НИЛ «Гамма Технологии»

Криптографический модуль Tumar CSP

Настройка и работа модуля с Mozilla Firefox и Mozilla Thunderbird в MacOS/Linux

Руководство пользователя

398-600400083267- СКЗИ 08.2.04.3-5.0.1-2012

Алматы 2012

АННОТАЦИЯ

Настоящий документ содержит инструкции по использованию криптографического модуля ТумарCSP в операционной системе MacOS в программах: Mozilla Firefox и почтового клиента Mozilla Thunderbird.

Документ предназначен для пользователей программы.

ОГЛАВЛЕНИЕ

1 Требования к программному обеспечению

«Tumar CSP» предназначен для функционирования в ОС:

– MacOS;

– Linux.

На компьютере должно быть установлено средство криптографической защиты информации TumarCSP версии 5.x.

Установка программы «Tumar CSP» осуществляется путем запуска исполнимого файла SetupCSPx64.exe.

Дополнительно на компьютере должны быть установлены:

– Mozilla Firefox .

– Mozilla Thunderbird.

В ключевом контейнере пользователя должны быть размещены ключ и цепочка сертификатов.

2 Установка и настройка TumarCSP

2.1 Установка TumarCSP

1. Для установки TumarCSP для Mac OS запустить терминал (консоль).


Инструкция по установке размещена http://gamma.kz/products/tumar-csp/72.html).

2. Перейти в каталог с архивом TumarCSP.

3. Разархивировать дистрибутив:
```
gzip –d TumarCSP_mac64_5.2.x.x.x.tgz
tar –xvf TumarCSP_mac64_5.2.x.x.x.tar
```

4. Перейти в разархивированный каталог:
```
cd TumarCSP5.2
```

5. Запустить установочный скрипт с параметром **install**:
```
./setup_csp.sh install
```

6. Убедиться, что на консоли отображены записи:
```
Installing TumarCSP 5.2.x.x.x for mac64...START
Installing TumarCSP 5.2.x.x.x for mac64...STOP
```

7. Установка TumarCSP выполнена.

2.2 Настройка ключевого контейнера

1. Создать произвольный каталог для хранения ключей, например каталог Users/name/keys:

```
mkdir /Users/name/keys
```

2. Поместить ключевой контейнер, полученный от УЦ (например: USER.bin) в созданный каталог.

3. Установить права **-rwxr-xr-x** на файл USER.bin

4. Настроить ключевой профайл для данного ключевого контейнера. Для этого требуется отредактировать файл **/TumarCSP/etc/cptumar.conf**, т.е привести его к виду:

```
[profiles]
FSystem=file://USER@//Users/name/keys
```

ПРИМЕЧАНИЕ: если ключи в формате p12 (например: keys_rsa.p12 и keys_gost.p12), то для настройки ключа p12 необходимо в файле /TumarCSP/etc/cptumar.conf прописать:

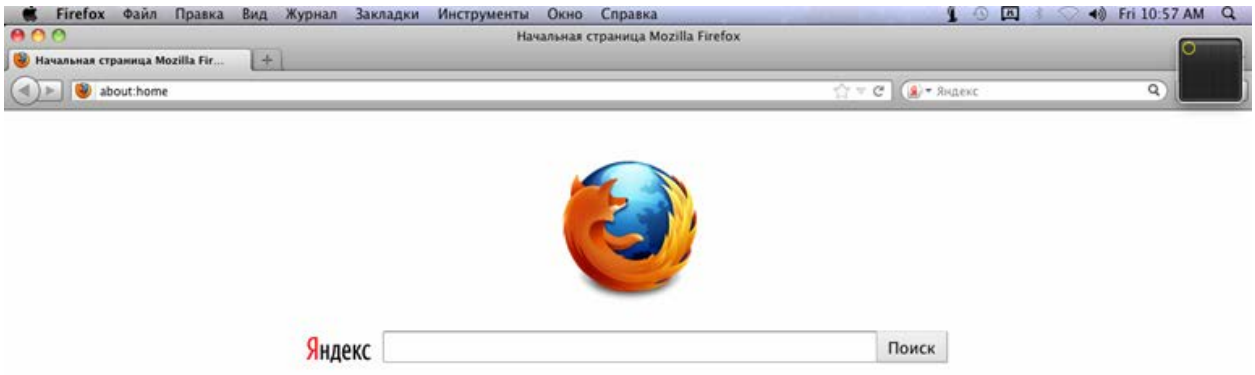
```
[profiles]
TumarRSA = file://keys_rsa:passwd_rsa@//Users/name/keys?ext=p12
TumarGOST = file://keys_gost:passwd_gost@//Users/name/keys?ext=p12

,где:
passwd_rsa - пароль для контейнера keys_rsa.p12
passwd_gost - пароль для контейнера keys_gost.p12
/Users/name/keys – каталог, в котором находятся ключевые контейнеры
keys_rsa.p12 и keys_gost.p12.
```

По аналогии настраиваются ключи форматов pem и pfx.

2 Настройка браузера Mozilla Firefox

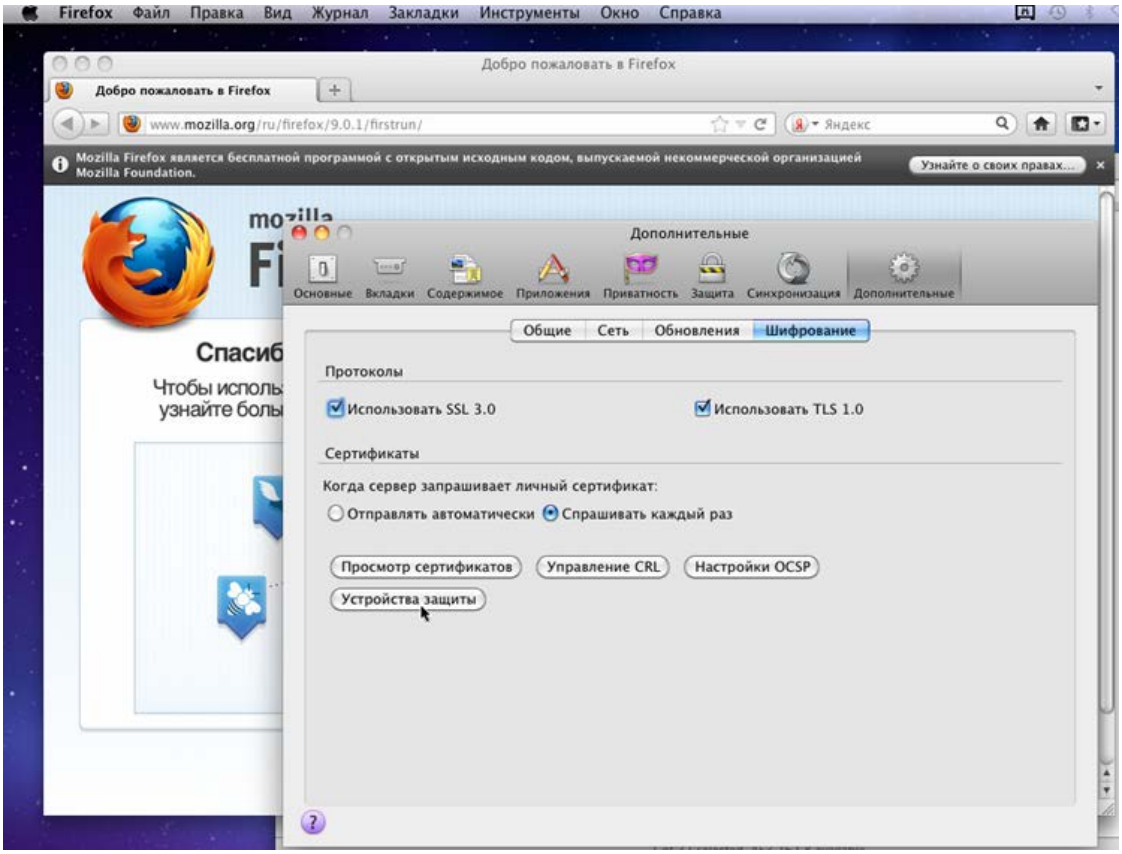
2.1 Настройка криптографии в браузере

1. Запустить браузер.

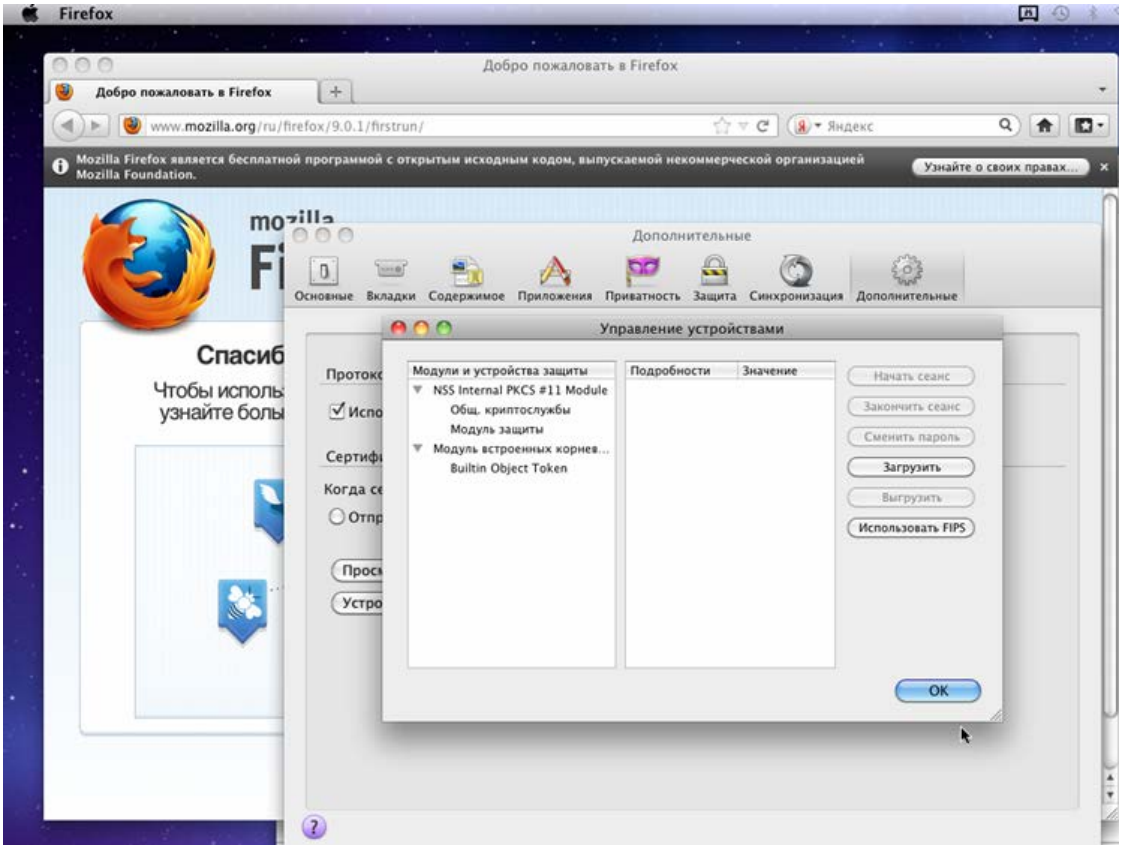


2. В главном меню перейти в **Firefox→Настройки**

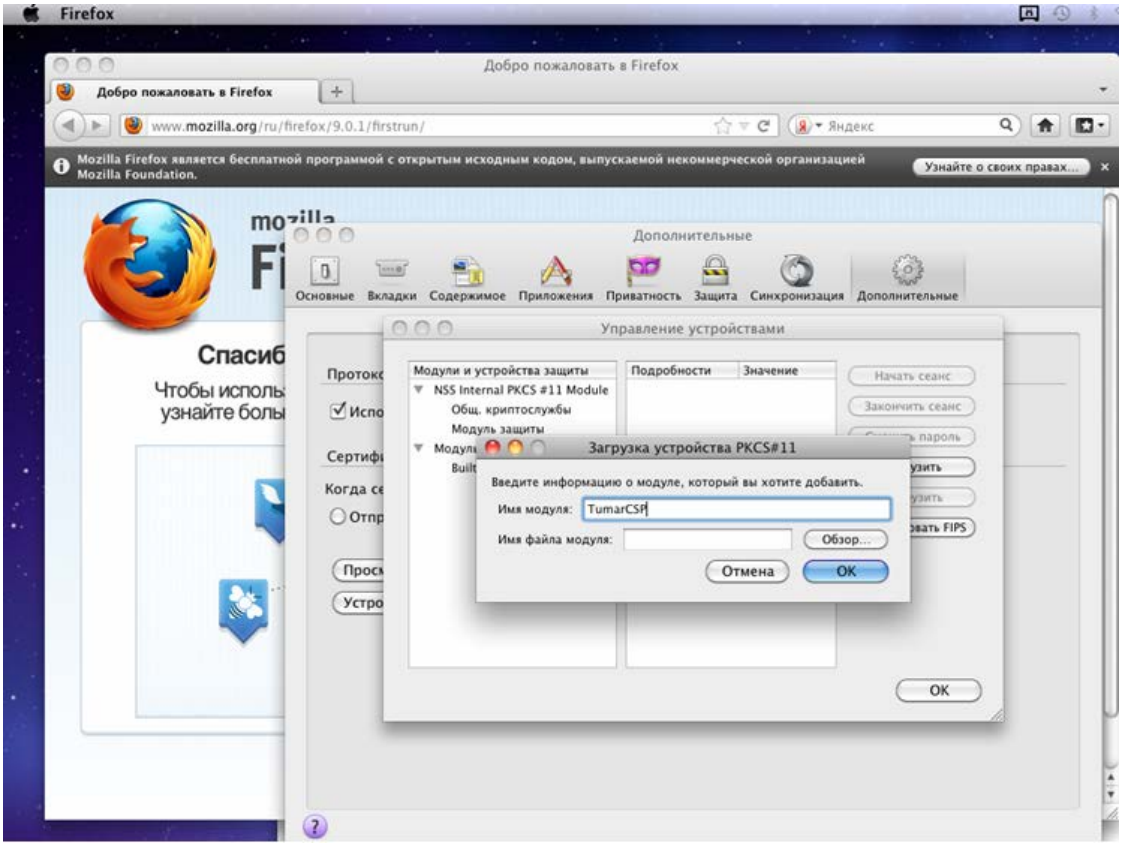
3. В окне *Настройки* выбрать закладку **Дополнительные →Шифрование →Устройства защиты**



4. В окне *Управление устройствами* нажать на кнопку **Загрузить**.

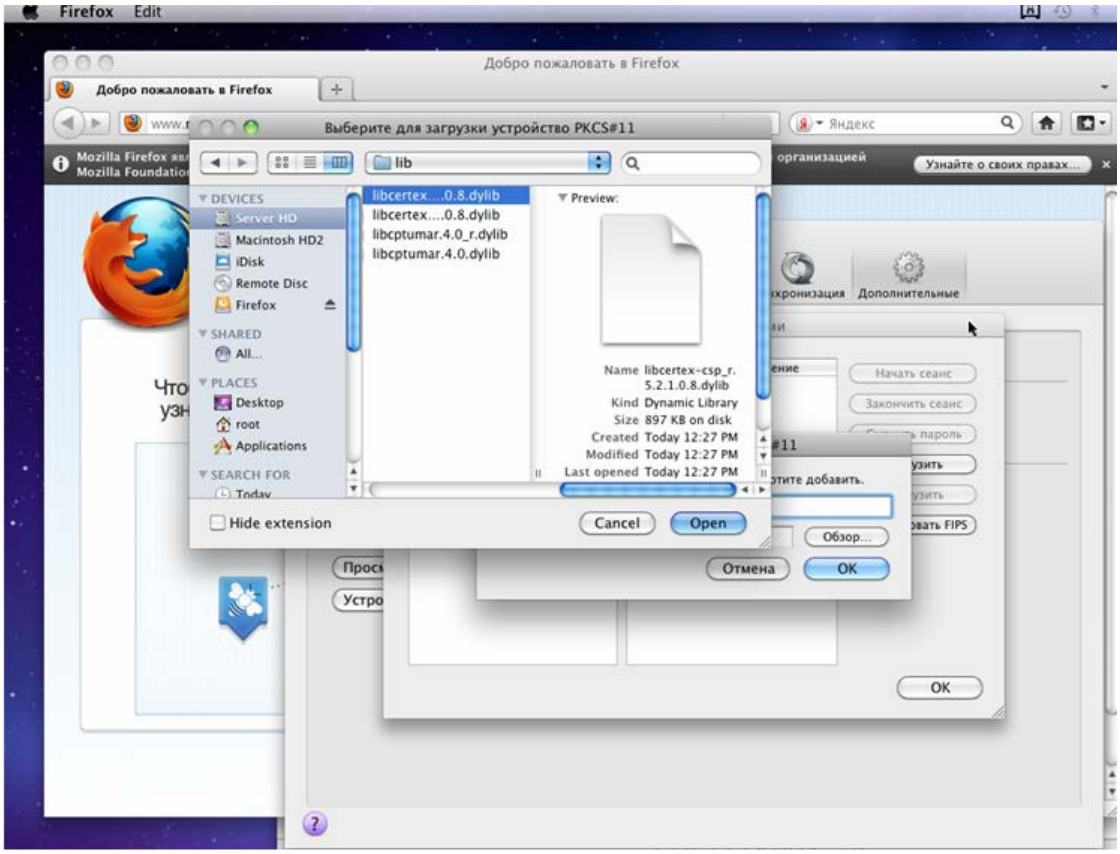


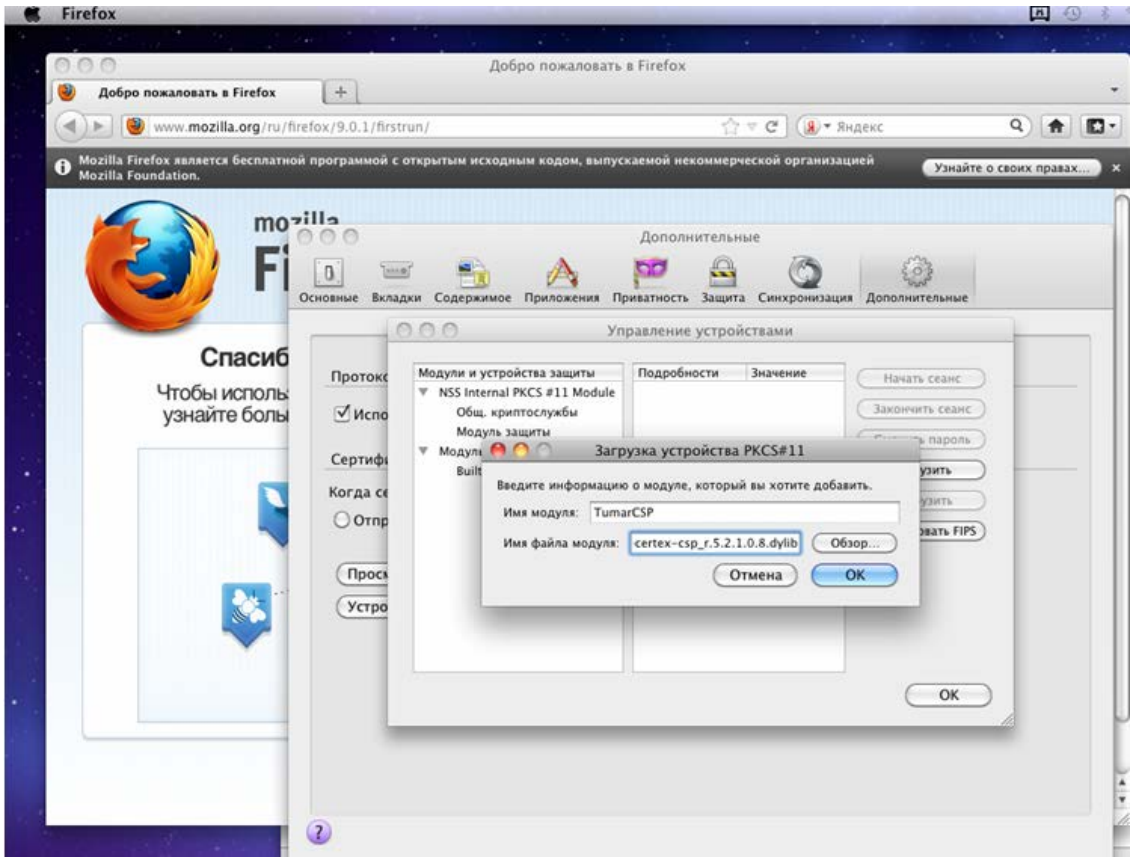
5. Убедиться, что открылось окно *Загрузка устройства PKCS#11*.



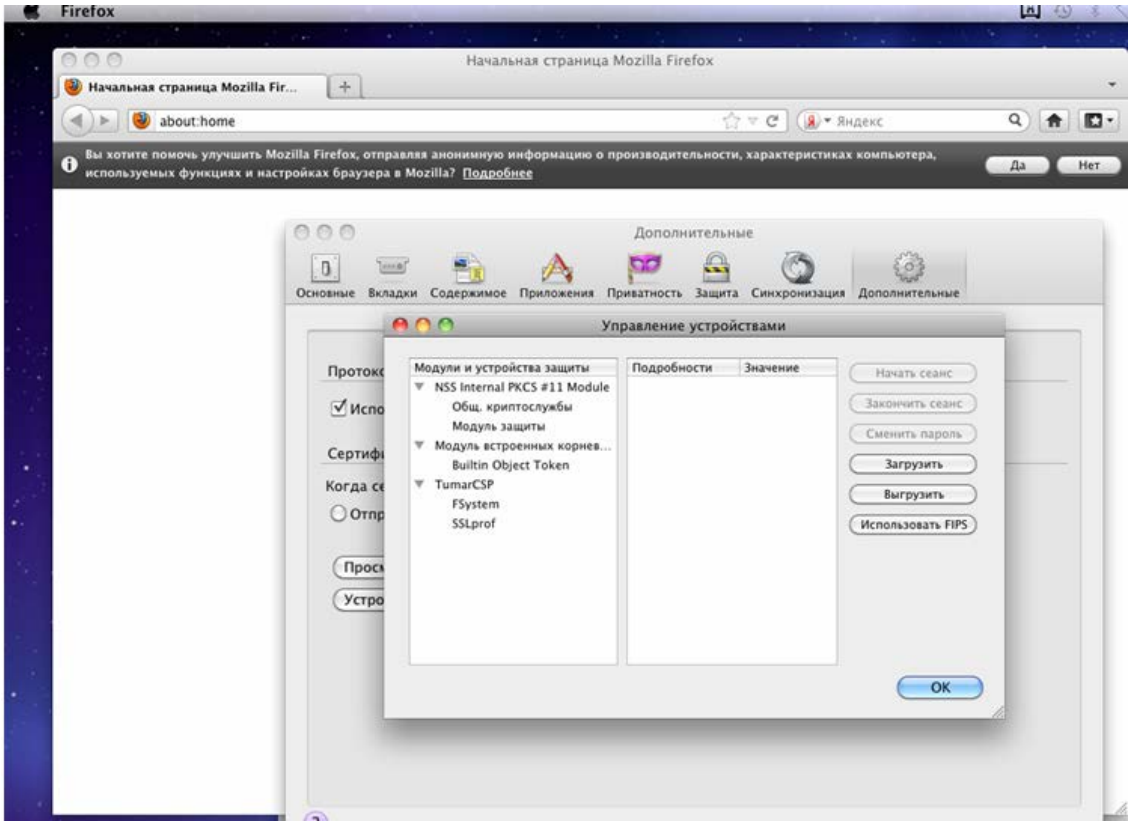
6. В окне *Загрузка устройства PKCS#11*:
   - вписать произвольное имя модуля (например, TumarCSP);

– справа от поля *Имя файла модуля* нажать на кнопку **Обзор** и выбрать на файловой системе библиотеку **libcertex-csp.5.2.x.x.x.dylib** или **libcertex-csp_r.5.2.x.x.x.dylib,** где x.x.x – версия релиза ПО;
– нажать на кнопку **ОК**.





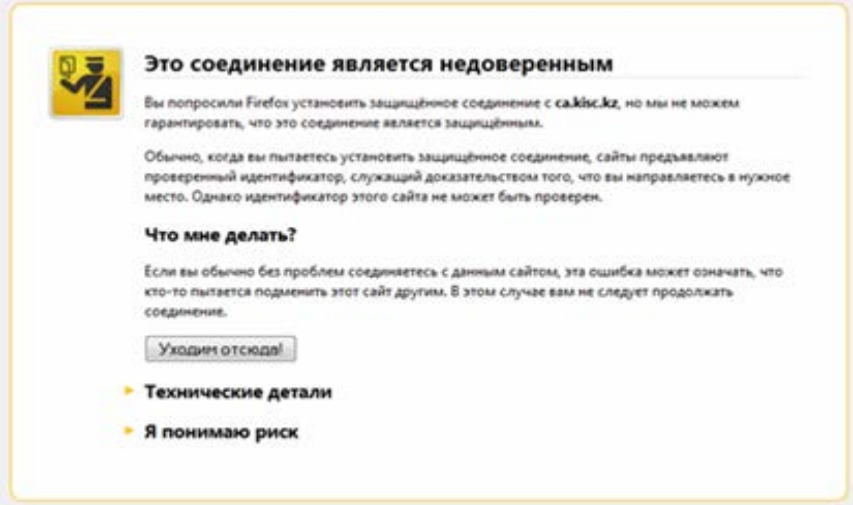
7. Убедиться, что в списке модулей и устройств защиты отображены все профайлы, настроенные на ключевую информацию – это профайл **FSystem** и **SSLprof**. Нажать на кнопку **ОК**.



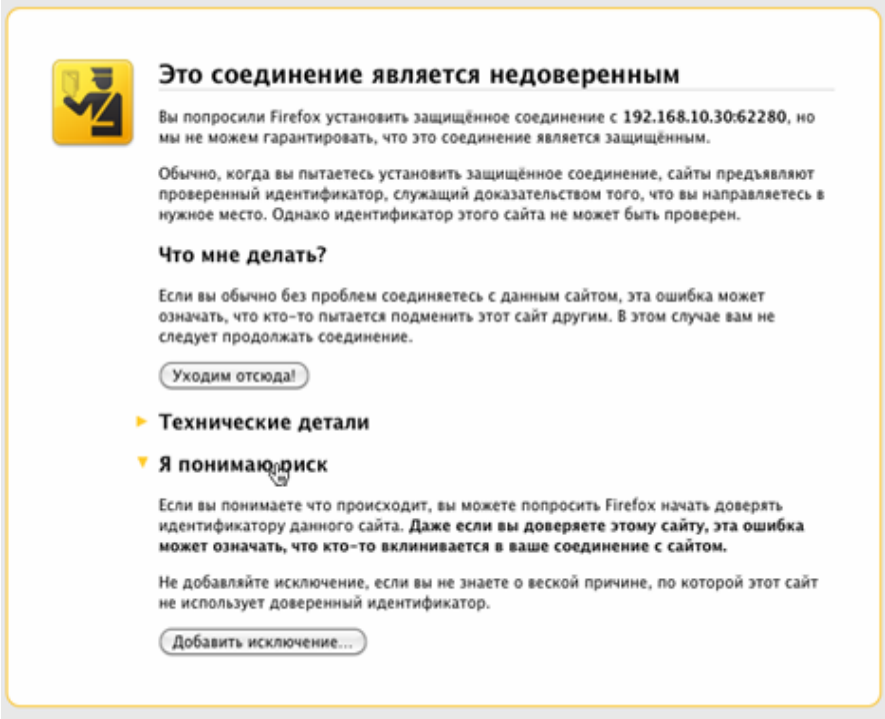
8. Настройки криптографии для Mozilla Firefox выполнены. Теперь можно использовать SSL на сайтах, требующих SSL-соединение.

2.2 Установка SSL соединения

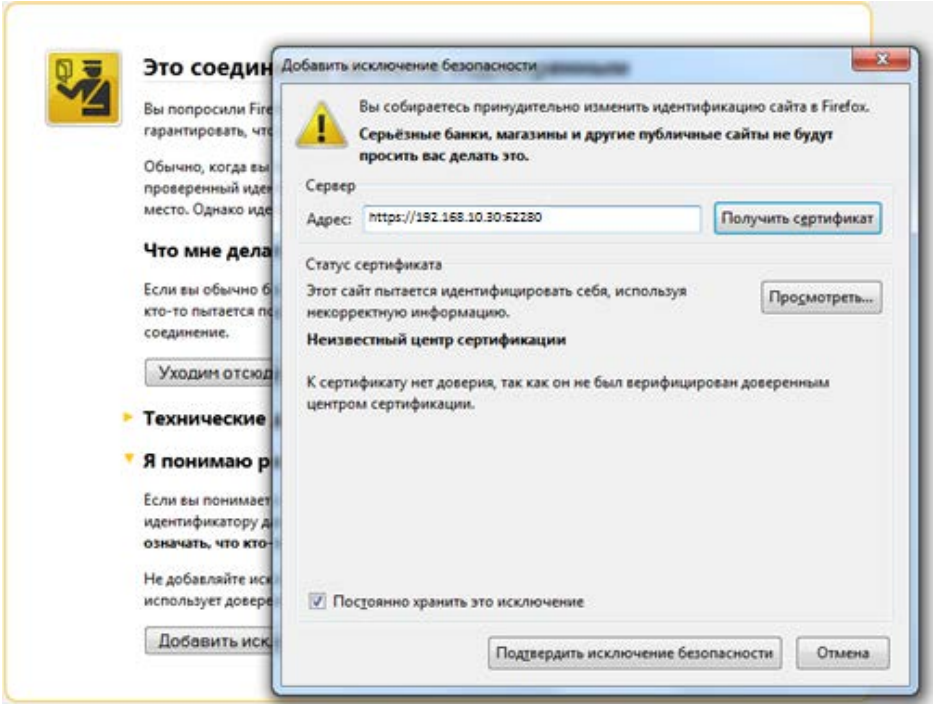
1. При первом входе на ресурс, требующий SSL соединение, отобразится окно как на рисунке, нажмите на кнопку **Я принимаю риск**.



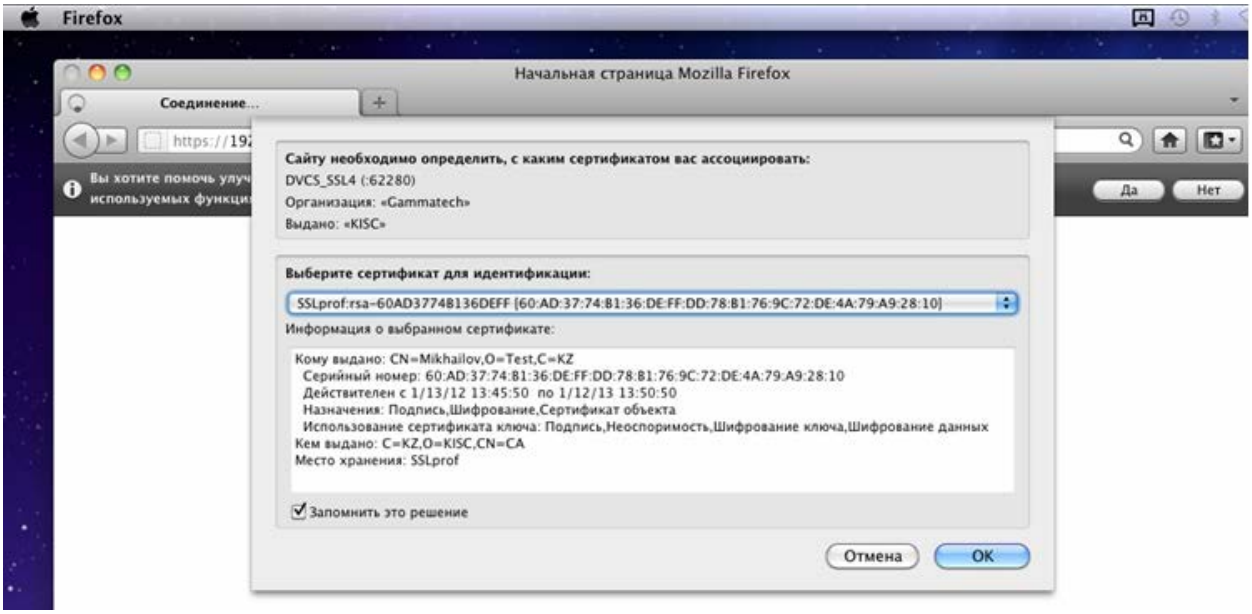
2. Следующий шаг – нажмите на кнопку **Добавить исключение…**



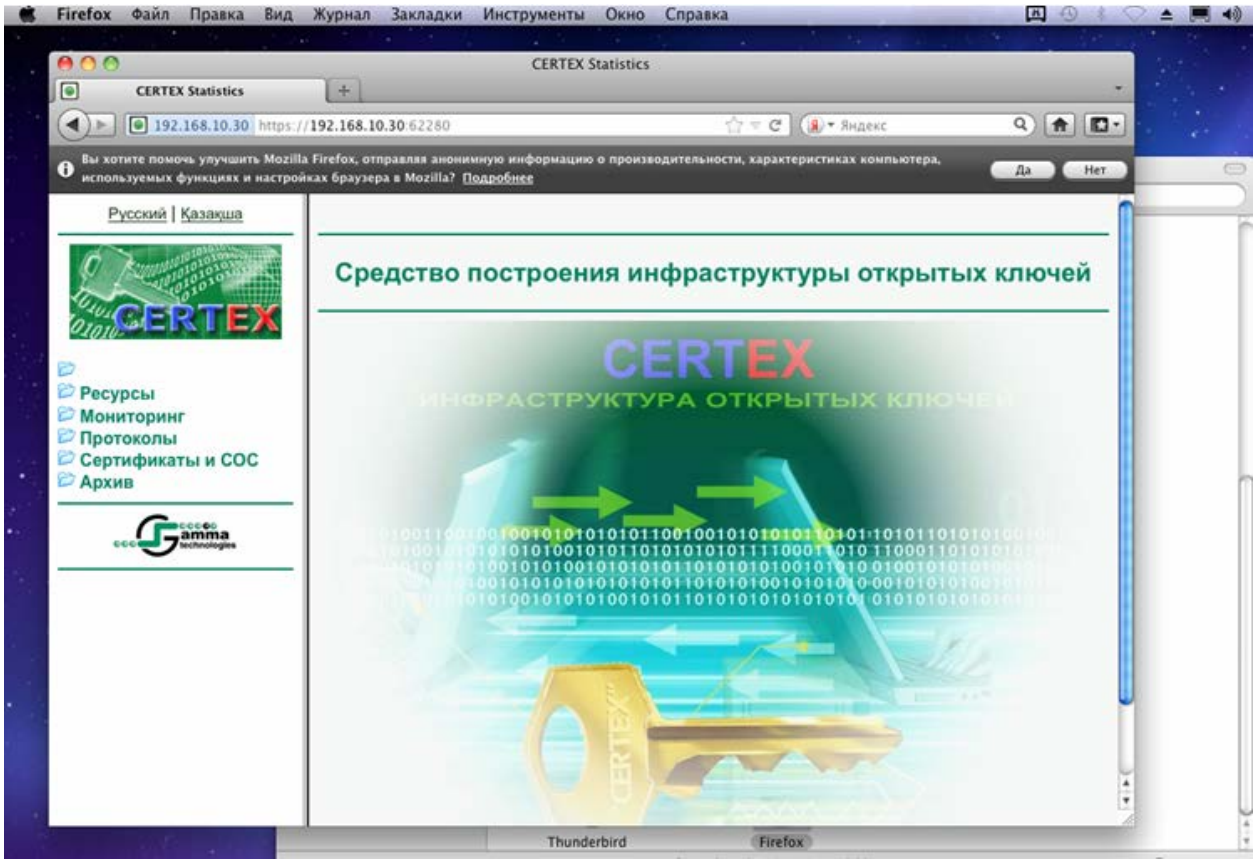
3. В окне *Добавить исключение* нажмите на кнопку **Подтвердить исключение безопасности**.



4. В окне *Запрос идентификации пользователя* необходимо выбрать сертификат для выполнения SSL-соединения и нажать на кнопку **ОК**.



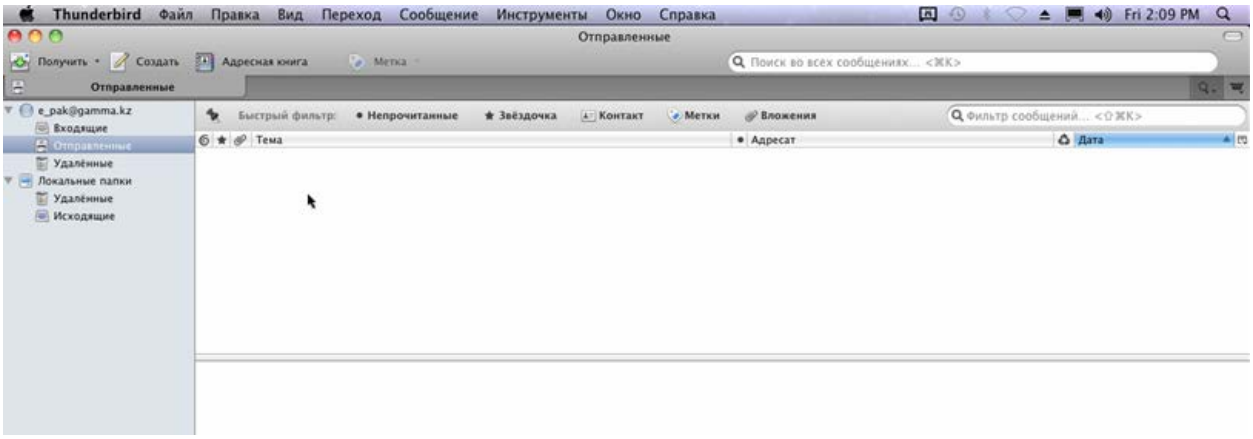
5. При корректном выполнении действий по пп. 1-4 – успешный вход на ресурс



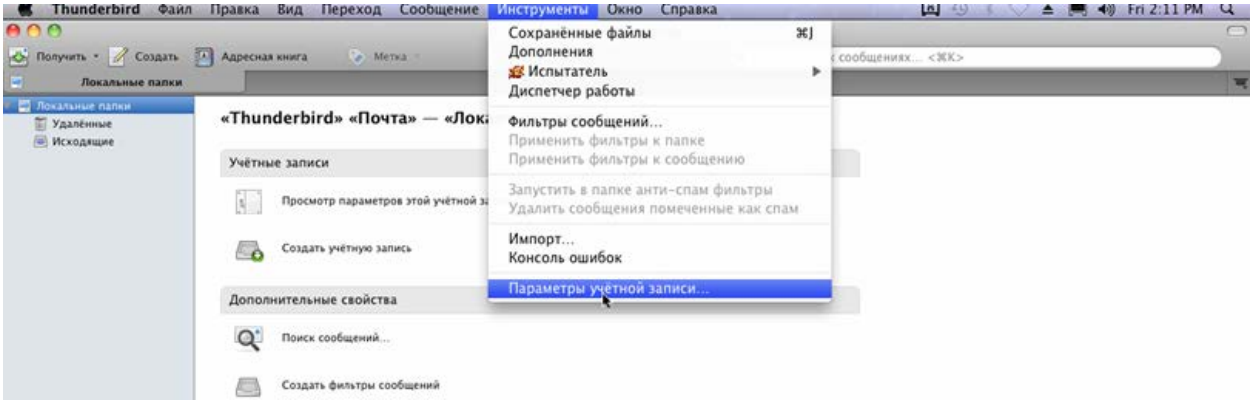
3 Настройка и работа с почтовым клиентом Mozilla Thunderbird

3.1 Настройка учетной записи в ПО Mozilla Thunderbird

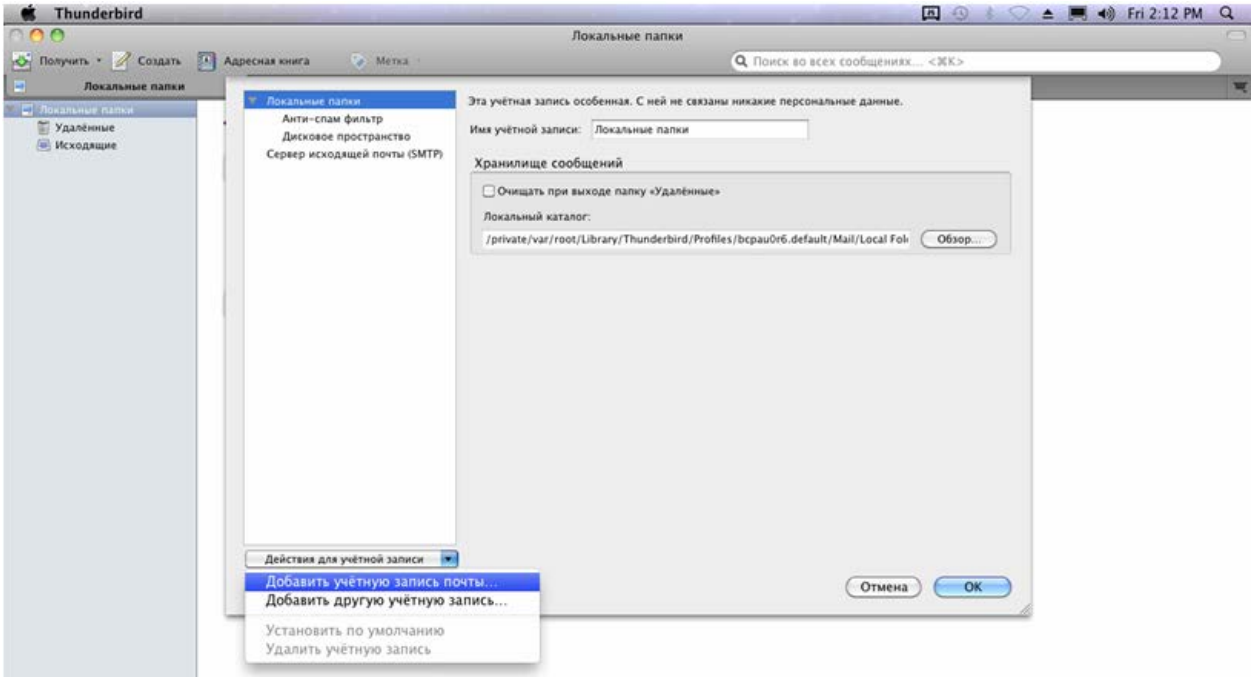
1. Запустить ПО Mozilla Thunderbird.



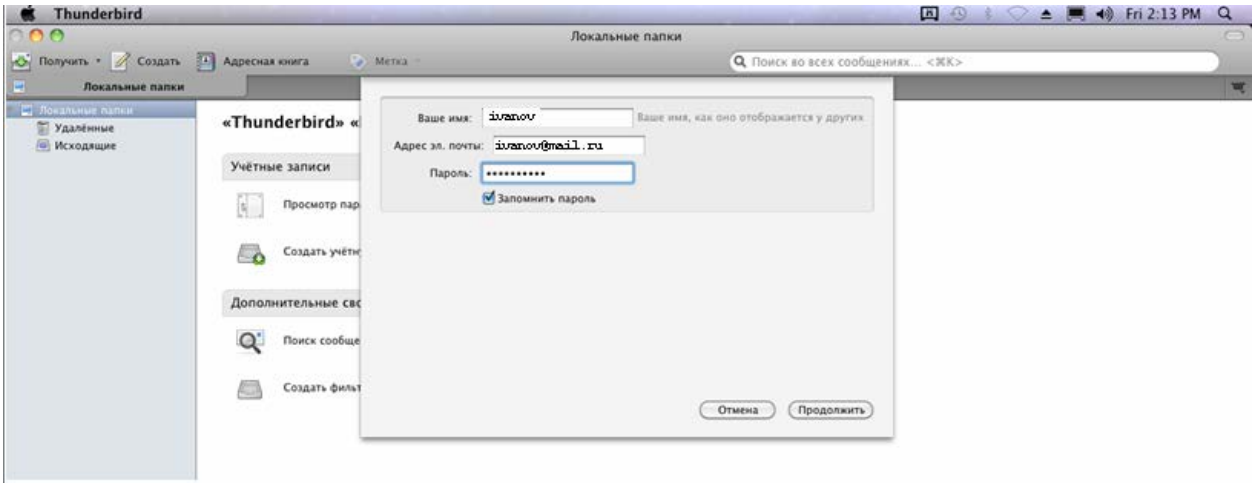
2. В главном меню перейти в **Инструменты→Параметры учётной записи** и настроить учетную запись для требуемого пользователя.



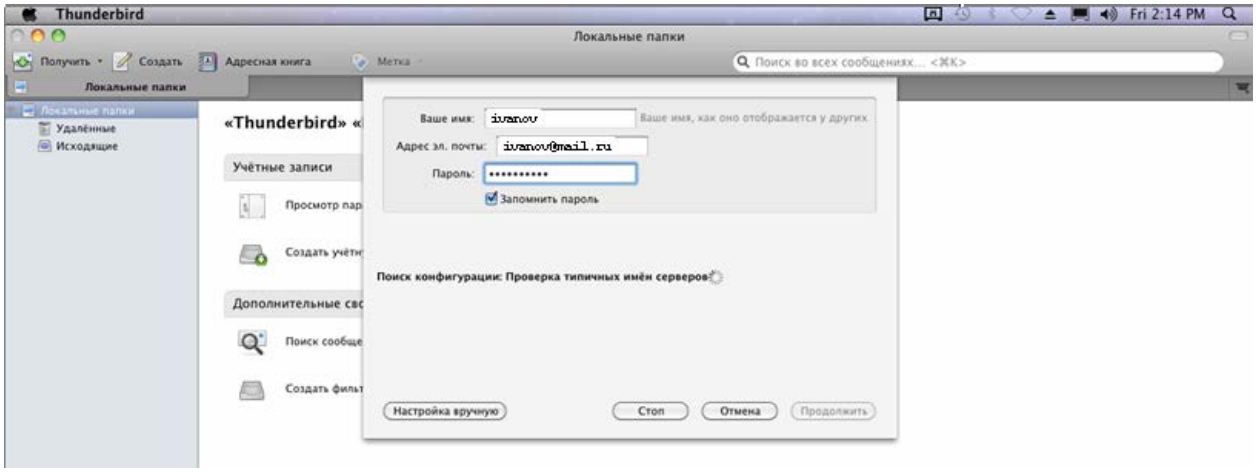
3. В поле *Локальные папки* нажать на кнопку **Добавить учетную запись почты**.



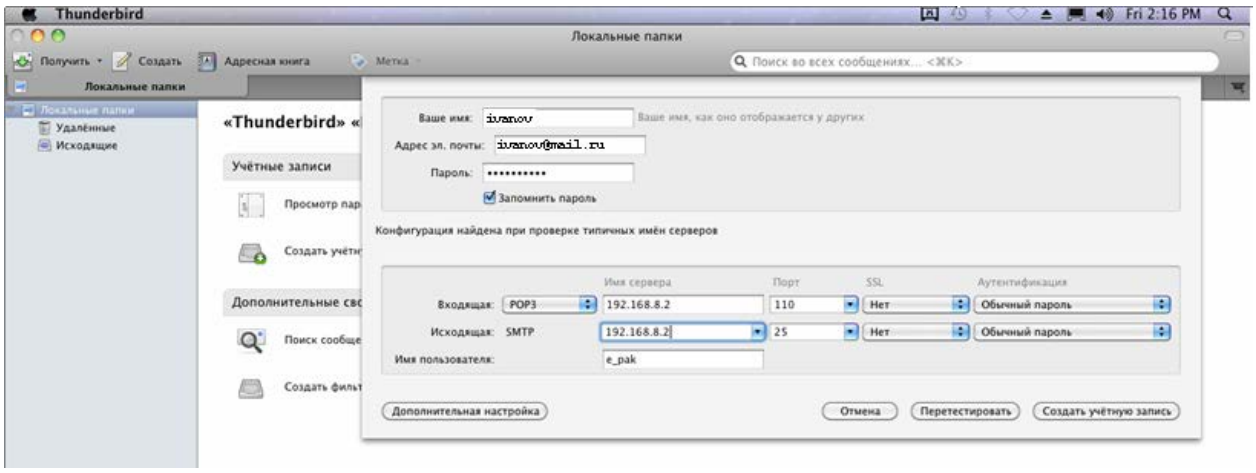
4. Ввести данные в форму и нажать на кнопку **Продолжить**.



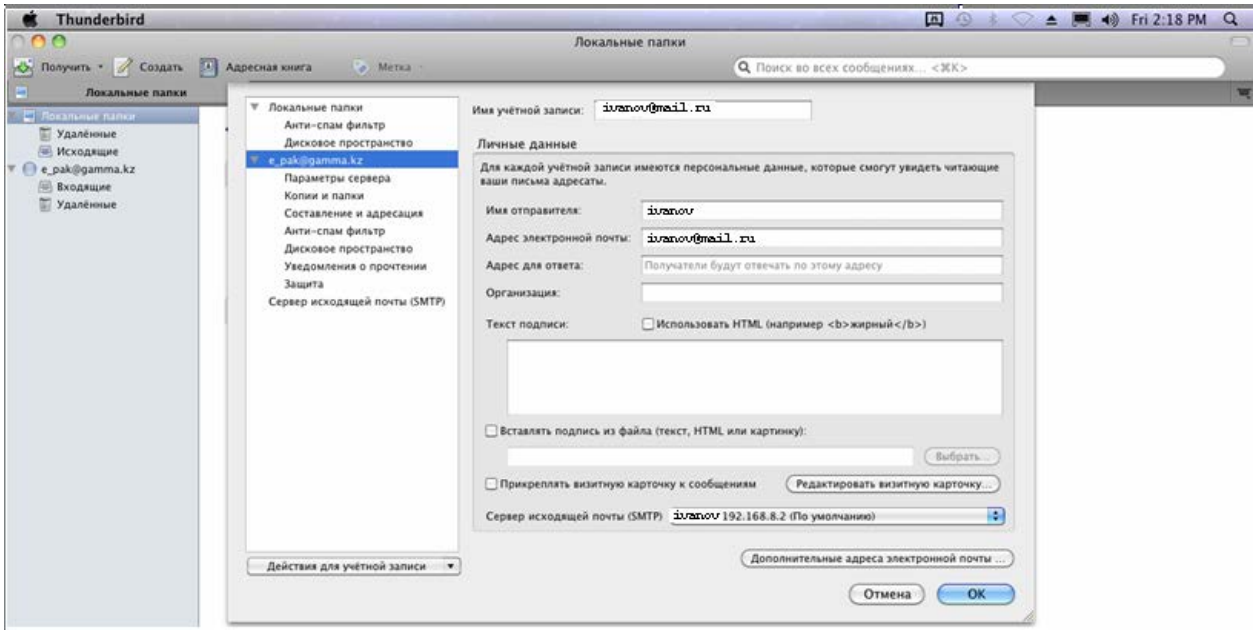
5. Нажать на кнопку **Настройка вручную**.



6. В открывшейся форме ввести требуемые настройки:



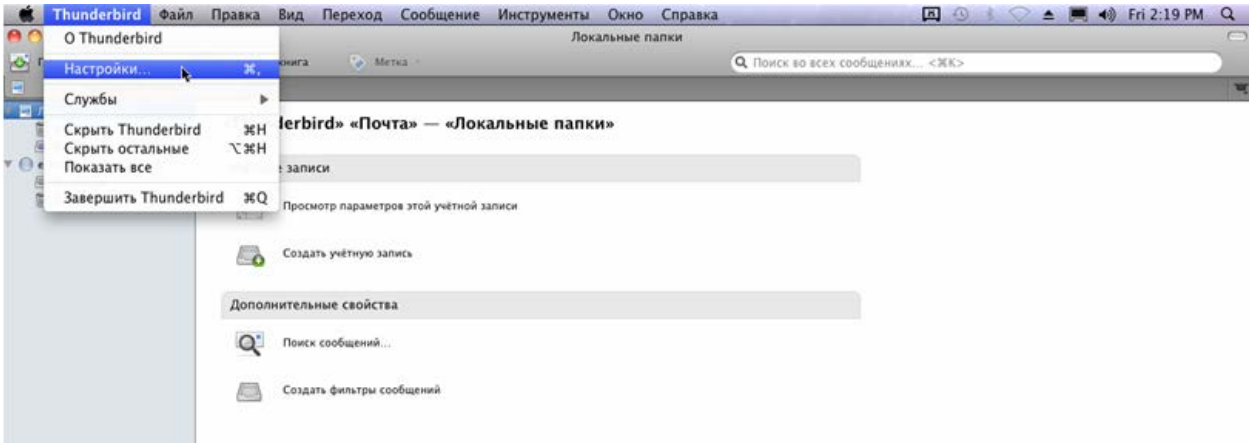
7. При необходимости нажать на кнопку **Дополнительная настройка** для ввода дополнительных настроек.



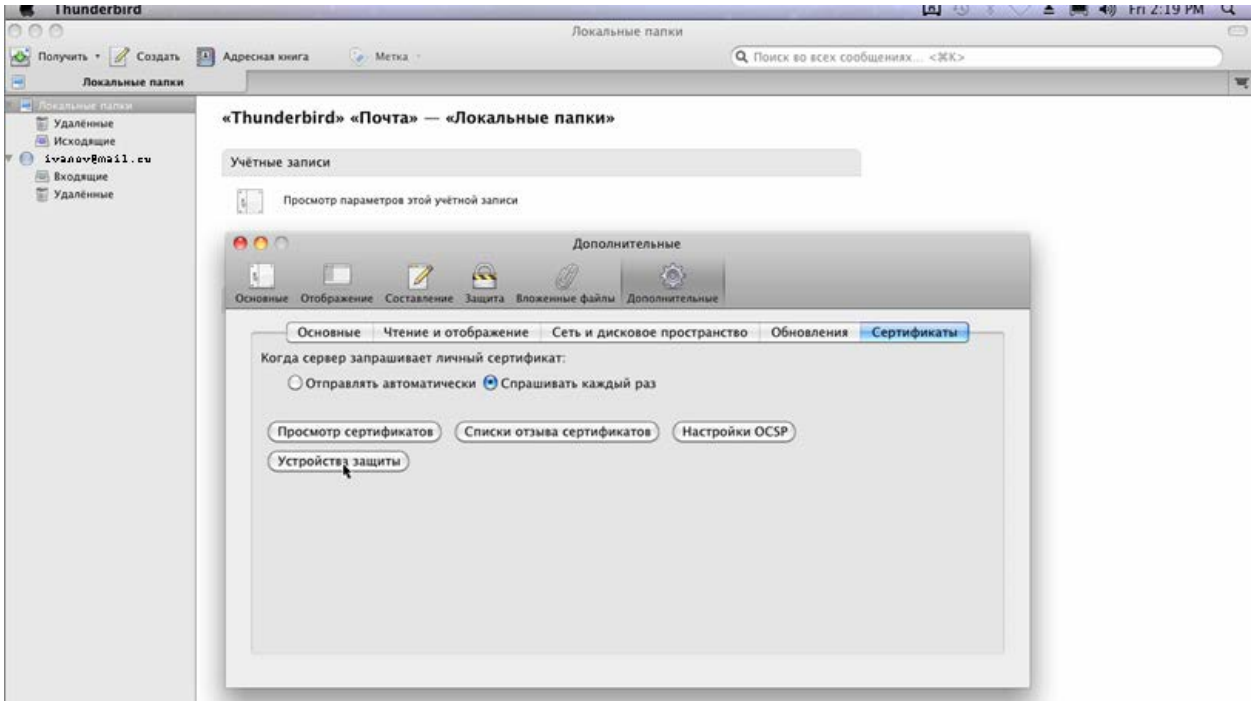
8. Для завершения настроек нажать на кнопку **ОК**.

3.2 Настройка ПО Mozilla Thunderbird для работы с криптографией

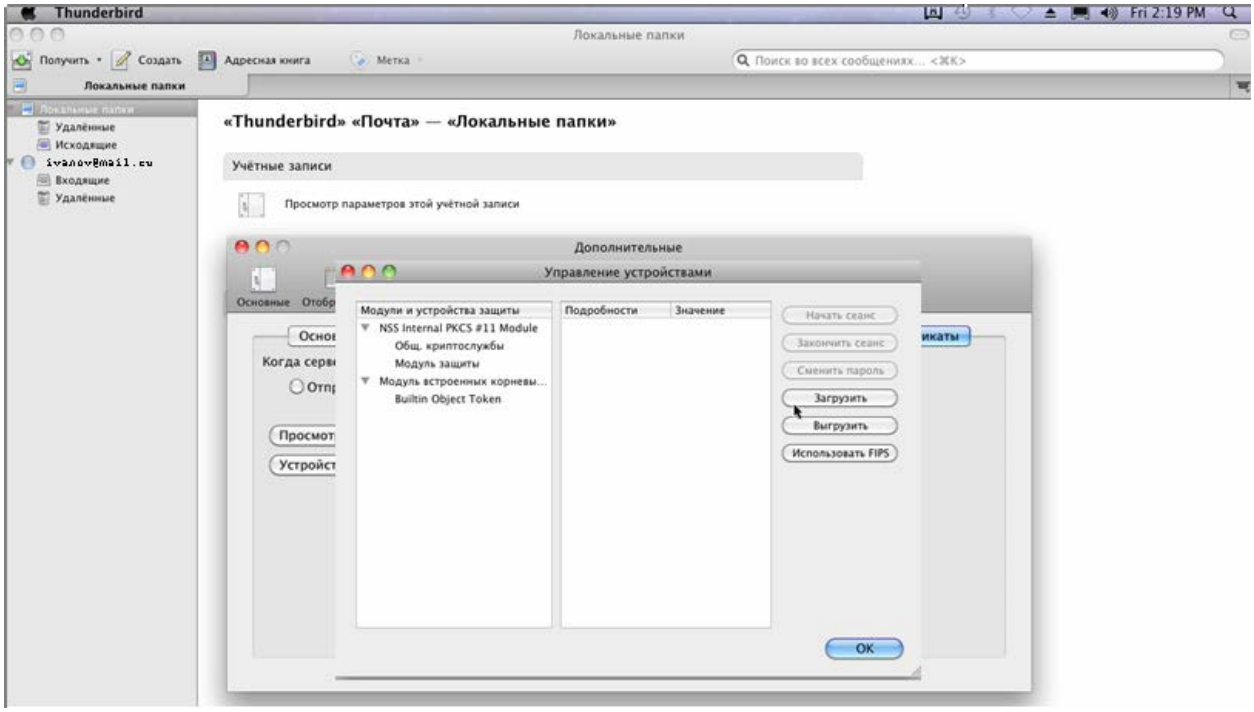
1. В главном меню программы перейти в **Инструменты→Настройки** для настроек криптографии.



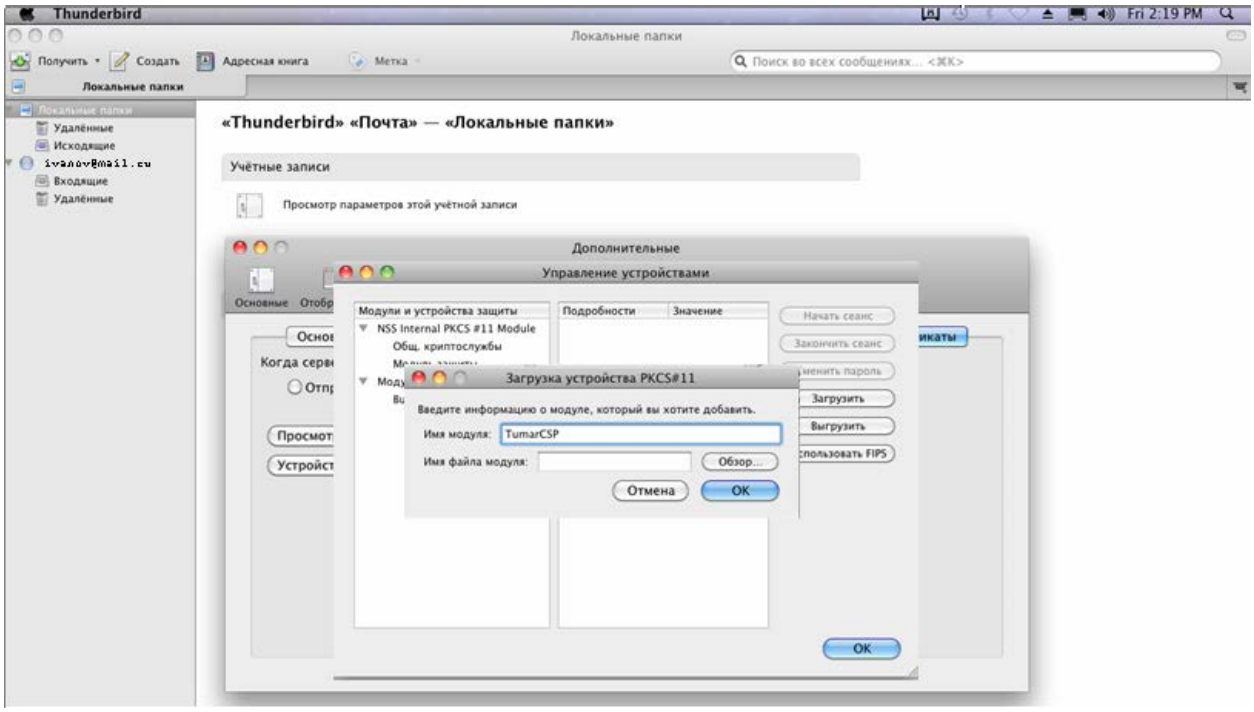
2. В окне *Настройки* выбрать закладку **Дополнительные→Сертификаты→ Устройства защиты**.

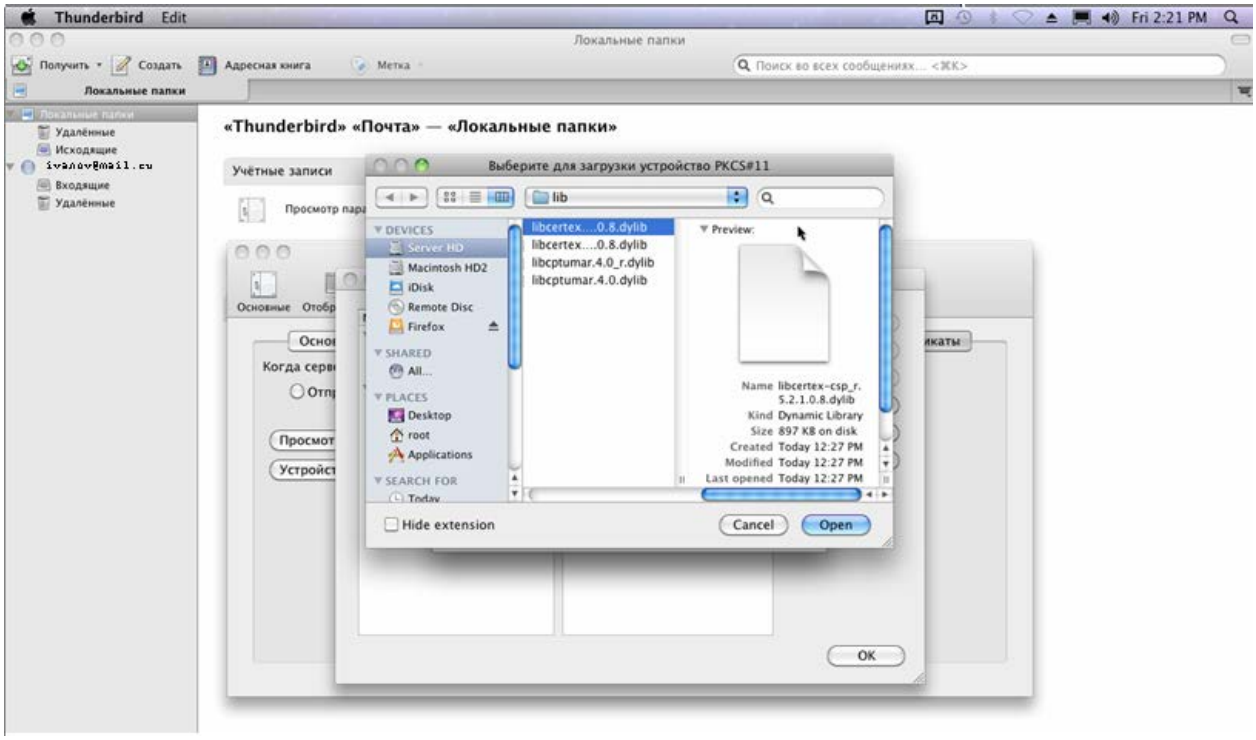


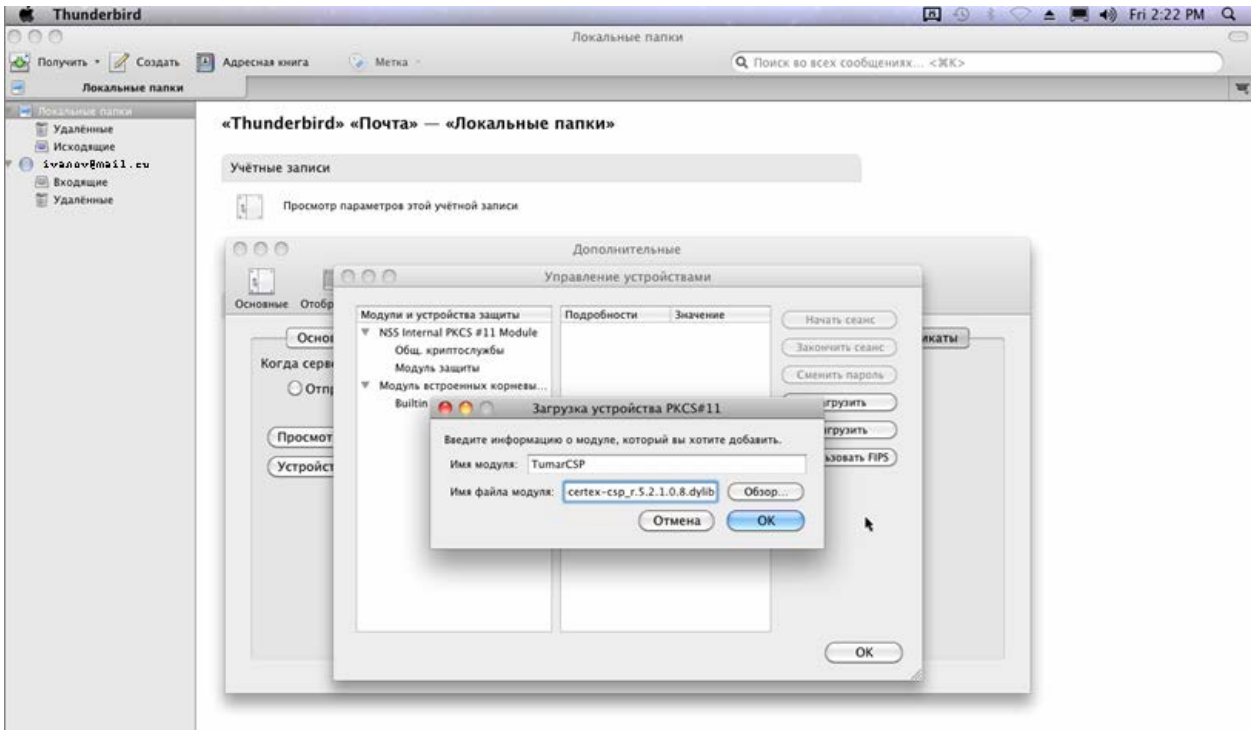
3. В окне *Управление устройствами* нажать на кнопку **Загрузить**.



4. Убедиться, что открылось окно *Загрузка устройства PKCS#11*.
5. В окне *Загрузка устройства PKCS#11*:
   - вписать произвольное имя модуля (например, TumarCSP);
   - справа от поля *Имя файла модуля* нажать на кнопку **Обзор** и выбрать на файловой системе библиотеку **libcertex-csp.5.2.x.x.x.dylib** или **libcertex-csp_r.5.2.x.x.x.dylib,** где x.x.x – версия релиза ПО;
   - нажать на кнопку **ОК**.

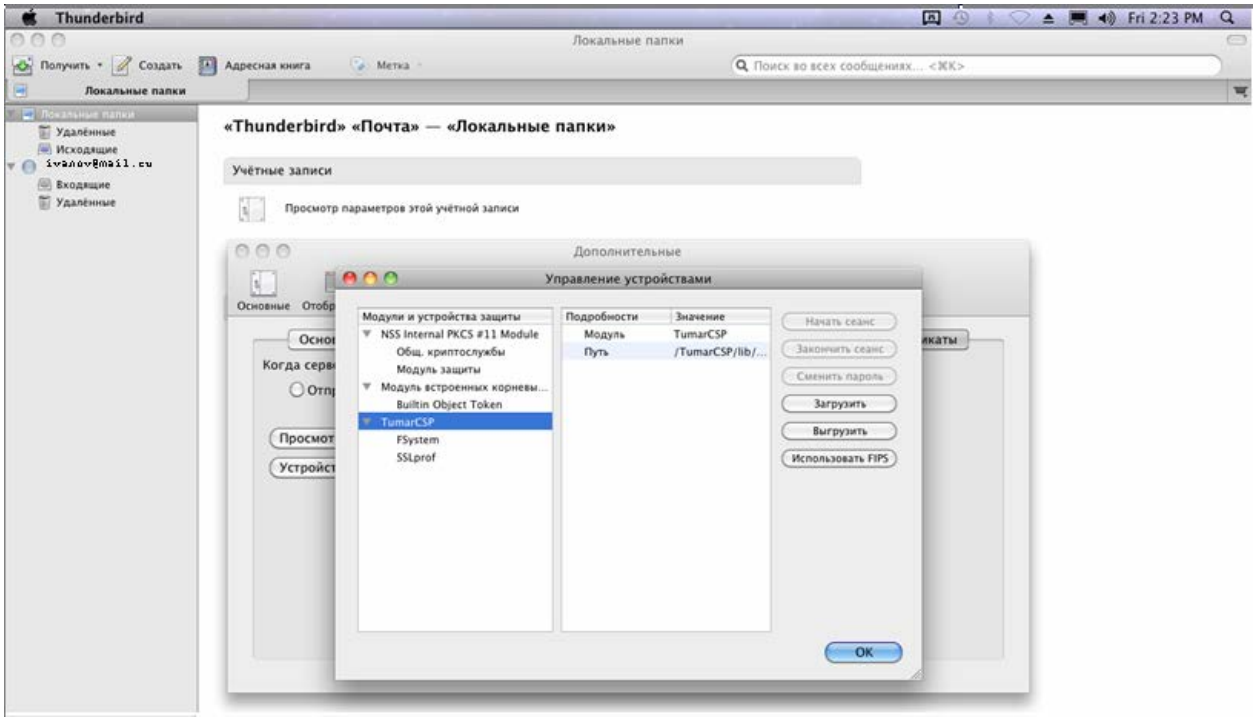




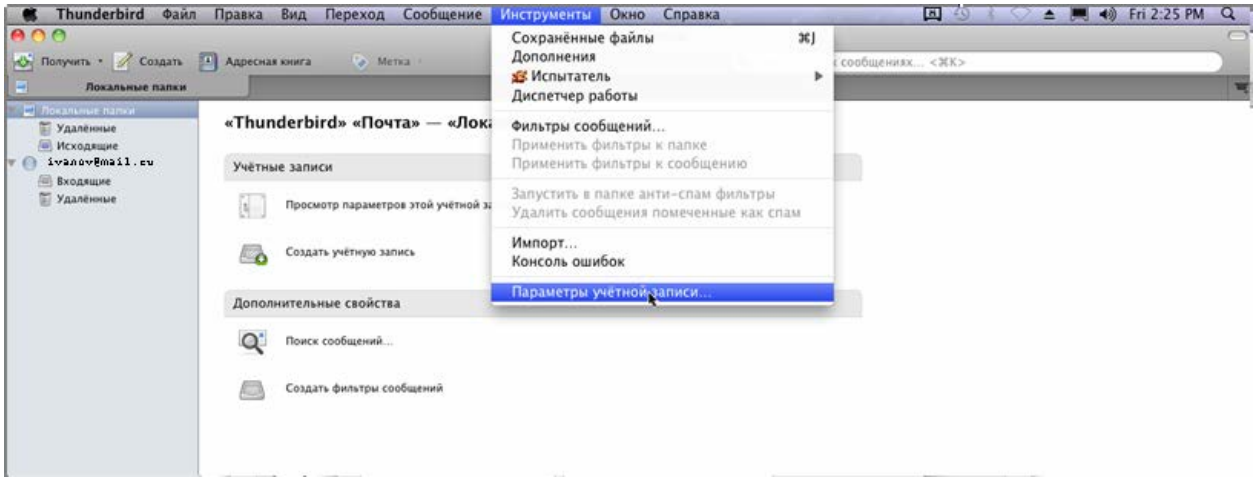


6. Убедиться, что в списке модулей и устройств защиты отображены все профайлы, настроенные на ключевую информацию – профайл **FSystem** и **SSLprof**.

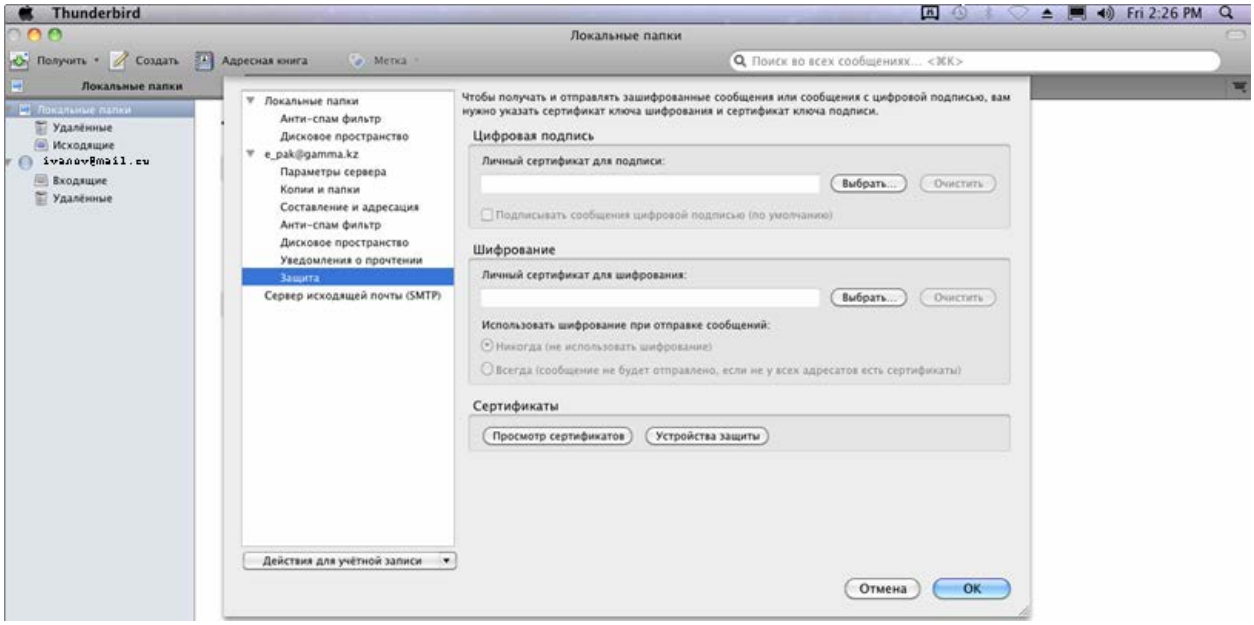
7. Нажать на кнопку **ОК**.



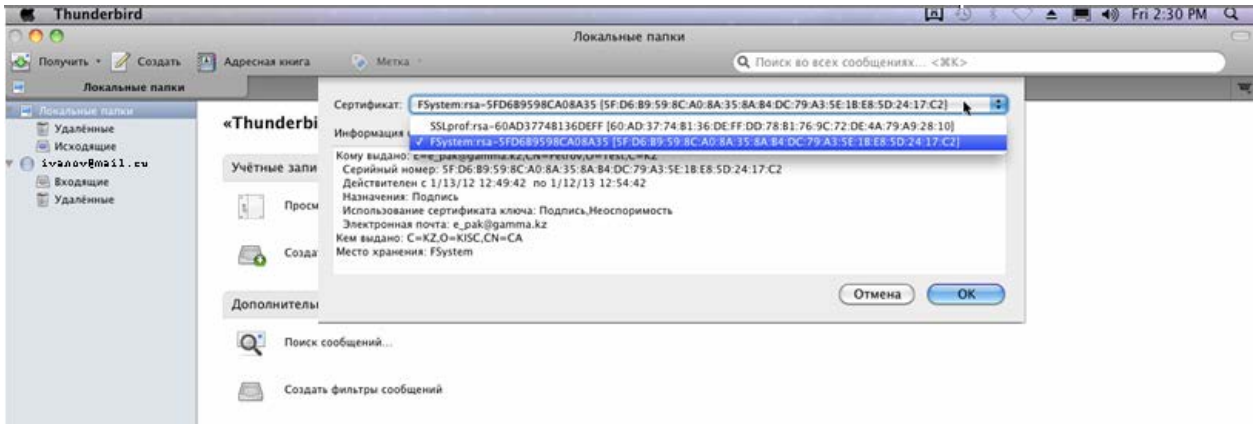
8. В главном меню выбрать **Инструменты →Параметры учетной записи…**



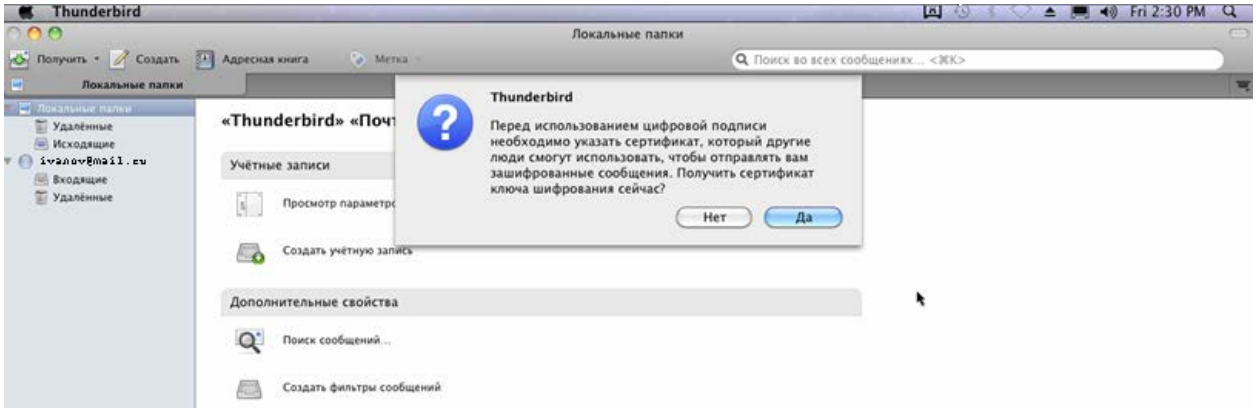
9. Перейти на закладку **Защита** и в поле **Личный сертификат для подписи** нажать на кнопку **Выбрать**.



10. В открывшемся окне выбрать из списка сертификат для подписи и нажать на кнопку **ОК**.



11. В сообщении системы для выбора сертификата для шифрования нажать на кнопку **Нет**.



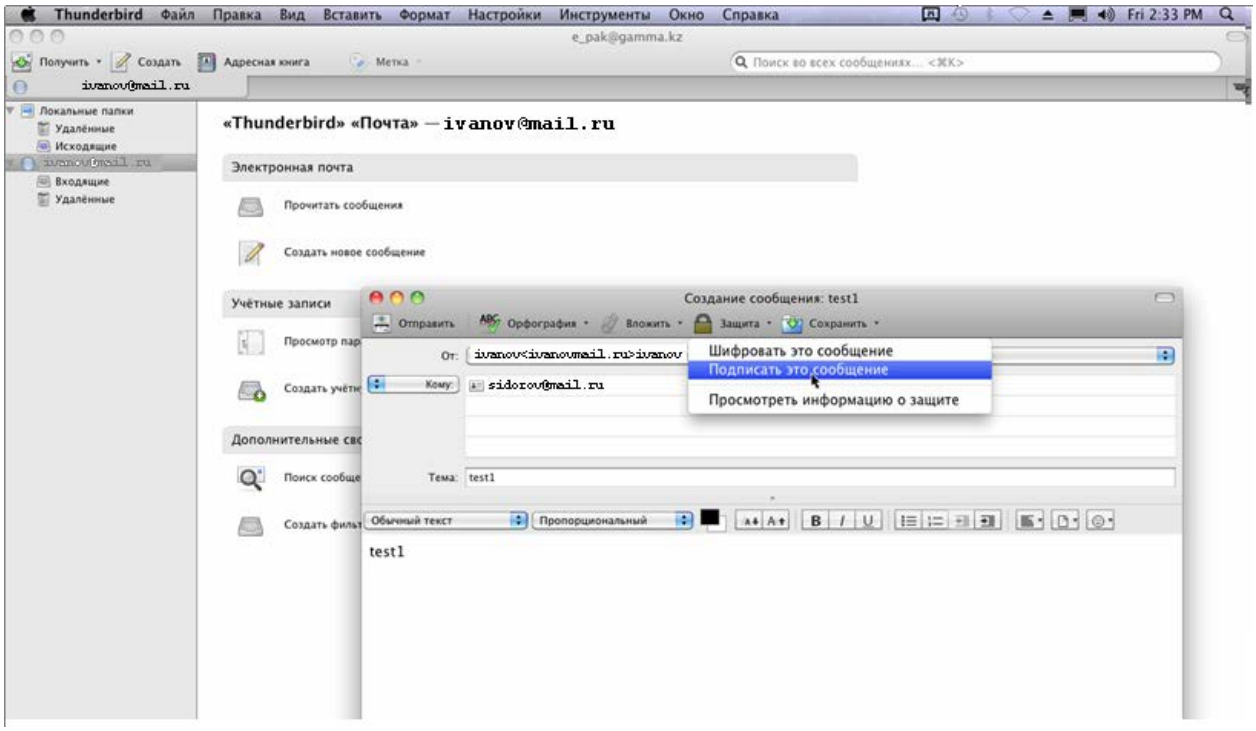
12. Для завершения настроек нажать на кнопку **ОК** в открывшемся окне:

13. Настройки криптографии выполнены.

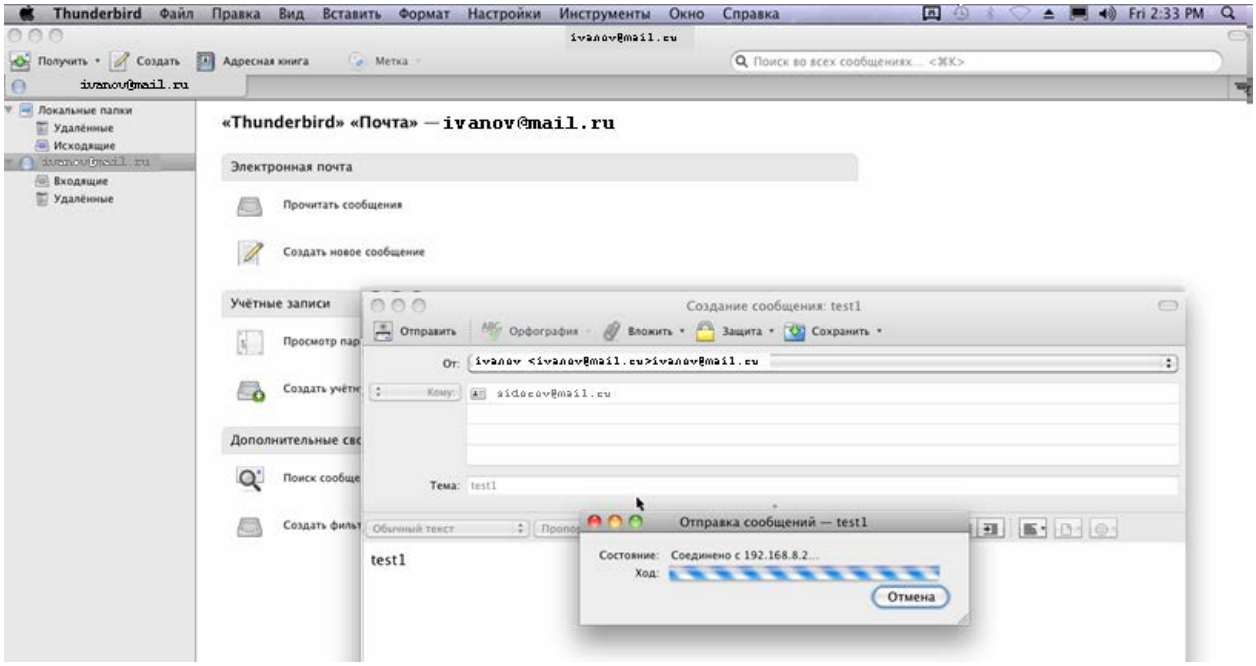
3.3 Получение и отправка подписанных сообщений в ПО Mozilla Thunderbird

Для отправки сообщений:

1. Запустить почтовую программу.
2. Создать сообщение.
3. В меню **Защита** выбрать строку **Подписать это сообщение**.

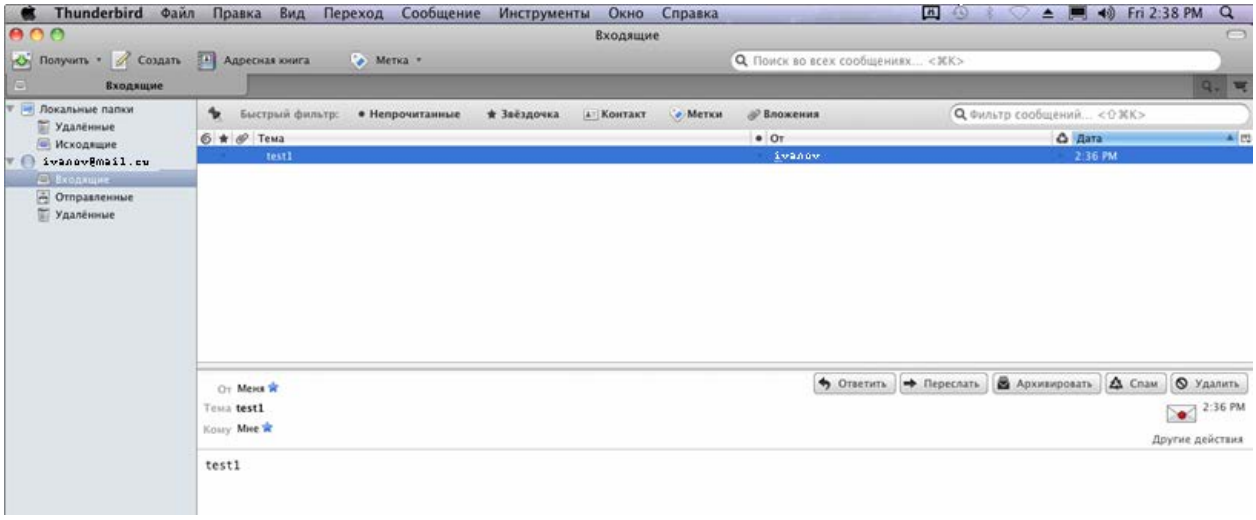


4. Дождаться отправки сообщения



Получение сообщений:

При получении подписанных сообщений с использованием ключей, к которым есть доверие, отобразится значок с сообщением .

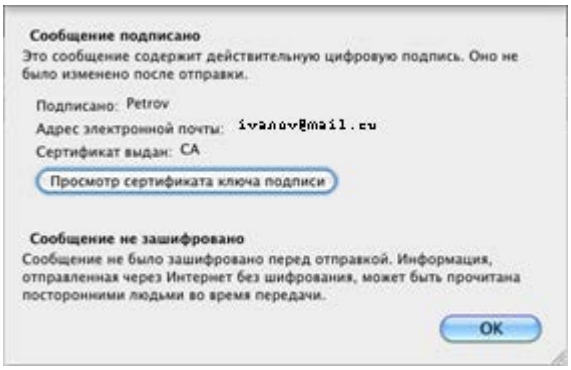


3.4.1 Проверка сообщений, подписанных доверенным сертификатом

При получении подписанных сообщений на ключах, к которым есть доверие, отобразится значок сообщения без крестика 

Для проверки подписи выполните следующие действия:

1. Нажмите на значок сообщения для отображения окна свойств подписи:
2. В открывшемся окне нажмите на кнопку **Просмотр сертификата ключа подписи**.



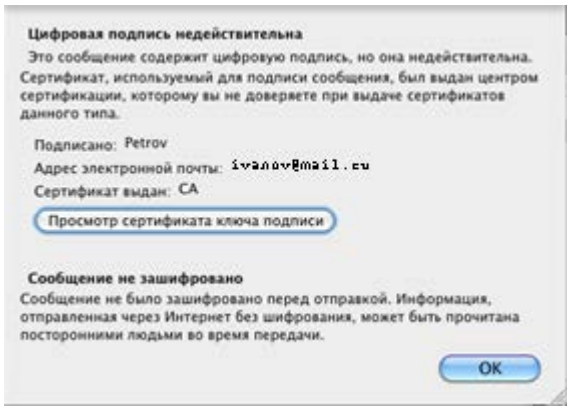
3. В поле *Основное* отображается информация об отправителе сообщения.

3.4.2 Получение и проверка сообщений, подписанных неизвестным сертификатом

При получении подписанных сообщений на ключах, к которым нет доверия, отобразится значок сообщения с крестиком 

Для проверки подписи выполните следующие действия:

1. Нажмите на значок  для отображения окна свойств подписи:



2. Для просмотра сертификата нажмите на кнопку **Просмотр сертификата ключа подписи**.

3. В поле *Основное* отображается информация об отправителе сообщения.