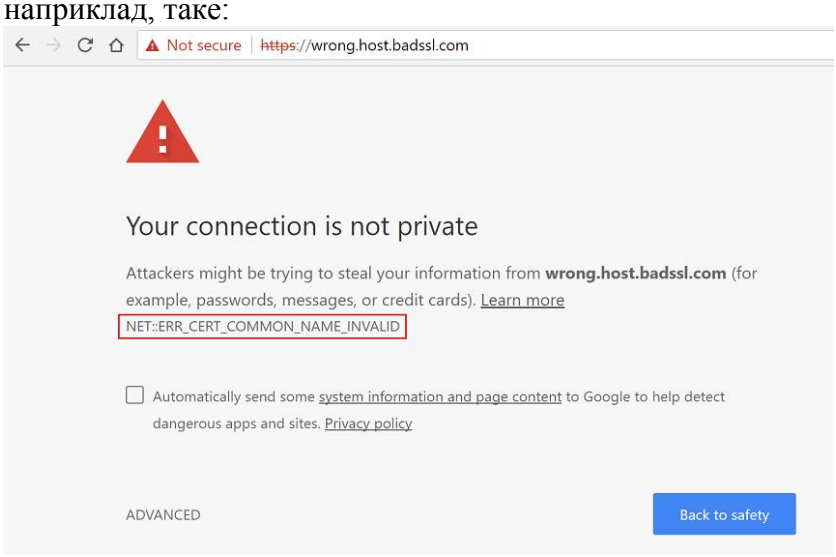
Інструкція щодо оновлення електронного кореневого сертифікату безпеки для сайтів

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 унеможливлює втручання злодіїв у передачу даних та подальшу компрометацію чи «крадіжку» інформації, зокрема, паролів, особистої інформації, тощо.

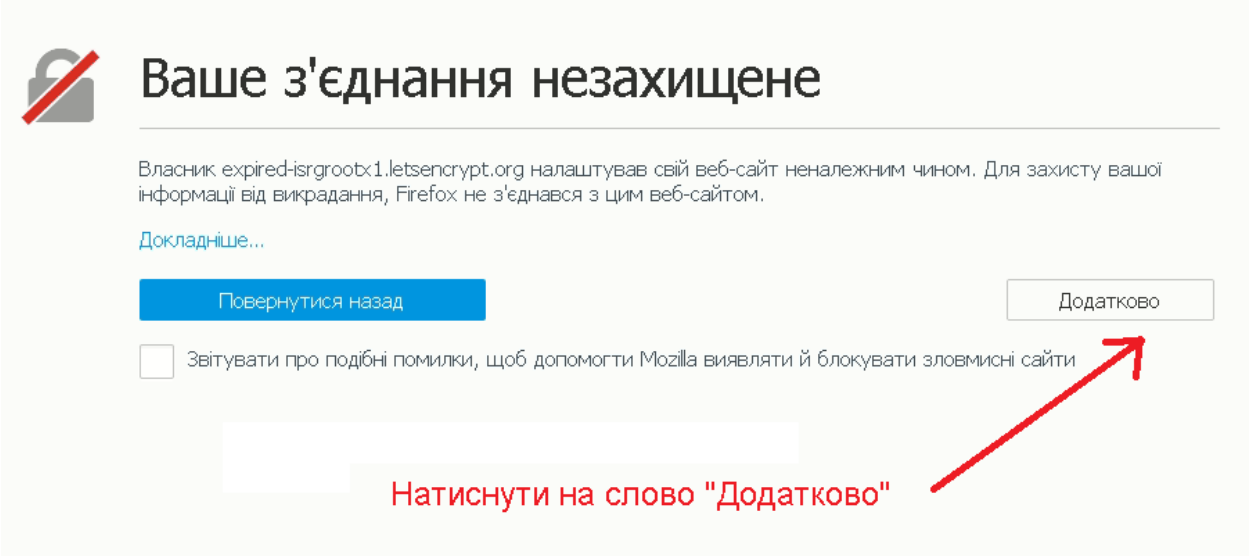
Кожен сертифікат, включаючи кореневі, має свій термін придатності. Тож, нещодавно сплив термін придатності кореневого сертифікату організації з сертифікації Let’s Encrypt, який використовувався багатьма сайтами, включаючи сайти ХНАДУ, оскільки послуги Let’s Encrypt є безкоштовними (з певними обмеженнями). 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 кореневих сертифікатів у системі немає, браузер не може засвідчити достовірність даних з сайту, і сайт не відкривається.

Що робити?

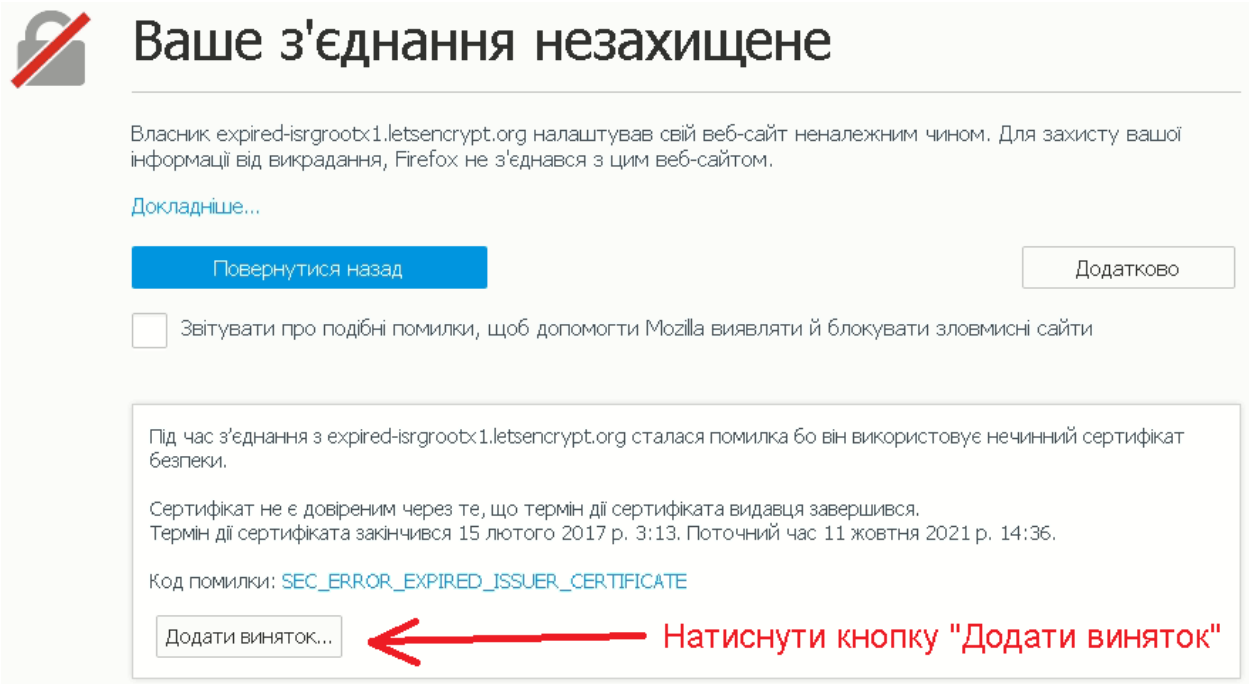
Треба оновити сертифікат вручну.
Спочатку візьміть ПК, що має підключення до Інтернет та встановлені відповідні оновлення операційної системи або хоча б сертифікатів. Перейдіть за посиланням та скачайте файл сертифікату.

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

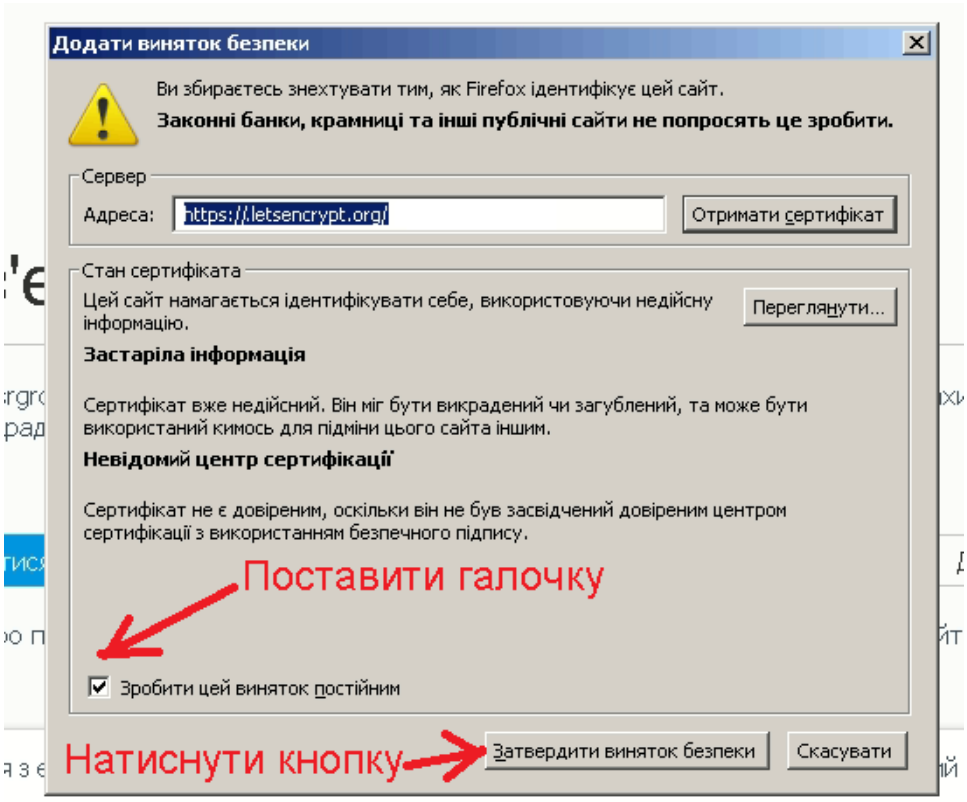
Можна також спробувати скачати новий сертифікат безпосередньо на тому комп'ютері, де виникла проблема із сертифікатом. Після переходу за посиланням при отриманні попередження натисніть кнопку «Додатково» у вікні браузера.



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

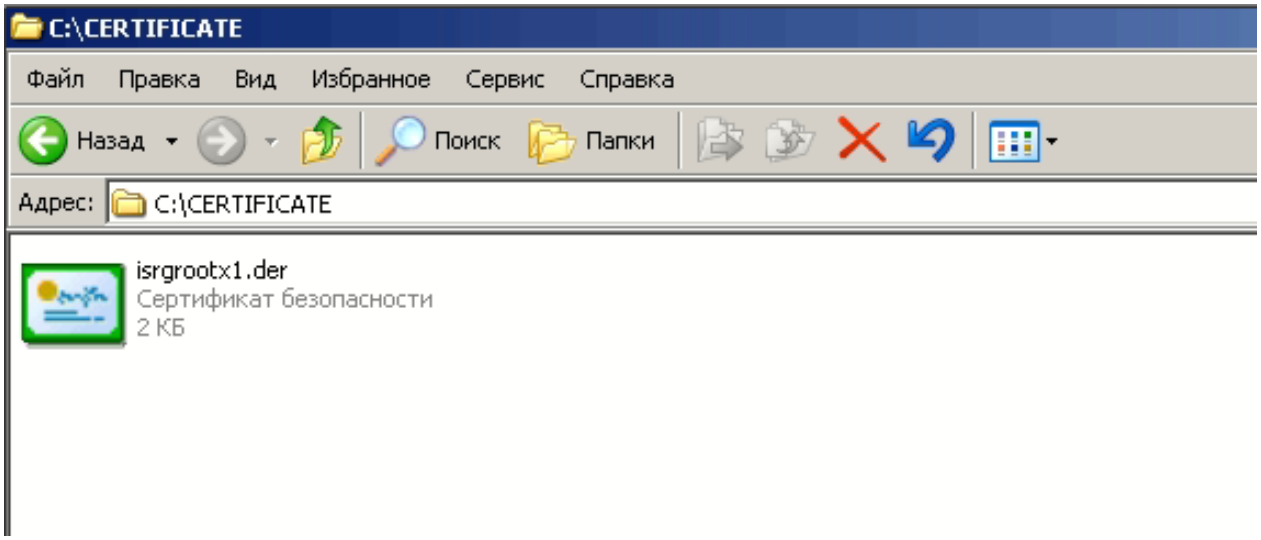


У наступному вікні встановіть галочку «Зробити цей виняток постійним» та натисніть кнопку «Затвердити виняток безпеки».

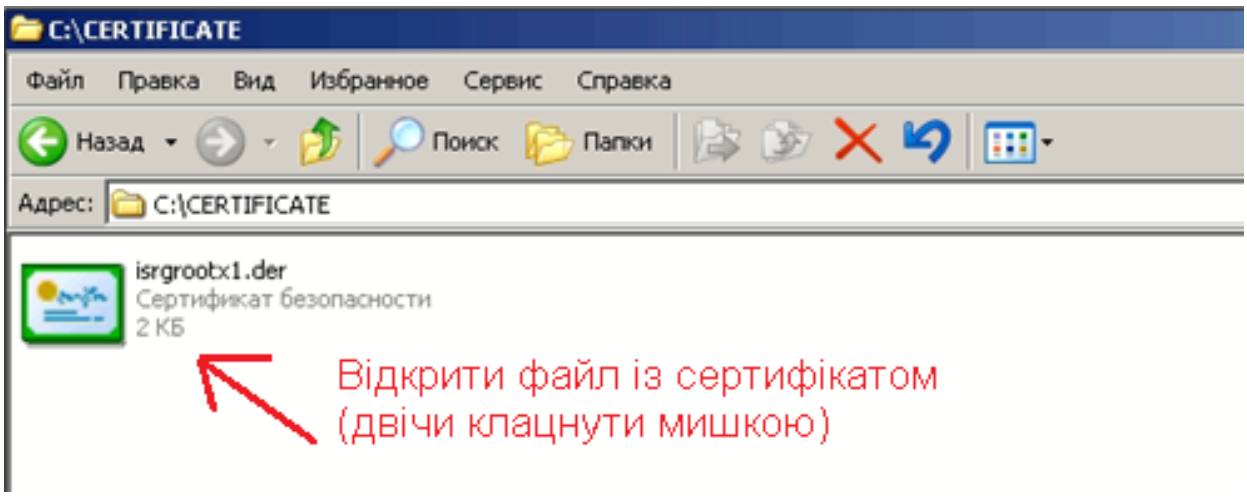


Після цього браузер перейде до сторінки, де можна скачати сертифікат.

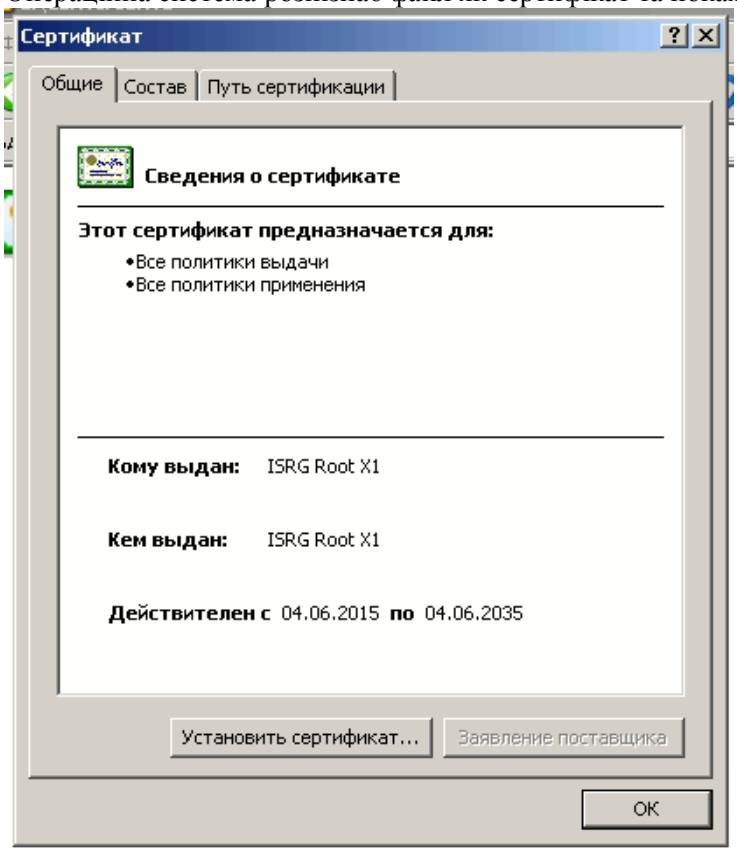
Якщо ви отримали цю інструкції по електронній пошті, то файл сертифікату має бути вкладений у електронний лист, і тоді скачувати його з сайту нема потреби.
Збережіть його на жорсткому диску ПК.



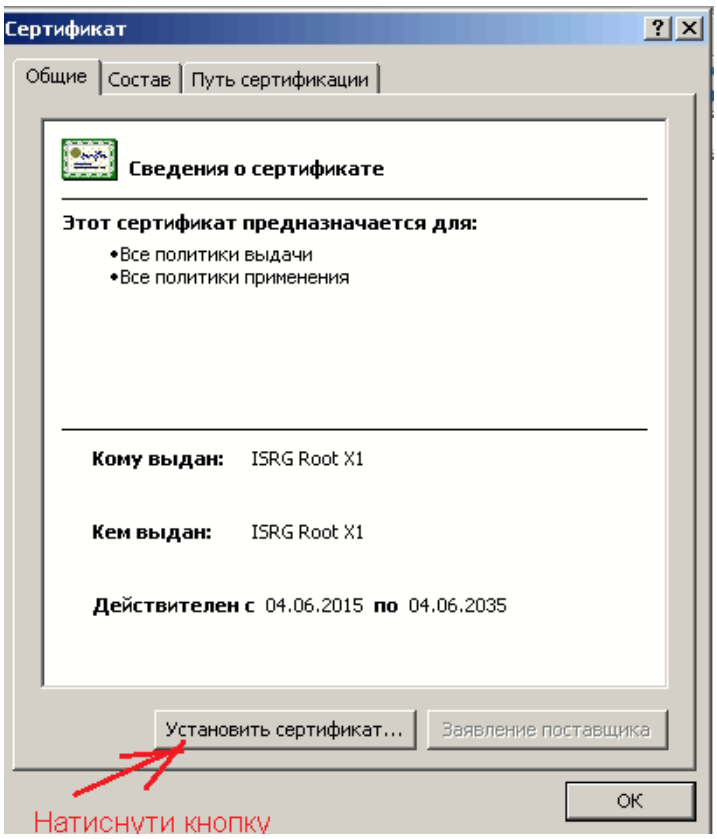
Відкрийте файл подвійним «кліком» мишки на ньому.



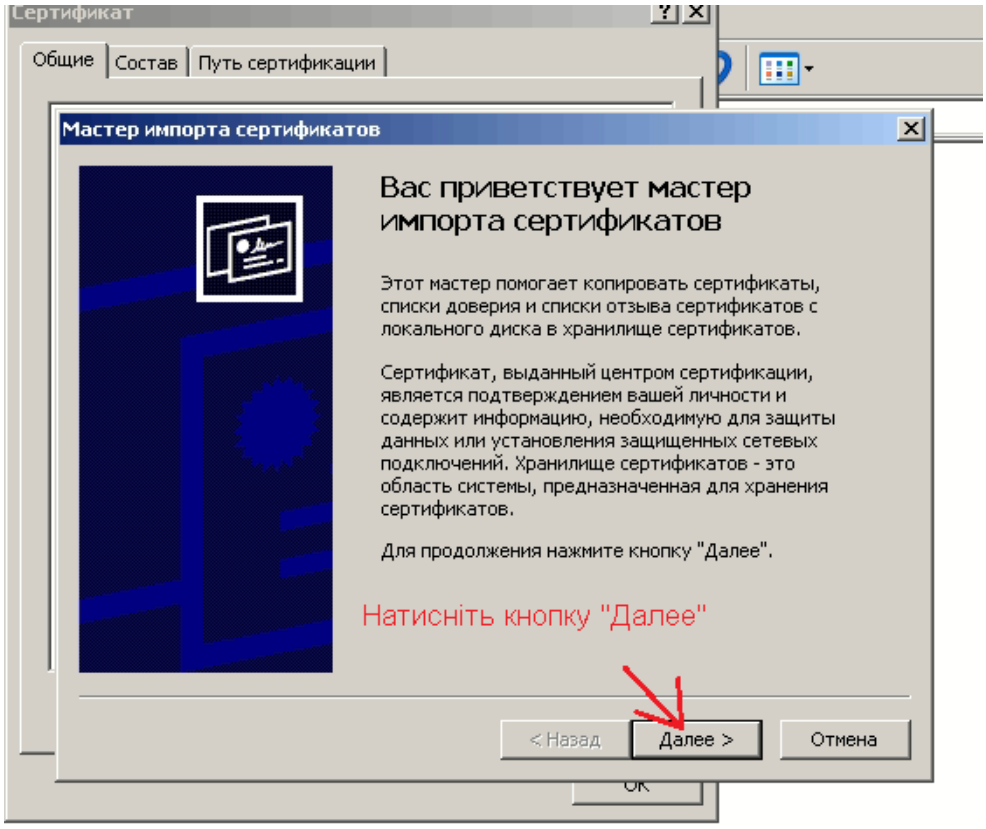
Операційна система розпізнає файл як сертифікат та покаже його властивості



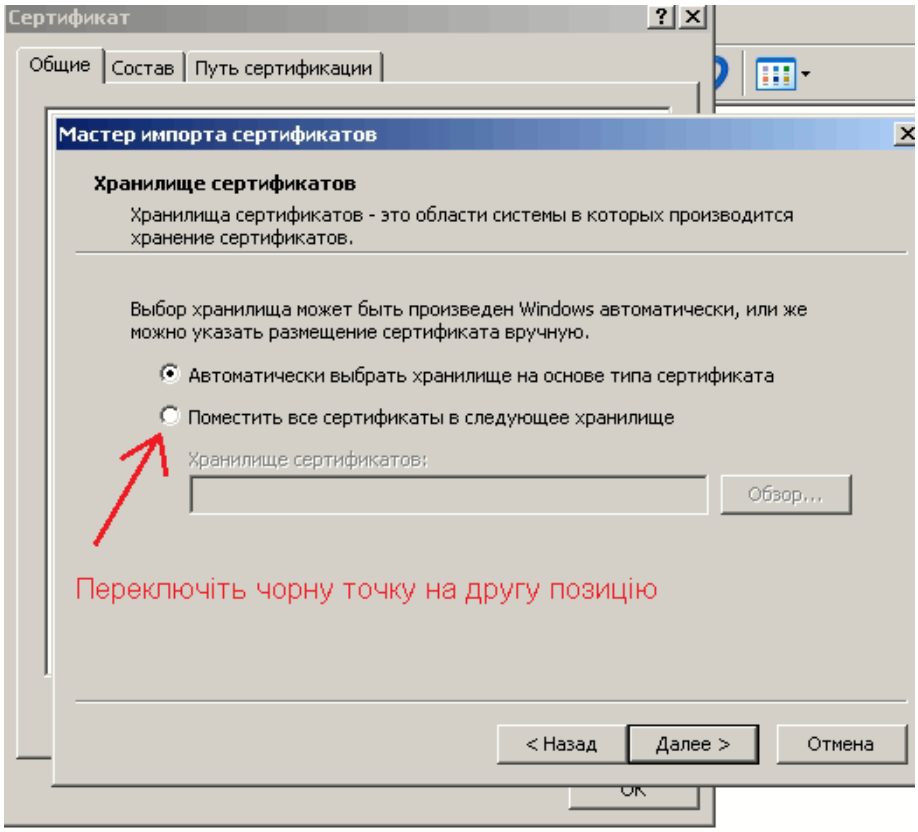
Тепер почніть встановлення сертифікату. Натисніть кнопку «Установить сертификат»



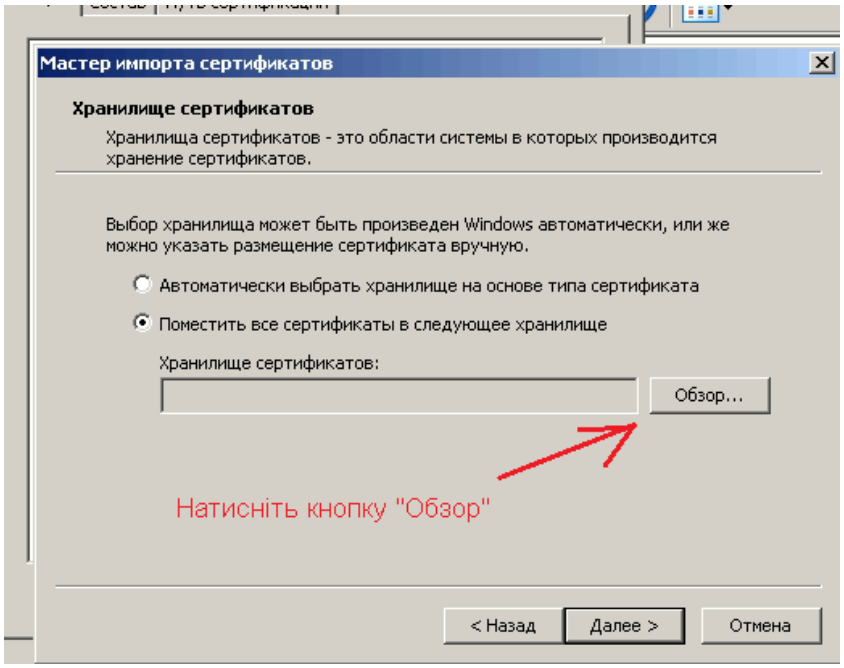
Запуститься «Мастер импорта сертификатов». Натисніть кнопку «Далее»



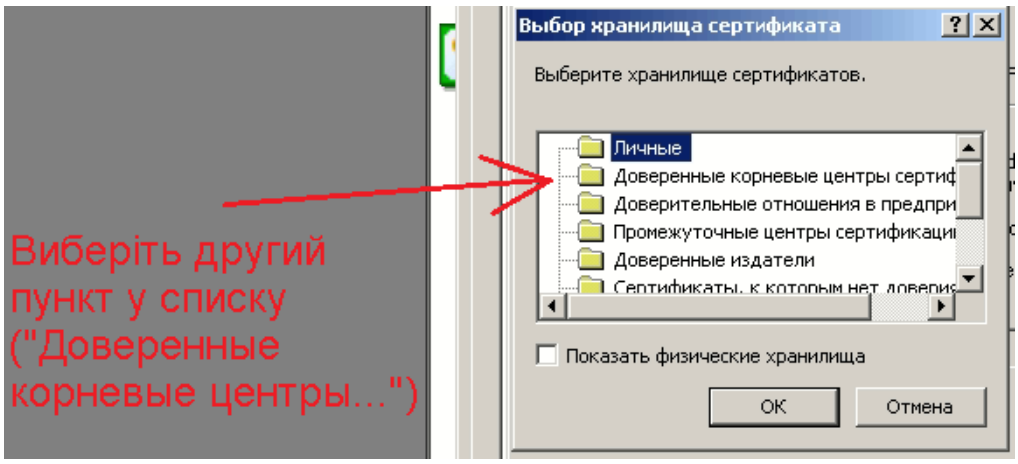
Вкажіть правильне місце для зберігання сертифікату



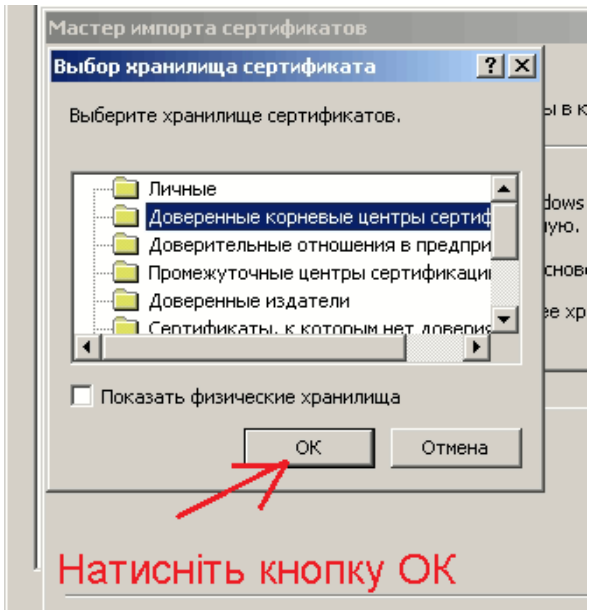
Натисніть кнопку «Обзор», щоби вибрати правильне місце для зберігання сертифіката.



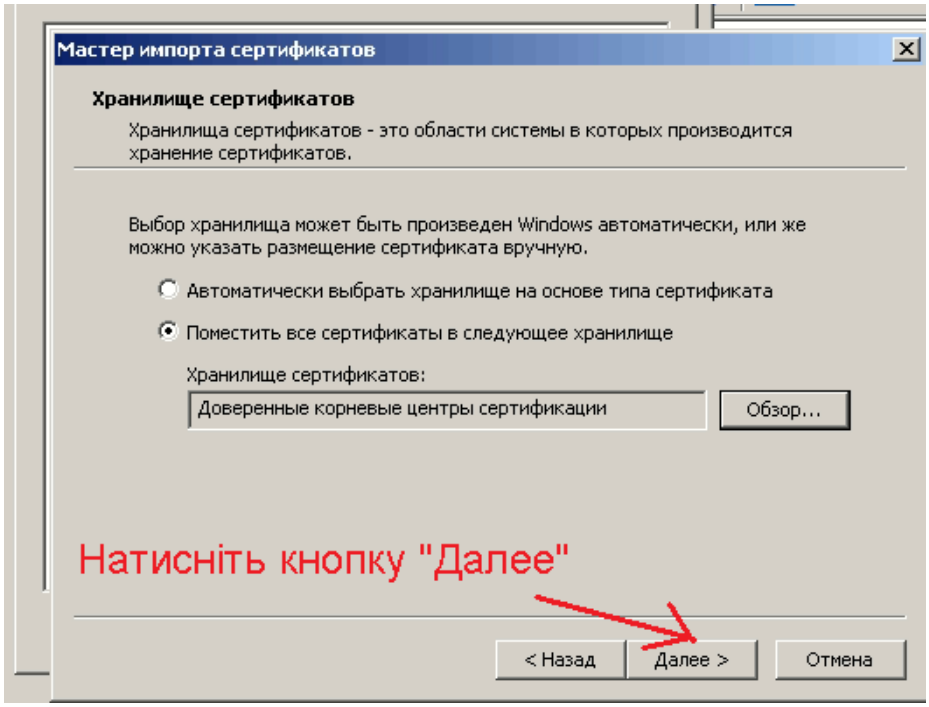
Оскільки сертифікат є кореневим, то вкажіть папку «доверенные корневые центры сертификации»



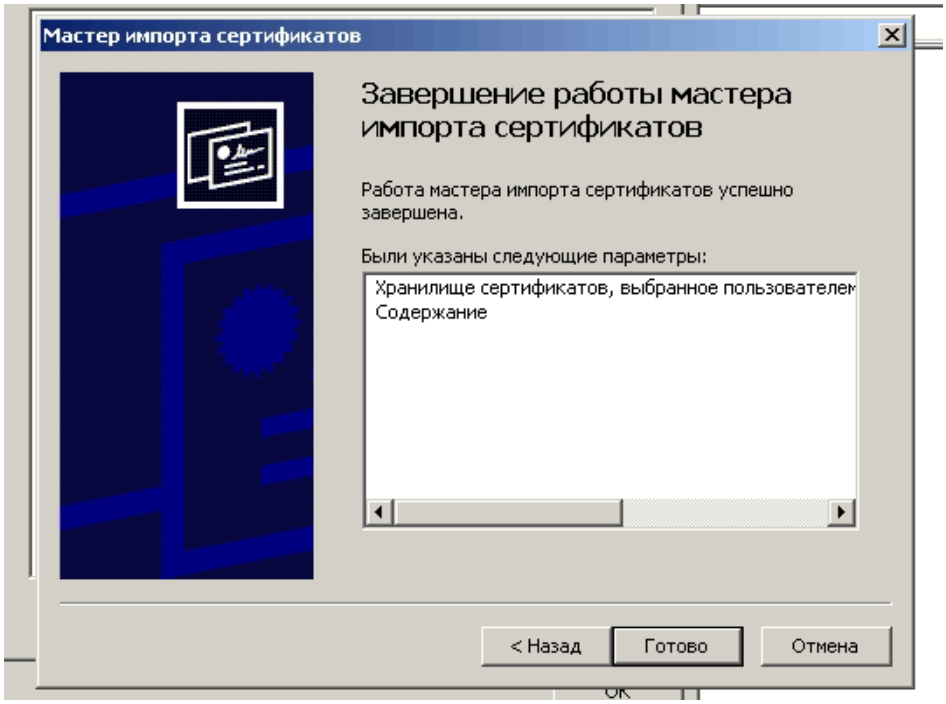
Натисніть кнопку ОК



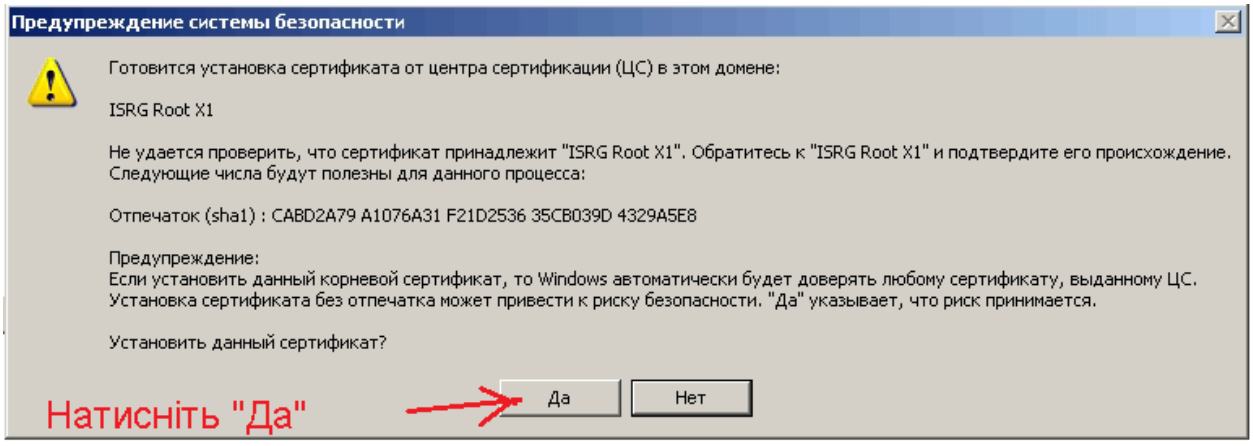
Подивіться, чи вибрали ви правильне місце зберігання сертифікату та натисніть «Далее»



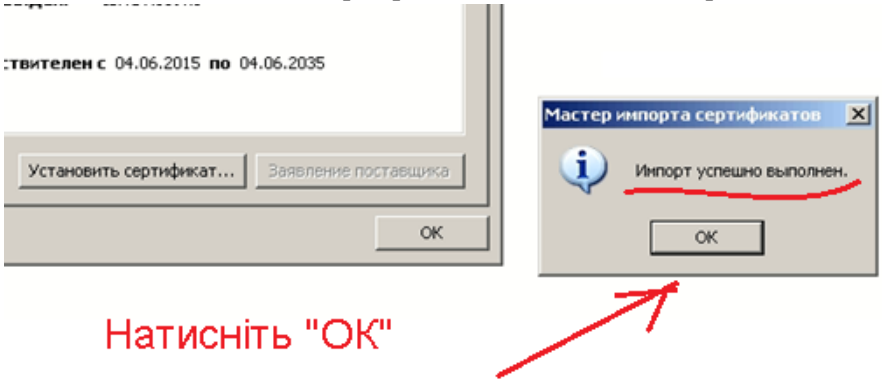
Потім натисніть «Готово»



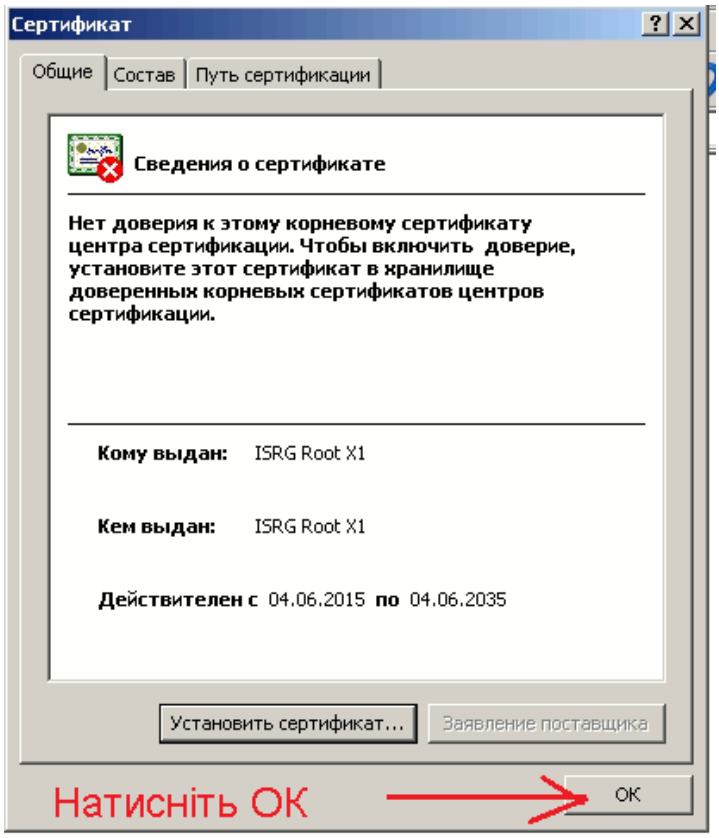
Якщо система видає таке попередження, натисніть кнопку «Да»



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



Натисніть «ОК щоби закрити вікно сертифікату

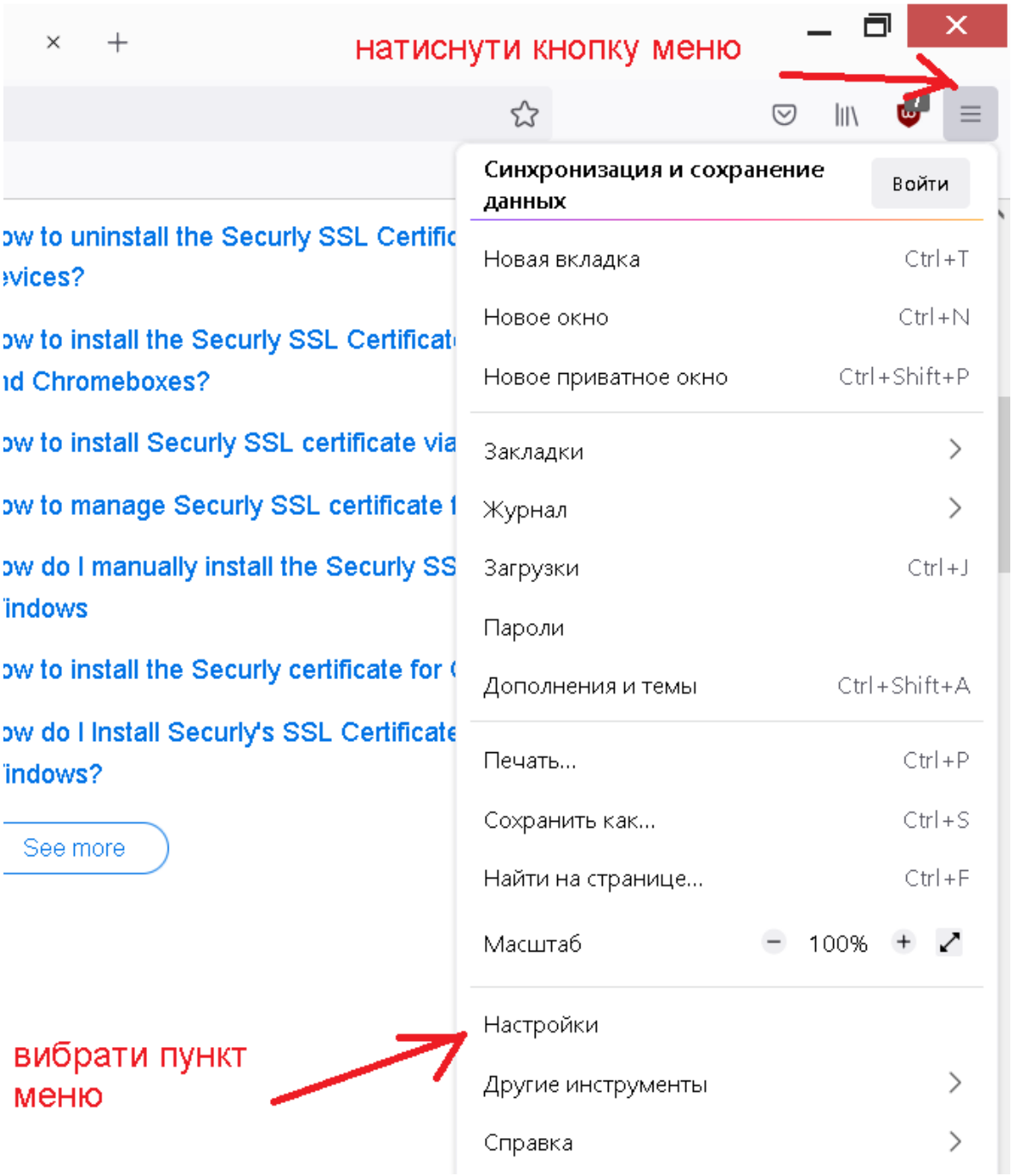


Зауваження щодо браузера Mozilla Firefox

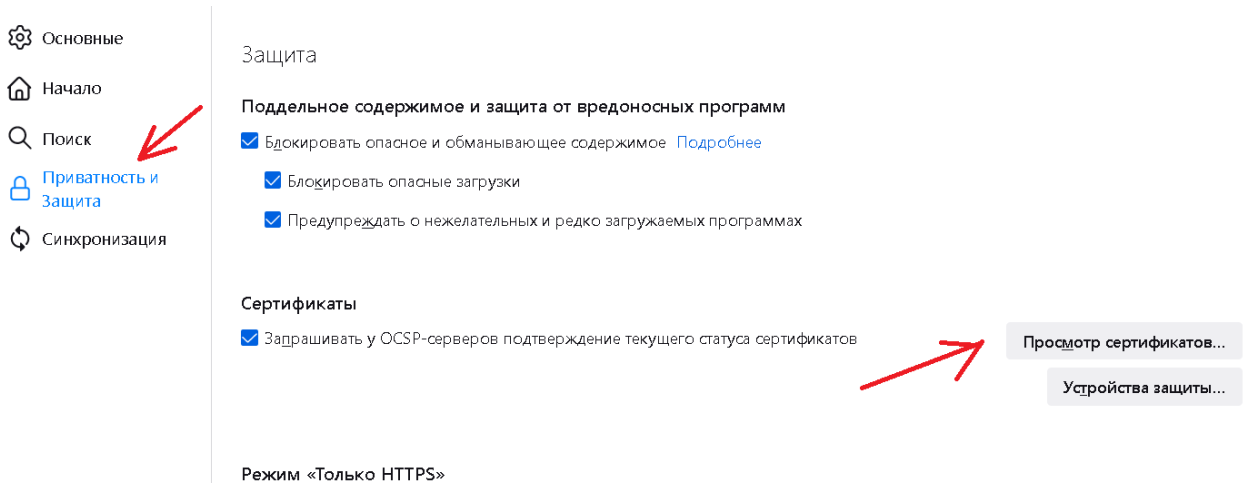
Mozilla Firefox має власний механізм роботи із сертифікатами, тому може виникнути ситуація, коли встановлений за вказаною вище інструкцією новий кореневий сертифікат не спрацьовує у Mozilla Firefox.

Що робити з Firefox

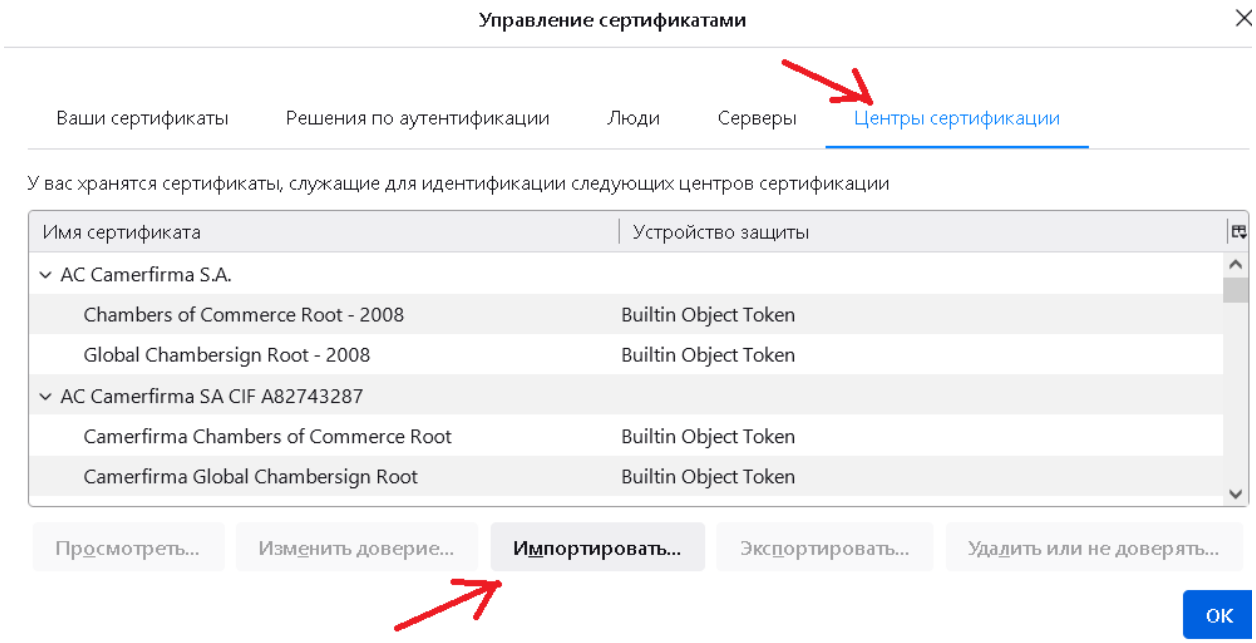
Запустіть браузер Mozilla Firefox та перейдіть у налаштування. Для цього натисніть кнопку входу у меню та виберіть пункт «Настройки» («Налаштування», «Options»).



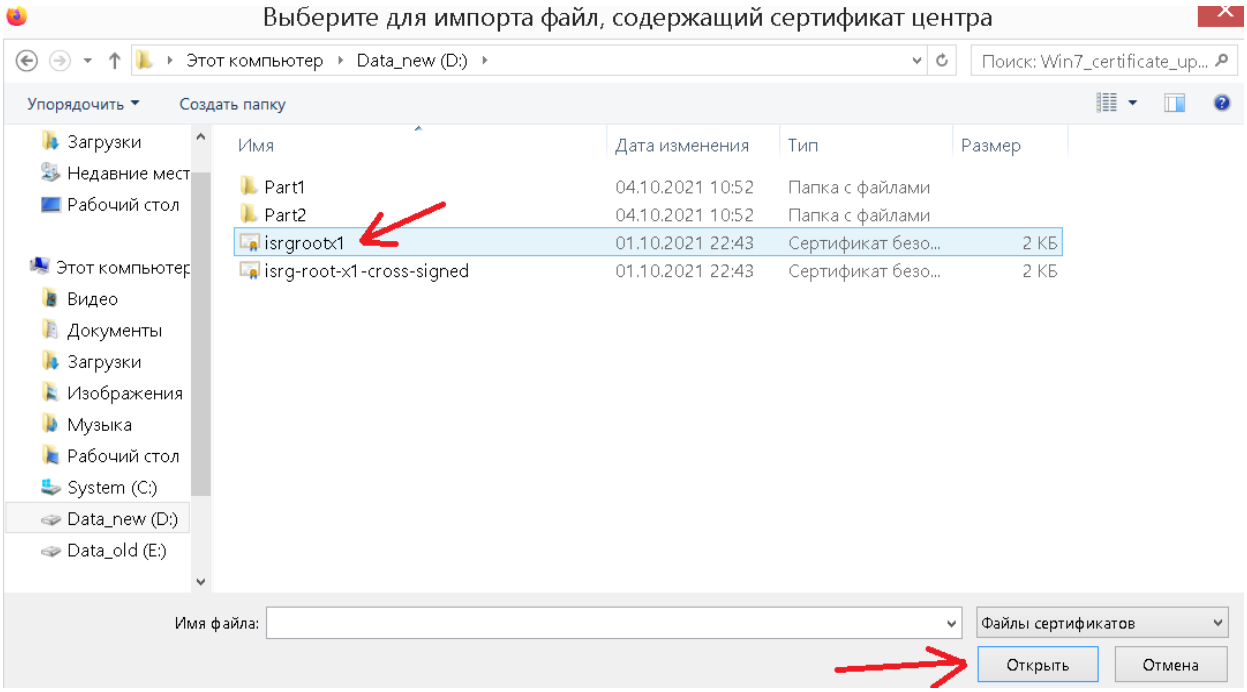
Виберіть пункт «Приватность и защита» («Privacy and security») та натисніть кнопку «Просмотр сертификатов»



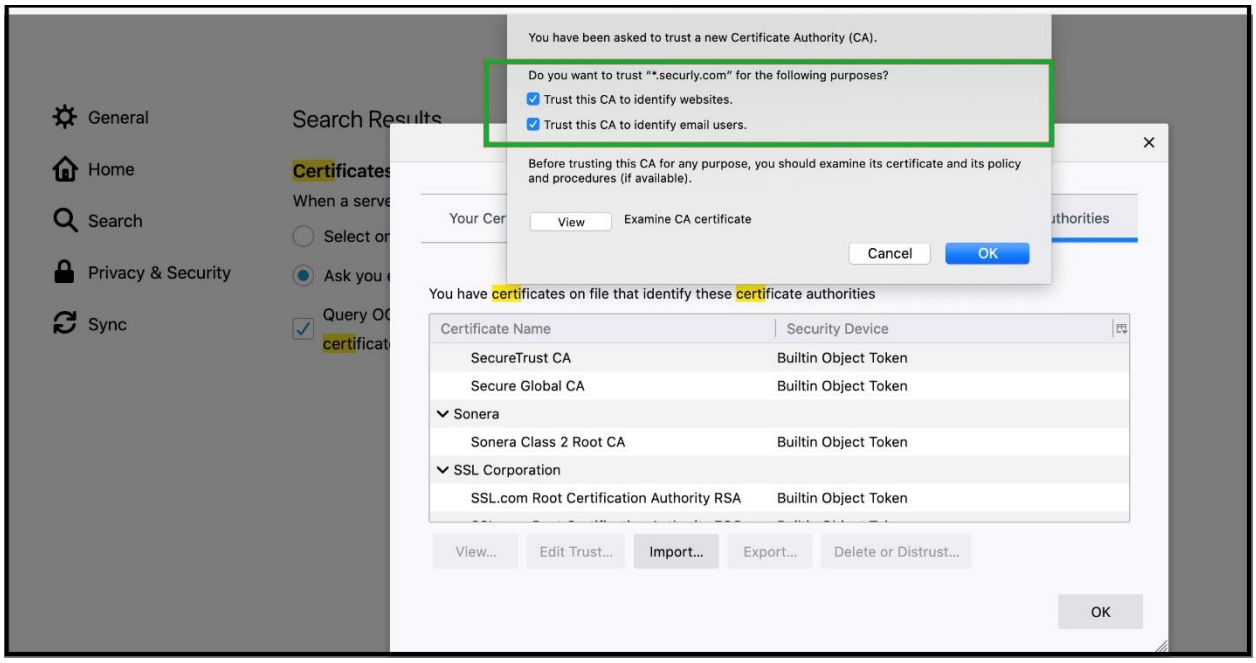
Виберіть вкладку «Центри сертифікації» та натисніть кнопку «Імпортувати»



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.