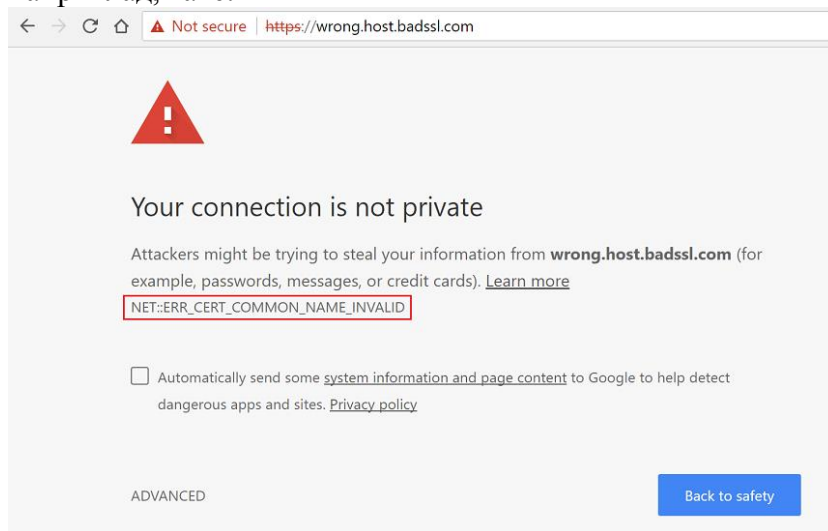


Інструкція щодо оновлення електронного кореневого сертифікату безпеки для сайтів

Опис проблеми

Нещодавно у багатьох співробітників, які мають ПК зі старими версіями операційної системи Windows та у яких вимкнене автоматичне оновлення системи, перестали відкриватися деякі сайти, зокрема офіційний сайт ХНАДУ та навчальний сайт ХНАДУ.

При спробі зайти на сайт виникає повідомлення про проблему із сертифікатом, наприклад, таке:



Суть питання

У теперішній час більшість сайтів у мережі Інтернет з метою інформаційної безпеки використовують протоколи шифрування передачі даних та засвідчення справжності своєї електронної адреси. Для цього використовується система електронних сертифікатів, які видаються визнаними центрами сертифікації. Центр сертифікації має свій «кореневий» сертифікат, яким засвідчує сертифікати різних окремих сайтів, а сертифікатом сайту засвідчується достовірність його електронної адреси. Крім того, за допомогою сертифіката шифруються дані, що передаються між сайтом та відвідувачами. Це унеможливує втручання злодіїв у передачу даних та подальшу компрометацію чи «крадіжку» інформації, зокрема, паролів, особистої інформації, тощо.

Кожен сертифікат, включаючи кореневі, має свій термін придатності. Тож, нещодавно вплив термін придатності кореневого сертифікату організації з сертифікації Let's Encrypt, який використовувався багатьма сайтами, включаючи сайти ХНАДУ, оскільки послуги Let's Encrypt є безкоштовними (з певними обмеженнями). Зазвичай, ці сертифікати мають автоматично оновлюватися із використанням функції автоматичного оновлення системи Windows разом з іншими оновленнями операційної системи. Але якщо користувачі ПК вимкнули автоматичне оновлення Windows або використовують старі версії Windows, які вже не підтримуються фірмою Microsoft, та для яких вже не надходять автоматичні оновлення, то нових корневих сертифікатів у системі немає, браузер не може засвідчити достовірність даних з сайту, і сайт не відкривається.

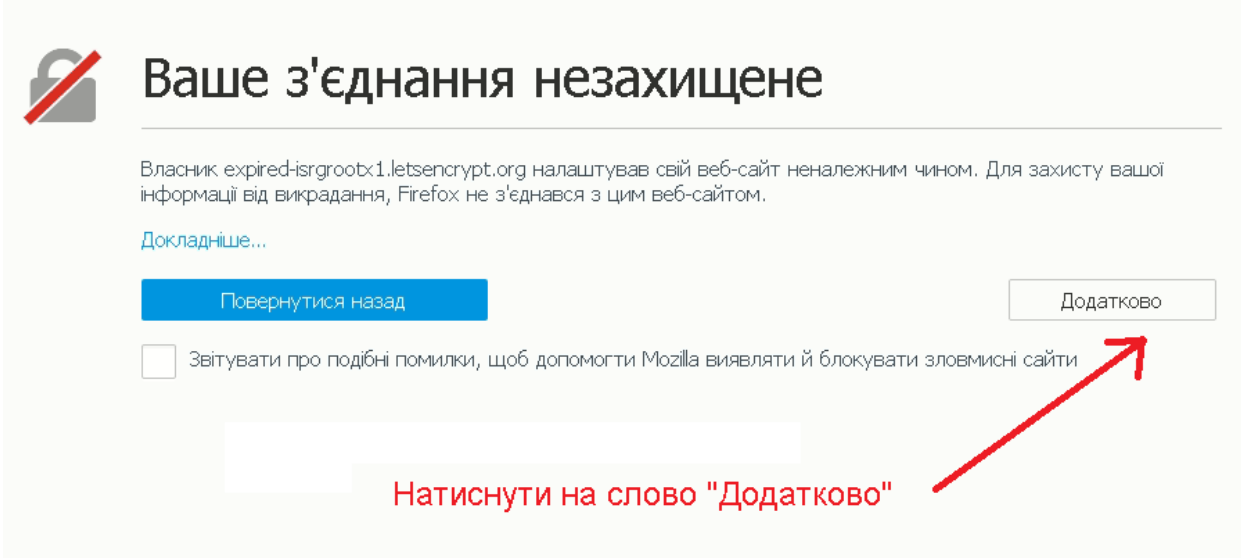
Що робити?

Треба оновити сертифікат вручну.

Спочатку візьміть ПК, що має підключення до Інтернет та встановлені відповідні оновлення операційної системи або хоча б сертифікатів. Перейдіть за посиланням та скачайте файл сертифікату.

<https://letsencrypt.org/certs/isrgrootx1.der>

Можна також спробувати скачати новий сертифікат безпосередньо на тому комп'ютері, де виникла проблема із сертифікатом. Після переходу за посиланням при отриманні попередження натисніть кнопку «Додатково» у вікні браузера.



Ваше з'єднання незахищене

Власник expired-isrgrootx1.letsencrypt.org налаштував свій веб-сайт неналежним чином. Для захисту вашої інформації від викрадання, Firefox не з'єднався з цим веб-сайтом.

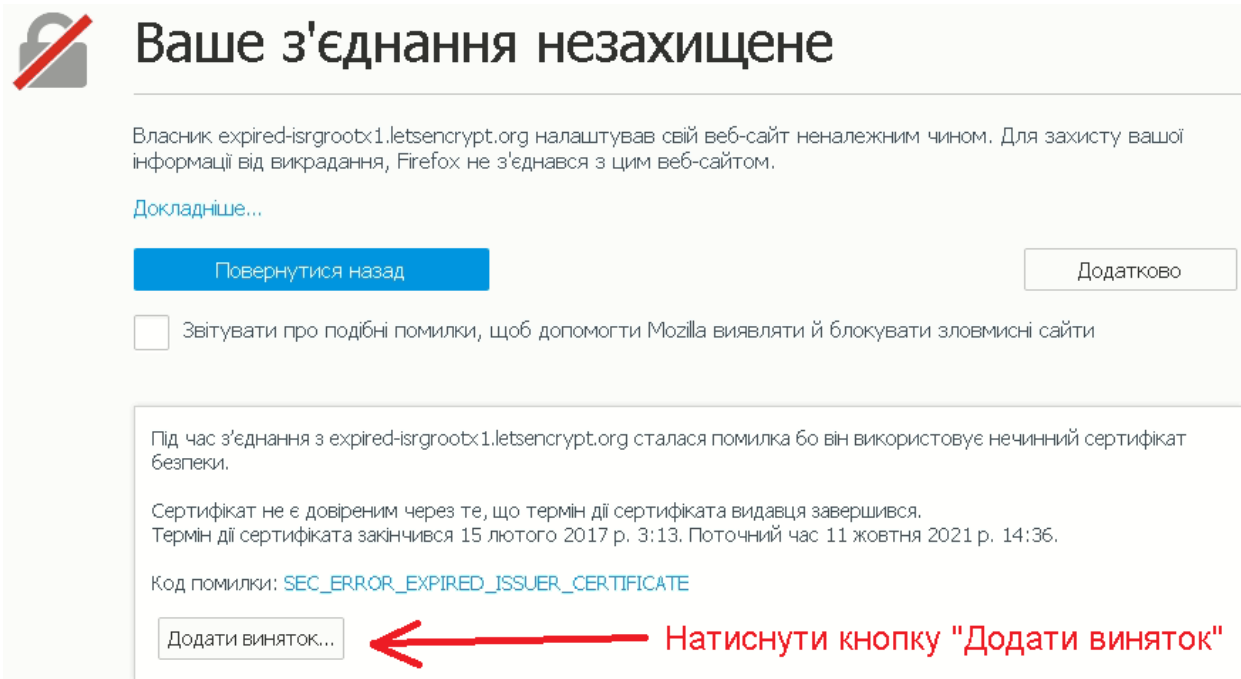
[Докладніше...](#)

[Повернутися назад](#) [Додатково](#)

Звітувати про подібні помилки, щоб допомогти Mozilla виявляти й блокувати зловмисні сайти

Натиснути на слово "Додатково"

Браузер запропонує зробити виняток для даного сайту. Натисніть кнопку «Додати виняток»



Ваше з'єднання незахищене

Власник expired-isrgrootx1.letsencrypt.org налаштував свій веб-сайт неналежним чином. Для захисту вашої інформації від викрадання, Firefox не з'єднався з цим веб-сайтом.

[Докладніше...](#)

[Повернутися назад](#) [Додатково](#)

Звітувати про подібні помилки, щоб допомогти Mozilla виявляти й блокувати зловмисні сайти

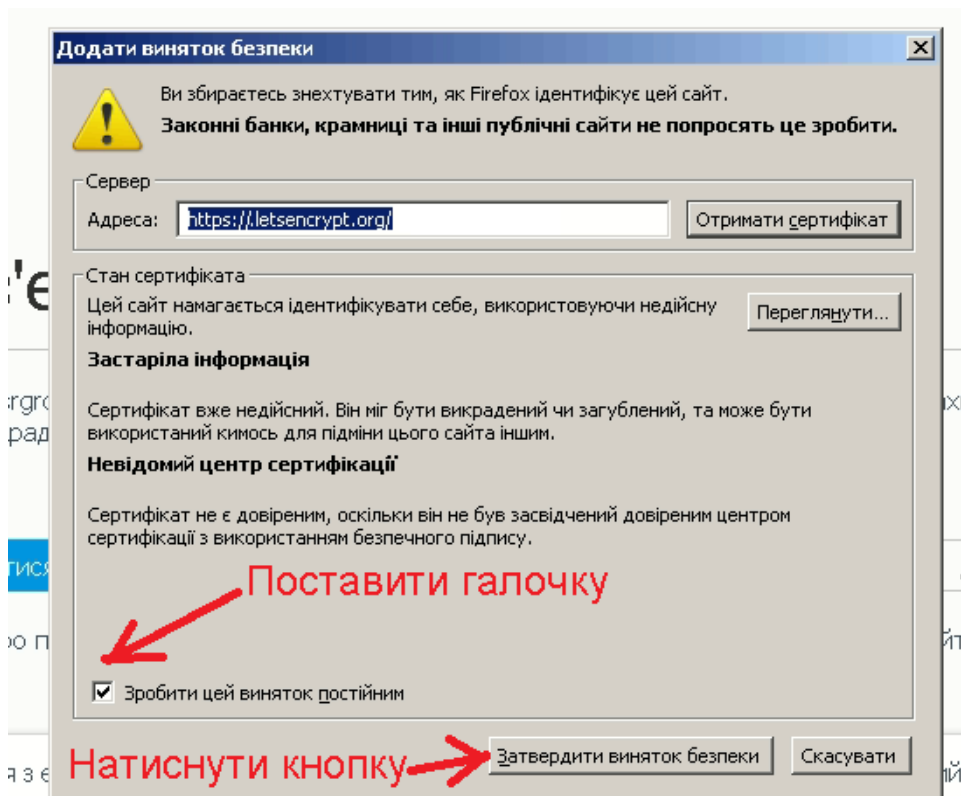
Під час з'єднання з expired-isrgrootx1.letsencrypt.org сталася помилка бо він використовує нечинний сертифікат безпеки.

Сертифікат не є довіреним через те, що термін дії сертифіката видавця завершився.
Термін дії сертифіката закінчився 15 лютого 2017 р. 3:13. Поточний час 11 жовтня 2021 р. 14:36.

Код помилки: `SEC_ERROR_EXPIRED_ISSUER_CERTIFICATE`

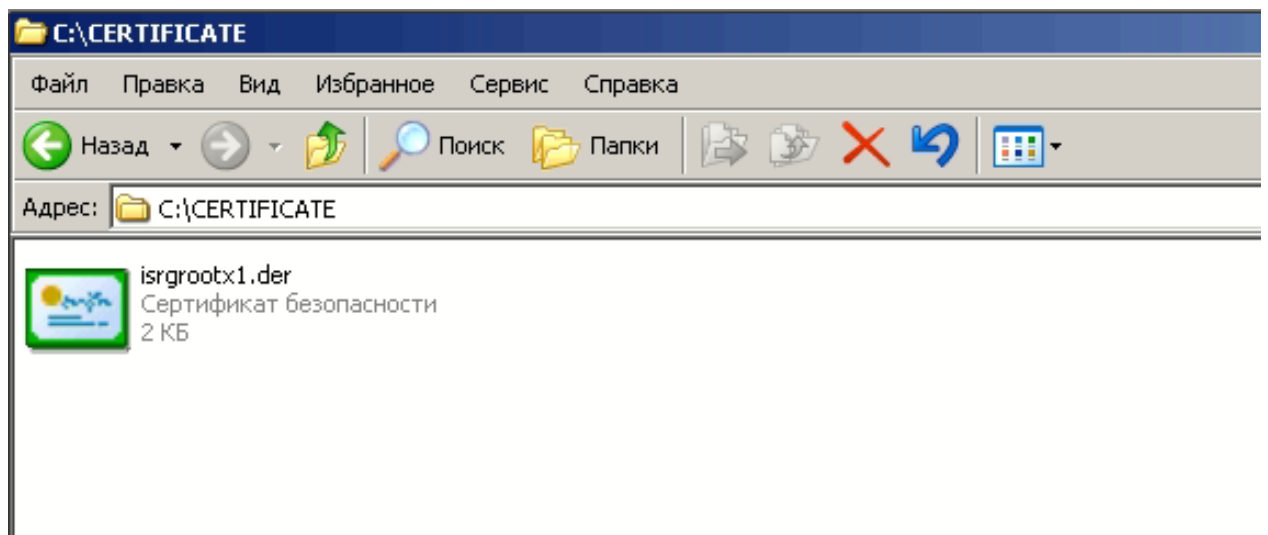
[Додати виняток...](#) Натиснути кнопку "Додати виняток"

У наступному вікні встановіть галочку «Зробити цей виняток постійним» та натисніть кнопку «Затвердити виняток безпеки».

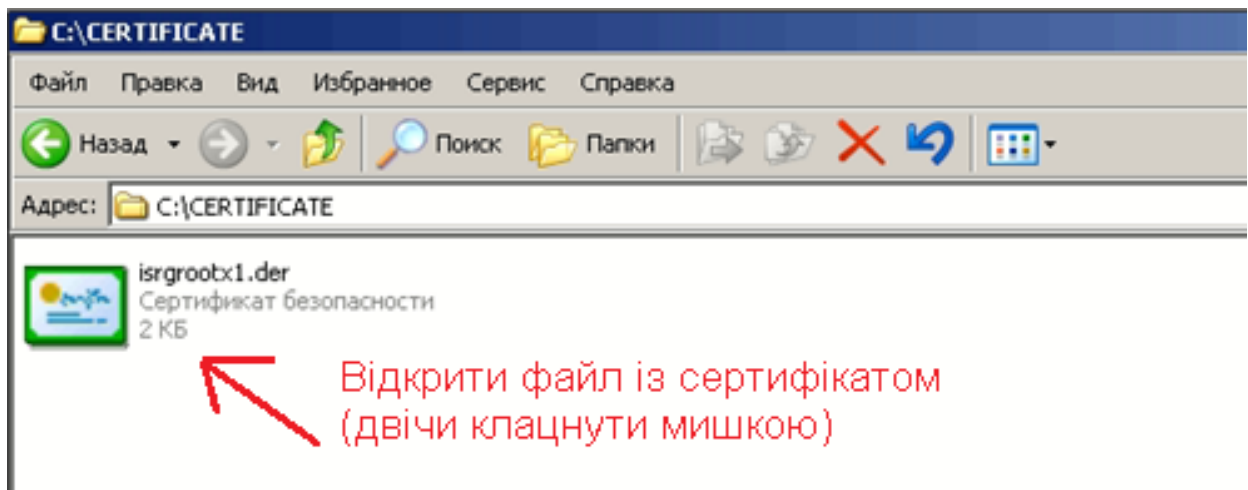


Після цього браузер перейде до сторінки, де можна скачати сертифікат.

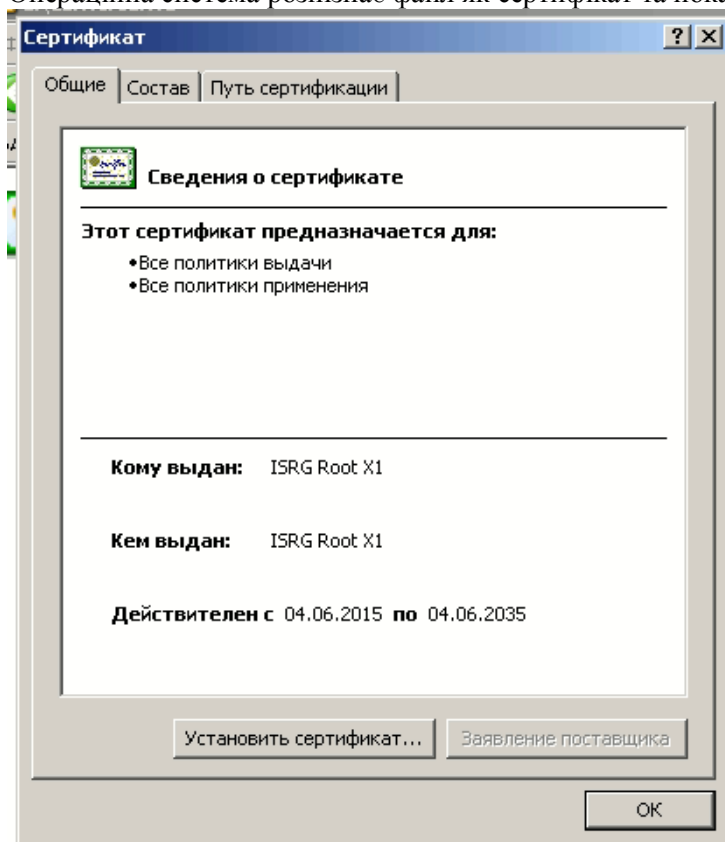
Якщо ви отримали цю інструкції по електронній пошті, то файл сертифікату має бути вкладений у електронний лист, і тоді скачувати його з сайту нема потреби. Збережіть його на жорсткому диску ПК.



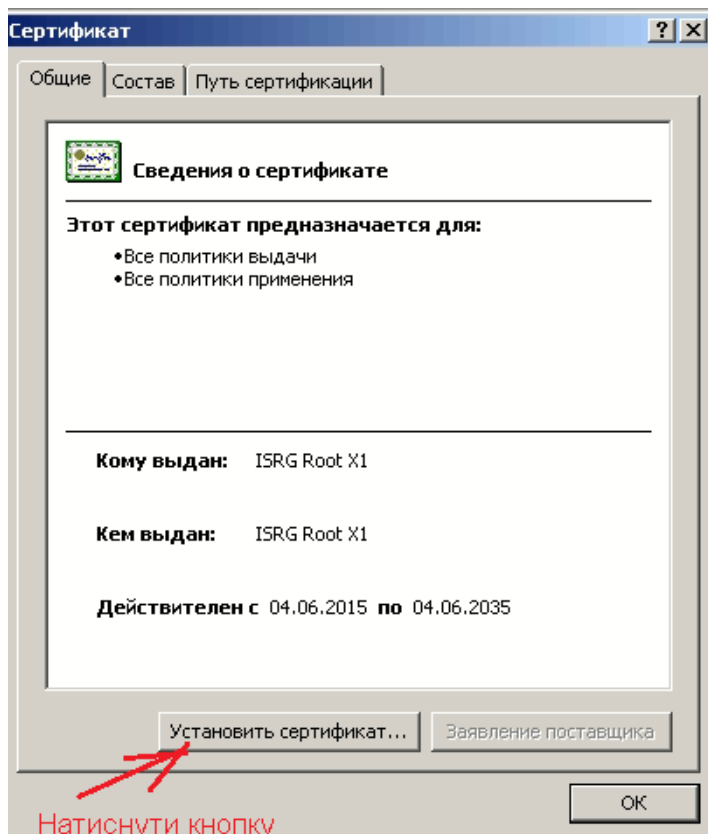
Відкрийте файл подвійним «кліком» мишки на ньому.



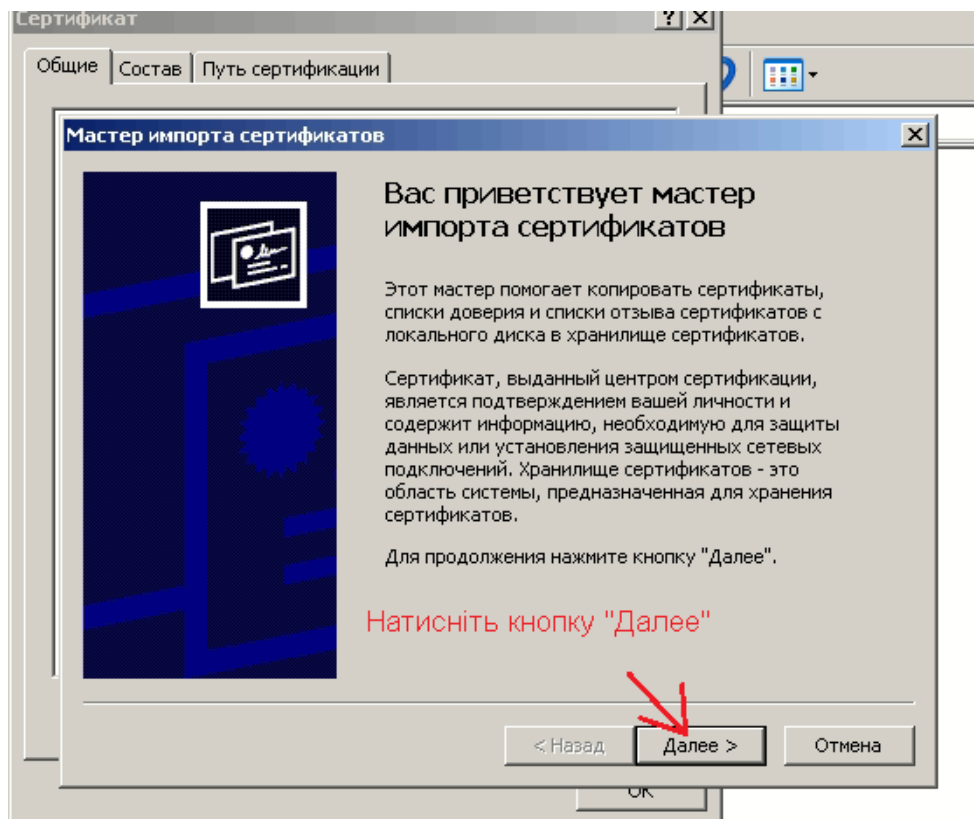
Операційна система розпізнає файл як сертифікат та покаже його властивості



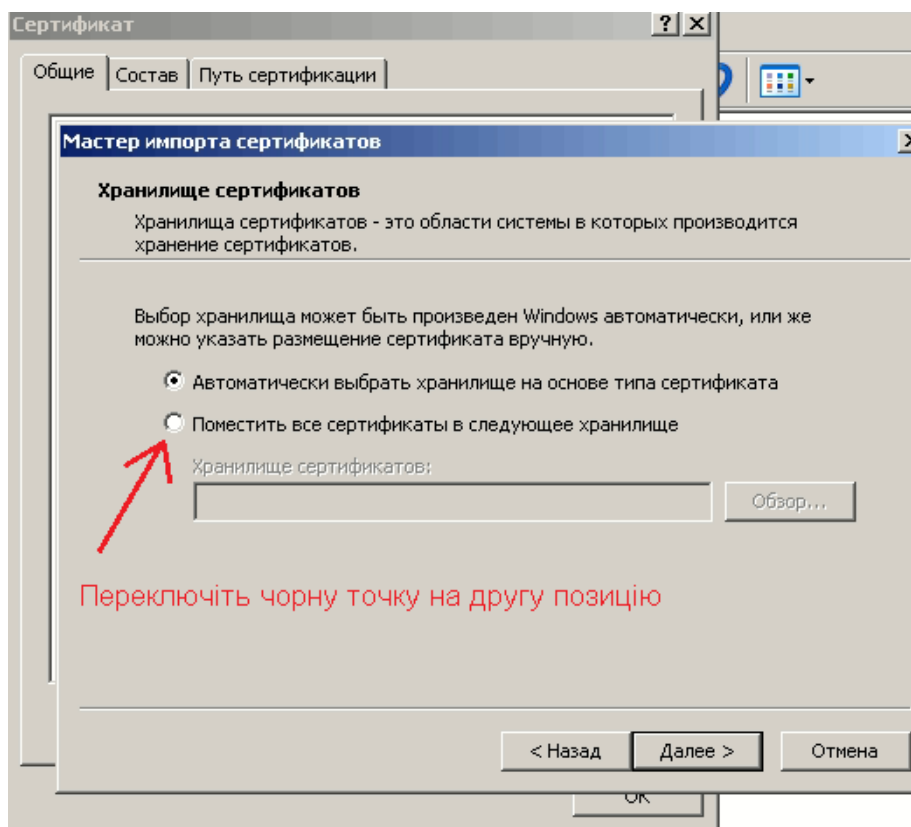
Тепер почніть встановлення сертифікату. Натисніть кнопку «Установить сертификат»



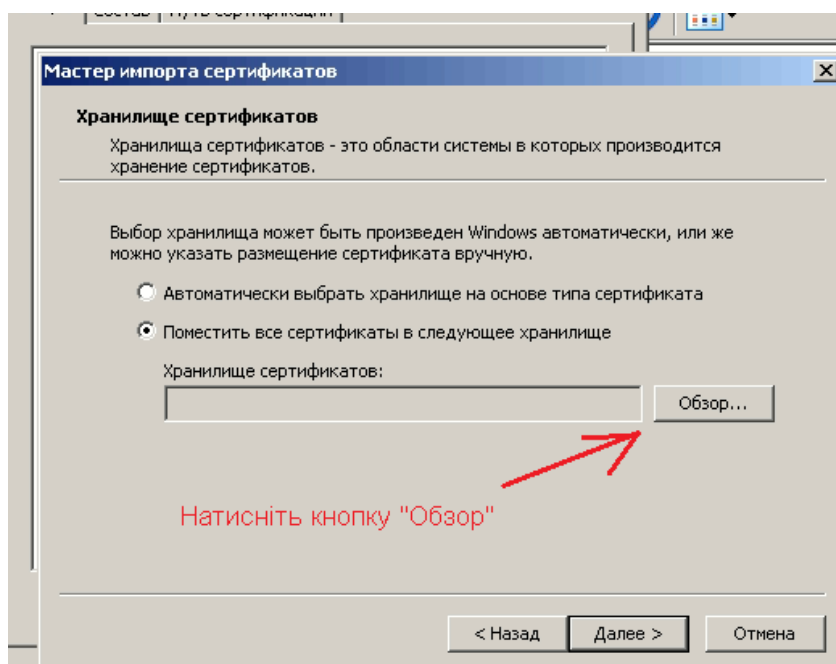
Запуститься «Мастер импорта сертификатов». Натисніть кнопку «Далее»



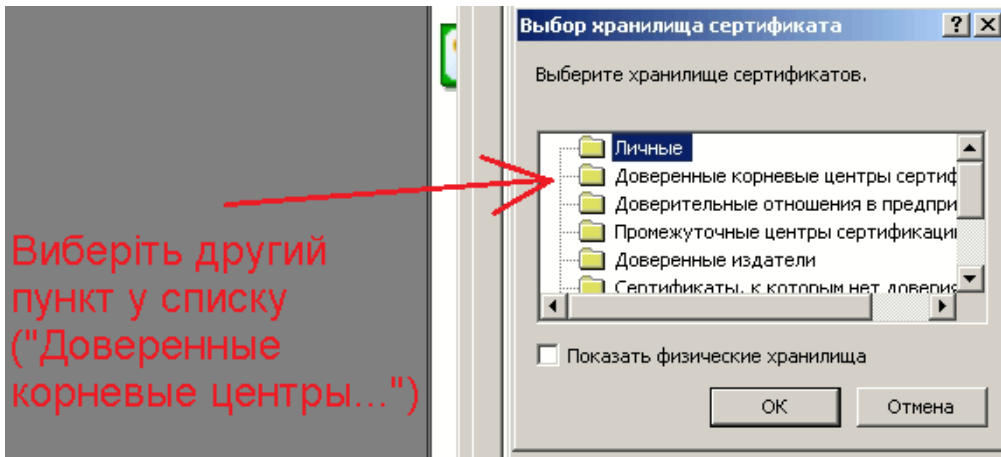
Вкажіть правильне місце для зберігання сертифікату



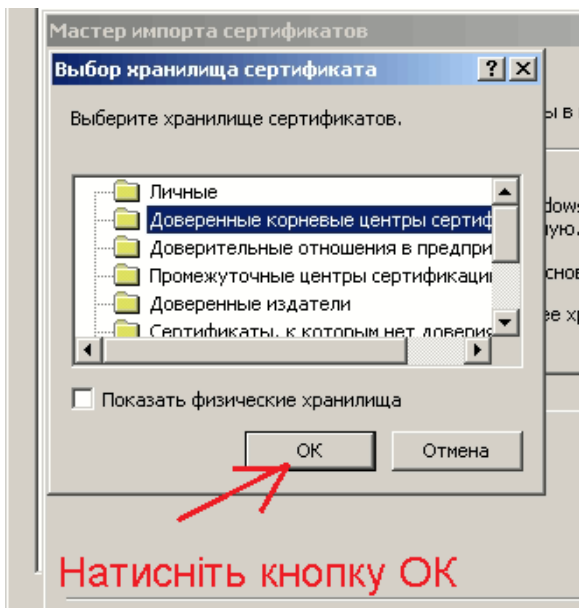
Натисніть кнопку «Обзор», щоби вибрати правильне місце для зберігання сертифіката.



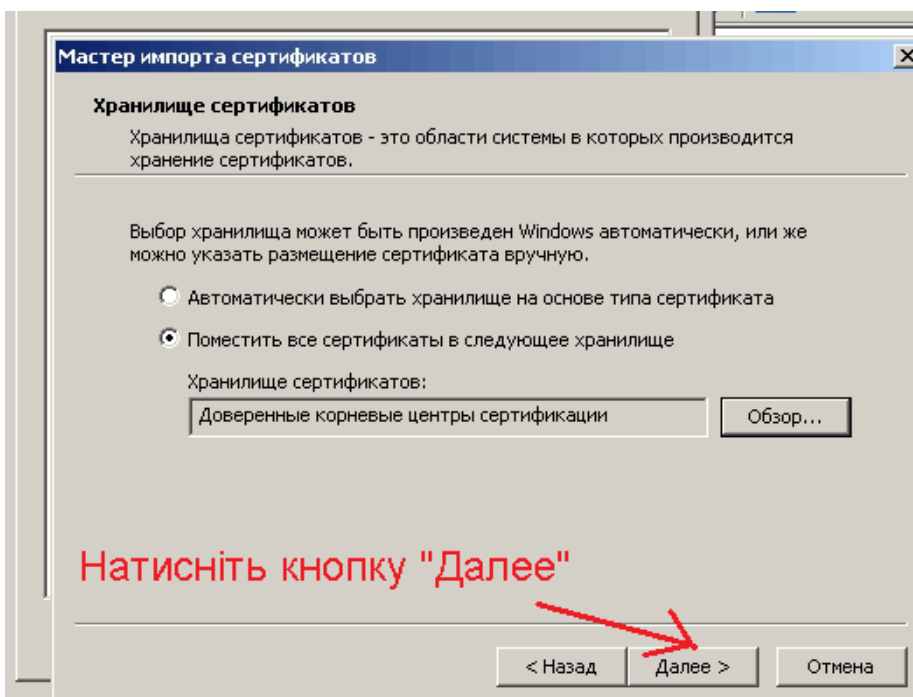
Оскільки сертифікат є корневим, то вкажіть папку «доверенные корневые центры сертификации»



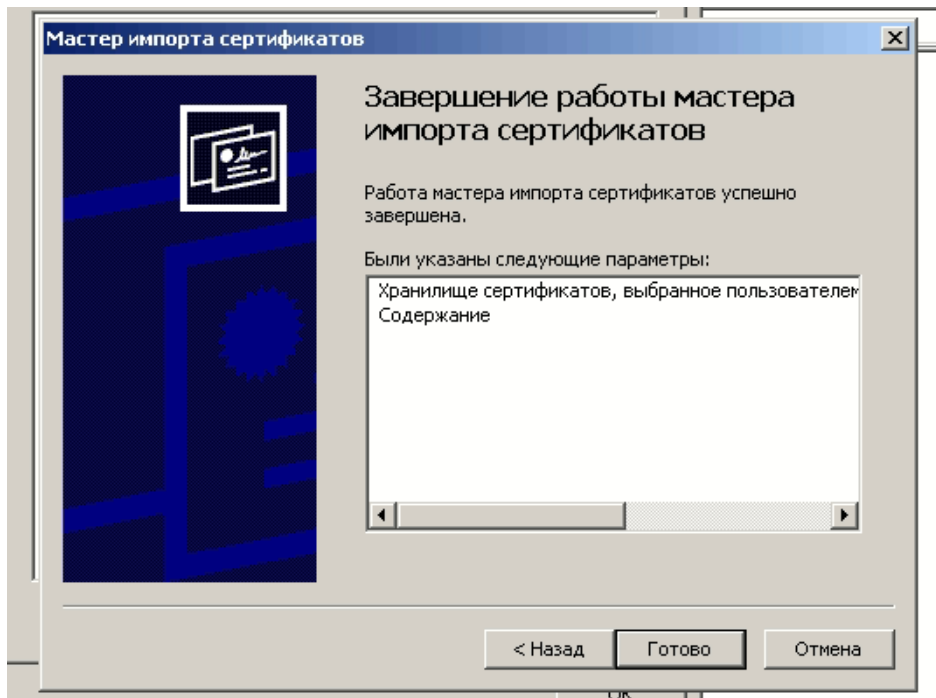
Натисніть кнопку ОК



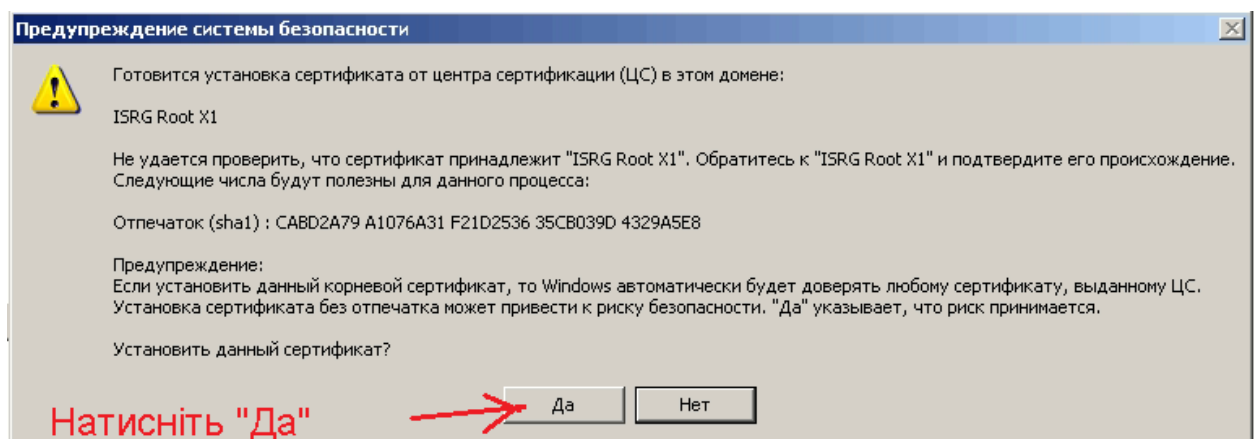
Подивіться, чи вибрали ви правильне місце зберігання сертифікату та натисніть «Далее»



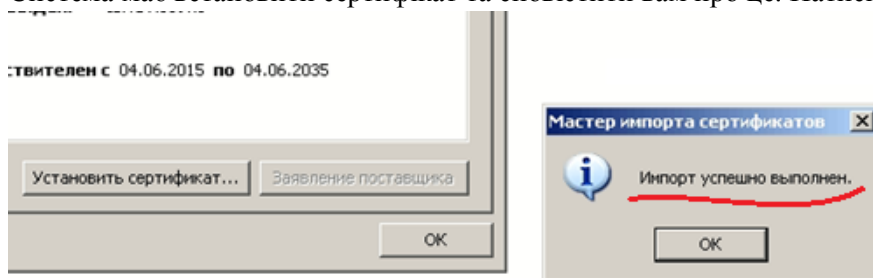
Потім натисніть «Готово»



Якщо система видає таке попередження, натисніть кнопку «Да»

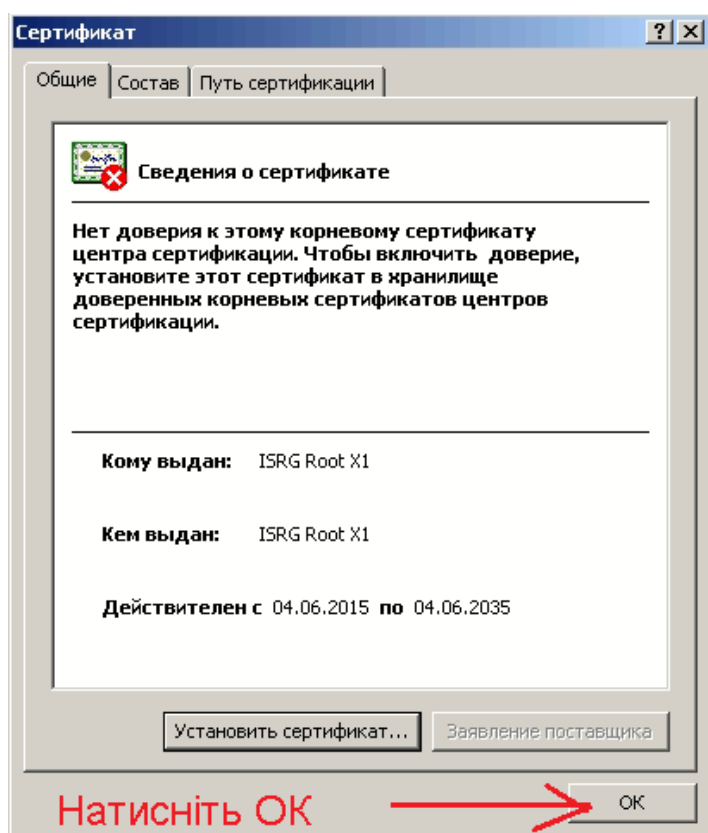


Система має встановити сертифікат та сповістити вам про це. Натисніть «ОК»



Натисніть "ОК"

Натисніть «ОК» щоб закрити вікно сертифікату

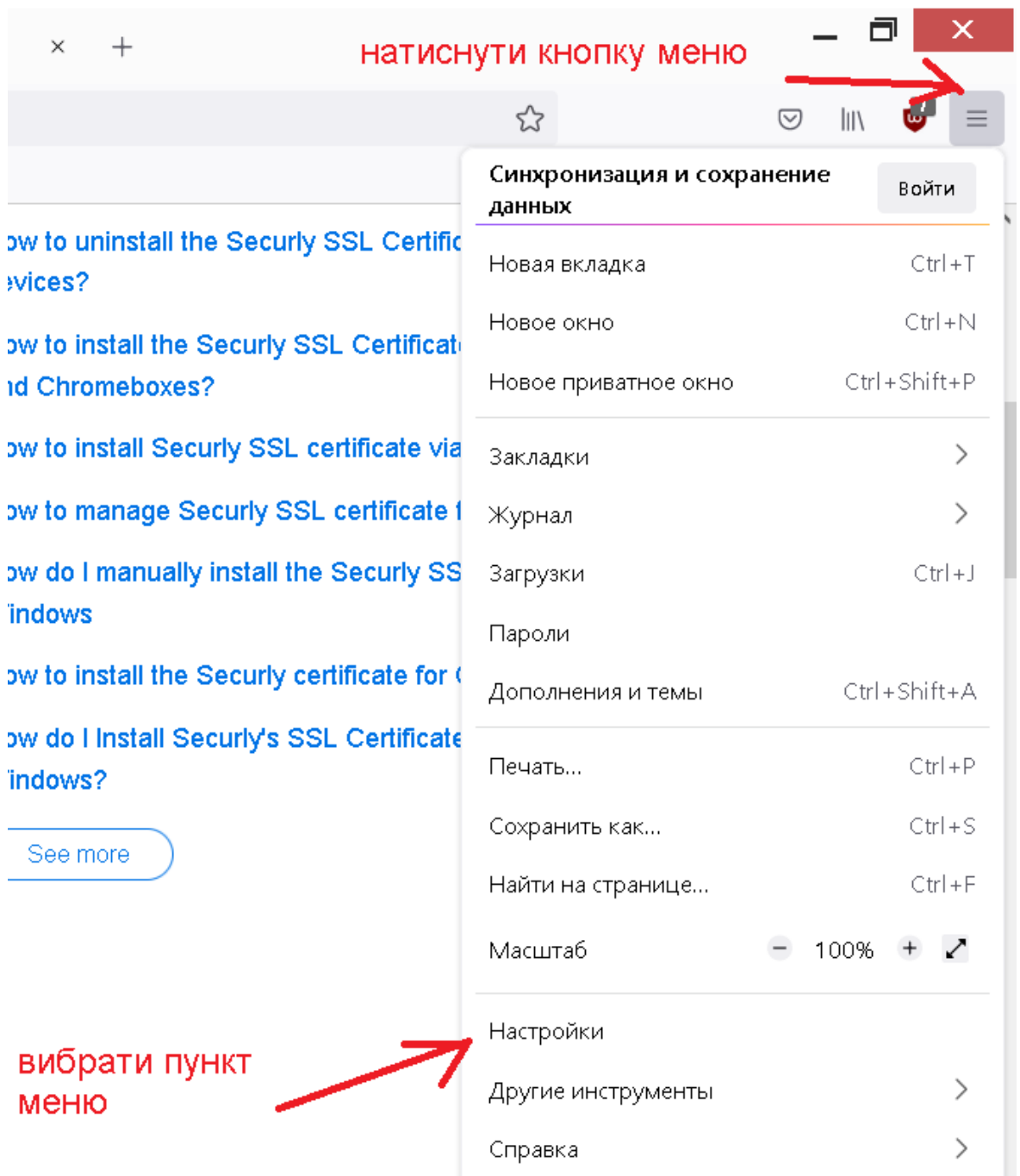


Зауваження щодо браузера Mozilla Firefox

Mozilla Firefox має власний механізм роботи із сертифікатами, тому може виникнути ситуація, коли встановлений за вказаною вище інструкцією новий кореневий сертифікат не спрацює у Mozilla Firefox.

Що робити з Firefox

Запустіть браузер Mozilla Firefox та перейдіть у налаштування. Для цього натисніть кнопку входу у меню та виберіть пункт «Настройки» («Налаштування»), «Options»).



Виберіть пункт «Приватность и защита» («Privacy and security») та натисніть кнопку «Просмотр сертификатов»

Основное

Начало

Поиск

Приватность и Защита

Синхронизация

Защита

Поддельное содержимое и защита от вредоносных программ

- Блокировать опасное и обманывающее содержимое [Подробнее](#)
- Блокировать опасные загрузки
- Предупреждать о нежелательных и редко загружаемых программах

Сертификаты

- Запрашивать у OCSP-серверов подтверждение текущего статуса сертификатов

Просмотр сертификатов...

Устройства защиты...

Режим «Только HTTPS»

Виберіть вкладку «Центри сертифікації» та натисніть кнопку «Імпортувати»

Управление сертификатами

Ваши сертификаты Решения по аутентификации Люди Серверы **Центры сертификации**

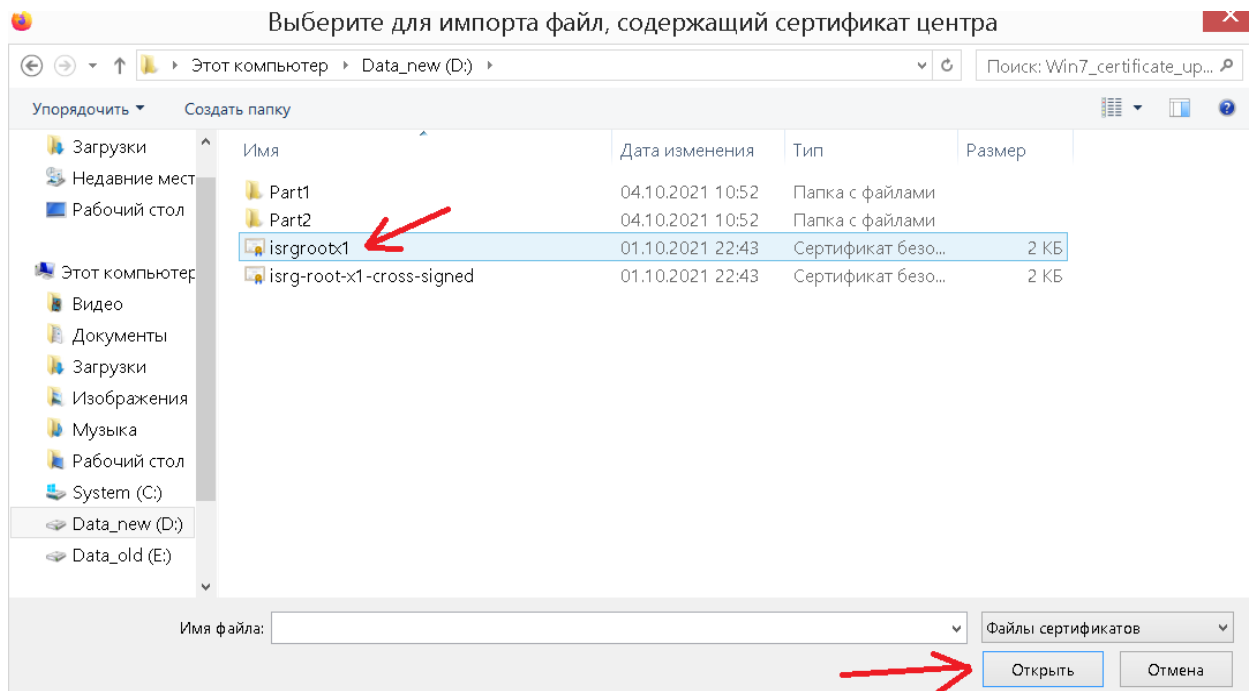
У вас хранятся сертификаты, служащие для идентификации следующих центров сертификации

Имя сертификата	Устройство защиты
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Built-in Object Token
Global Chambersign Root - 2008	Built-in Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Built-in Object Token
Camerfirma Global Chambersign Root	Built-in Object Token

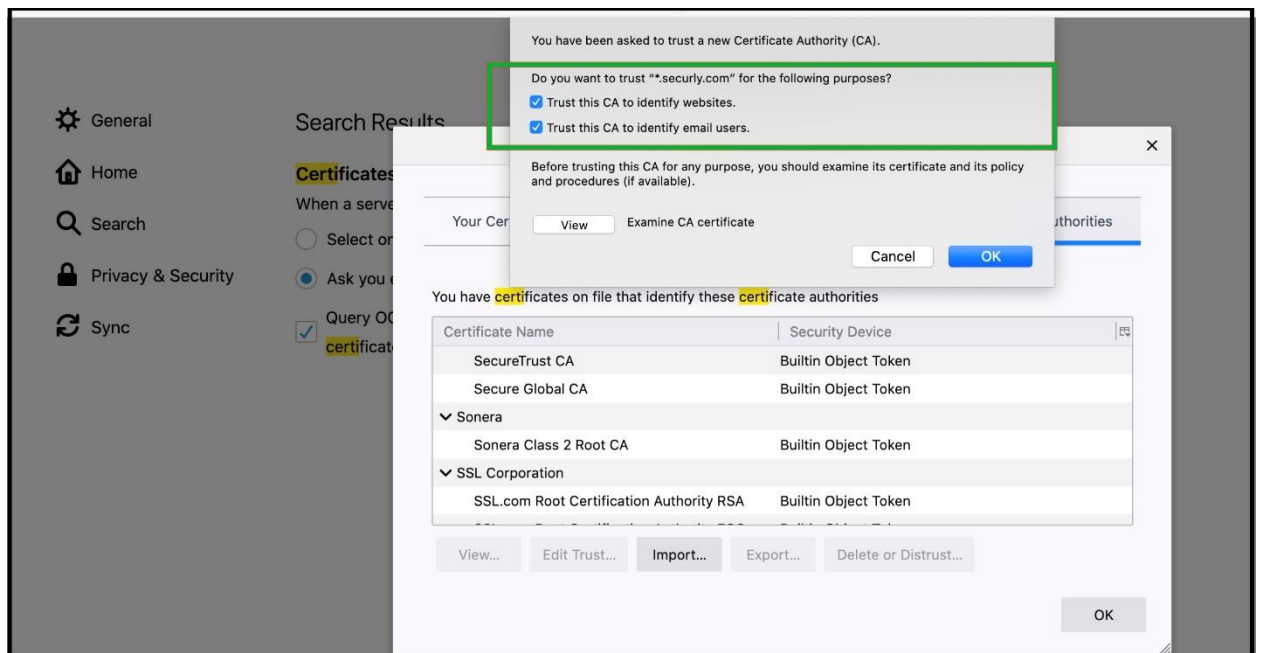
Просмотреть... Изменить доверие... **Импортировать...** Экспортировать... Удалить или не доверять...

ОК

Виберіть файл з сертифікатом



Вирине віконце, де слід поставити всі «галочки» та натиснути «ОК»



Програма має сповістити про успішне встановлення сертифікату.

Натисніть «ОК» у попередньому віконці та вийдіть з налаштувань Firefox.