

## Импорт хранилища ключей в формате PKCS#12, содержащего сертификат открытого ключа и личный ключ, в браузер Internet Explorer (версия 8.0)

Большинство браузеров и почтовых программ придерживается стандарта хранения ключевой пары PKCS#12 (Public-Key Cryptography Standard № 12). Данный стандарт определяет файловый формат, используемый для хранения личного (секретного, закрытого) ключа в сопровождении сертификата открытого ключа. Поскольку в файле PKCS#12 (файле с расширением \*.p12) хранится и сертификат, и личный ключ, с этим файлом необходимо быть столь же осторожными, как и с личным ключом.

1. Пусть, для определённости, личный ключ *JankaKupala\_userkey.pem* и выданный удостоверяющим центром сертификат *JankaKupala\_Certificate.pem* находятся в каталоге *ключи*, который доступен по следующему пути *D:\OpenSSL\openssl\bin\ключи*. Чтобы создать хранилище ключей в формате PKCS#12 выполните команду криптографического пакета программ OpenSSL:

```
openssl pkcs12 -export -in D:\OpenSSL\openssl\bin\ключи\JankaKupala_Certificate.pem  
-inkey D:\OpenSSL\openssl\bin\ключи\JankaKupala_userkey.pem -descert -out  
D:\OpenSSL\openssl\bin\ключи\JankaKupala_Keystore.p12
```

При выполнении команды Вам необходимо ввести пароль к Вашему личному ключу *JankaKupala\_userkey.pem*. Затем требуется создать (ввести и подтвердить) пароль к Вашему хранилищу ключей *JankaKupala\_Keystore.p12*. Требования к сложности пароля такие же, как и к паролю для активации личного ключа (рисунок 1).

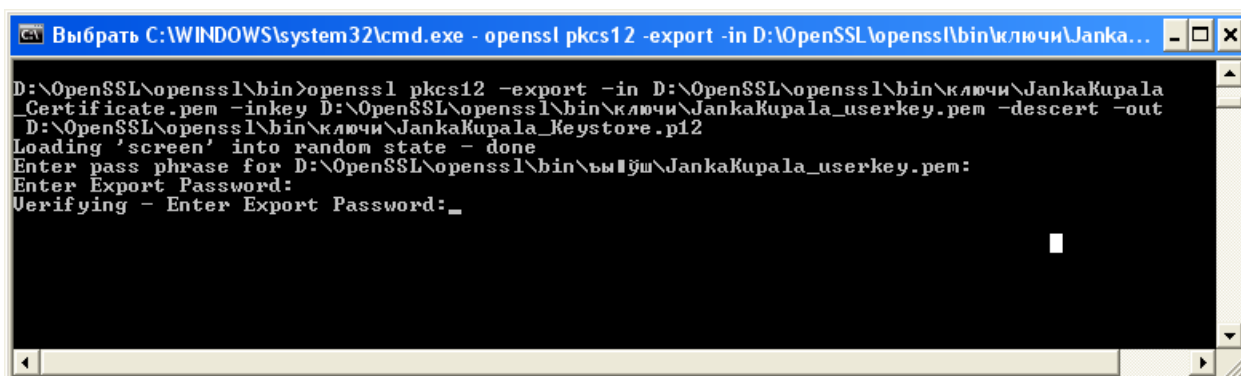


Рисунок 1 – Выполнение команды создания хранилища ключей

Пусть полученное хранилище ключей в формате PKCS#12 *JankaKupala\_Keystore.p12*, также будет находиться в каталоге *ключи*.

2. Сохраните корневой сертификат удостоверяющего центра <http://ca.grid.by/bygca-cacert.der> в каталоге *ключи*.

3. Запустите Internet Explorer.

4. Сначала необходимо импортировать корневой сертификат удостоверяющего центра *bygca-cacert.der* (рисунки 2 – 7).

В меню *Сервис* выберите пункт *Свойства обозревателя*. В появившемся окне выберите вкладку *Содержание*. На вкладке *Содержание* нажмите кнопку *Сертификаты* (рисунок 2).

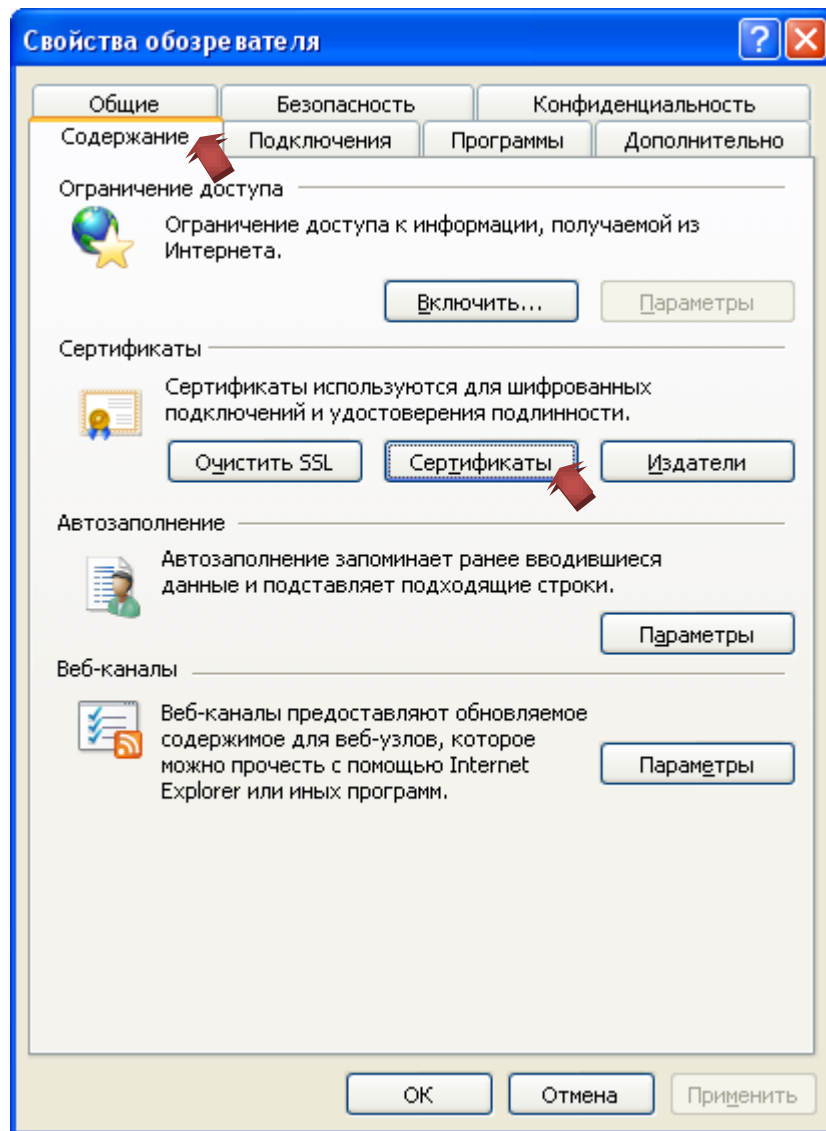


Рисунок 2 – Кнопка *Сертификаты* на вкладке *Содержание* в окне *Свойства обозревателя*

В появившемся окне выберите вкладку *Доверенные корневые центры сертификации* (рисунок 3).

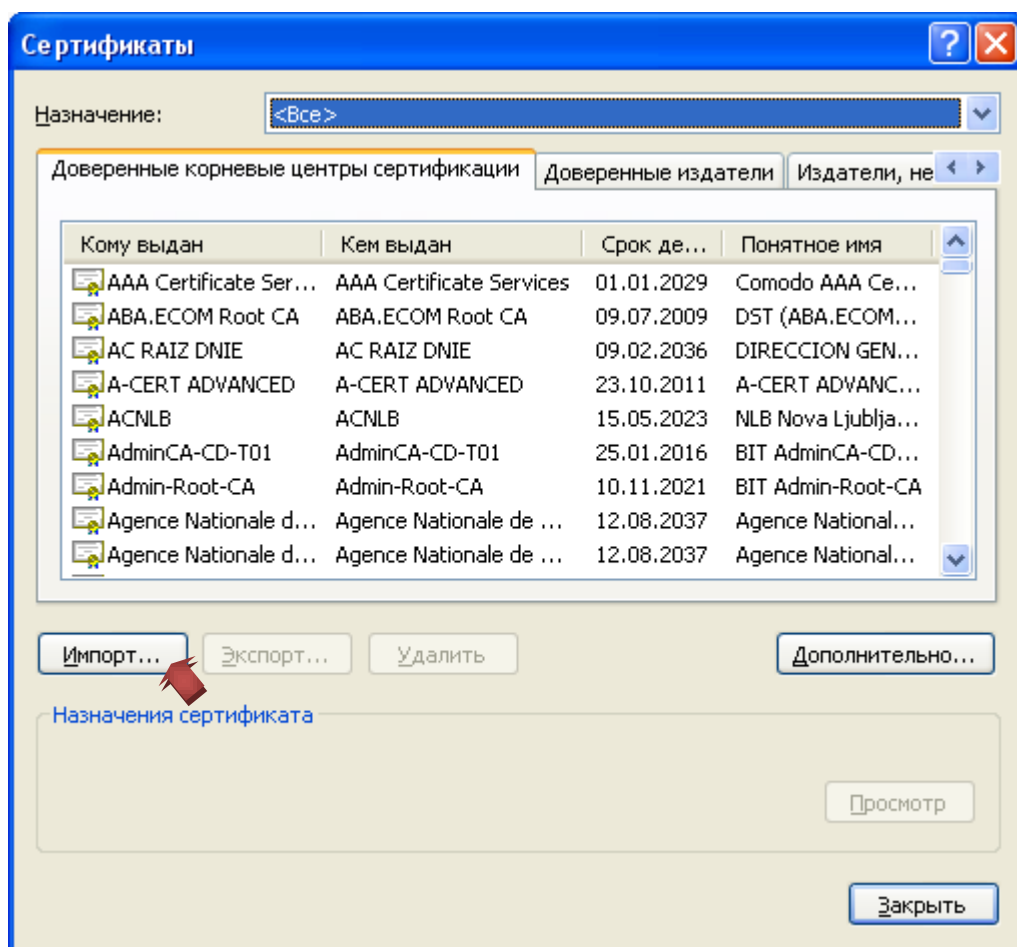


Рисунок 3 – Вкладка *Доверенные корневые центры сертификации* в окне *Сертификаты*

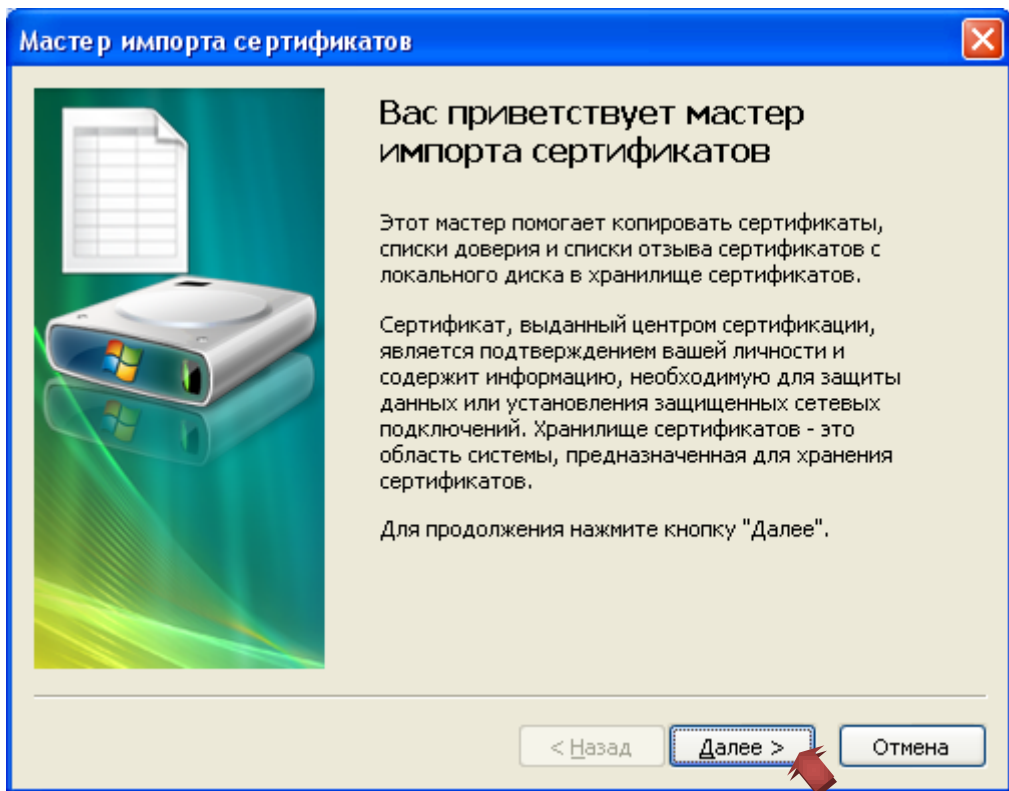


Рисунок 4 – Мастер импорта сертификатов. Приветствие

Укажите импортируемый файл (рисунок 5).

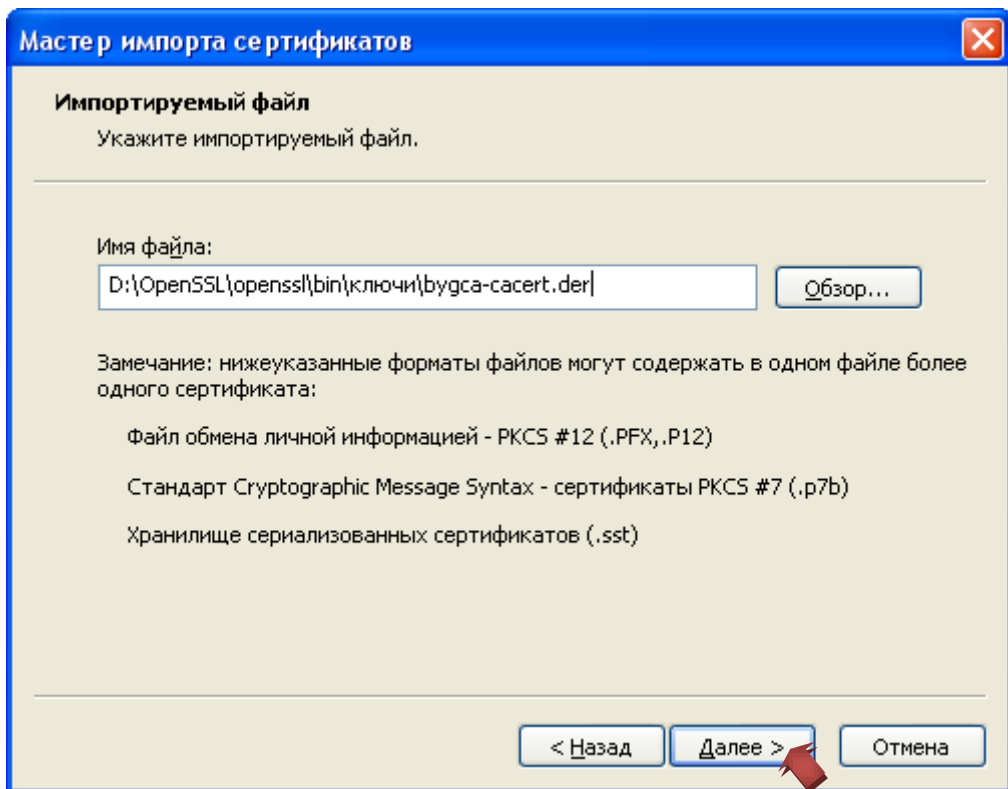


Рисунок 5 – Мастер импорта сертификатов. Выбор файла.

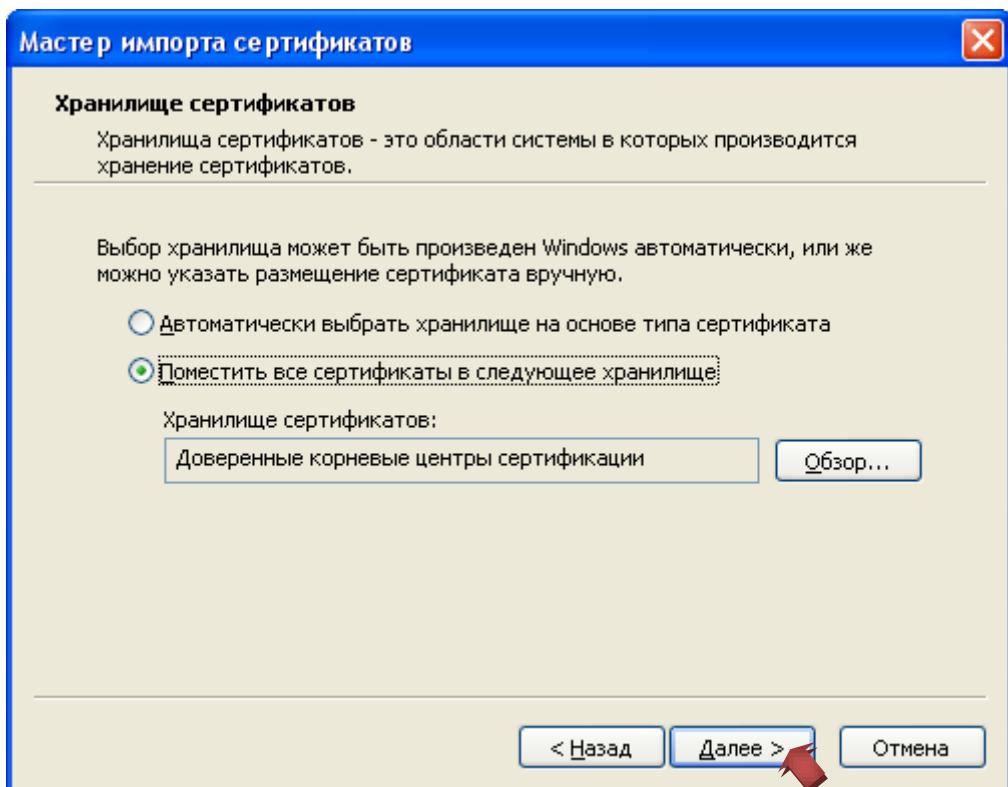


Рисунок 6 – Мастер импорта сертификатов. Выбор хранилища.

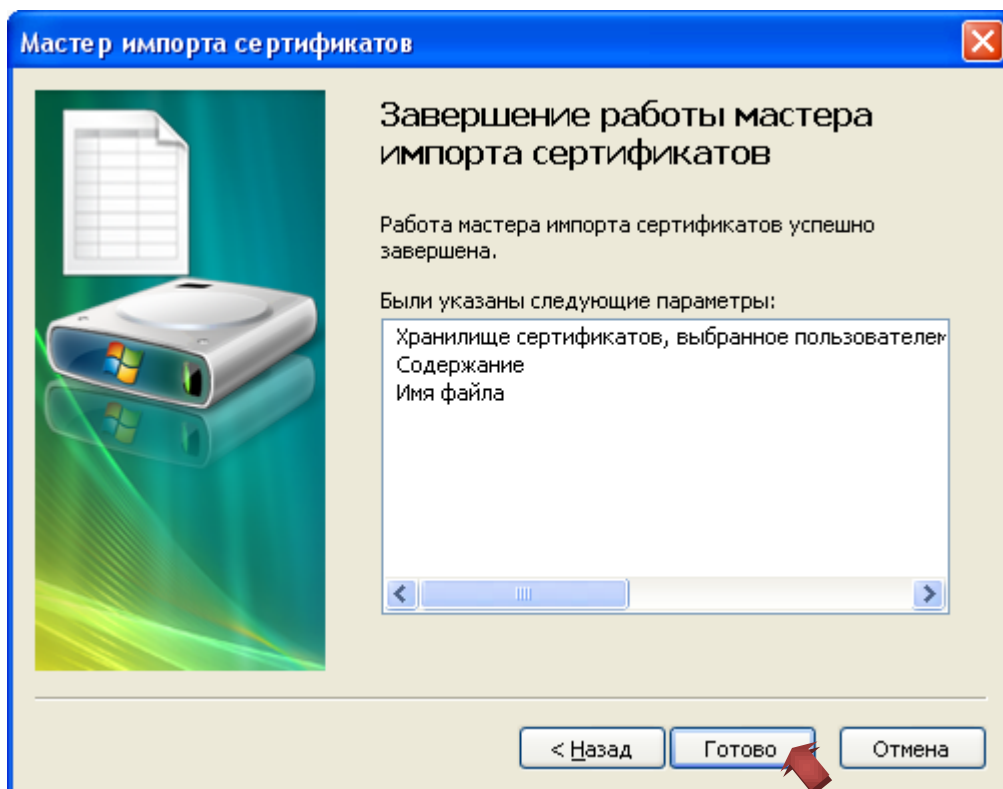


Рисунок 7 – Мастер импорта сертификатов. Завершение работы

5. Далее для импорта хранилища ключей в формате PKCS#12 *JankaKupala\_Keystore.p12* (рисунки 8 – 15) необходимо выбрать в меню *Сервис* пункт *Свойства обозревателя*, в появившемся окне выбрать вкладку *Содержание*, на вкладке *Содержание* нажать кнопку *Сертификаты* (рисунок 8).

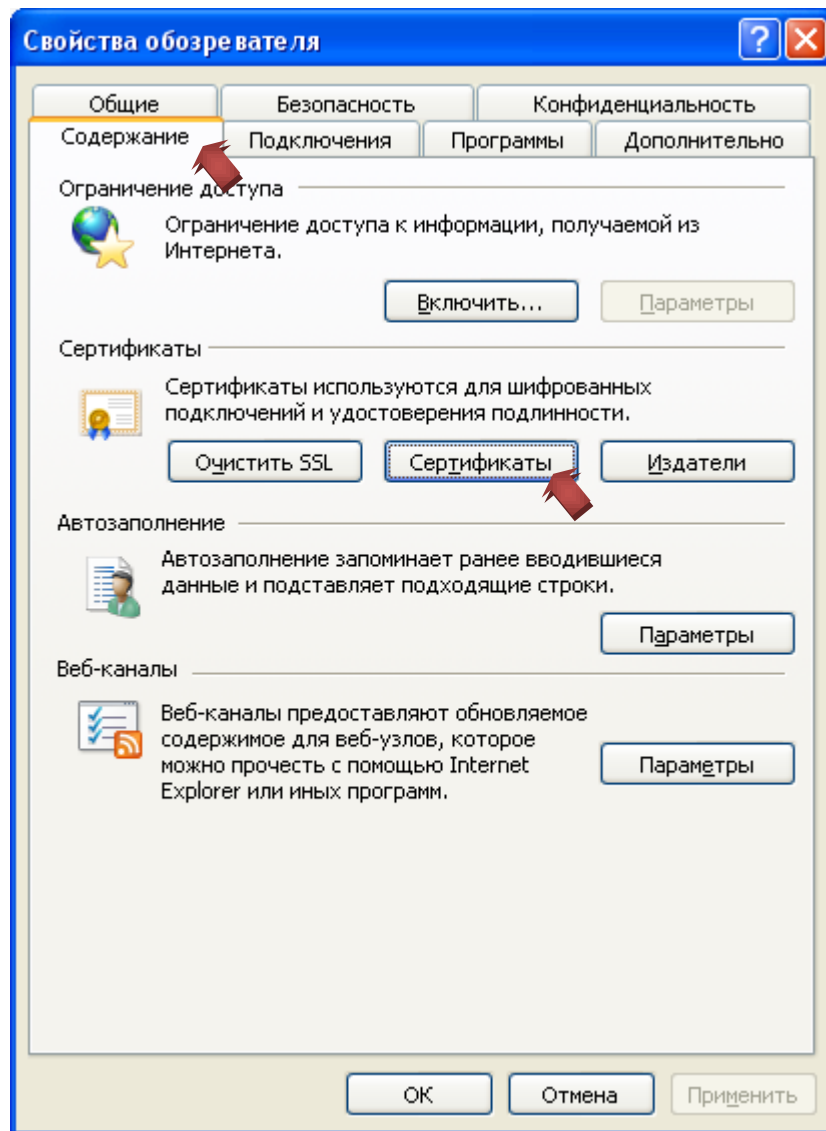


Рисунок 8 – Кнопка *Сертификаты* на вкладке *Содержание* в окне *Свойства обозревателя*

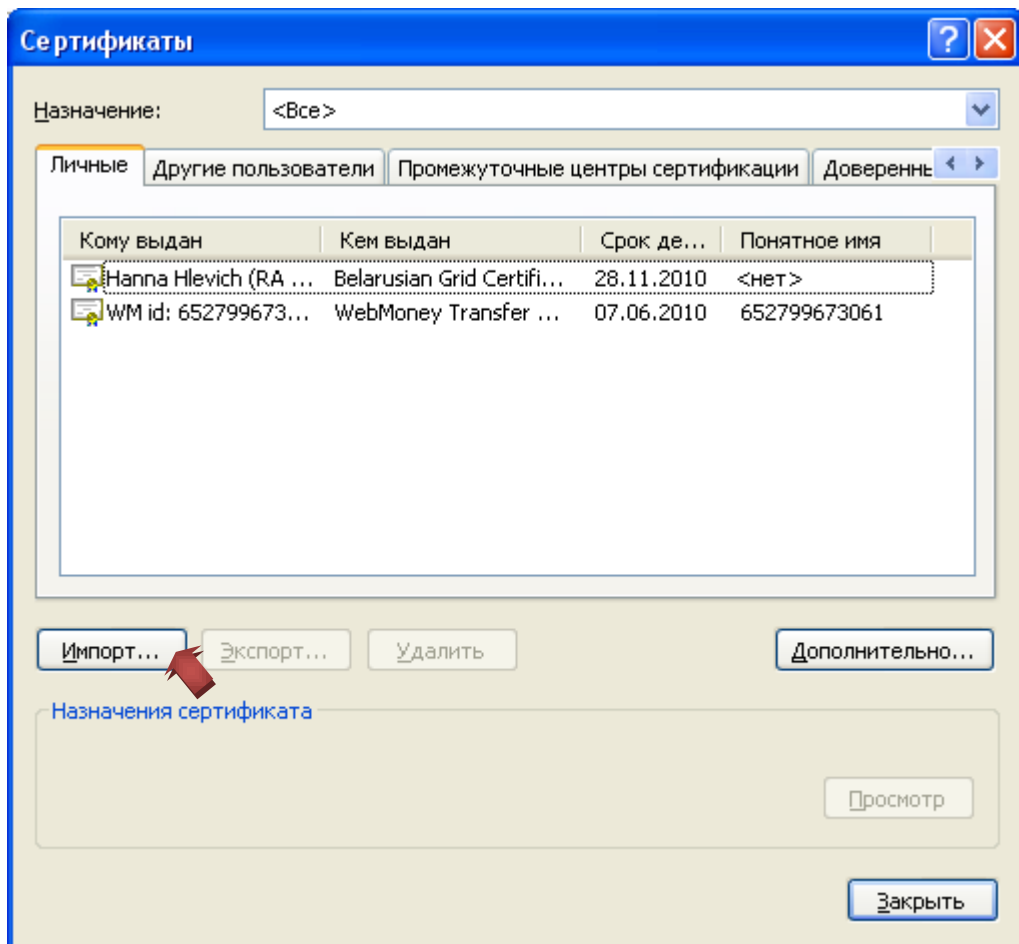


Рисунок 9 – Вкладка *Личные* в окне *Сертификаты*

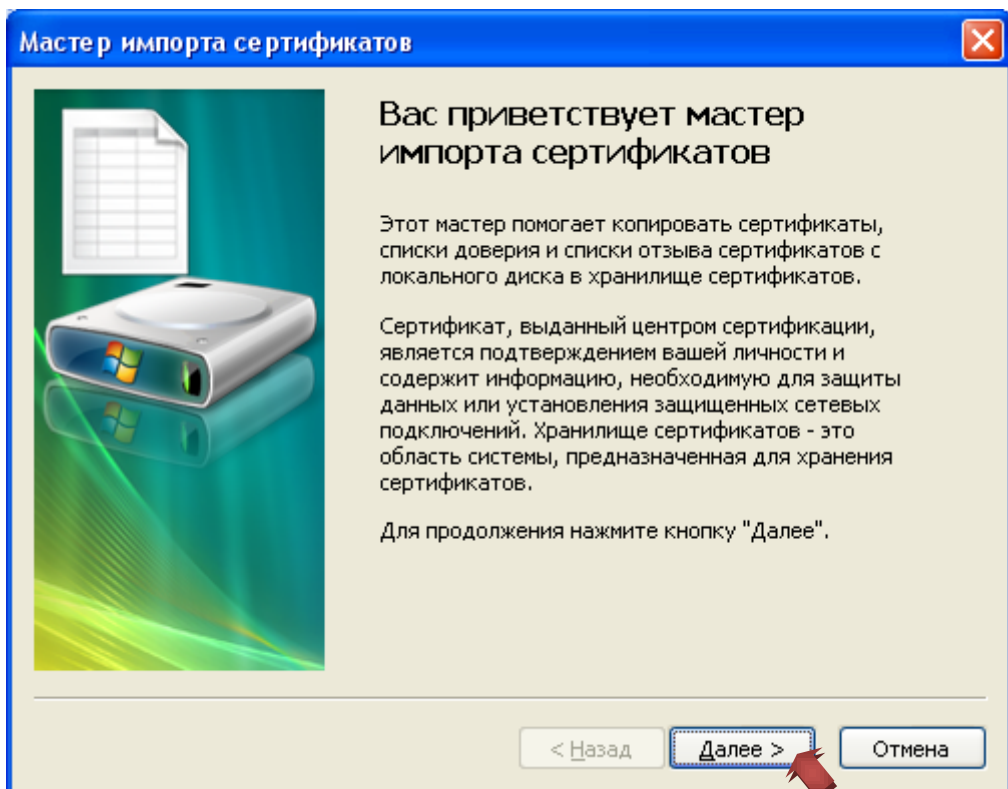


Рисунок 10 – Мастер импорта сертификатов. Приветствие

Укажите импортируемый файл (рисунок 11).

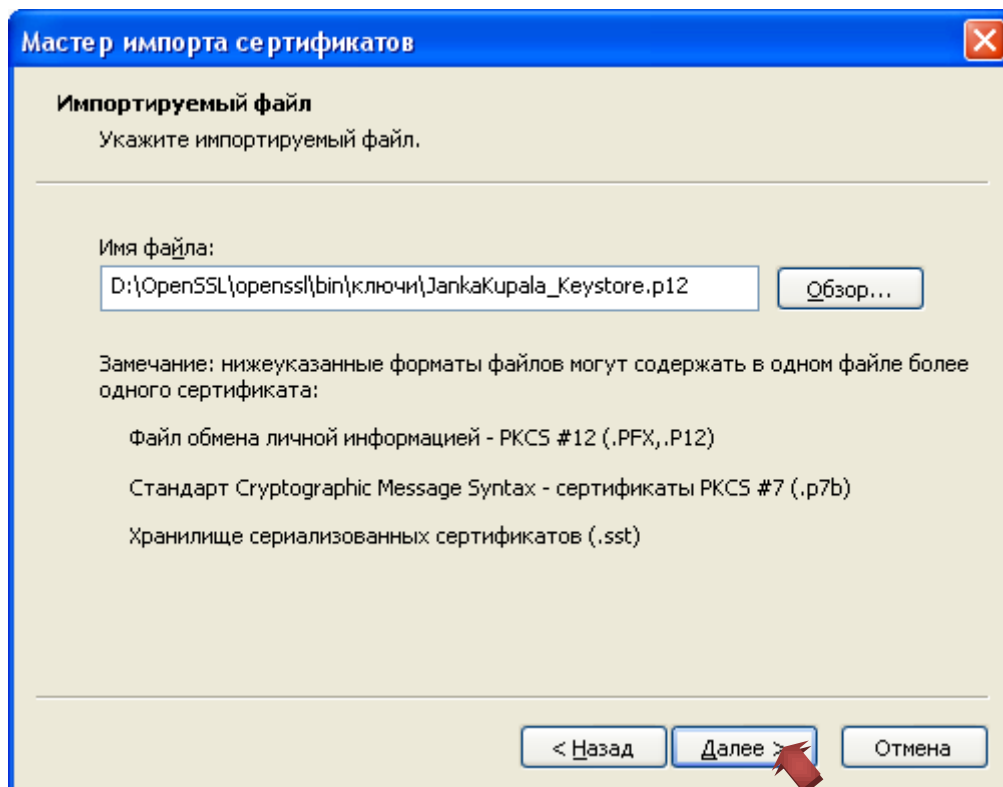


Рисунок 11 – Мастер импорта сертификатов. Выбор файла.

Введите пароль к Вашему хранилищу ключей *JankaKupala\_Keystore.p12*. Включите усиленную защиту (рисунок 12).

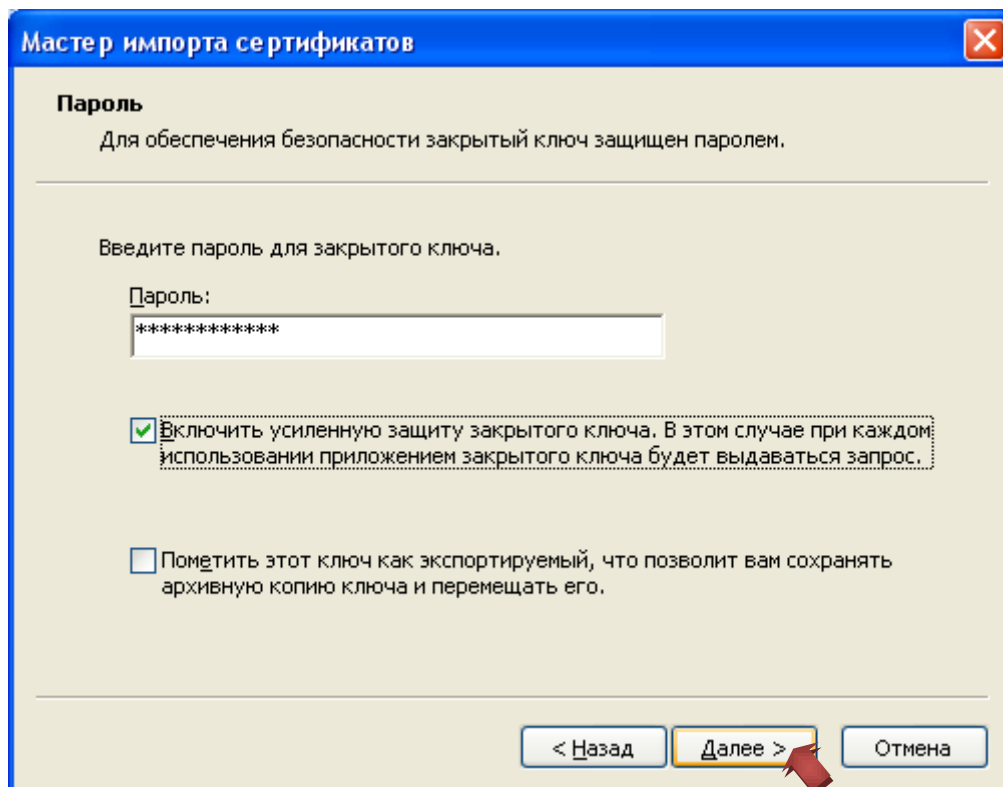


Рисунок 12 – Мастер импорта сертификатов. Ввод пароля

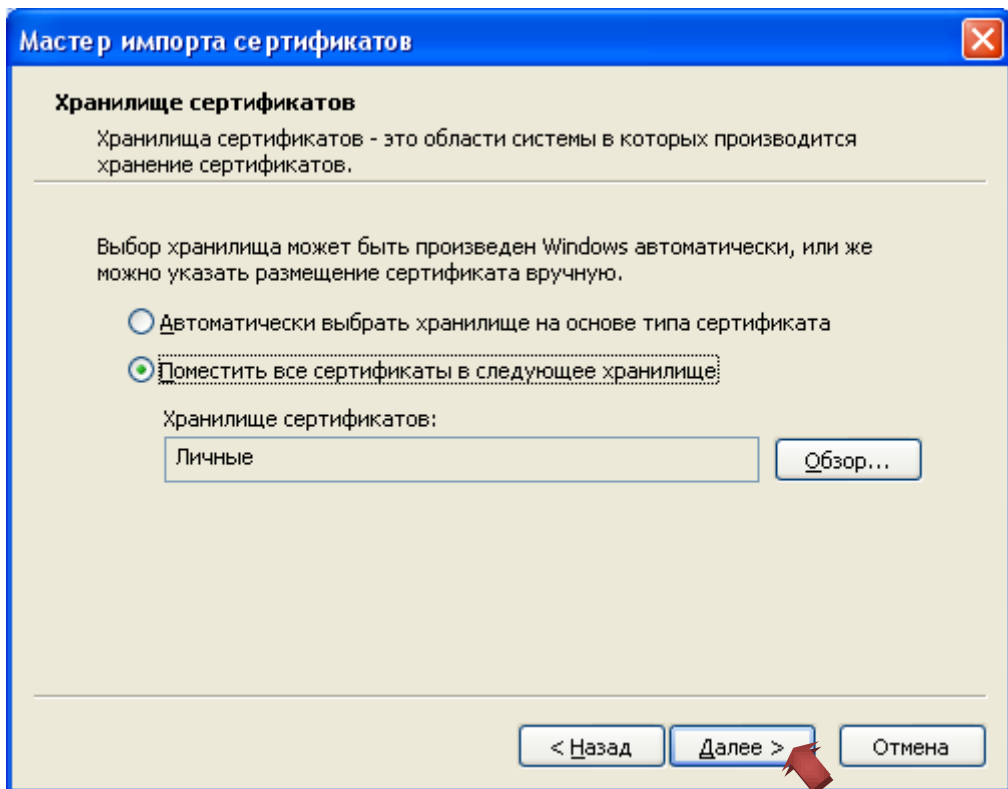


Рисунок 13 – Мастер импорта сертификатов. Выбор хранилища.

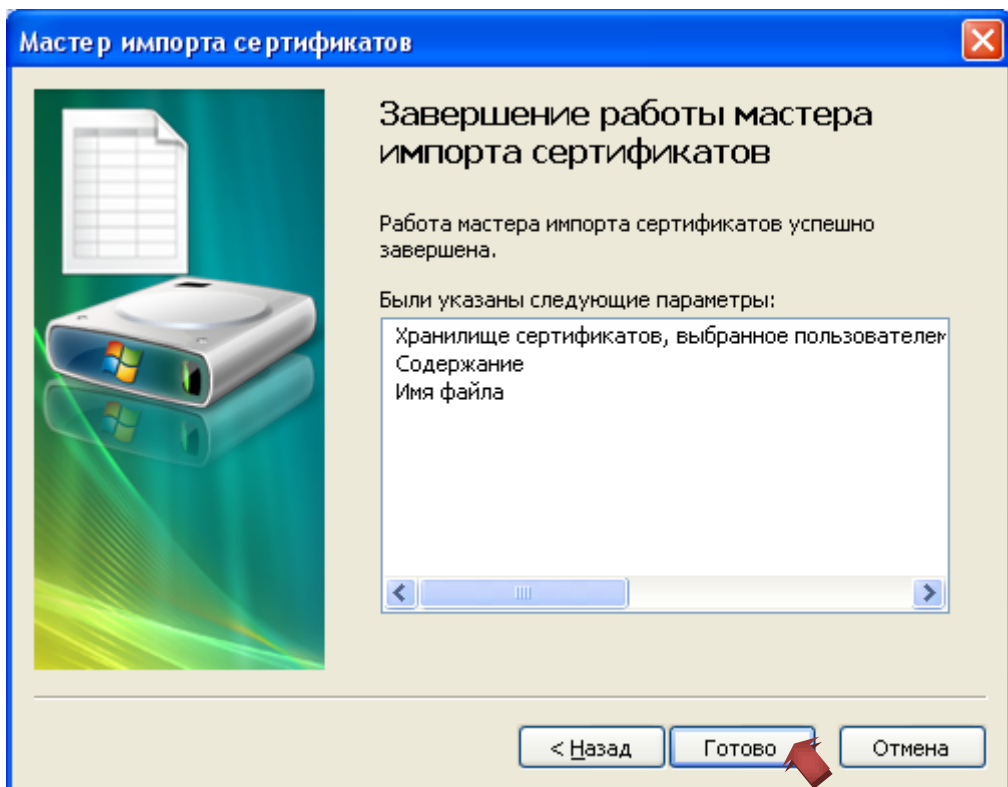


Рисунок 14 – Мастер импорта сертификатов. Завершение работы

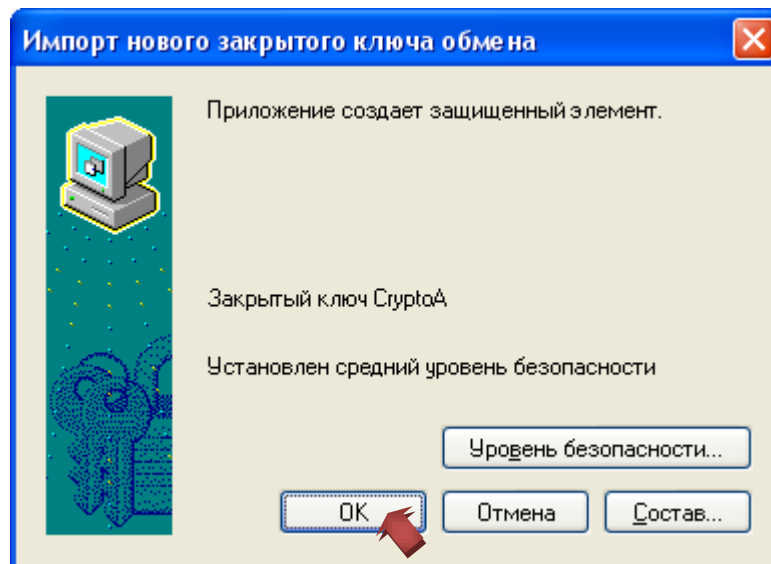


Рисунок 15 – Импорт нового закрытого ключа обмена. Установка уровня безопасности

6. Для проверки работоспособности импортированного хранилища ключей в формате PKCS#12 перейдите по ссылке <https://jabber.grid.by/test.php>.  
При попытке входа должно появиться окно:

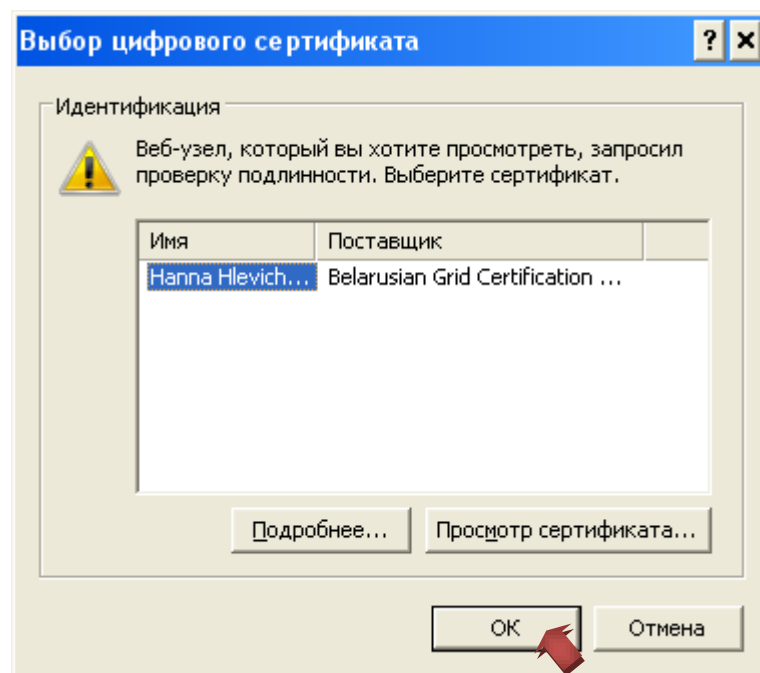


Рисунок 16 – Использование импортированного хранилища ключей

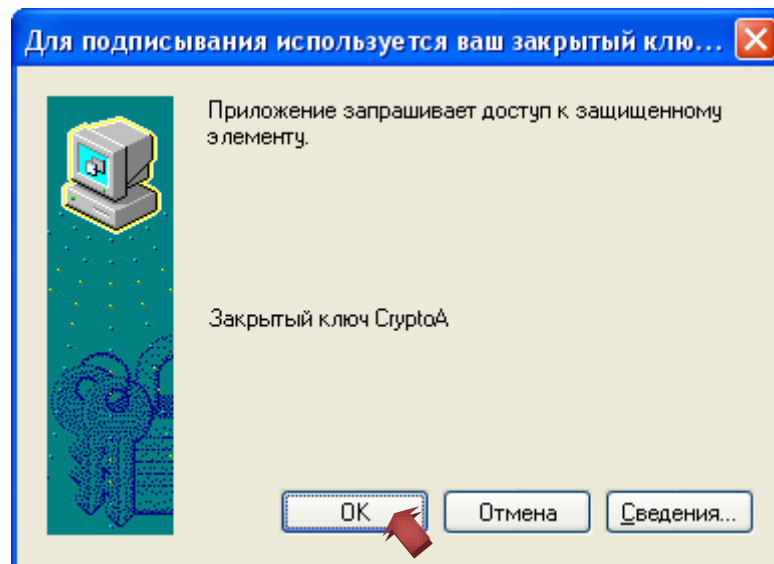


Рисунок 17 – Использование импортированного хранилища ключей

Если импорт хранилища ключей в формате PKCS#12 был произведен успешно, то загрузится страница с базовой информацией о Вашем сертификате, а также ссылки на полезные веб-ресурсы, которыми можно пользоваться только при наличии сертификата:

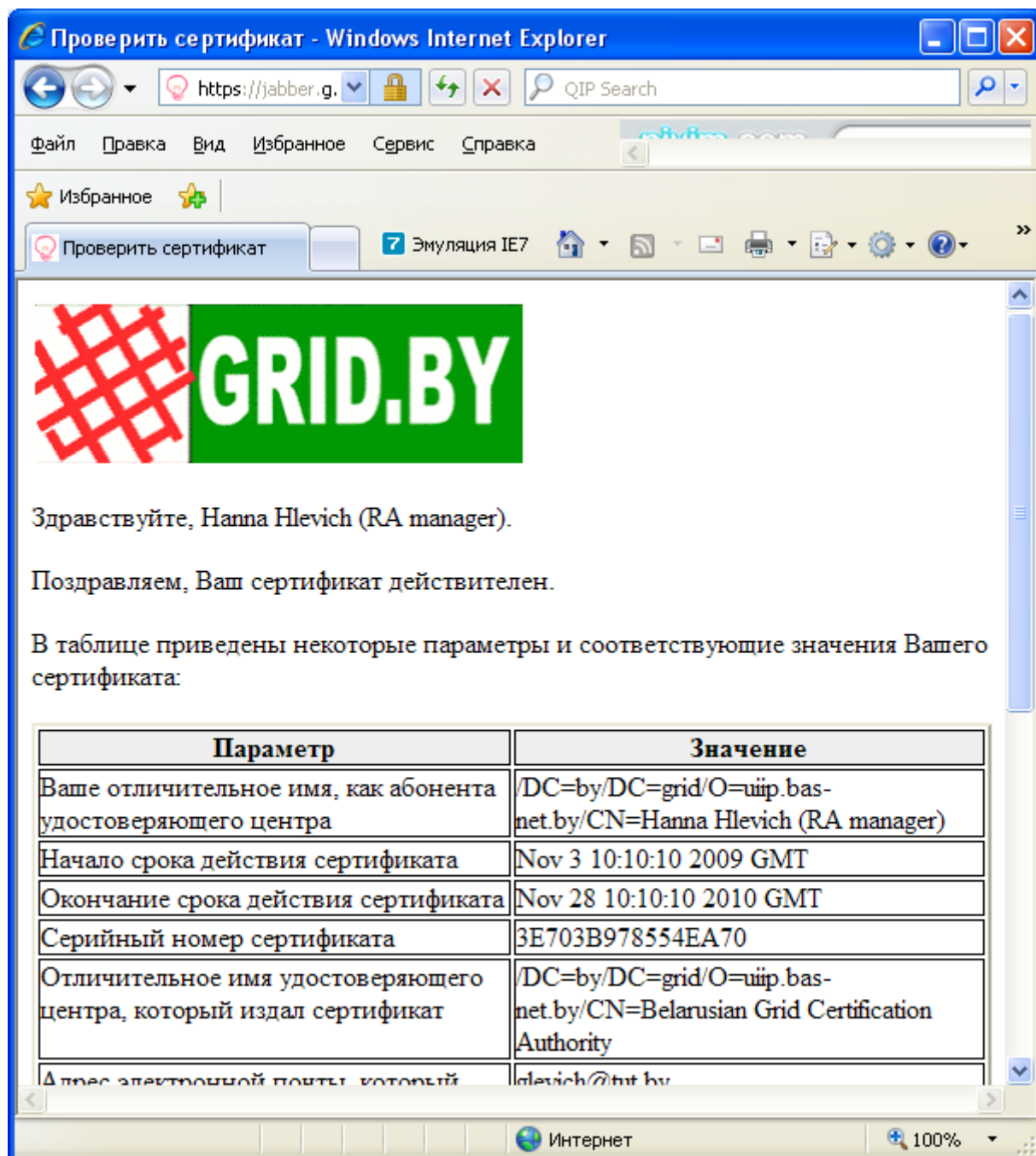


Рисунок 18 – Страница с базовой информацией о сертификате