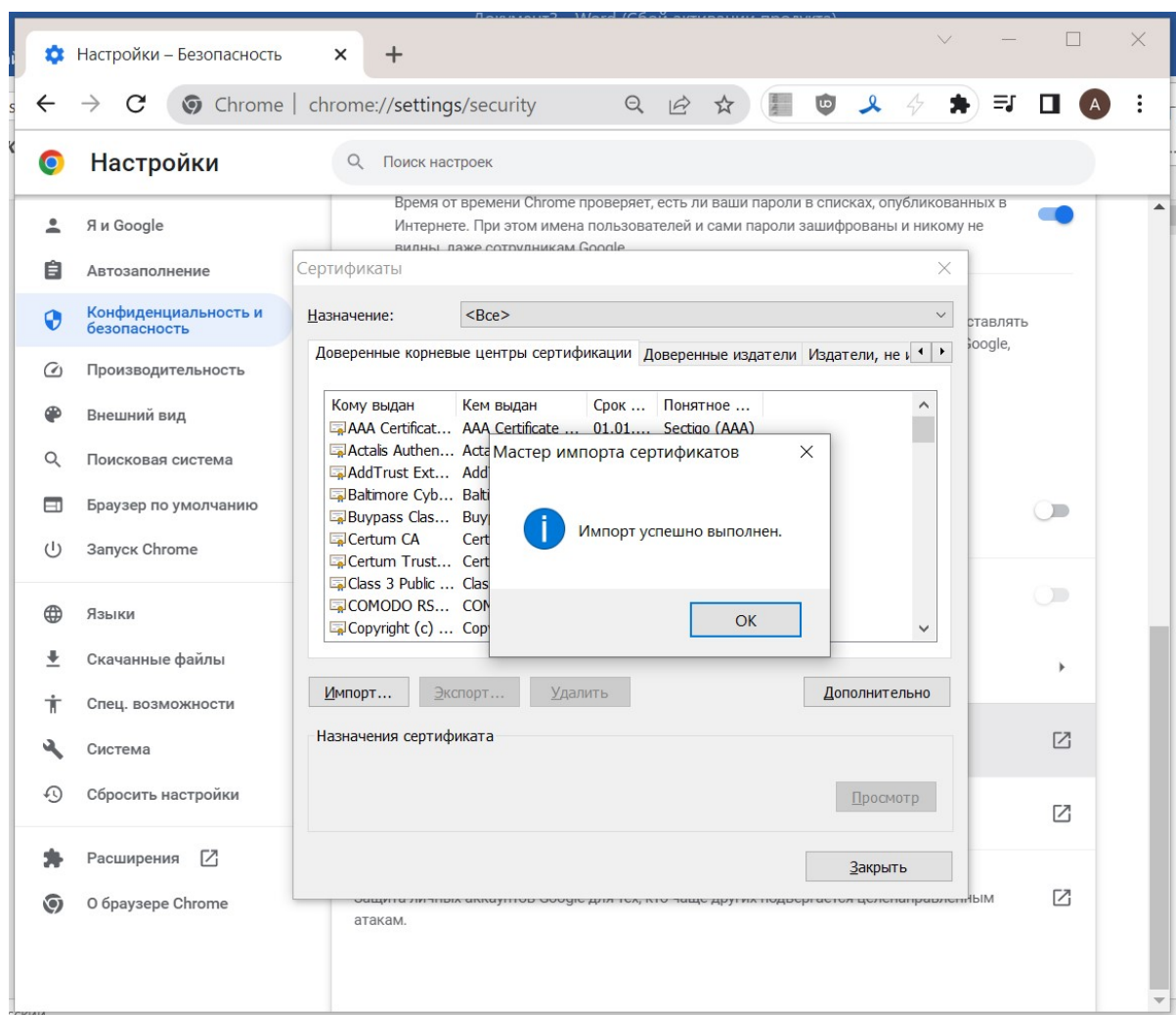
Сертификат будет импортирован после нажатия кнопки "Готово".

Были указаны следующие параметры:

Хранилище сертификатов, выбранное пользователем	Доверенные корневые центры сертификации
Содержимое	Сертификат
Файл	C:\Users\baksheev.a.ZIC\Desktop\...

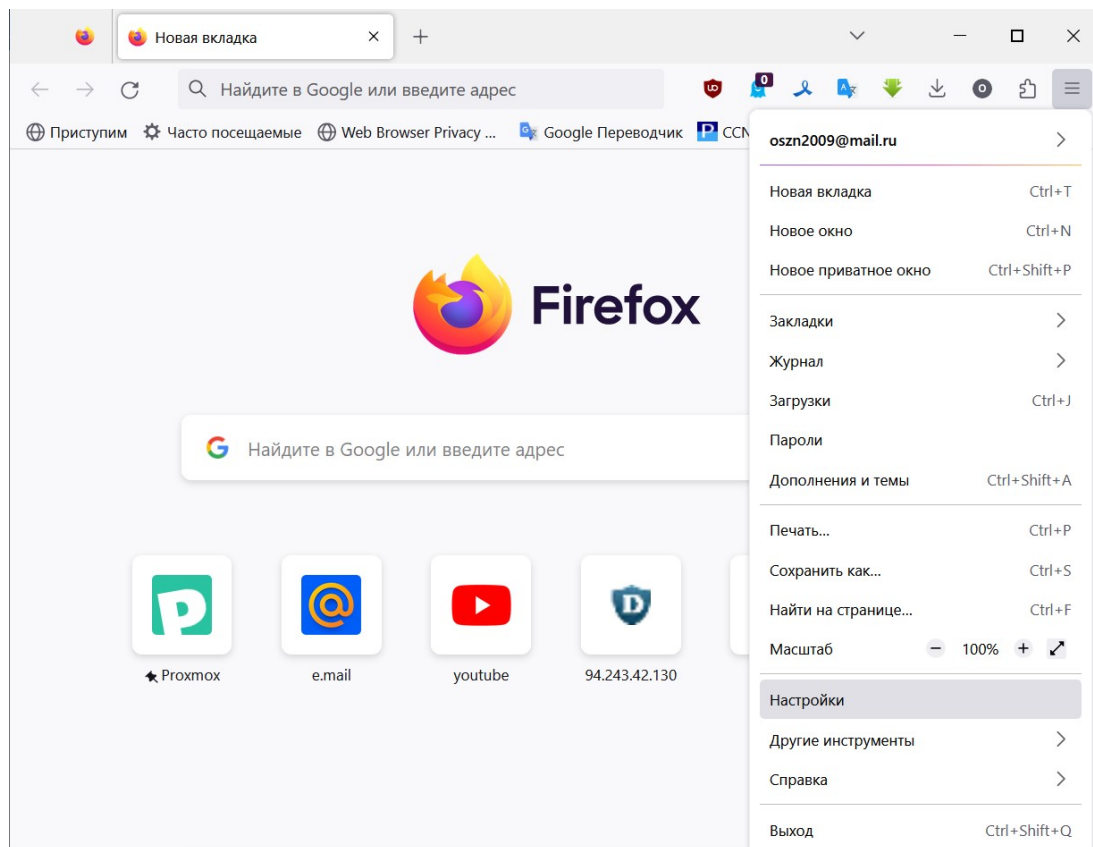
Готово

Отмена

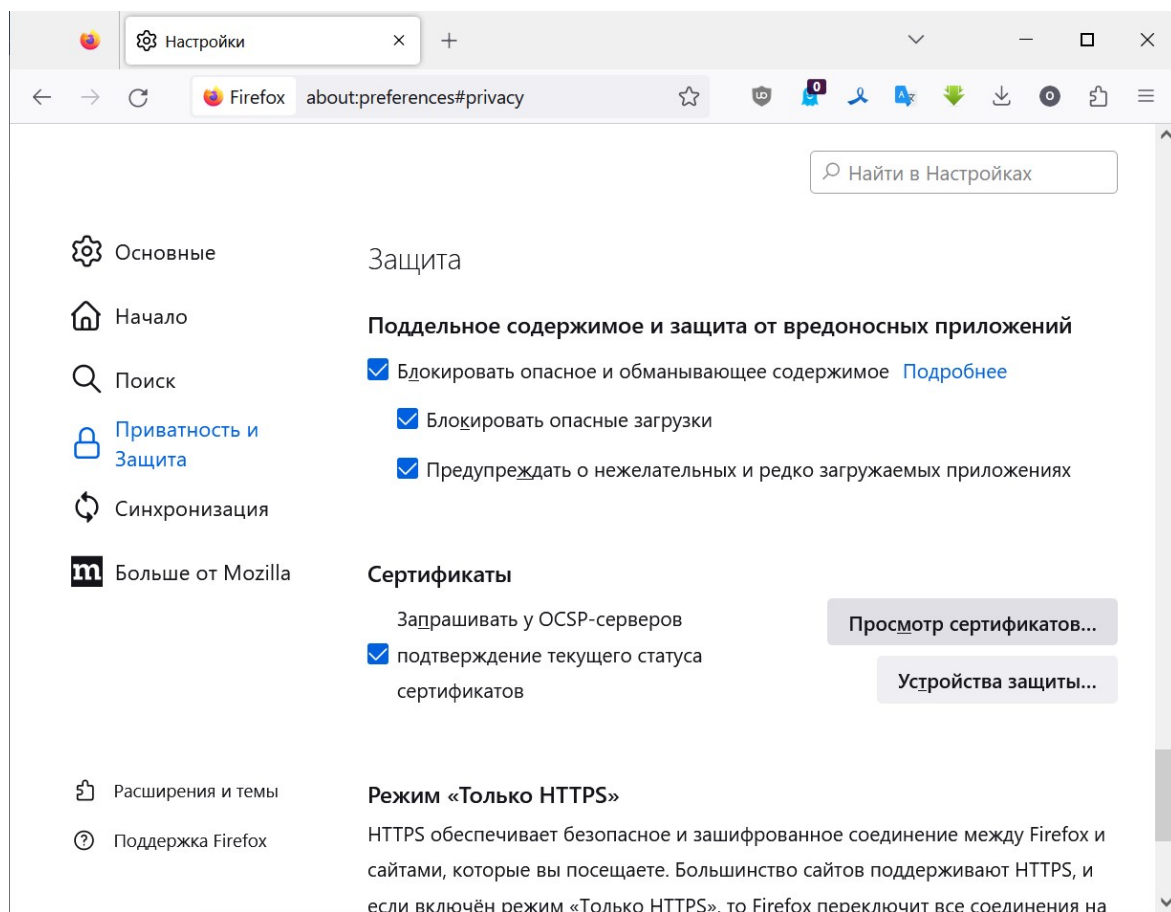


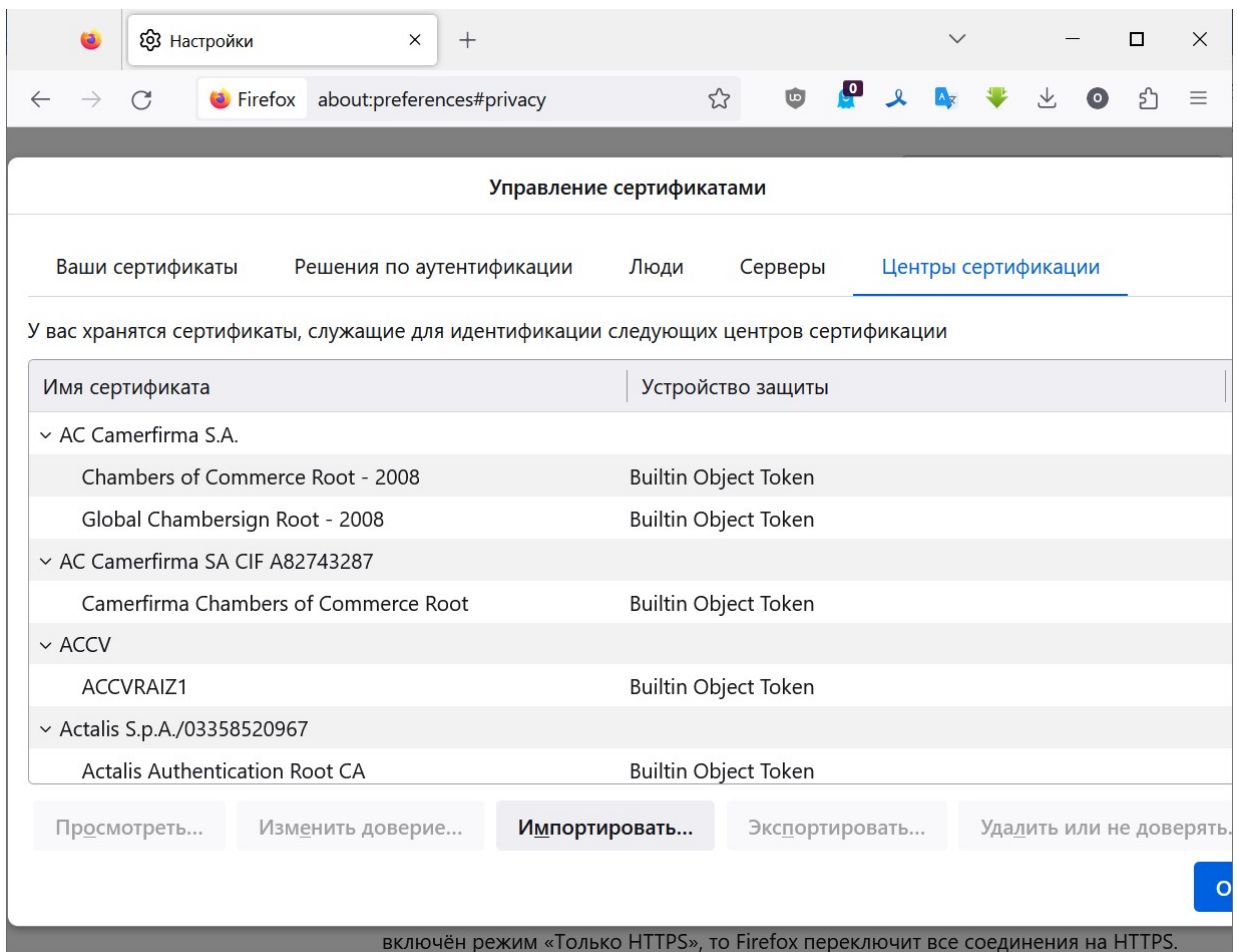
Добавление корневого сертификата в браузер Mozilla Firefox.

1) Настройки:

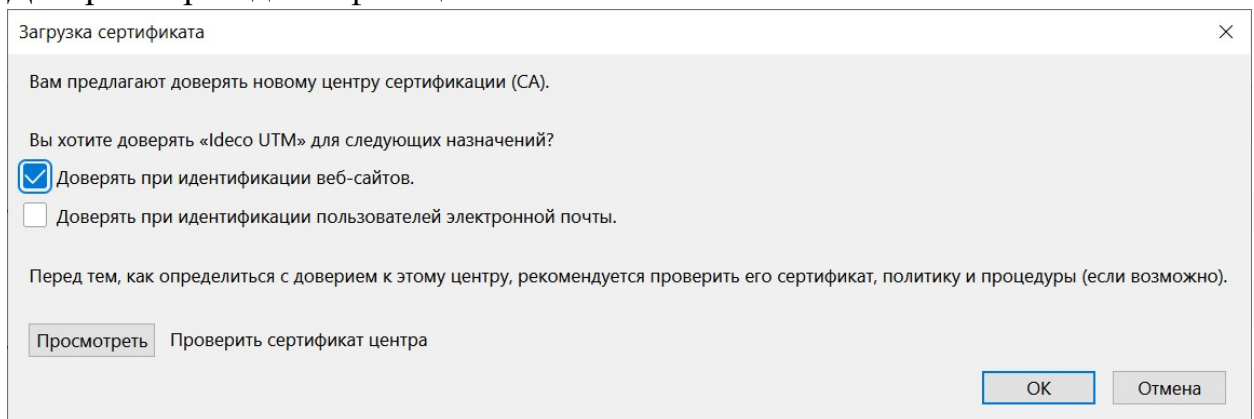


2) Приватность и защита → Просмотр сертификатов:



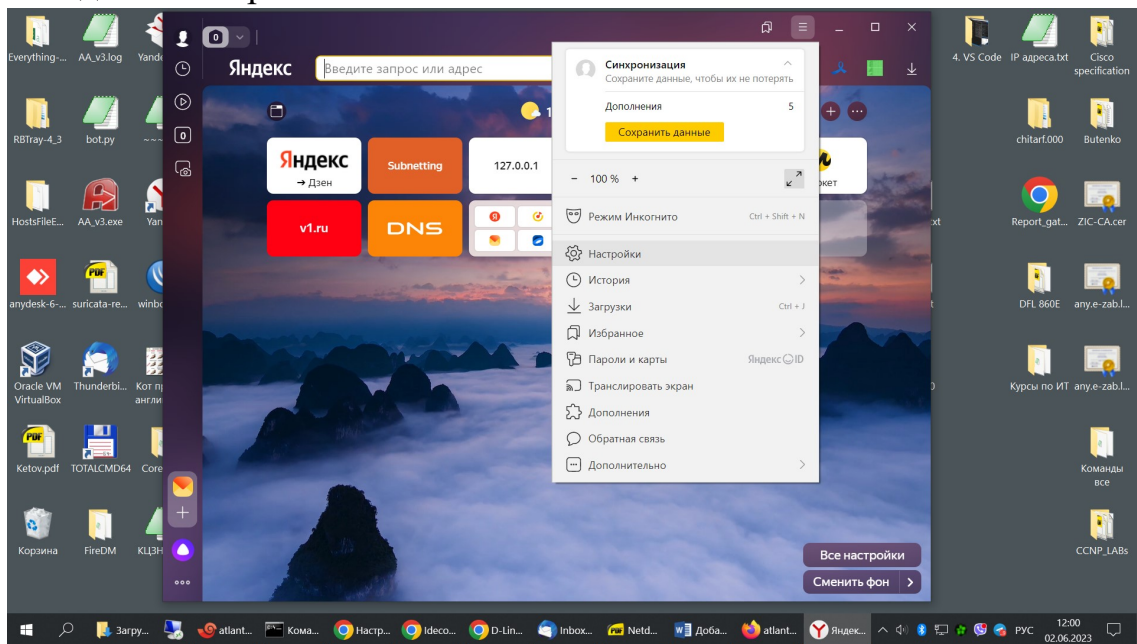


3) Импортировать -> Выбираем файл сертификата root_ca.crt. Далее, отмечаем Доверять при идентификации веб-сайтов:

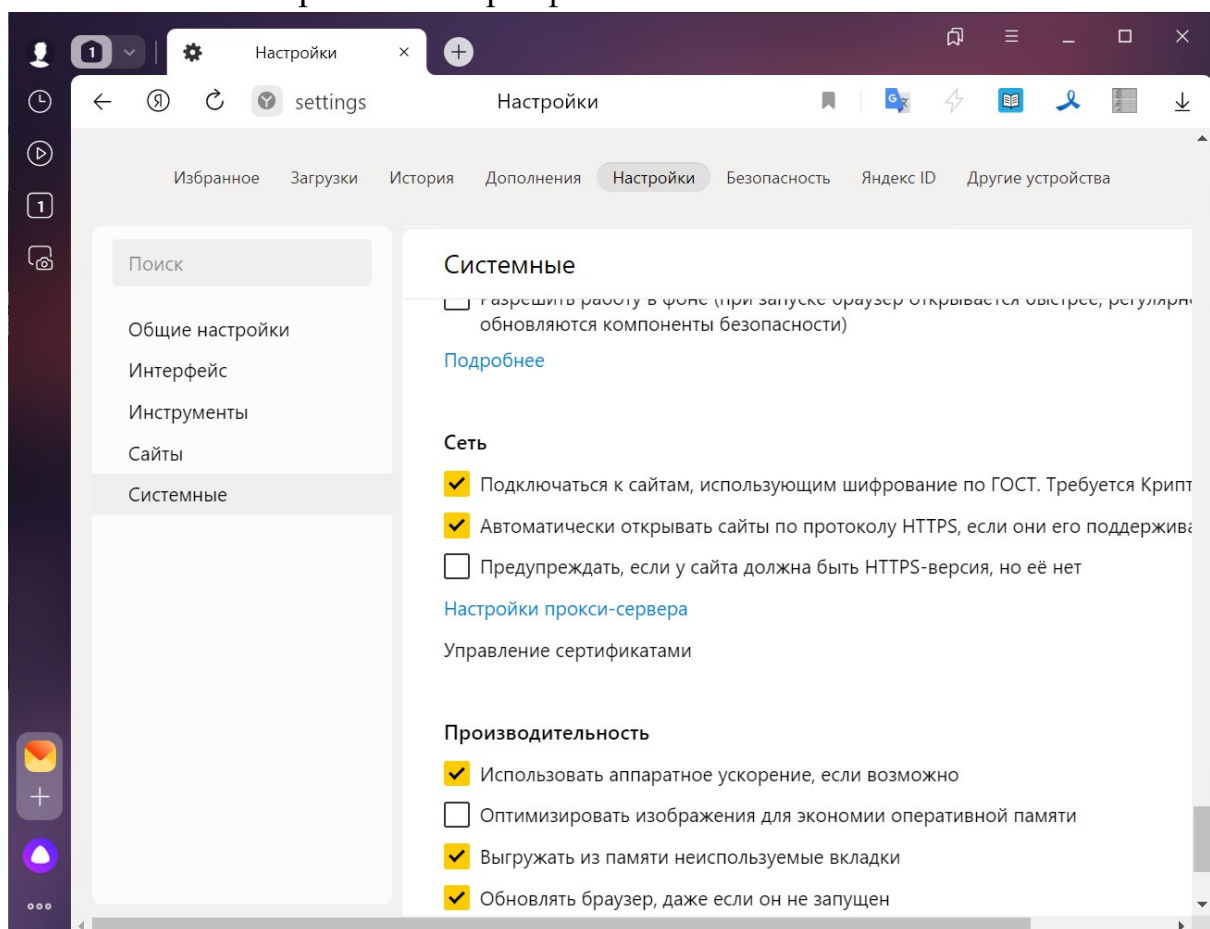


Добавление корневого сертификата в Яндекс браузер.

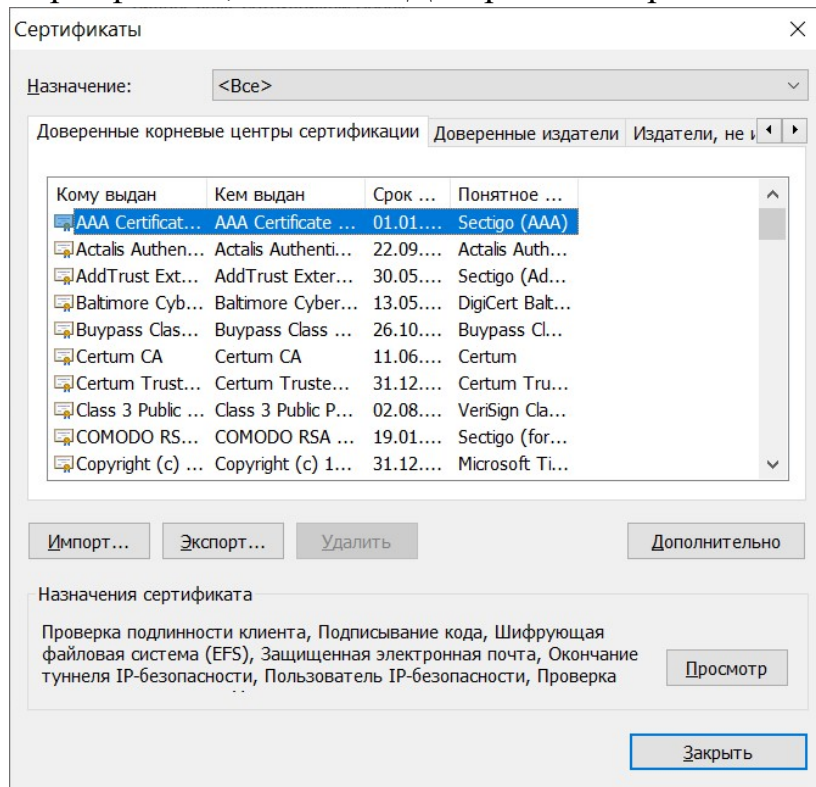
- 1) Яндекс браузер использует тоже хранилище, что и Chrome. При совместном использовании достаточно добавить сертификат в один из них. Заходим в настройки:



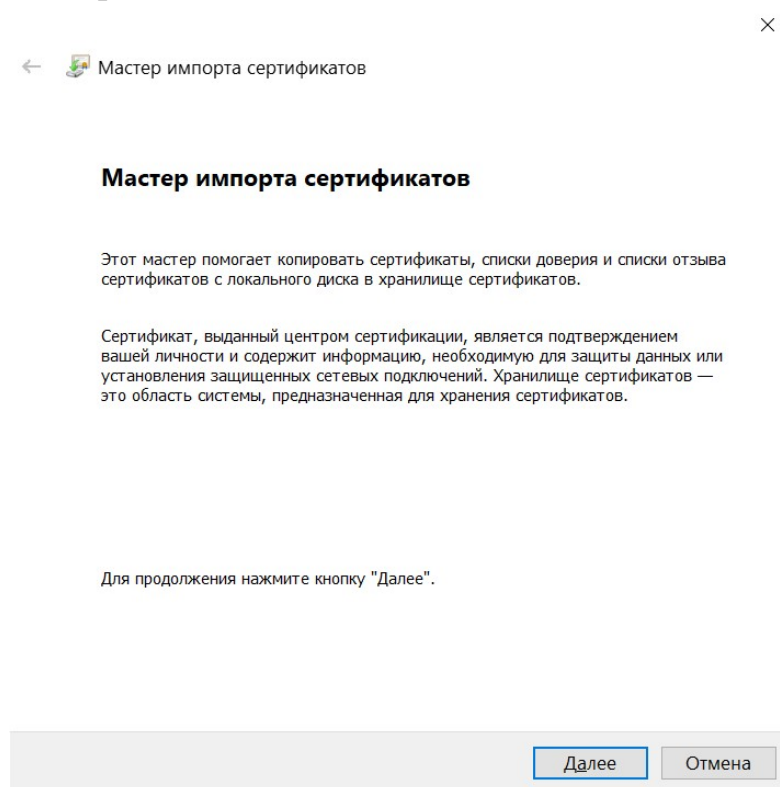
- 2) Системный -> Управление сертификатами:



3) Сертификаты, вкладка – Доверенные корневые центры сертификации:



4) Импорт:



5) Выбираем файл сертификата root_ca.crt:

←  Мастер импорта сертификатов

Импортируемый файл

Укажите файл, который вы хотите импортировать.

Имя файла:

Обзор...

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

Файл обмена личной информацией - PKCS #12 (.PFX, .P12)

Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)

Хранилище сериализованных сертификатов (.SST)

Далее

Отмена

6) Далее:

←  Мастер импорта сертификатов

Хранилище сертификатов

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

Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.

☐ Автоматически выбрать хранилище на основе типа сертификата

☒ Поместить все сертификаты в следующее хранилище

Хранилище сертификатов:

Доверенные корневые центры сертификации

Обзор...

Далее

Отмена

Завершение мастера импорта сертификатов

Сертификат будет импортирован после нажатия кнопки "Готово".

Были указаны следующие параметры:

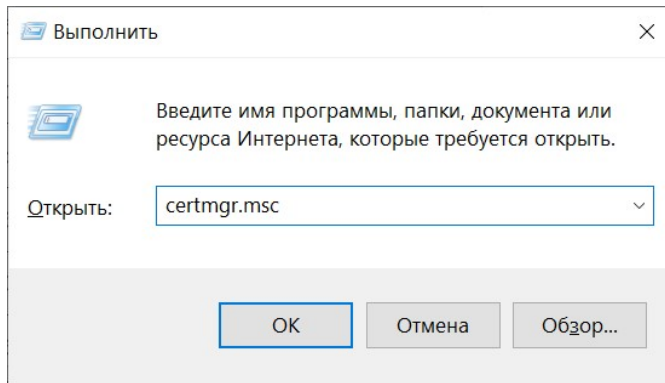
Хранилище сертификатов, выбранное пользователем	Доверенные корневые центры сертификации
Содержимое	Сертификат
Файл	C:\Users\baksheev.a.ZIC\Desktop\...

Готово

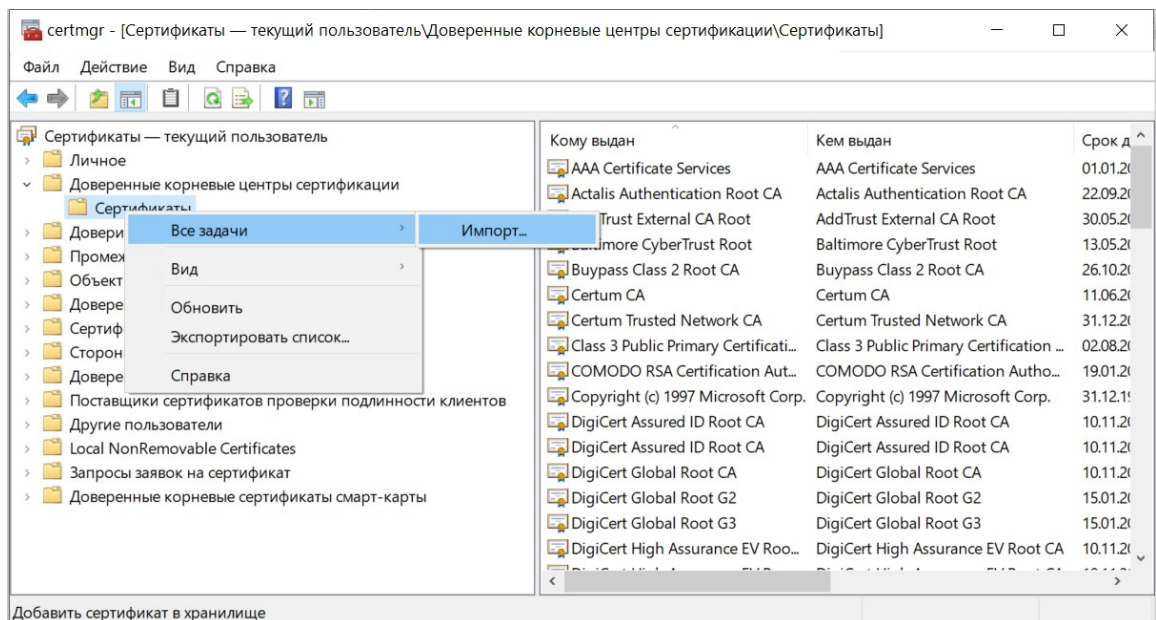
Отмена

Установка сертификата в хранилище ОС Windows для браузера Explorer/Edge и некоторых др. программ.

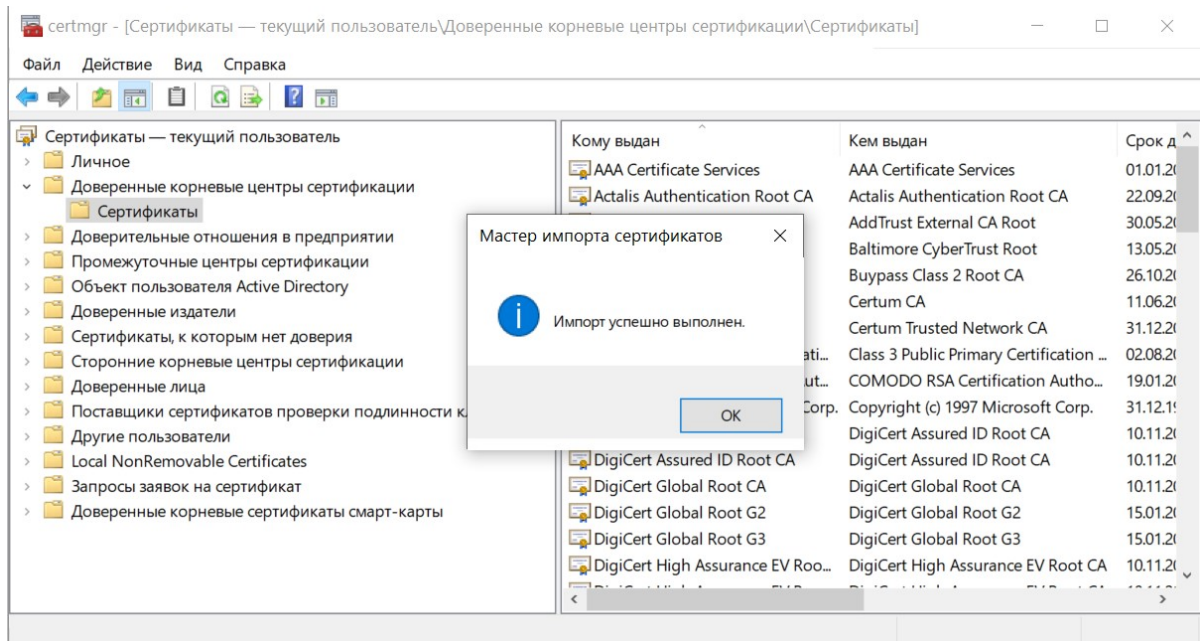
1) Нажимаем Win-x -> выполнить -> certmgr.msc



2) Доверенные корневые центры сертификации -> Сертификаты, правой кнопкой мышки – Все задачи -> Импорт...:



3) Далее -> Далее -> Готово:



Добавление корневого сертификата в Linux (Альт Линукс).

- 1) Скачать корневой сертификат.
- 2) В P10 и P9 для установки корневых сертификатов необходимо поместить файлы сертификатов в каталог: `/etc/pki/ca-trust/source/anchors/` и обновить общесистемный список доверенных сертификатов.
- 3) Выполнить команду для перемещения сертификата «CA_kspd.crt»:
`cp /home/user/CA_kspd.crt /etc/pki/ca-trust/source/anchors/`

Пример команды для обновления общесистемного списка доверенных сертификатов:

`update-ca-trust`

Добавление корневого сертификата в Linux (Astra Linux).

- 1) Предполагается, что корневой сертификат находится на рабочей машине.
- 2) Если сертификат в формате .cer, необходимо ввести команду
`openssl x509 -inform PEM -in /путь/до/сертификата/certificate.cer -out certificate.crt`
- 3) Скопировать полученный сертификат в папку `/usr/local/share/ca-certificates`:
`sudo cp /путь/до/сертификата/certificate.crt /usr/share/ca-certificates`
- 4) Выполнить команду:
`sudo update-ca-certificates`

После ввода должны появиться следующие строки, уведомляющие о правильном выполнении процедуры:

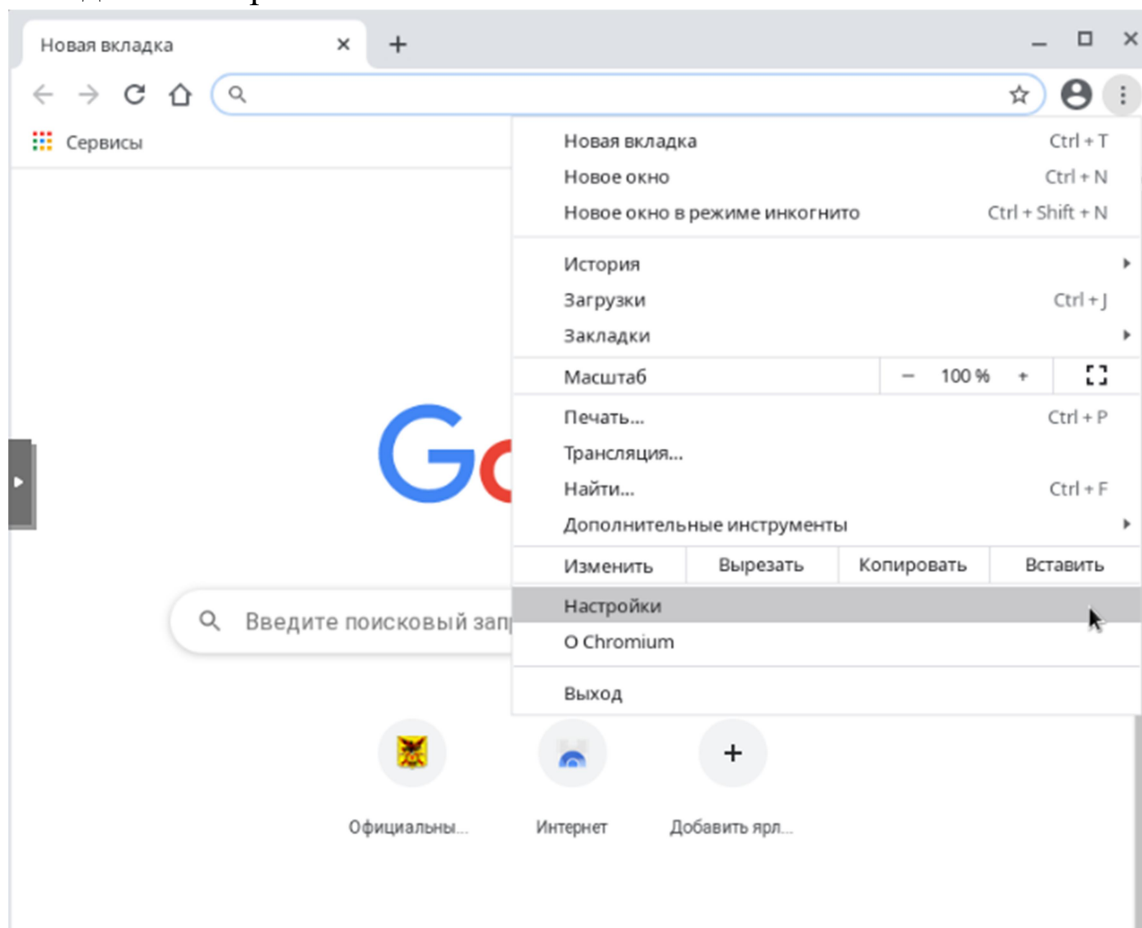
```
shikhanov@astra:~$ sudo update-ca-certificates
Updating certificates in /etc/ssl/certs...
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done
```

- 5) Чтобы убедиться в том, что коренной сертификат установился, можно ввести команду **`trust list`**, которая выведет список всех доверенных сертификатов, среди которых необходимо найти **KSPD Trusted Root**:

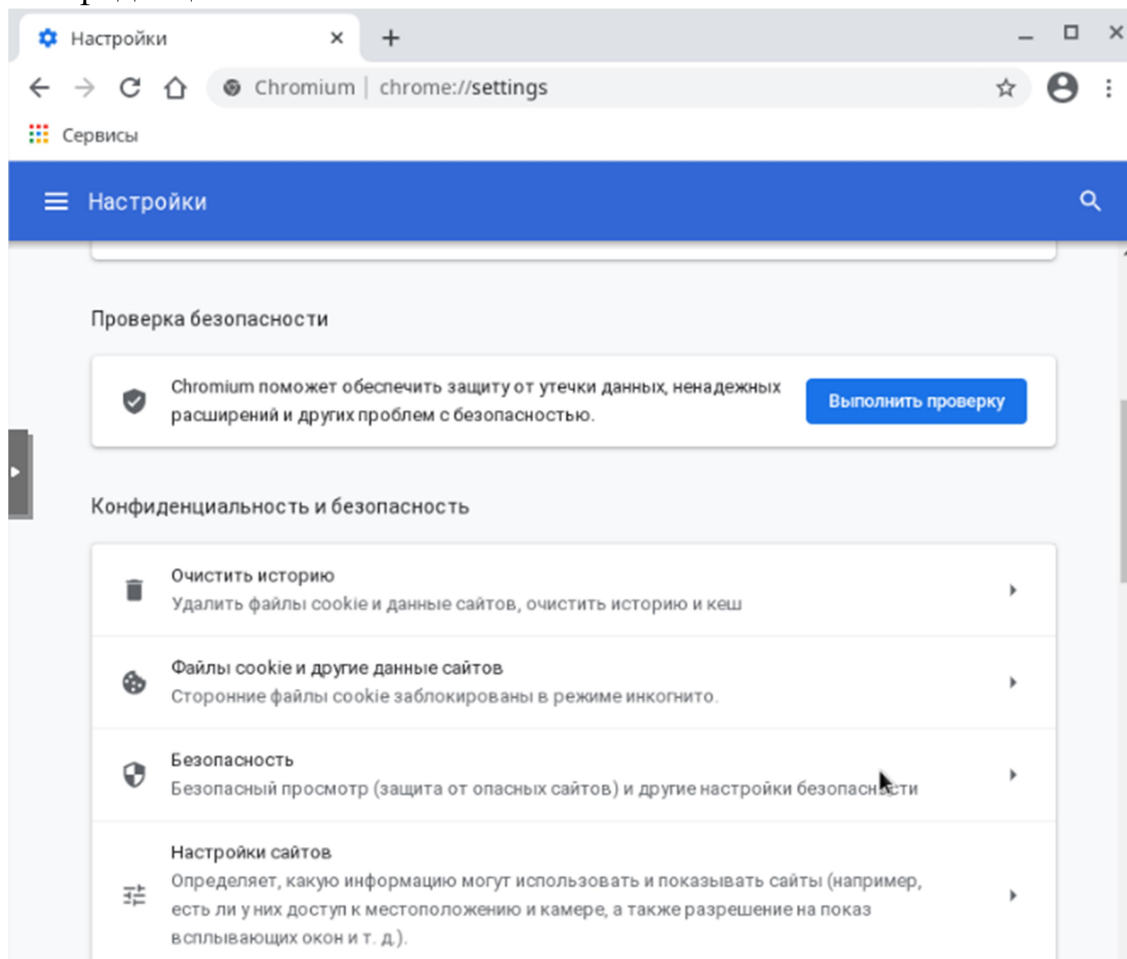
```
pkcs11: id=%0C%B9%81%52%E6%B2%0E%35%A9%1B%45%DE%CF%D9%7A%F5%EA%34%3F%8E; type=cert
type: certificate
label: KSPD Trusted Root CA
trust: anchor
category: authority
```


Добавление корневого сертификата в браузер Chrome/Chromium.

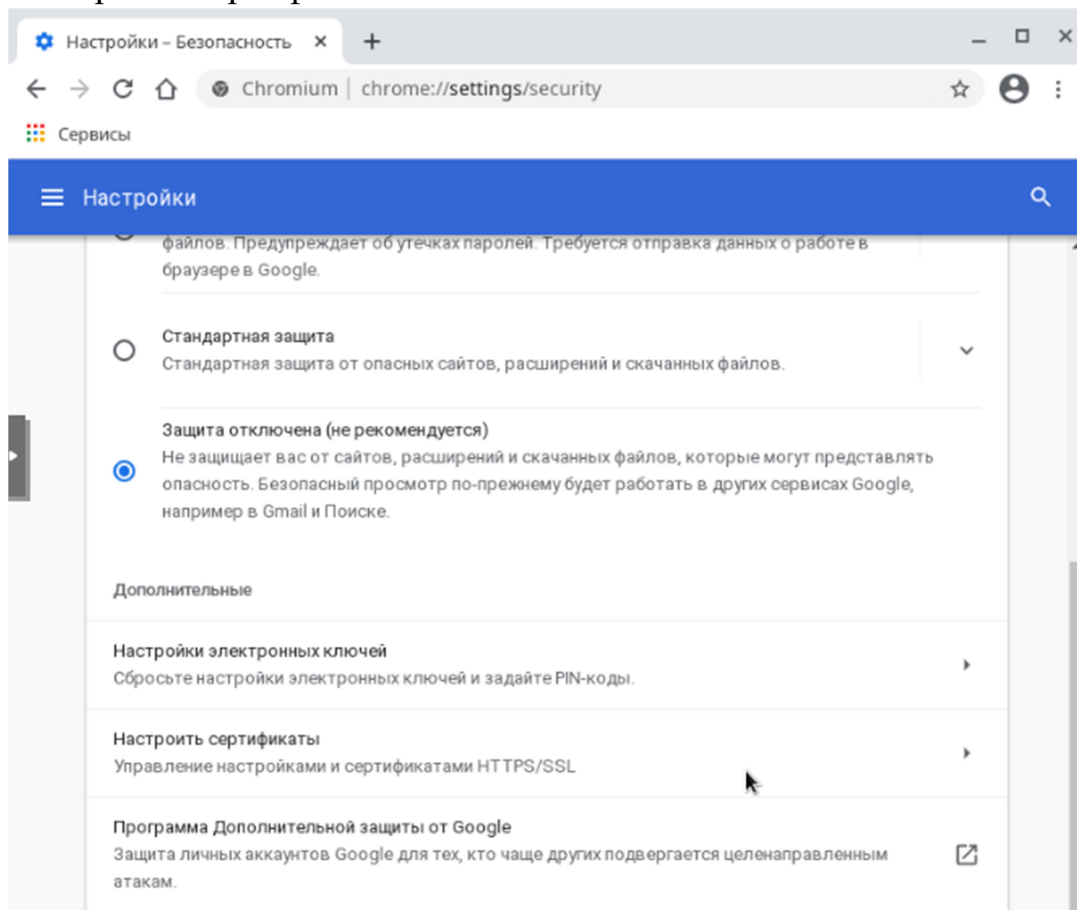
1) Заходим в настройки:



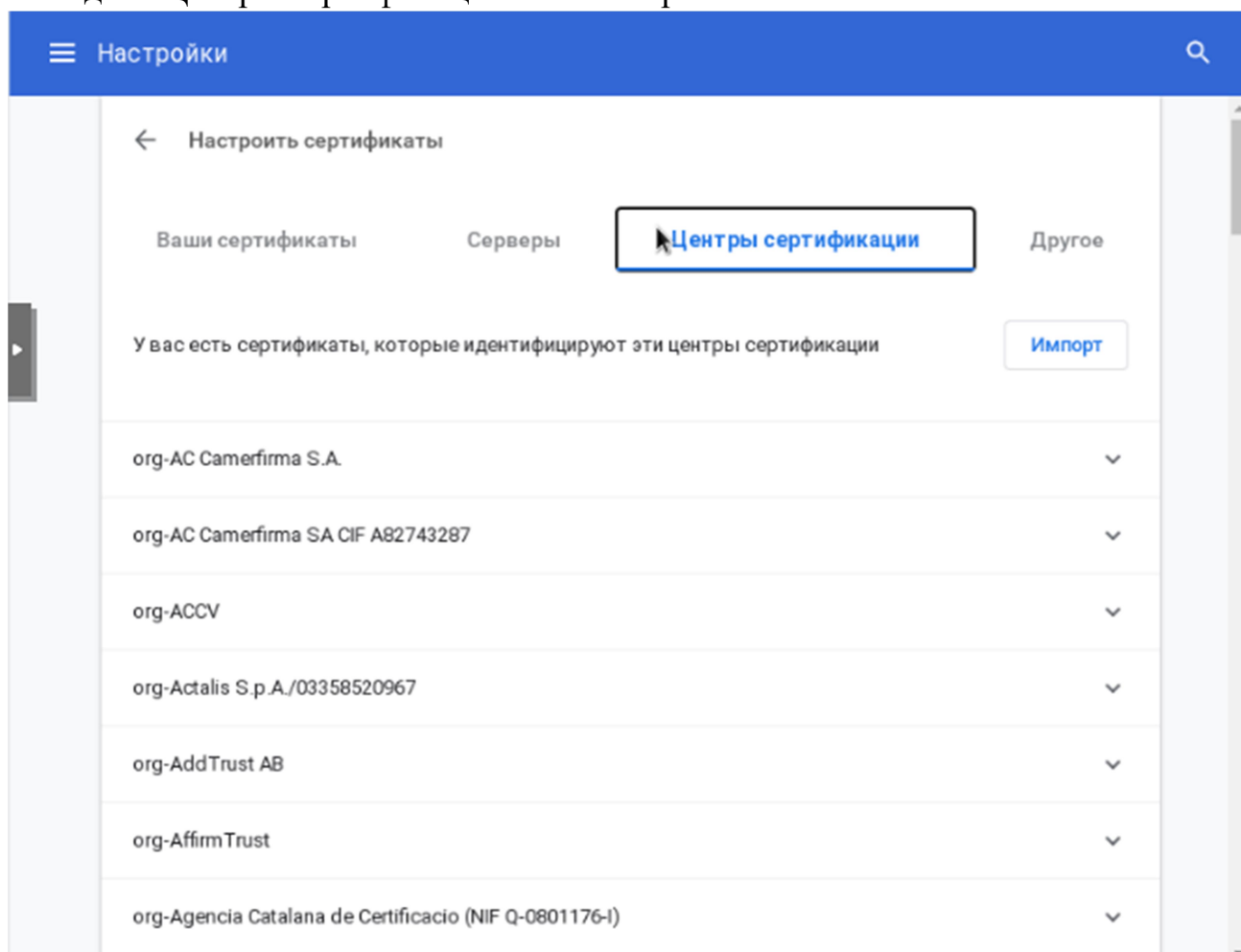
2) Конфиденциальность и безопасность - Безопасность:



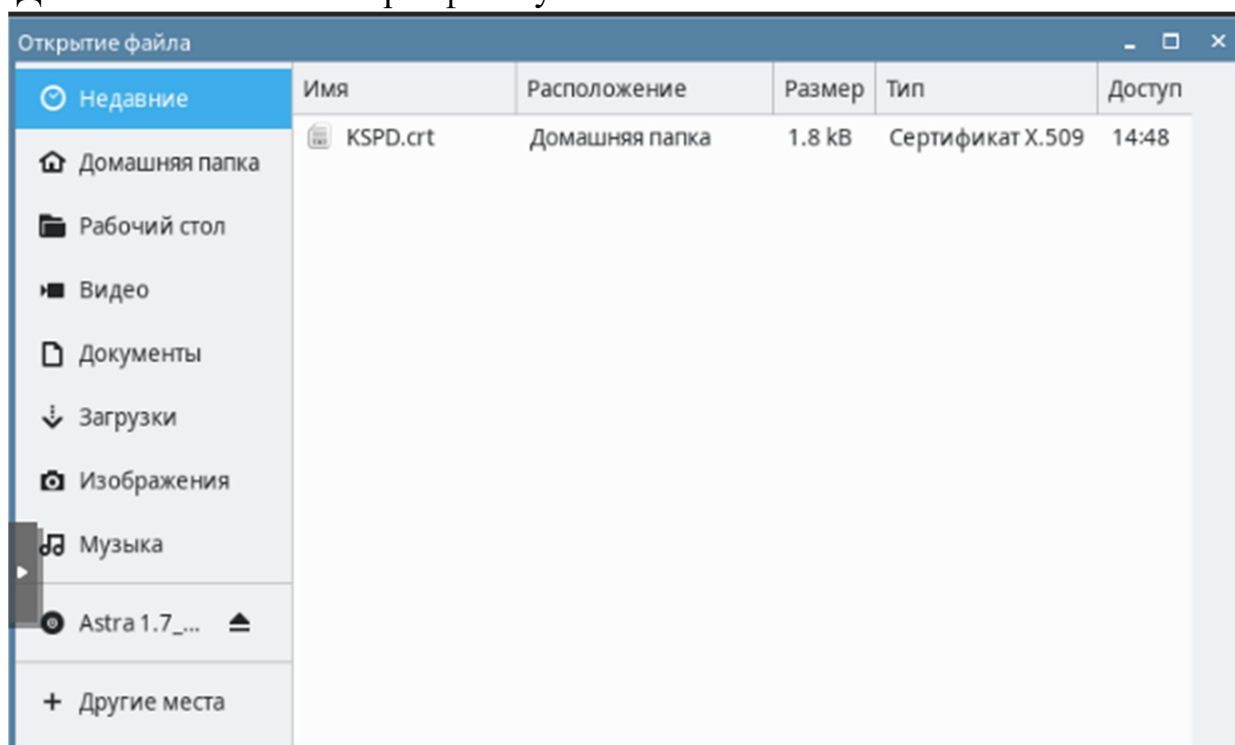
3) Настроить сертификаты:



4) Вкладка «Центры сертификации» -> Импорт:

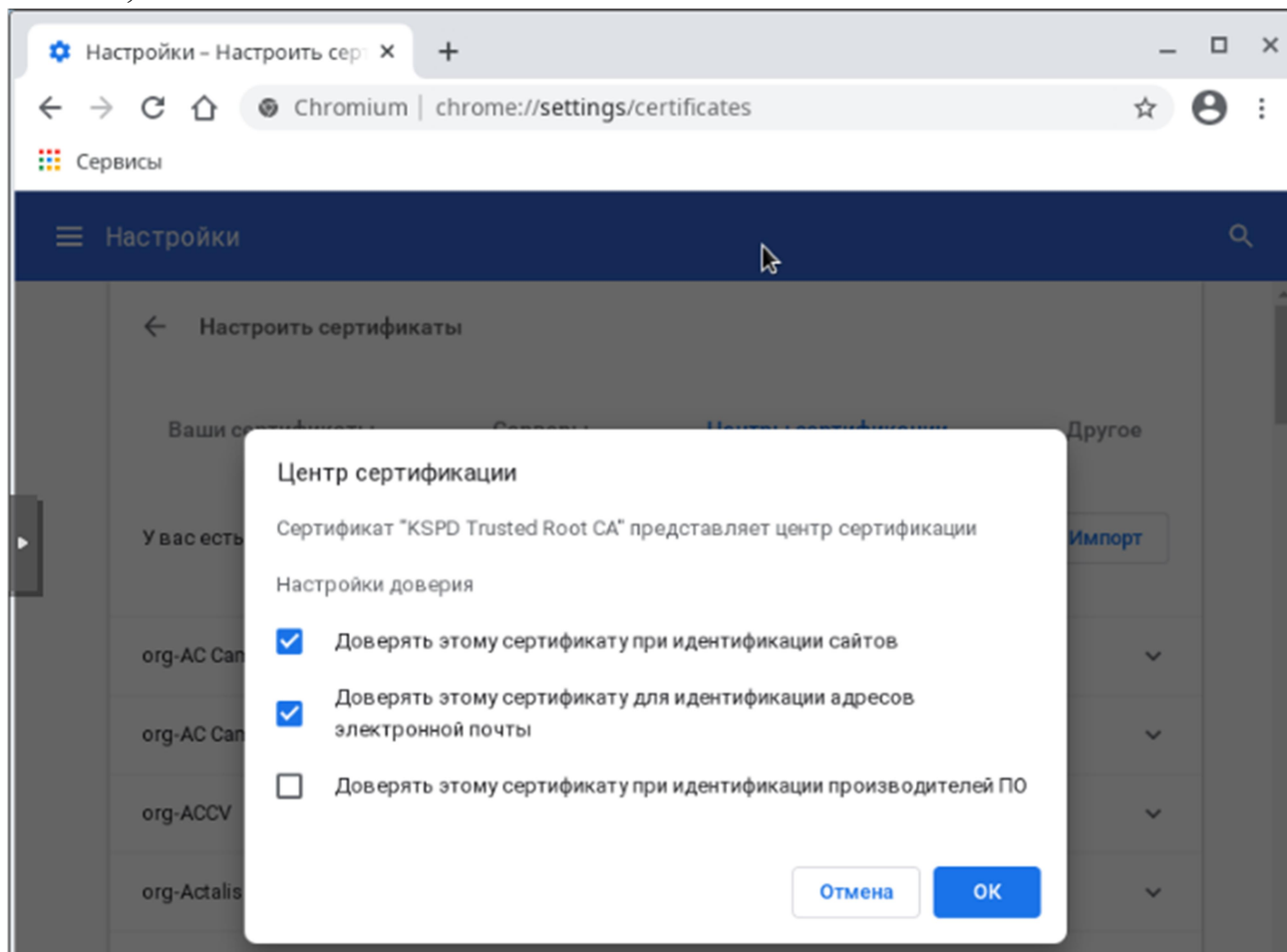


5) Двойным кликом по сертификату:



6) Поставить галочки «Доверять этому сертификату при идентификации сайтов» и «Доверять этому сертификату для идентификации адресов электронной

почты», нажать ОК:



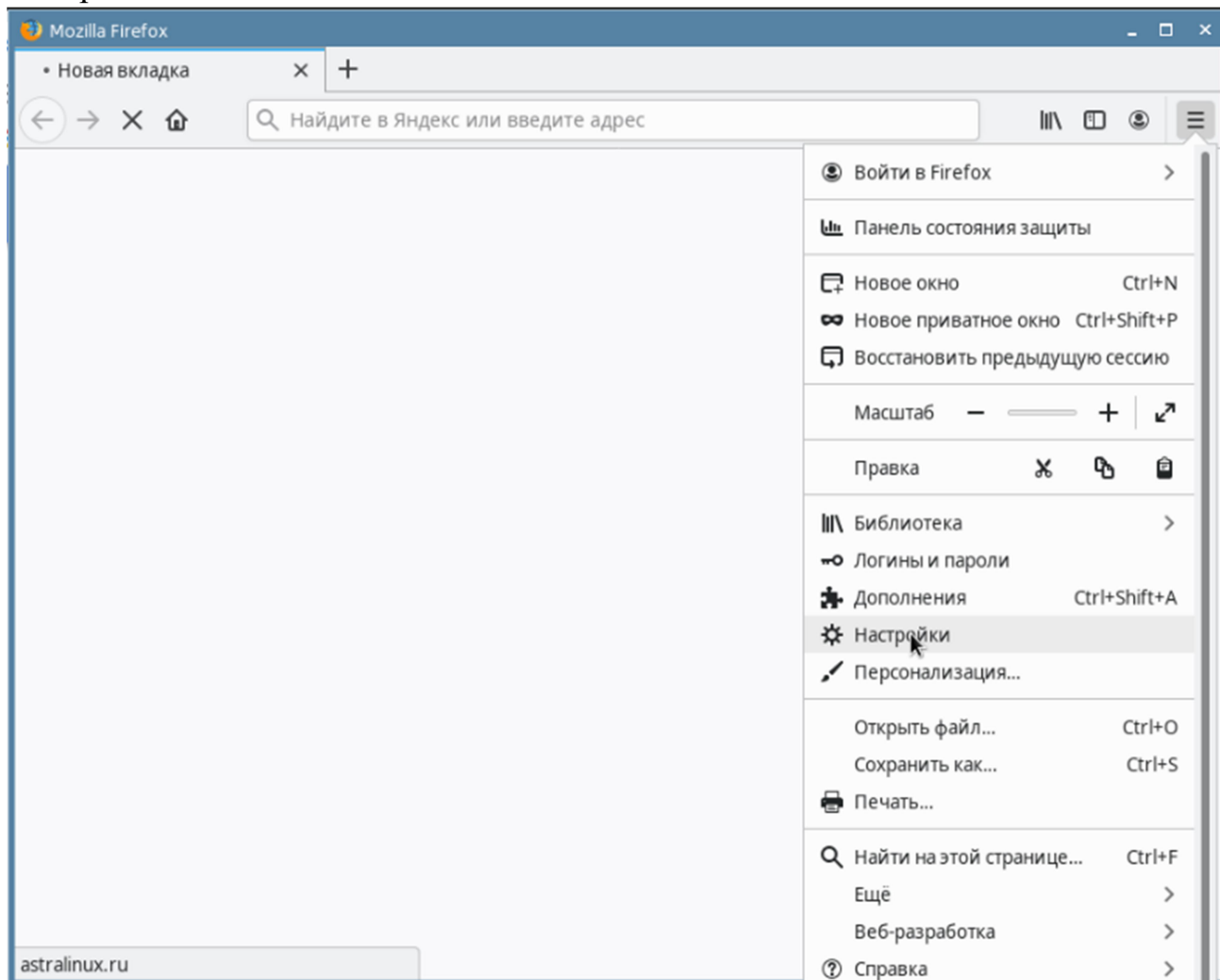
- 7) В списке сертификатов должен был появиться сертификат KSPD Trusted Root CA:

org-The Ministry of HCS, Energy, Digitalization and Communications

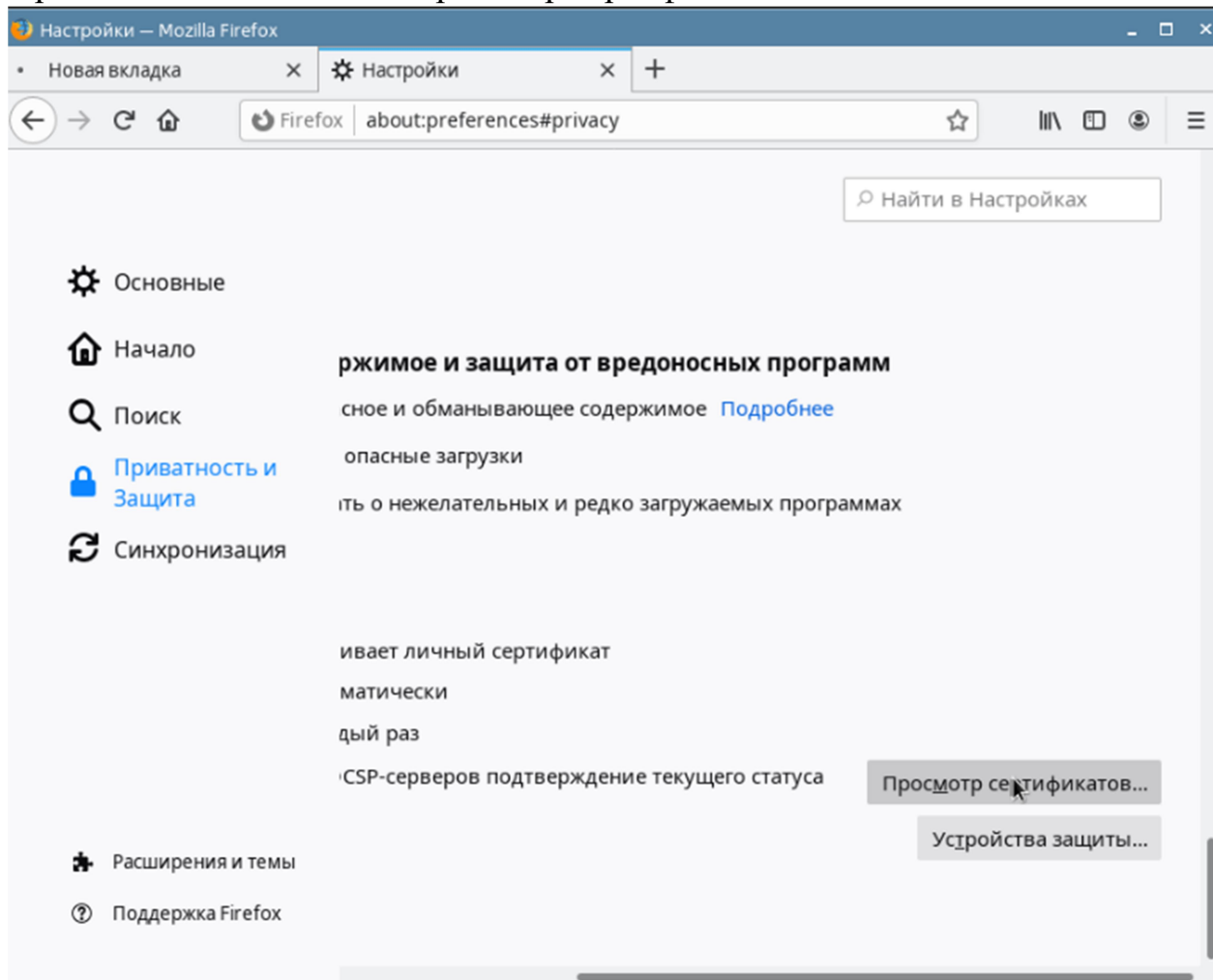
KSPD Trusted Root CA

Добавление корневого сертификата в браузер Mozilla Firefox.

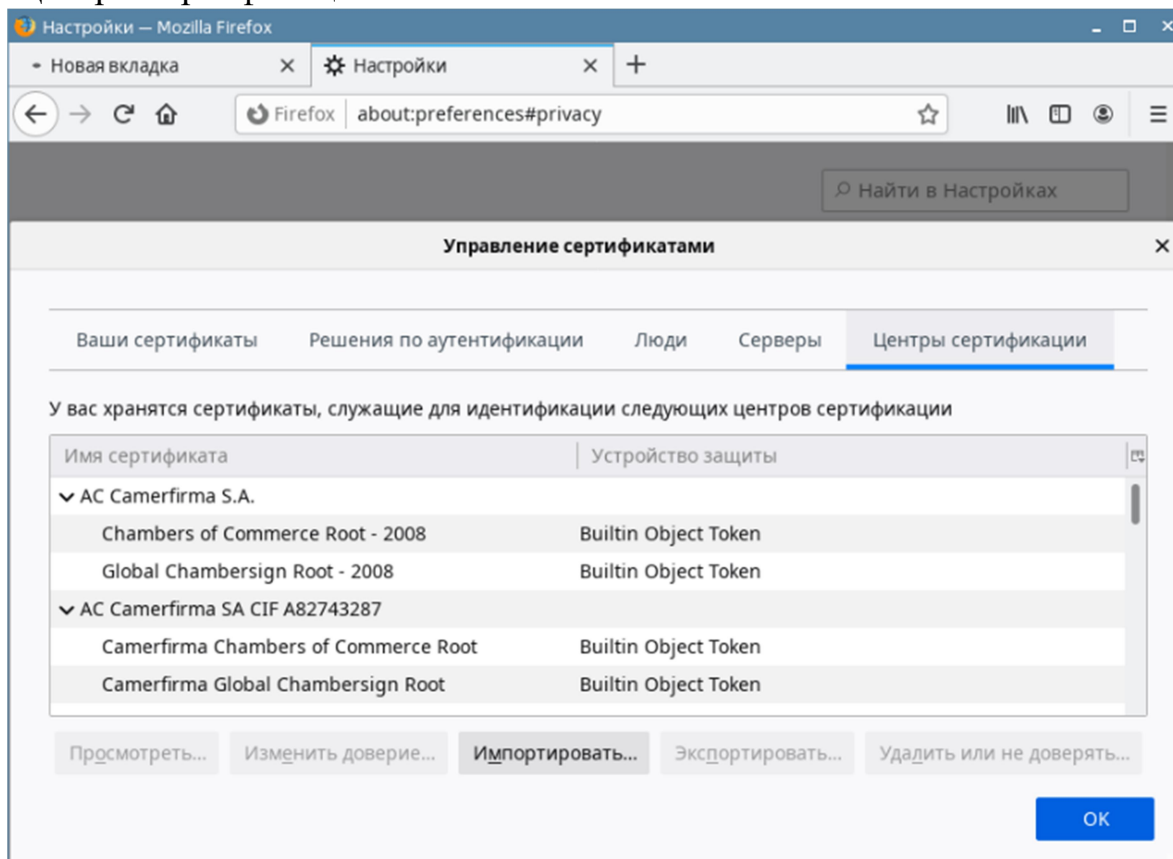
1) Настройки:



2) Приватность и защита → Просмотр сертификатов:

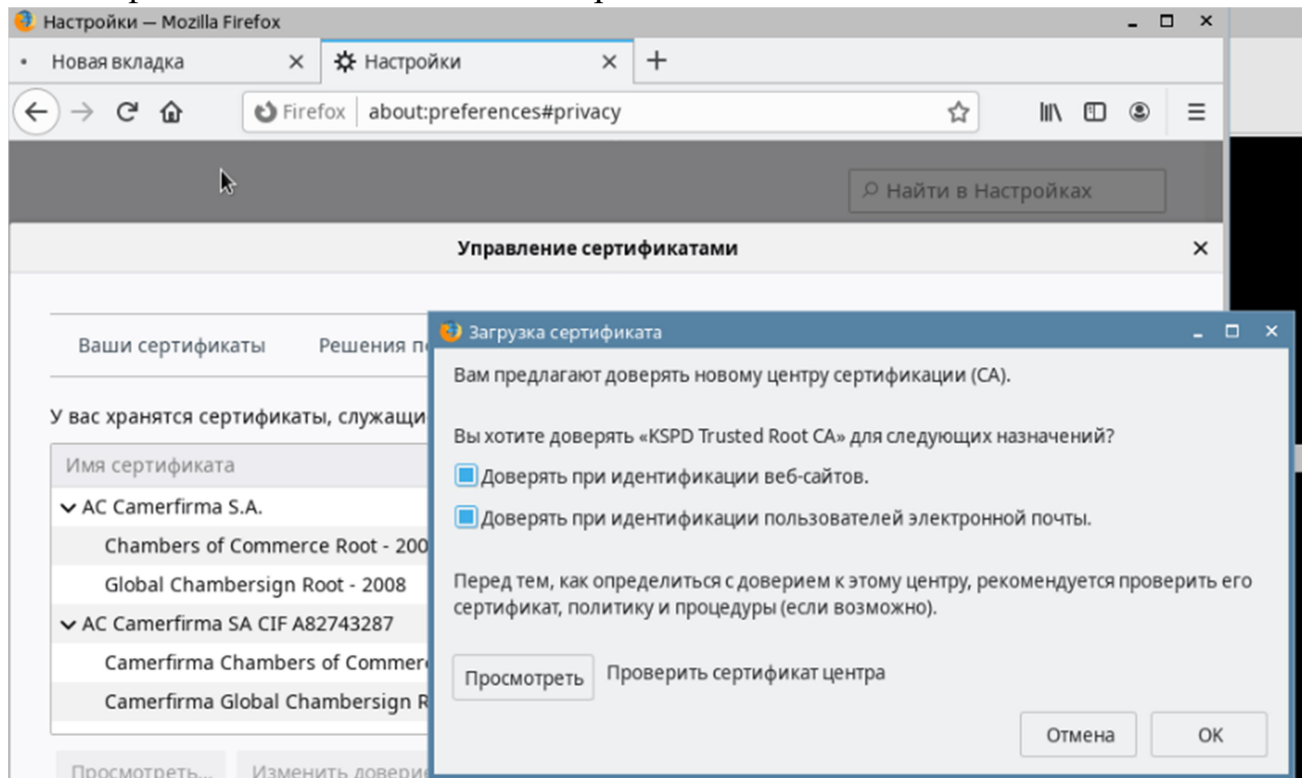


3) Центры сертификации:



4) Импортировать -> Выбираем файл сертификата.

Далее, отмечаем «Доверять при идентификации веб-сайтов» и «Доверять при идентификации пользователей электронной почты»:

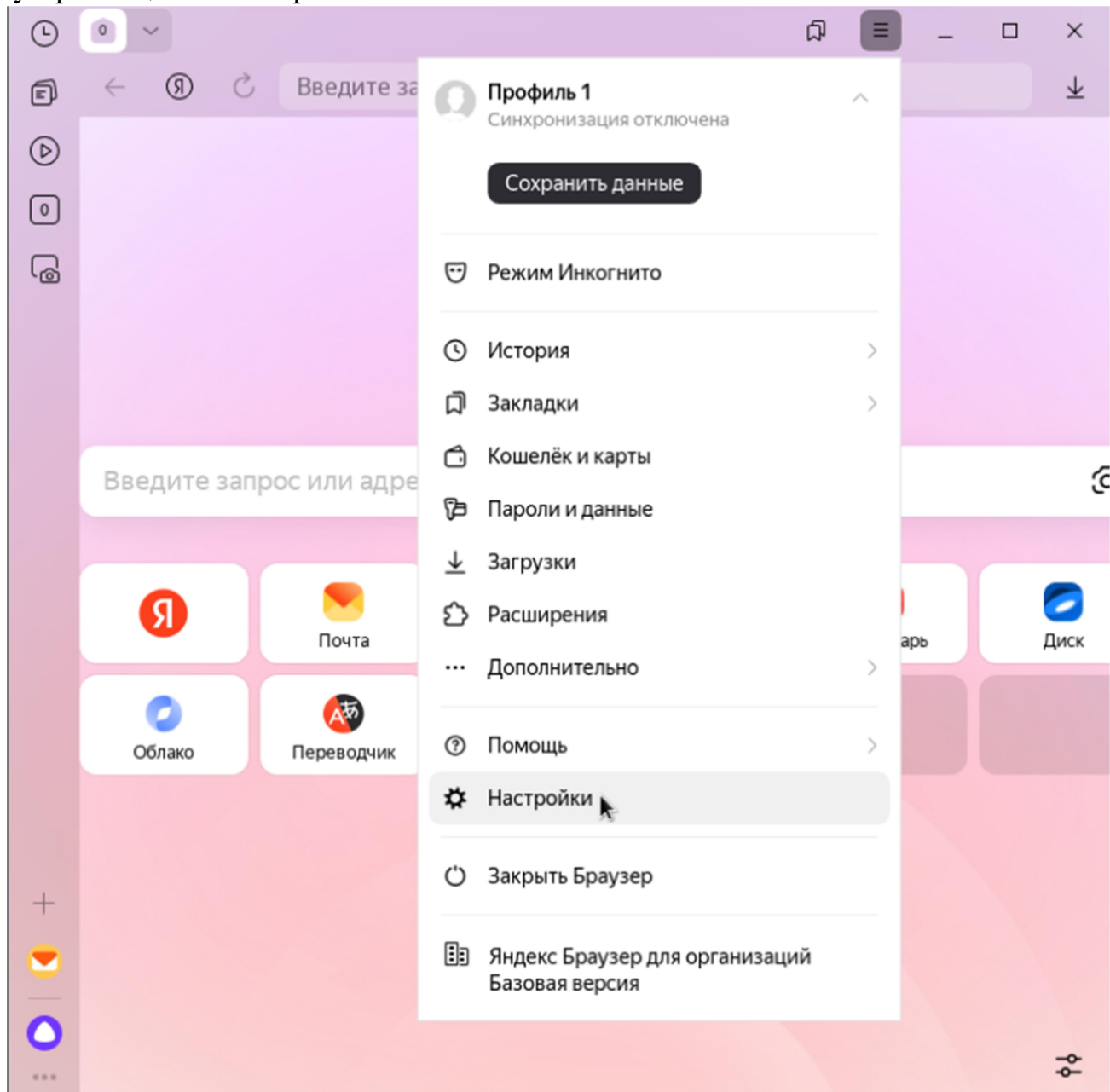


5) Находим в списке появившийся сертификат:

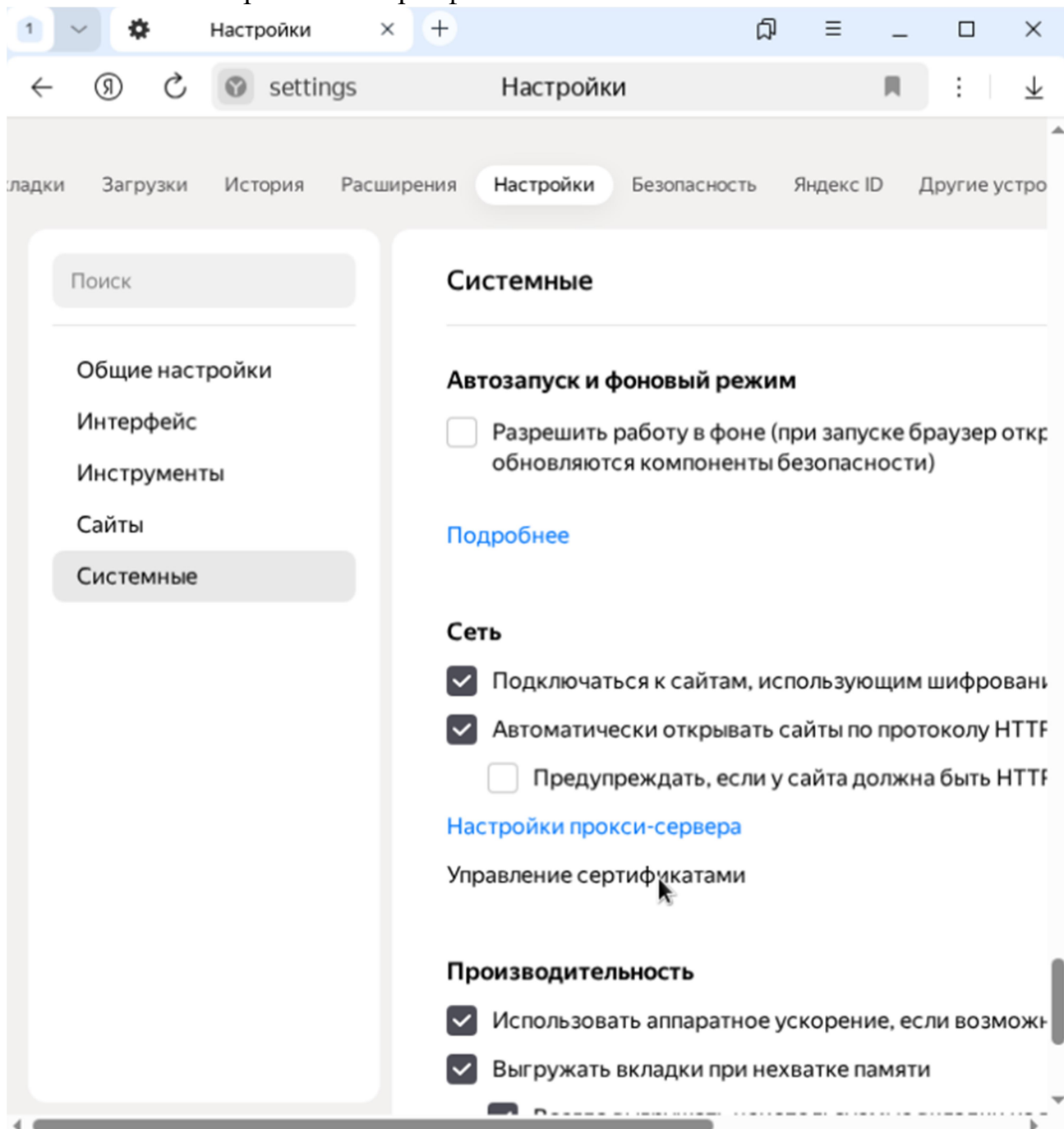
▼ The Ministry of HCS, Energy, Digitalization and Com...		
KSPD Trusted Root CA		Модуль защиты

Добавление корневого сертификата в Яндекс Браузер.

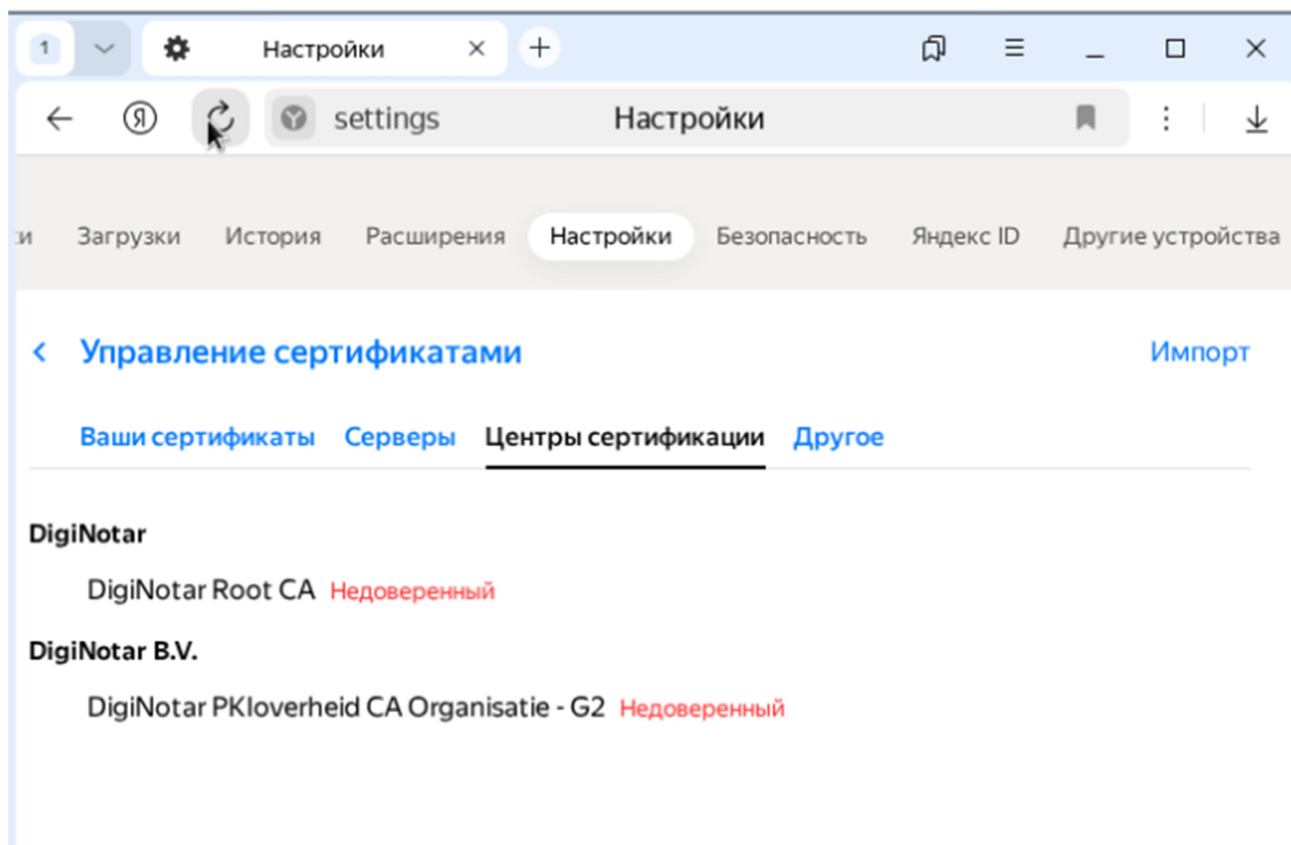
- 1) Хранилище сертификатов у Google Chrome и Yandex Browser одно и то же, так что при совместном использовании достаточно импортировать только в один браузер. Заходим в настройки:



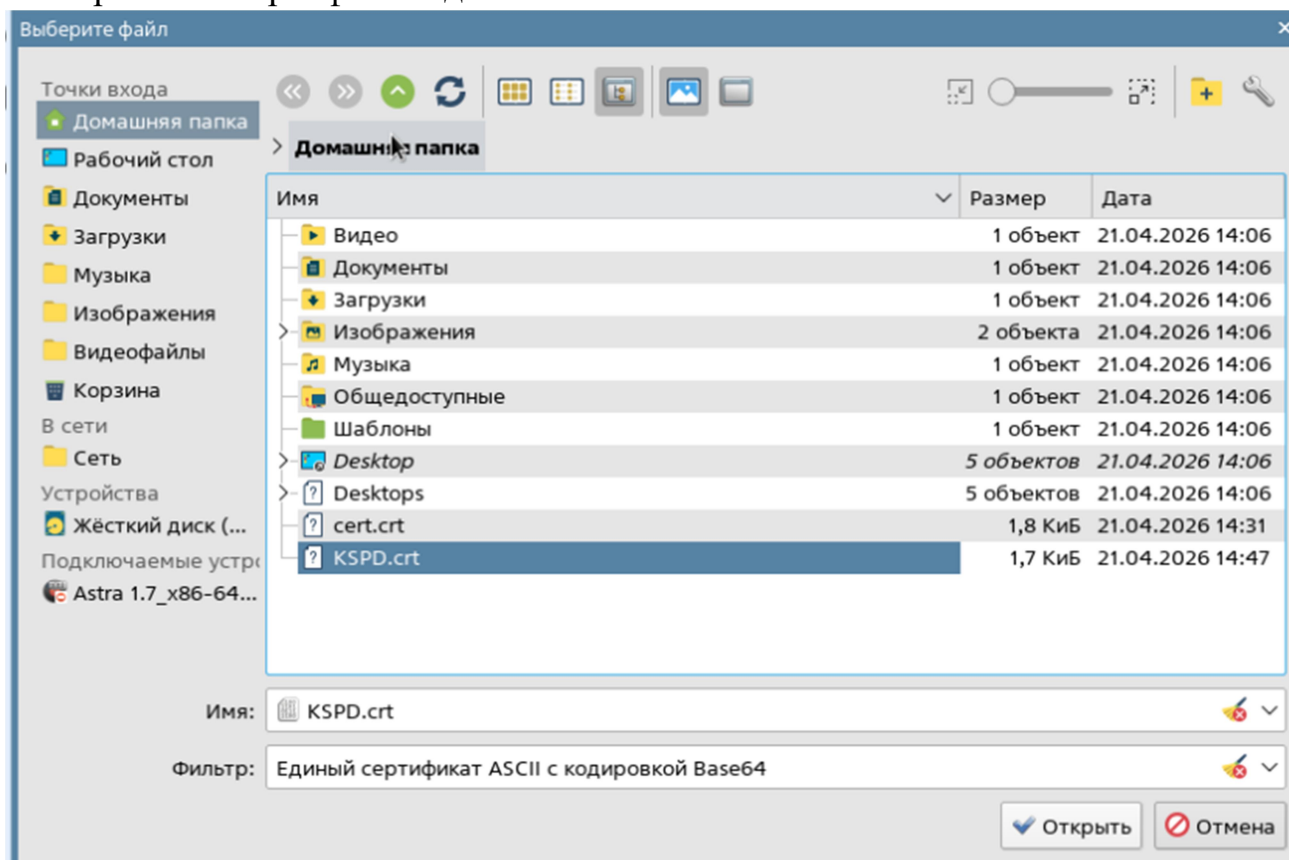
2) Системные -> Управление сертификатами:



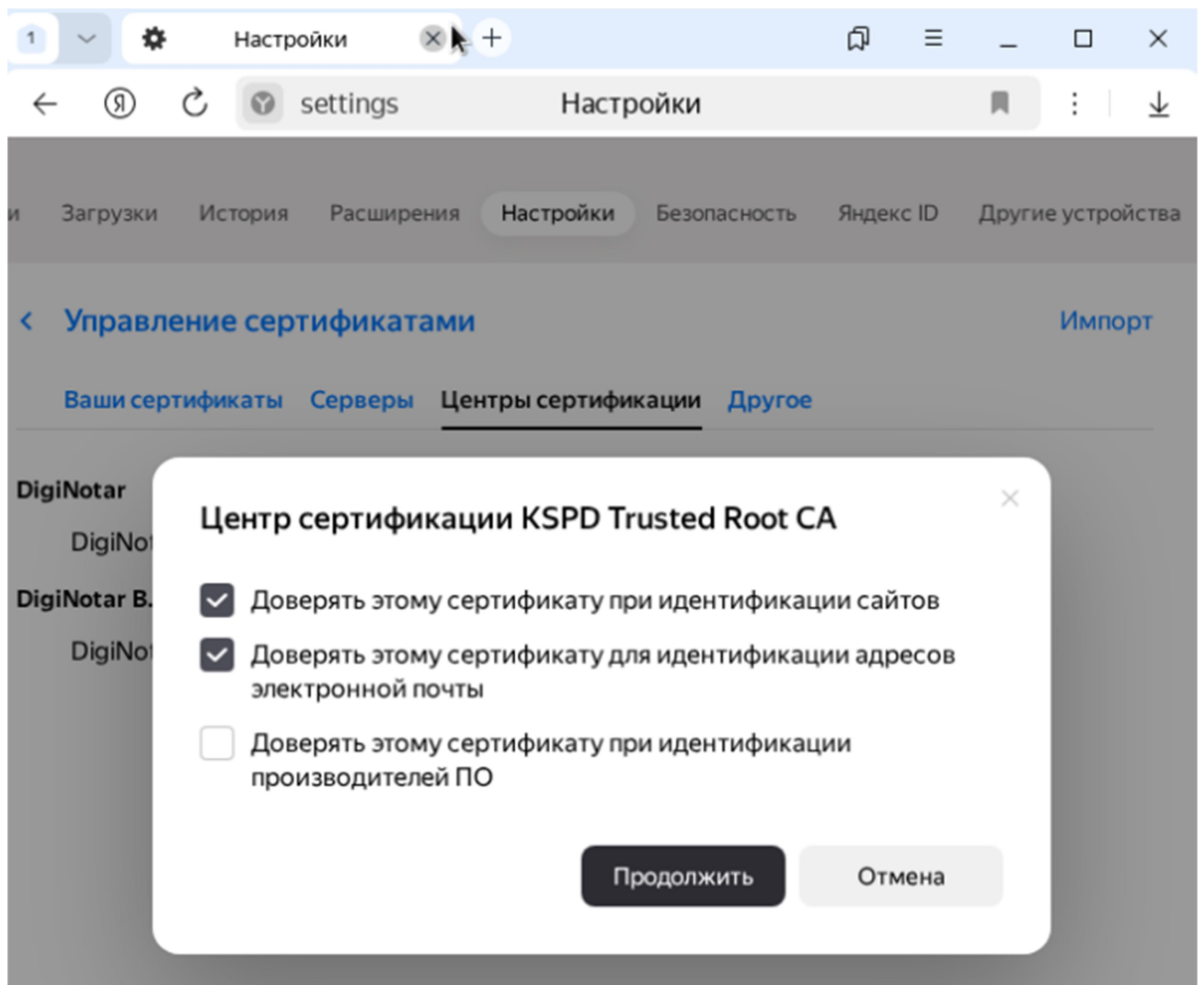
3) Центры сертификации -> Импорт



4) Выбор своего сертификата двойным кликом.



5) Установить галочки «Доверять этому сертификату при идентификации сайтов» и «Доверять этому сертификату при идентификации адресов электронной почты», нажать на кнопку «Продолжить»:



6) Проверить в списке установленный сертификат KSPD Trusted Root CA:

