МойОфис

Почта 2

В ВАРИАНТЕ ИСПОЛНЕНИЯ ГОСТ

Руководство пользователя

НАСТОЛЬНОЕ ПРИЛОЖЕНИЕ

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«МОЙОФИС ПОЧТА 2»
В ВАРИАНТЕ ИСПОЛНЕНИЯ ГОСТ

НАСТОЛЬНОЕ ПРИЛОЖЕНИЕ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

2.8G

На 26 листах

Москва
2024

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам.

Товарные знаки «МойОфис» и «MyOffice» принадлежат ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем.

Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе используются следующие сокращения (см. Таблицу 1):

Таблица 1 - Сокращения и расшифровки

Сокращение	Расшифровка
ОС	Операционная система
ПО	Программное обеспечение
ПО МойОфис	Программное обеспечение «МойОфис Почта» с поддержкой криптографической защиты данных

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение

«МойОфис Почта 2» в варианте исполнения ГОСТ - корпоративная почтовая система для ведения деловой переписки, планирования рабочего времени и управлениями контактами в государственных организациях и на коммерческих предприятиях, использующих отечественные средства криптографической защиты информации. Продукт позволяет шифровать и расшифровывать сообщения, подписывать сообщения электронной подписью сообщений и проверять электронную подпись отправителей. Взаимодействие всех клиентских приложений с серверными системами осуществляется по сетевым каналам, защищенным с помощью протокола TLS с использованием отечественной криптографии.

В состав продукта входят:

- Серверное программное обеспечение для обработки входящих и исходящих сообщений электронной почты, совместной работы с календарями и задачами, а также ведения адресных книг;
- Административная панель почтовой системы для управления пользователями, ресурсами и их группами, списками рассылок, доменами и тенантами.

В состав продукта входят следующие приложения для работы на компьютерах, в веб-браузерах и на мобильных устройствах:

- Веб-приложение для быстрой и удобной работы с электронными сообщениями, календарями, задачами и адресными книгами;
- Настольный почтовый клиент для работы с электронными сообщениями, календарями, задачами и адресными книгами на операционных системах Linux, Windows и macOS ;
- Мобильные почтовые приложения для работы с корпоративной почтовой системой МойОфис на смартфонах и планшетах с операционными системами Android и iOS.
- Мобильные приложения «МойОфис Фокус» для управления рабочими задачами, организации встреч и синхронизации календарей на мобильных устройствах в организациях, использующих отечественные средства обеспечения информационной безопасности на смартфонах и планшетах с операционными системами Android и iOS.

Подробное описание возможностей продукта приведено в документе «МойОфис Почта 2 в варианте исполнения ГОСТ. Функциональные возможности».

В данном документе рассматривается только функционал настольных приложений «МойОфис Почта», связанный с использованием средств криптографической защиты информации.

1.2 Системные требования

Перечень требований к программному и аппаратному обеспечению приведен в документе «МойОфис Почта 2 в варианте исполнения ГОСТ. Системные требования».

1.3 Ограничения

Перечень программного и аппаратного обеспечения, требуемого для доступа к настольным приложениям ПО МойОфис, указан в документе «МойОфис Почта 2 в варианте исполнения ГОСТ. Системные требования».

Поддерживаемые языки интерфейса:

- русский;
- английский;
- испанский;
- португальский;
- французский.

2 ПОДГОТОВКА К РАБОТЕ

Работа с приложениями ПО МойОфис с поддержкой криптографической защиты данных осуществляется при помощи программного обеспечения «КриптоПро CSP».

Для работы с приложениями ПО МойОфис с поддержкой криптографической защиты данных необходимо наличие серверной лицензии «КриптоПро CSP», а также действительный сертификат для каждой учетной записи, работающей с криптографической защитой данных.

В составе поставки ПО «МойОфис Почта» с поддержкой криптографической защиты данных доступны следующие дистрибутивы для самостоятельной установки настольного приложения «МойОфис Почта» (см. Таблицу 2).

Таблица 2 - Дистрибутивы настольных приложений

ОС	Файлы дистрибутива
Windows	MyOffice_Mail_PSN_Windows_2.8G.msi MyOffice_Mail_PSN_Windows_eng_2.8G.exe MyOffice_Mail_PSN_Windows_ru_2.8G.exe
Linux	MyOffice_Mail_PSN_Linux_2.8G.sh myofficemail-2.8G.x86_64.rpm
macOS	MyOffice_Mail_PSN_MacOS_2.8G.dmg

Для подготовки к работе с настольным приложением «МойОфис Почта» необходимо выполнить следующие шаги:

1. Проверить выполнение системных требований и, при необходимости, обратиться к системному администратору.
2. Установить и настроить следующее программное обеспечение в соответствии с инструкцией производителя (ООО "КРИПТО-ПРО"):
   - КриптоПро CSP (поддерживаемую версию согласно системным требованиям);
   - Библиотеку КриптоПро PKCS#11.
3. Если подготовка к работе с приложением «МойОфис Почта» осуществляется на ОС Windows, в `registry` необходимо сделать следующие изменения: в ветке `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CryptoPro\Cryptography\CurrentVersion\PKCS11\slot0` (для 64-разрядной ОС) или `HKEY_LOCAL_MACHINE\SOFTWARE\Crypto`

`Pro\Cryptography\CurrentVersion\PKCS11\slot0` (для 32-разрядной ОС) создать строковый параметр с именем **Firefox**, не меняя остальные значения.

4. Установить приложение «МойОфис Почта» так, как это описано в соответствующих разделах документа «МойОфис Почта, Настольные приложения. Руководство по установке».
5. Запустить приложение и ввести данные той учетной записи, от имени которой будет осуществляться работа на текущем компьютере.
6. Добавить личный сертификат авторизованного пользователя так, как это описано в разделе Добавить сертификат.

Приложение «МойОфис Почта» для ОС Windows считается установленным, если в результате действий, изложенных в разделе 2.2 документа «Почта 2. Руководство по установке настольного приложения», на рабочем столе пользователя и в главном меню ОС отображается ярлык (см. Рисунок 1), при активации которого приложение корректно открывается без выдачи сообщений о сбое в работе.

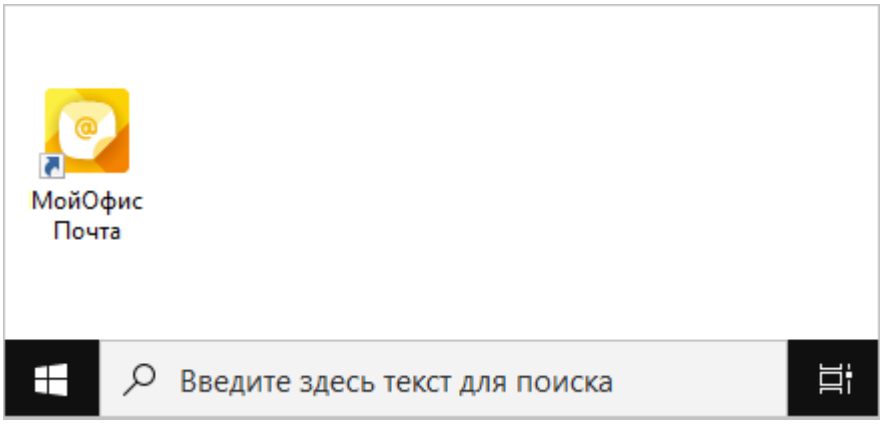

Рисунок 1 – Ярлык «МойОфис Почта» на рабочем столе ОС Windows

Приложение «МойОфис Почта» для ОС Linux считается установленным, если в результате действий, изложенных в разделе 2.3 документа «Почта 2. Руководство по установке настольного приложения», в меню приложений ОС отображается ярлык (см. Рисунок 2), при активации которого приложение корректно открывается без выдачи сообщений о сбое в работе.

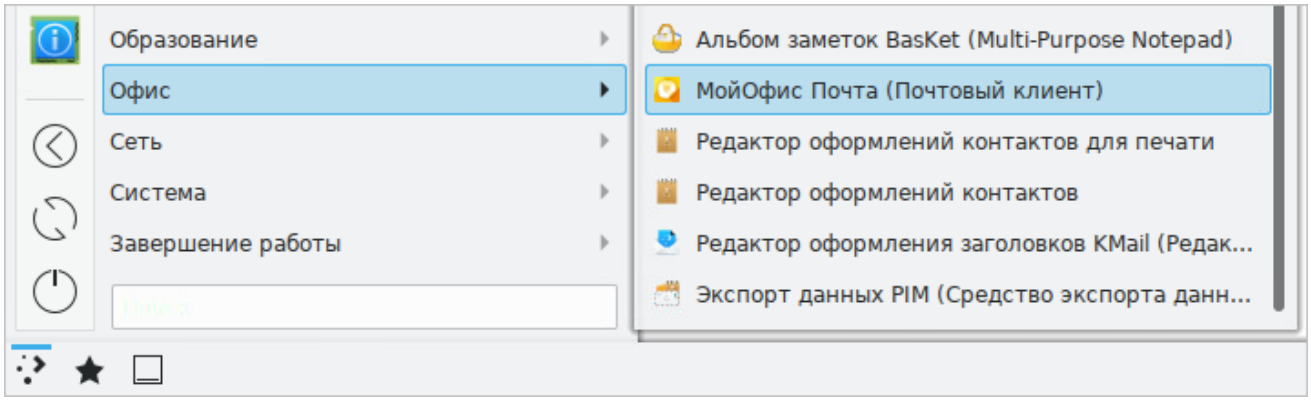

Рисунок 2 – Ярлык «МойОфис Почта» в меню приложений ОС Linux

Приложение «МойОфис Почта» для macOS считается установленным, если в результате действий, изложенных в разделе 2.4 документа «Почта 2. Руководство по установке настольного приложения», в окне **Программы** отображается ярлык (см. Рисунок 3), при активации которого приложение корректно открывается без выдачи сообщений о сбое в работе.

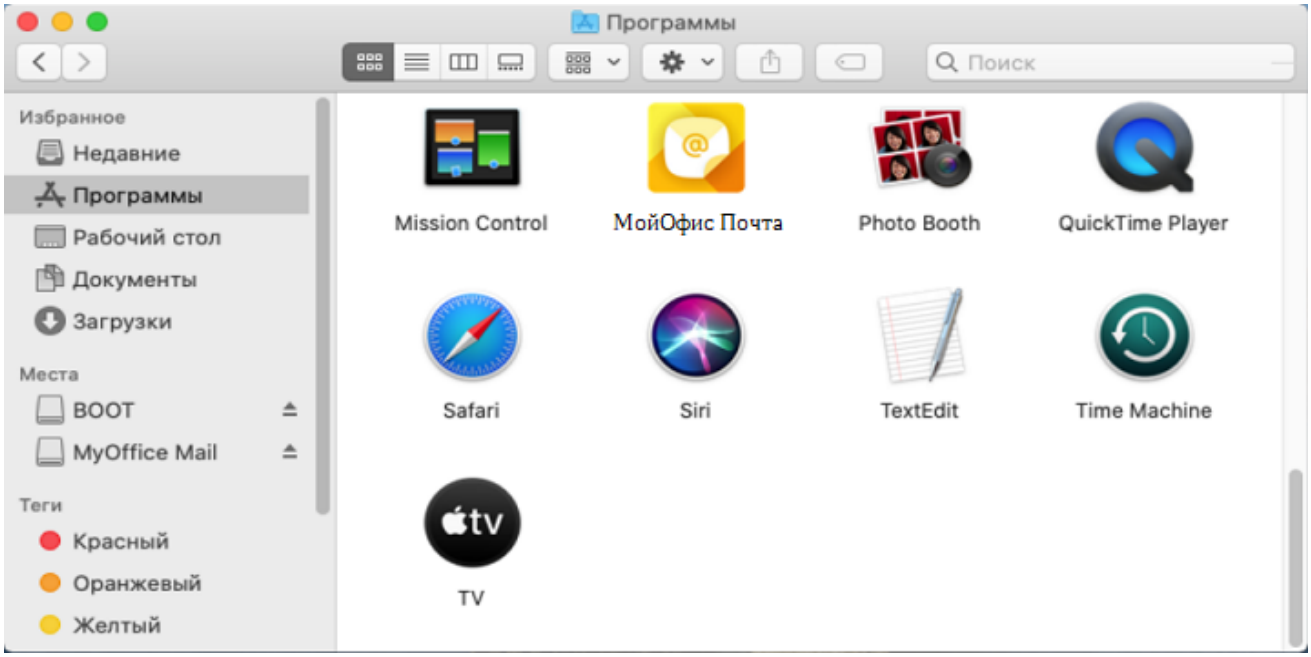

Рисунок 3 – Ярлык «МойОфис Почта» в меню приложений macOS

Для запуска приложения «МойОфис Почта» необходимо щелкнуть по его ярлыку на рабочем столе или в главном меню/меню приложений ОС.

3 СЕРТИФИКАТ БЕЗОПАСНОСТИ

3.1 Добавление сертификата безопасности

Чтобы добавить сертификат безопасности, выполните следующие действия:

1. На панели папок выделите имя учетной записи (см. Рисунок 4). На странице учетной записи выберите пункт **Шифрование**.

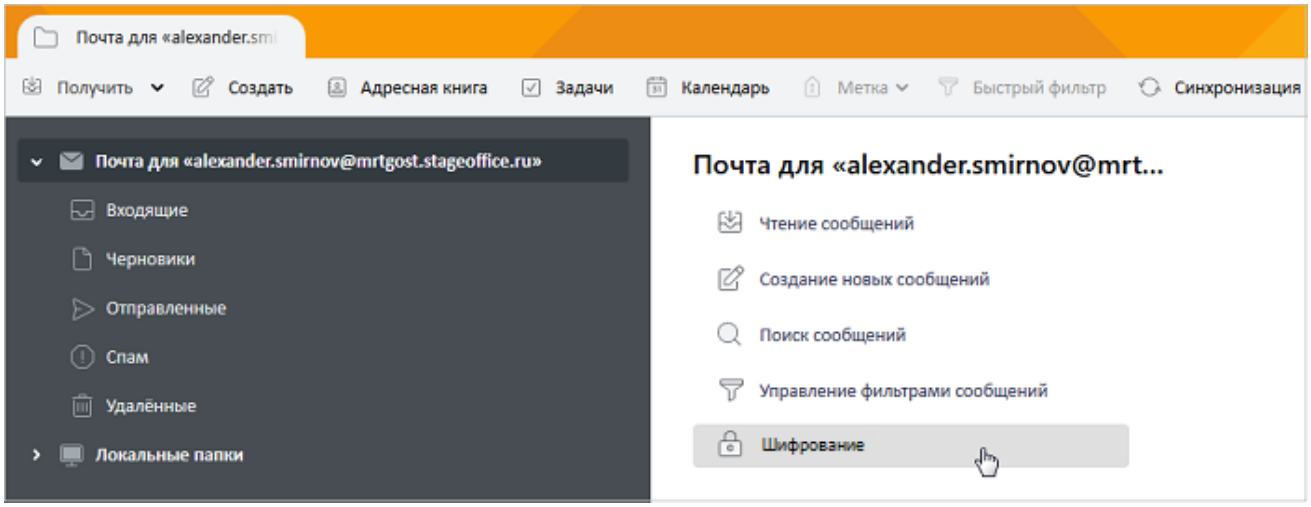

Рисунок 4 – Страница учетной записи

2. Во вкладке **Параметры учетной записи** (см. Рисунок 5) нажмите кнопку **Устройства защиты S/MIME**.

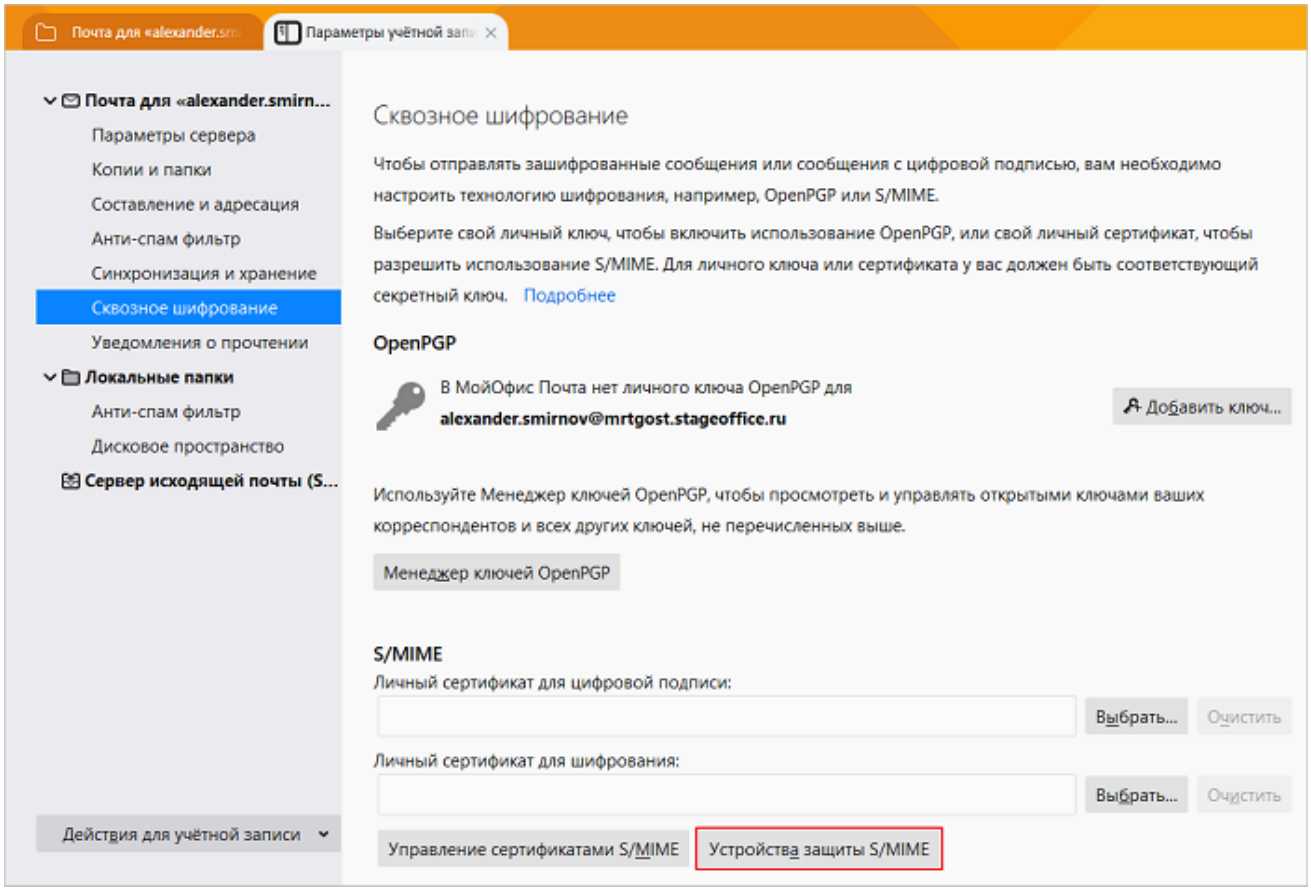

Рисунок 5 – Вкладка **Параметры учетной записи**

3. В окне **Управление устройствами** (см. Рисунок 6) нажмите кнопку **Загрузить**.

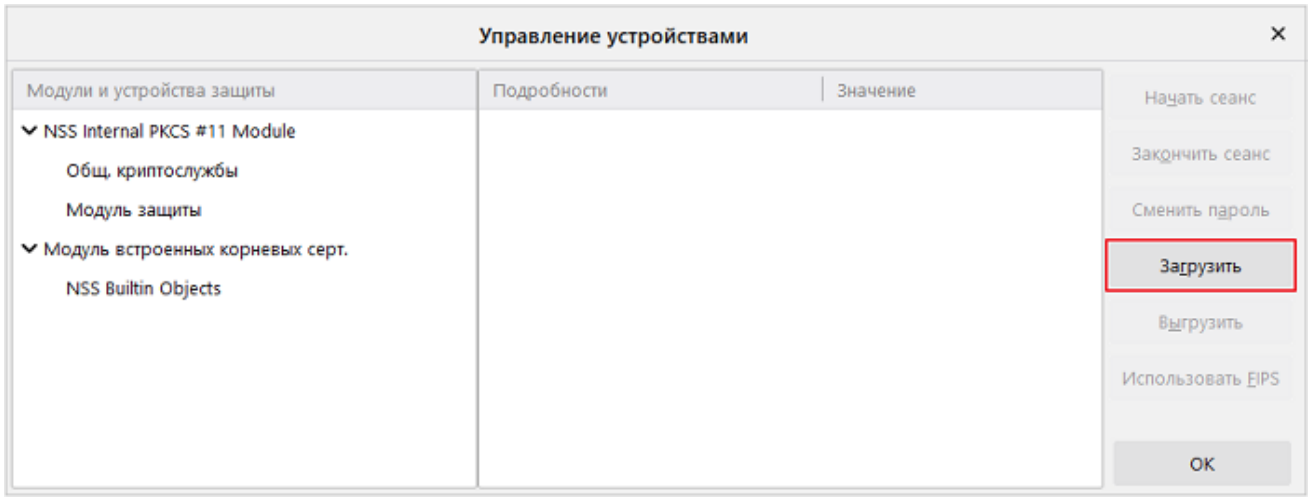

Рисунок 6 – Окно **Управление устройствами**

4. В окне **Загрузить драйвер устройства PKCS** (см. Рисунок 7), в поле **Имя модуля** укажите имя модуля. Например, **CryptoPro11**.

Нажмите кнопку **Обзор**. В ОС Windows укажите путь к библиотеке **C:\Program Files\Crypto Pro\CSP\cppkcs11.dll**, в ОС Linux укажите путь к библиотеке **opt\cprocsp\lib\amd64\libcppkcs11.so**. Указанный путь отобразится в поле **Имя файла модуля**.

5. Нажмите кнопку **ОК**.

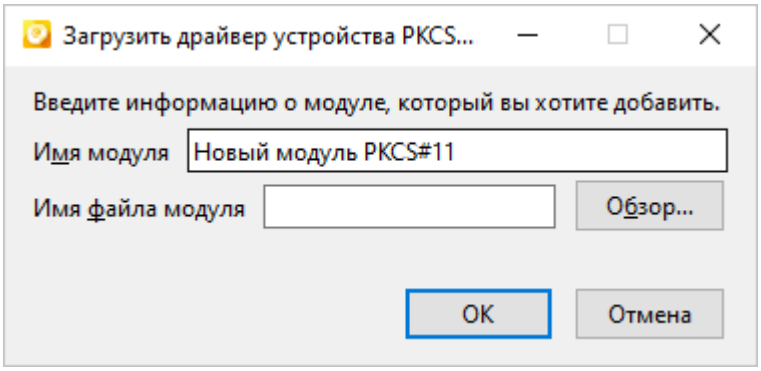

Рисунок 7 – Окно **Загрузить драйвер устройства PKCS**

6. В окне **Управление устройствами** отобразятся данные модуля (см. Рисунок 8). Нажмите кнопку **ОК**.

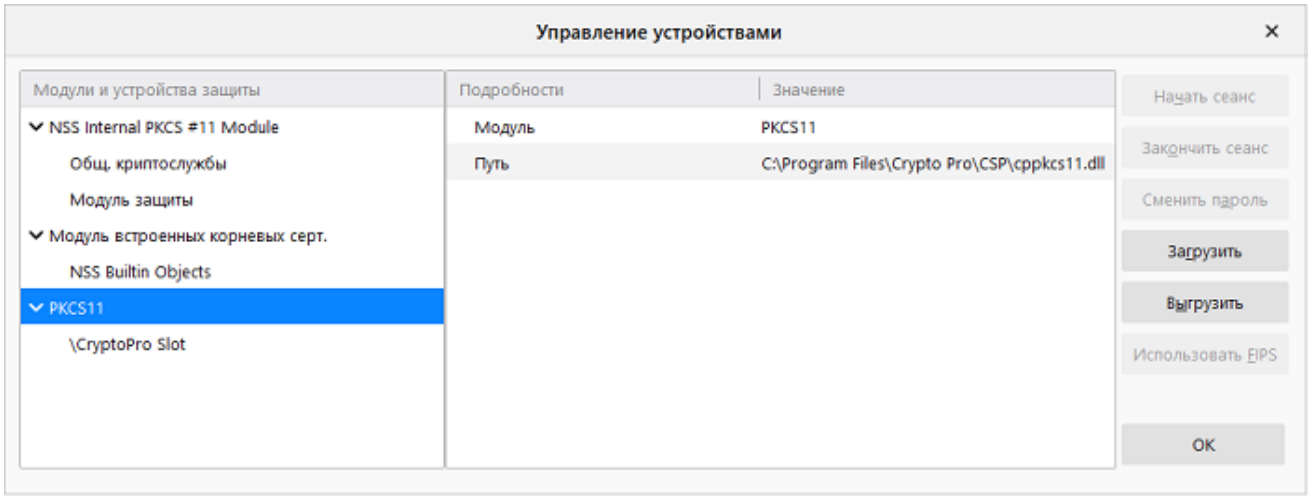

Рисунок 8 – Данные модуля

7. Во вкладке **Параметры учетной записи** (см. Рисунок 9) нажмите кнопку **Управление сертификатами S/MIME**.

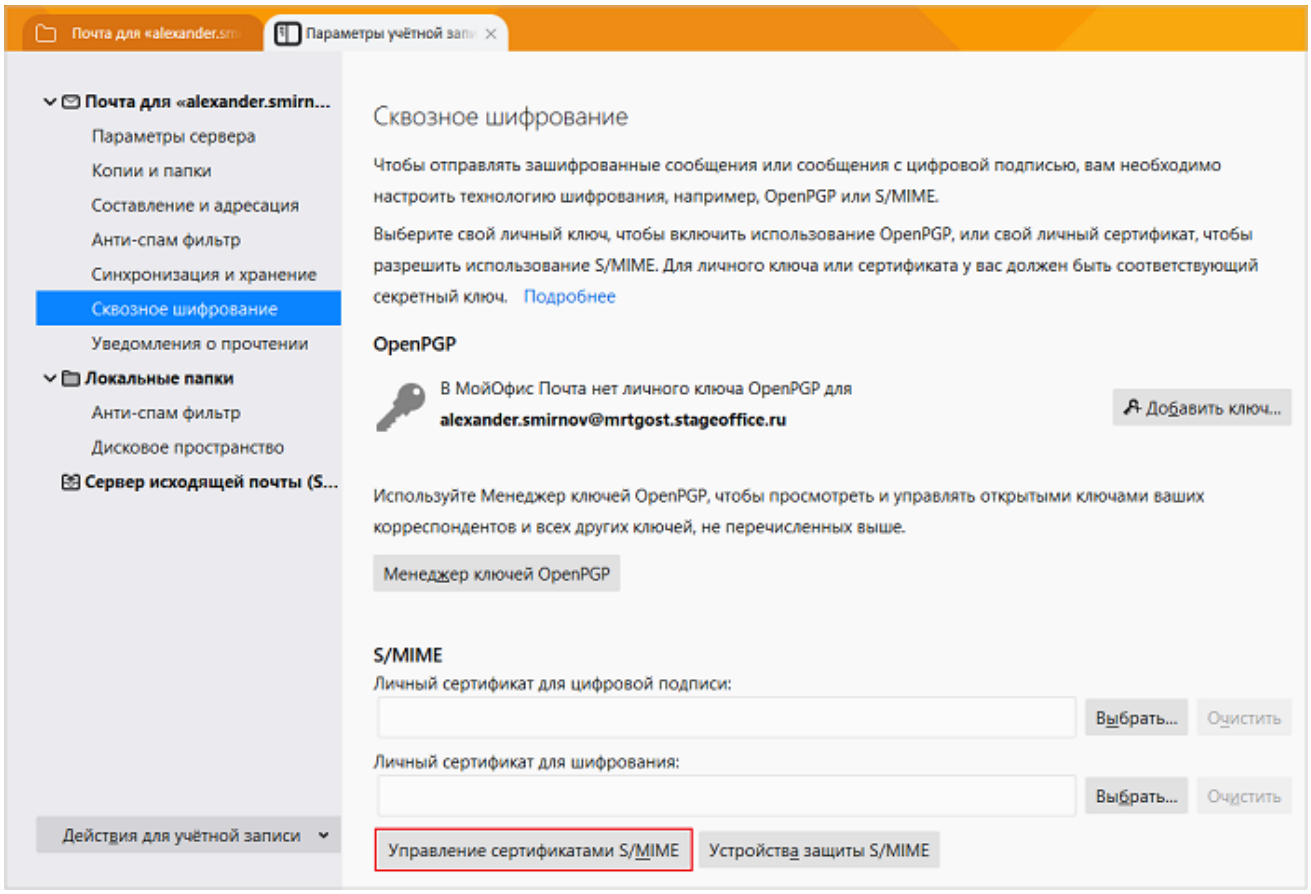

Рисунок 9 – Вкладка **Параметры учетной записи**

8. В окне **Управление сертификатами** выберите вкладку **Центры сертификации** (см. Рисунок 10).
9. Выполните следующие действия для каждого сертификата «КриптоПро», который содержится в списке:

   – Выделите имя сертификата и нажмите кнопку **Изменить доверие**.

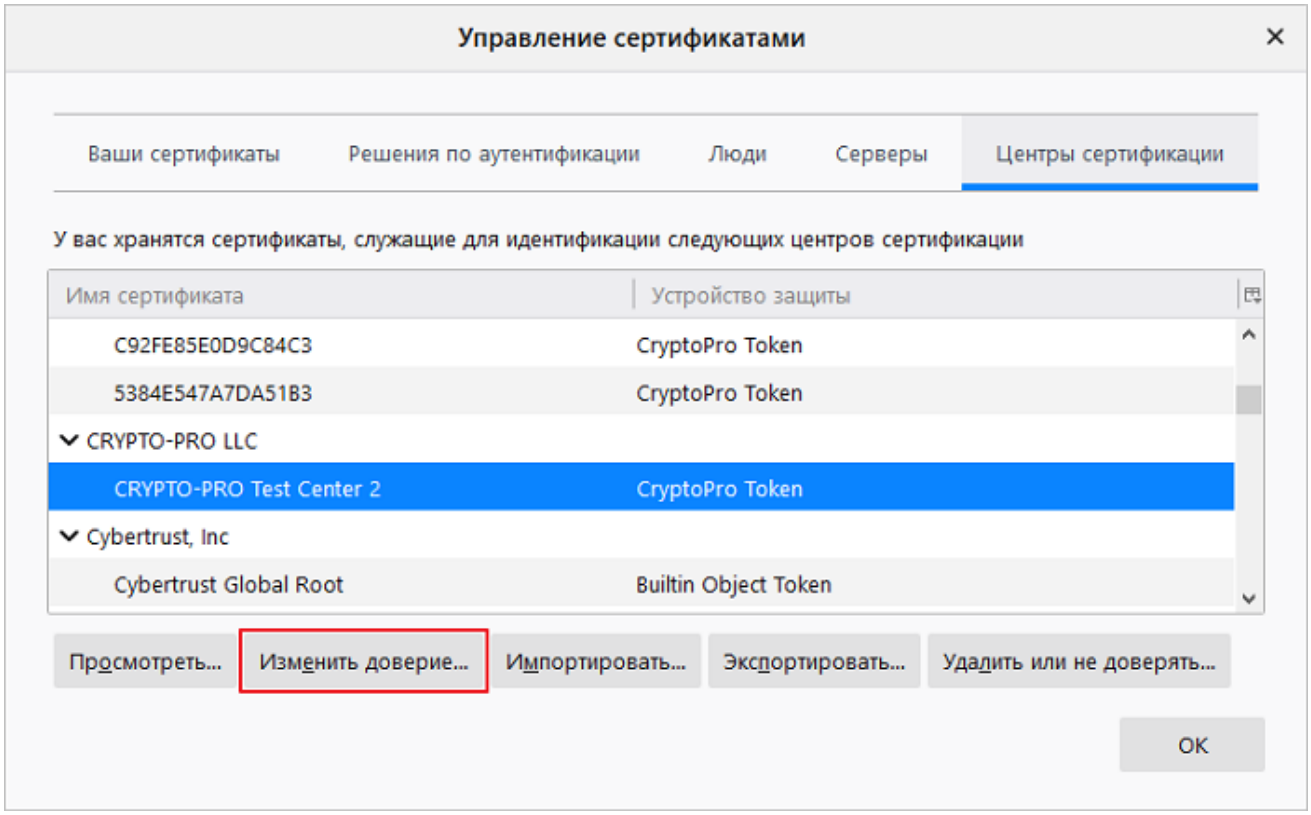

Рисунок 10 – Окно **Управление сертификатами**

– В окне **Изменение степени доверия сертификату CA** (см. Рисунок 11) поставьте флажок **Этот сертификат может служить для идентификации пользователей электронной почты** и нажмите кнопку **ОК**.

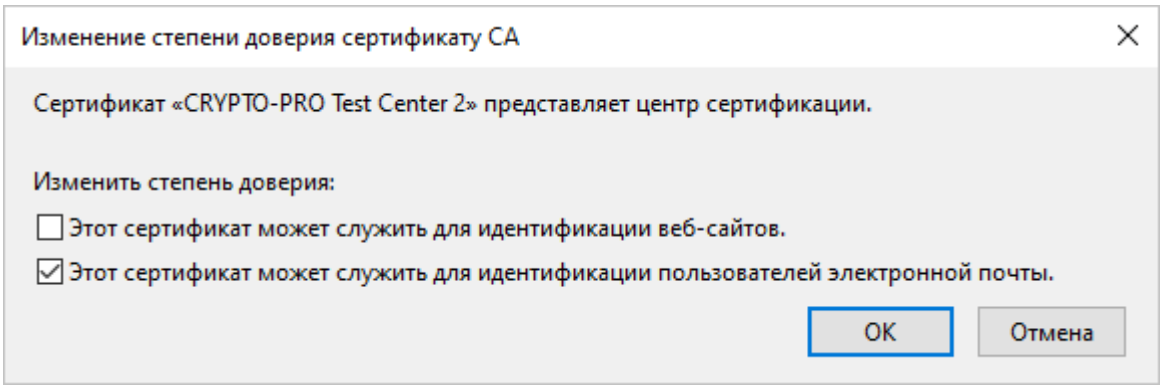

Рисунок 11 – Окно **Изменение степени доверия сертификату CA**

10. В окне **Управление сертификатами** (см. Рисунок 10) нажмите кнопку **ОК**.
11. Во вкладке **Параметры учетной записи** нажмите на кнопку **Выбрать** справа от поля **Личный сертификат для цифровой подписи** (см. Рисунок 12).

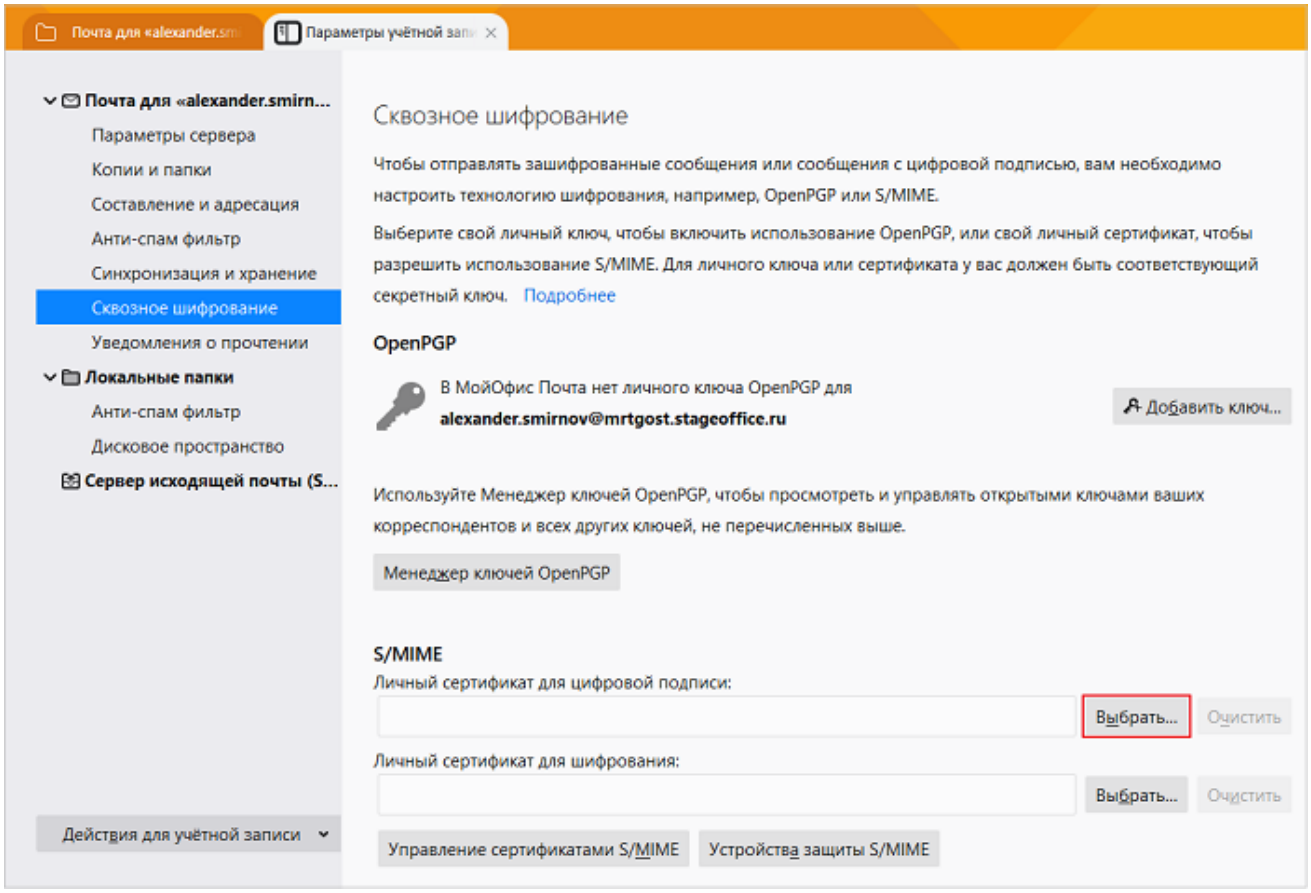

Рисунок 12 – Вкладка **Параметры учетной записи**

12. Убедитесь, что в окне **Выбор сертификата**, в поле **Сертификат** выбран личный сертификат авторизованного пользователя и нажмите кнопку **ОК** (см. Рисунок 13).

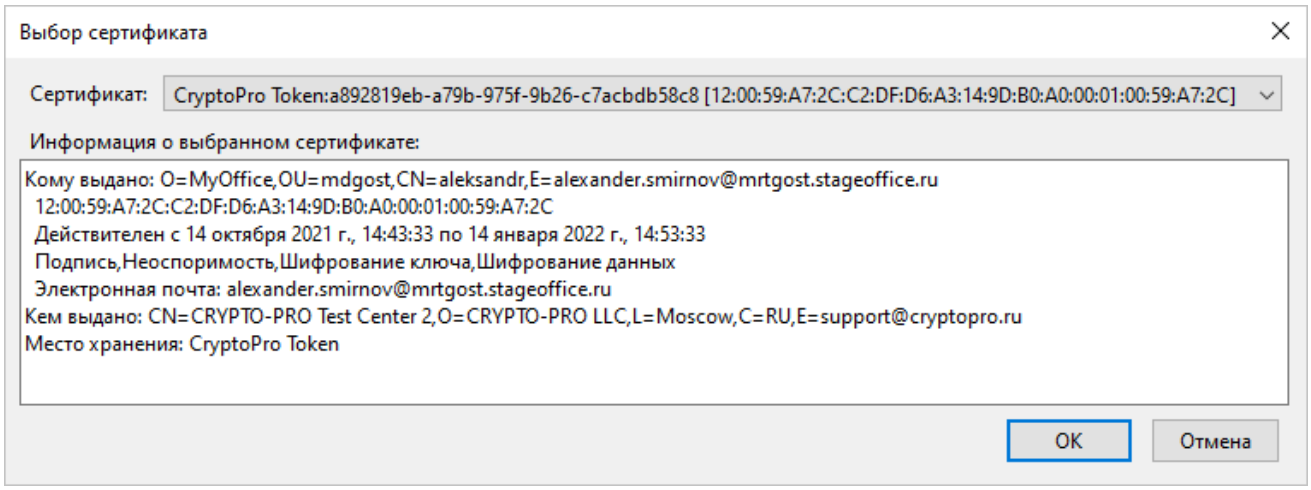

Рисунок 13 – Окно **Выбор сертификата**

13.В диалоговом окне, представленном на Рисунке 14, нажмите кнопку **Да**.

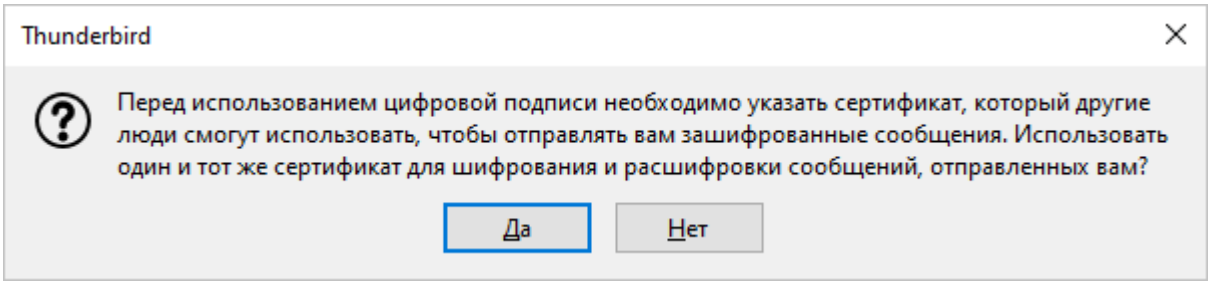

Рисунок 14 – Диалоговое окно

Выбранный сертификат отобразится в полях **Личный сертификат для цифровой подписи** и **Личный сертификат для шифрования** (см. Рисунок 15).

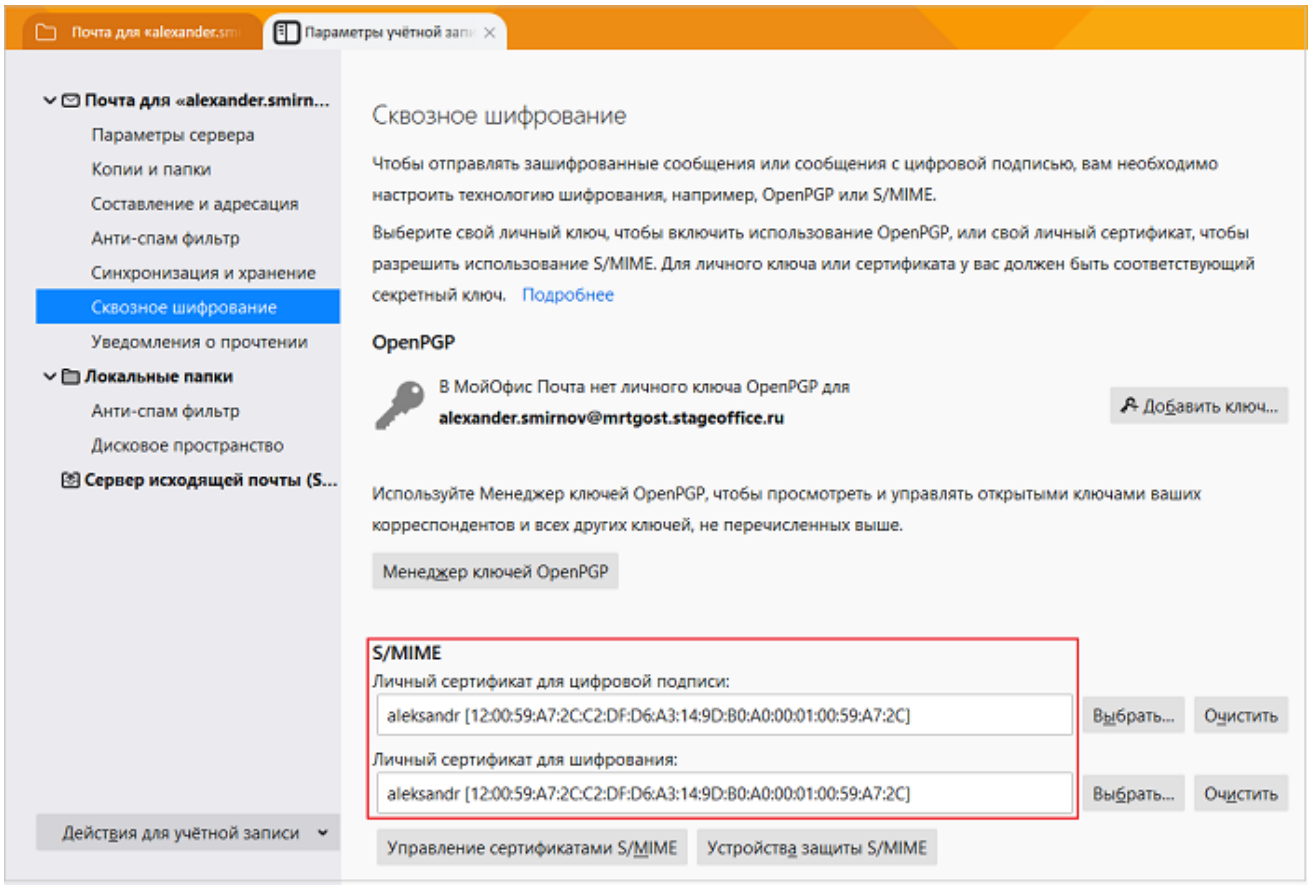

Рисунок 15 – Сертификат для цифровой подписи и шифрования

4 РАБОТА С ПИСЬМАМИ

4.1 Отображение списка писем

Подписанные и/или зашифрованные сообщения содержат индикацию в окне просмотра полученного сообщения (см. Рисунок 16):

– тип шифрования **S/MIME** или **OpenPGP**;

– – письмо зашифровано;

– – письмо подписано;

– – ошибка шифрования;

– – ошибка подписи.

В случае возникновения проблем (например, просроченный сертификат) символы шифрования или подписи будут перечеркнуты

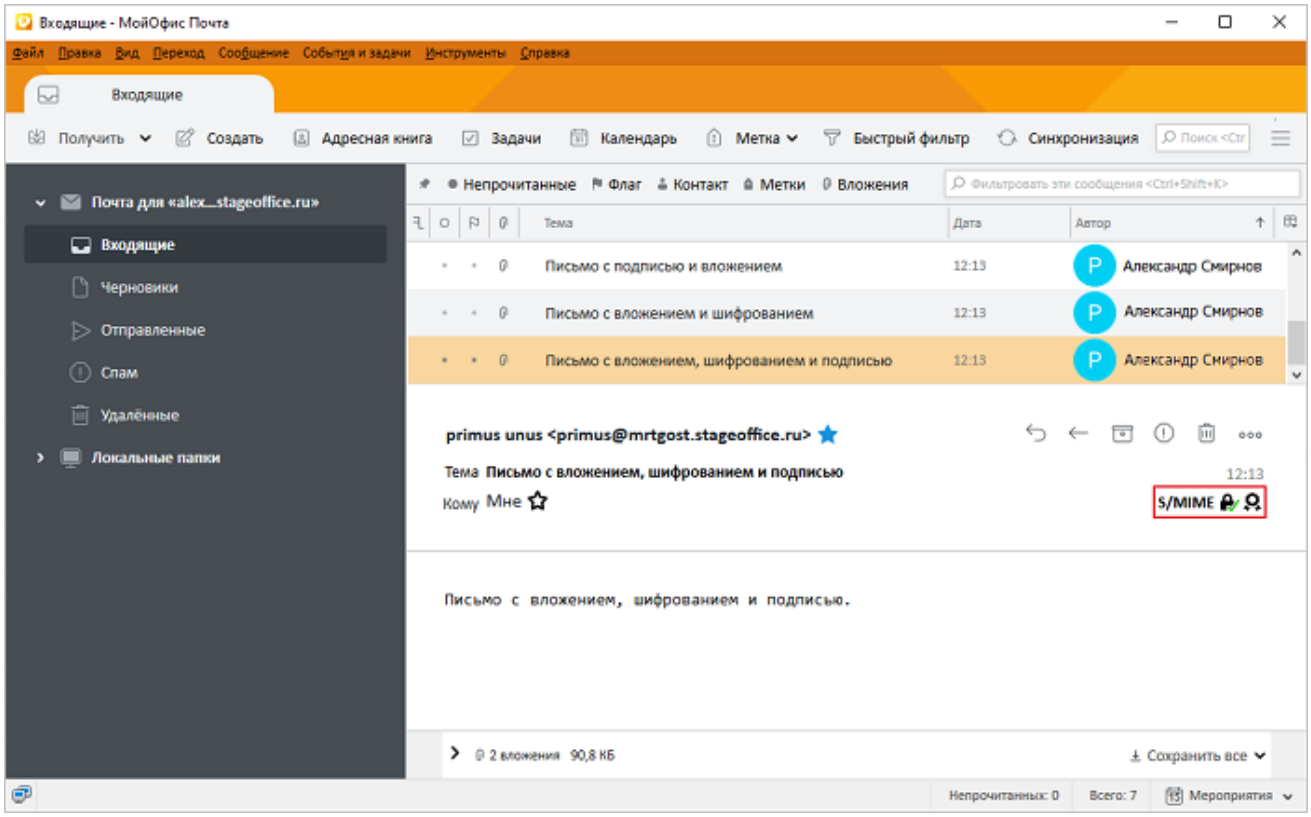

Рисунок 16 – Пример индикации шифрования и подписания полученного письма

4.2 Настройки сквозного шифрования

Сквозное шифрование (**e2ee**, **end-to-end-encryption**) электронной почты используется для защиты переписки от несанкционированного доступа. Без этой защиты посторонние лица смогут получить доступ к письмам и прочитать сообщения.

Использование сквозного шифрования требует внимательности всех участников переписки. Ошибки могут привести к открытию доступа для посторонних лиц, а также к невозможности восстановить данные в результате ошибочных действий с ключами.

Настройки сквозного шифрования находятся во вкладке **Параметры учетной записи**, в разделе **Сквозное шифрование** (см. Рисунок 17).

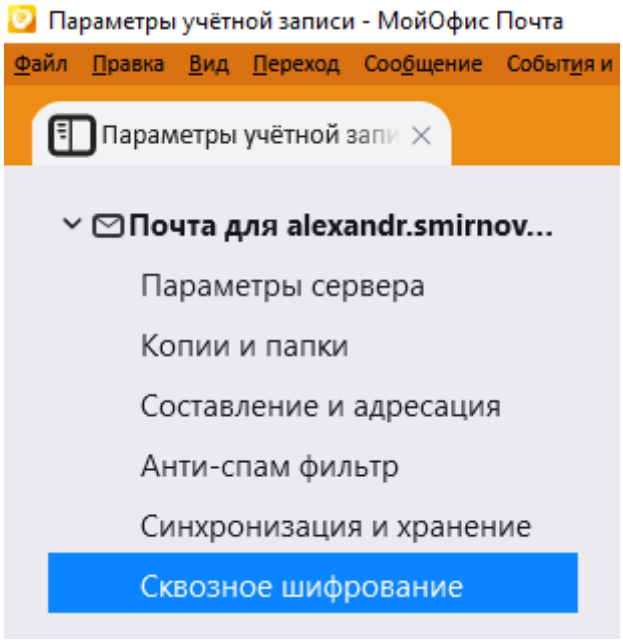

Рисунок 17 – Настройки сквозного шифрования

4.2.1 Настройки по умолчанию

Если требуется настроить автоматическое шифрование всех исходящих писем, во вкладке **Параметры учетной записи**, в разделе **Сквозное шифрование** (см. Рисунок 18) необходимо выбрать пункт **Требовать шифрование по умолчанию**.

Если требуется, чтобы все исходящие письма подписывались электронной подписью, должен быть установлен флажок **Добавлять цифровую подпись по умолчанию**.

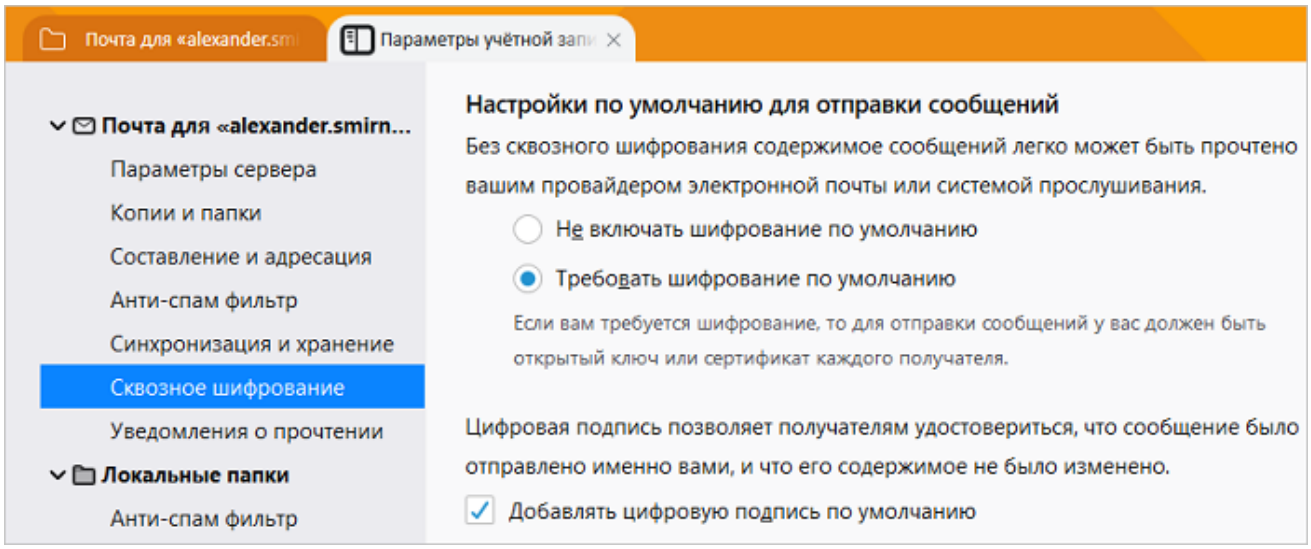

Рисунок 18 – Настройки по умолчанию для отправки сообщений

Чтобы отключить автоматическое выполнение операций подписания и/или шифрования всех исходящих писем, необходимо выбрать пункт **Не включать шифрование по умолчанию** и/или снять флажок **Добавлять цифровую подпись по умолчанию**.

Отключение операций подписания и/или шифрования для отдельного письма можно выполнить непосредственно в окне создания данного письма (см. разделы Подпись письма и Шифрование письма).

4.2.2 Дополнительные параметры шифрования

Для установки дополнительных параметров шифрования во вкладке **Параметры учетной записи**, в разделе **Сквозное шифрование** находится панель **Дополнительные параметры** (см. Рисунок 19).

Рисунок 19 – Дополнительные параметры шифрования

Дополнительные настройки:

1. **Прикреплять мой открытый ключ при добавлении цифровой подписи OpenPGP**. Открытый ключ в файле с именем «OpenPGP...» будет приложен к сообщениям при добавлениии цифровой подписи. Получатель сообщения может щелкнуть по нему правой кнопкой мыши, открыть контекстное меню, в котором выбрать «**Импорт ключа OpenPGP**».
2. **Шифровать тему сообщений OpenPGP**. При выборе данной настройки тема сообщения также будет зашифрована.
3. **Хранить черновики сообщений в зашифрованном формате**. При выборе данной настройки черновики будут зашифрованы.

Предпочитаемые технологии шифрования:

1. **Автовыбор на основе доступных ключей и сертификатов**. Выбирается шифрование на основе наличия доступных вариантов.
2. **Предпочитать OpenPGP**. Предпочтение отдается технологии шифрования OpenPGP (в случае, если настроены ключи OpenPGP).
3. **Предпочитать S/MIME**. Предпочтение отдается технологии шифрования S/MIME (в случае, если настроены сертификаты S/MIME).

4.3 Подпись письма

Чтобы подписать письмо с помощью электронной подписи, в окне создания нового письма нажмите на стрелку справа от кнопки **Защита** и установите флажок для операции **Подписать это сообщение** (см. Рисунок 20), если он не был установлен ранее (см. раздел Настройки по умолчанию).

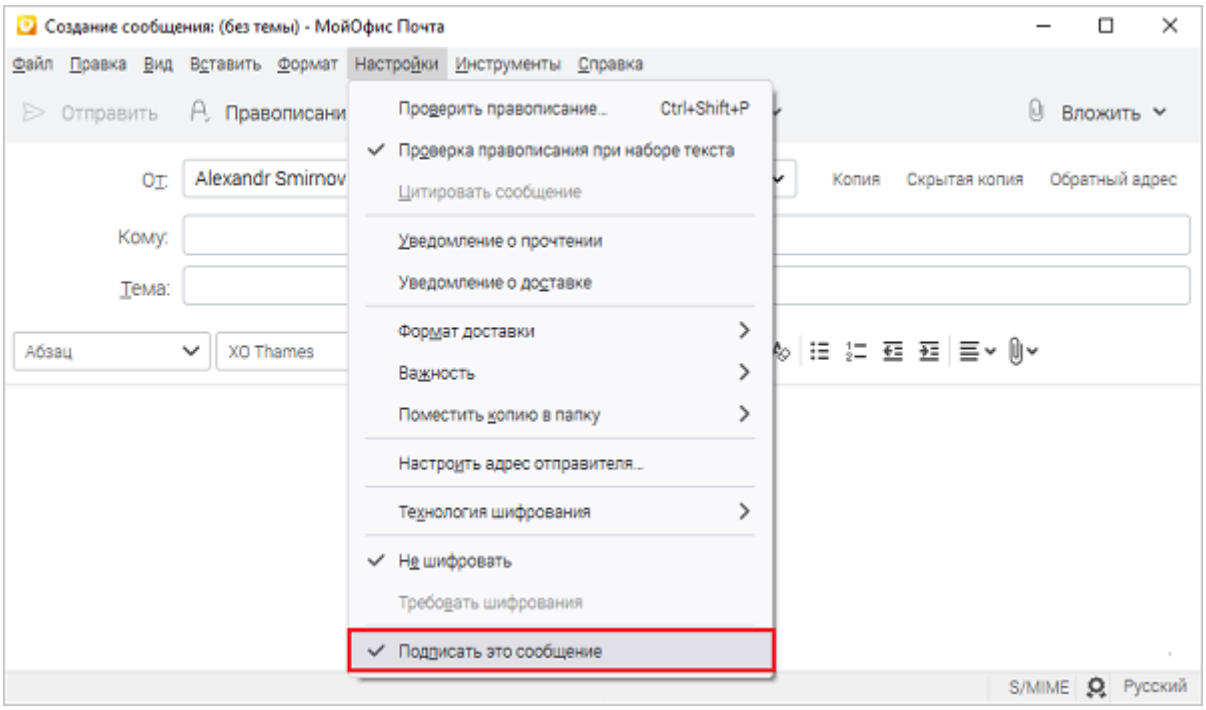

Рисунок 20 – Настройка подписи при создании нового письма

Выбранная операция отобразится в правом нижнем углу окна создания нового сообщения. Для отправки письма нажмите кнопку **Отправить**.

4.4 Шифрование письма

Для создания зашифрованного письма необходимо предварительно получить письмо с электронной подписью от требуемого адресата.

Чтобы зашифровать письмо, в окне создания нового письма нажмите на стрелку справа от кнопки **Защита** и выберите операцию **Требовать шифрования** (см. Рисунок 21), если она не была выбрана ранее (см. раздел Настройки по умолчанию).

При выборе операции шифрования автоматически выбирается операция подписи письма. Индикация шифрования и подписи отображается в правом нижнем углу окна создания нового сообщения.

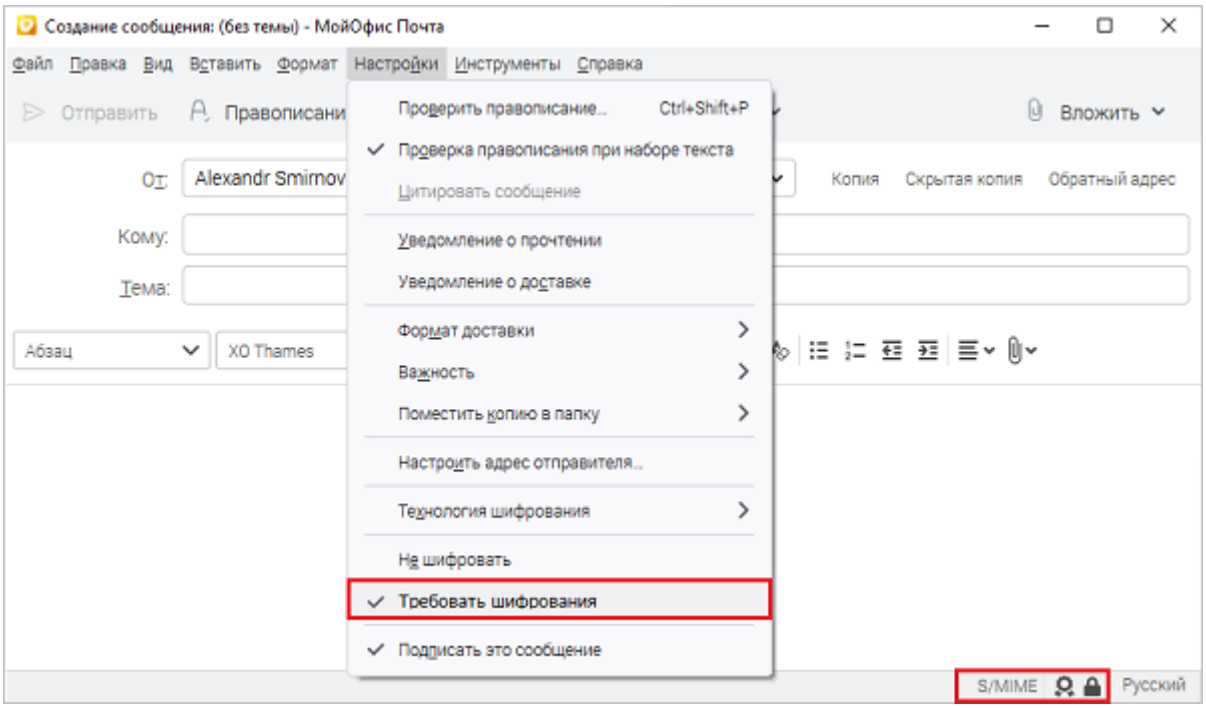

Рисунок 21 – Выбор операций при создании нового письма

При отправке письма автоматически проверяется наличие действительного сертификата безопасности у получателя. Наличие сертификатов получателей можно предварительно увидеть по нажатию **Безопасность / Просмотреть информацию о защите** (см. Рисунок 22).

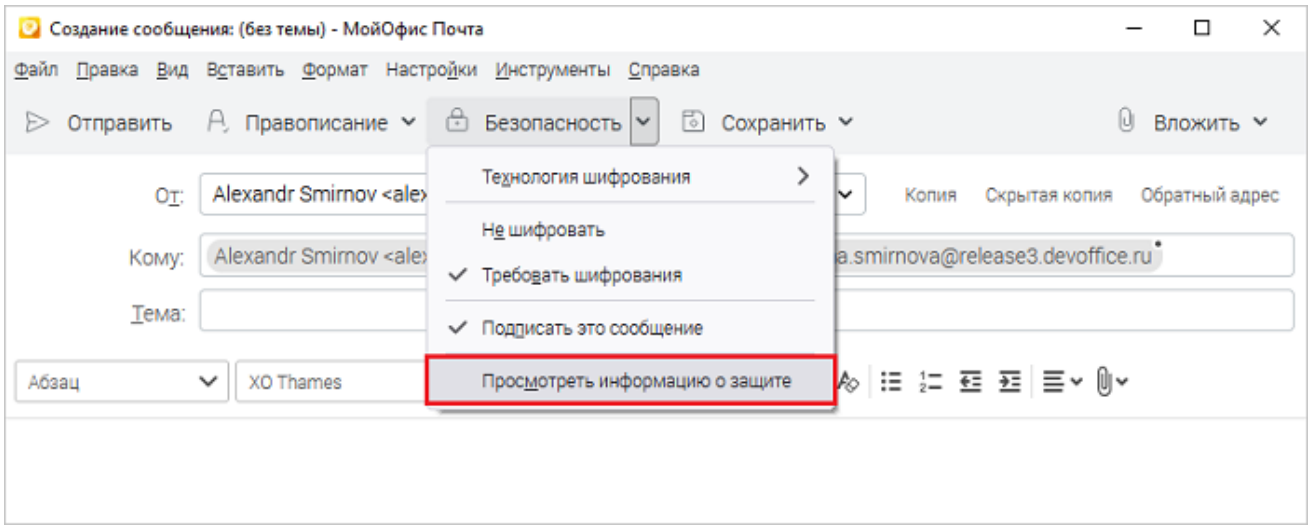

Рисунок 22 – Просмотр информации о сертификатах получателей письма

Список сертификатов получателей письма отобразится в открывшейся диалоговой панели (см. Рисунок 23).

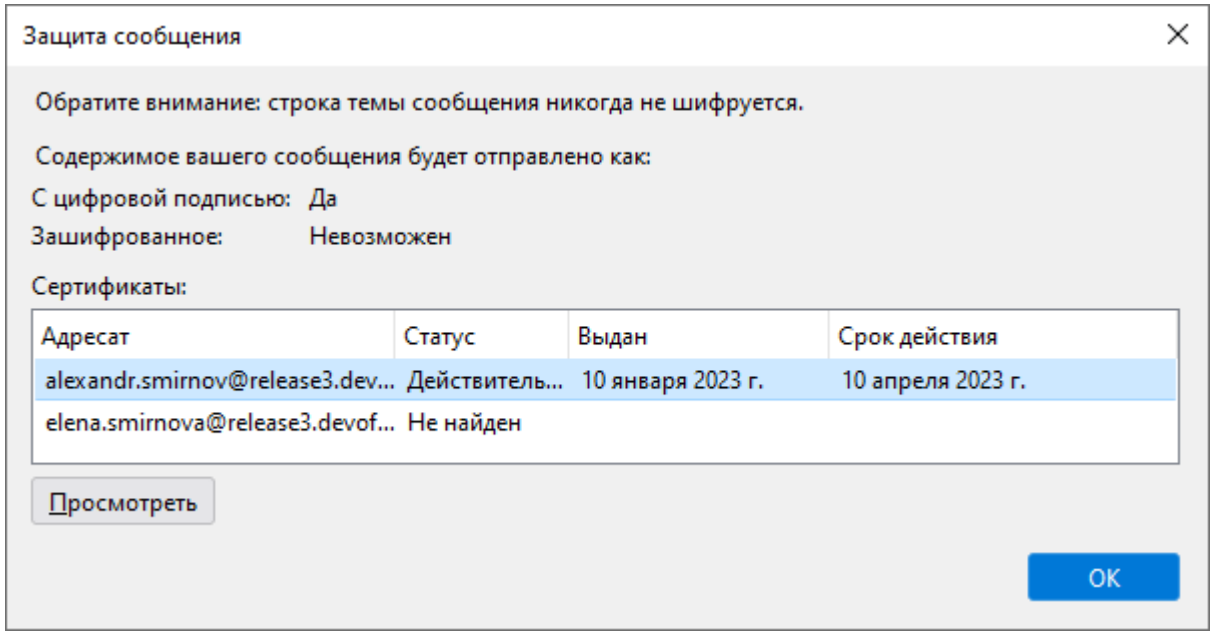

Рисунок 23 – Список сертификатов получателей письма

При нажатии на кнопку **Посмотреть** в основном окне приложения откроется новая закладка с детальной информацией о выбранном сертификате.

Если сертификат отсутствует, то при сохранении или отправке письма на экране возникает сообщение и письмо не отправляется (см. Рисунок 24).

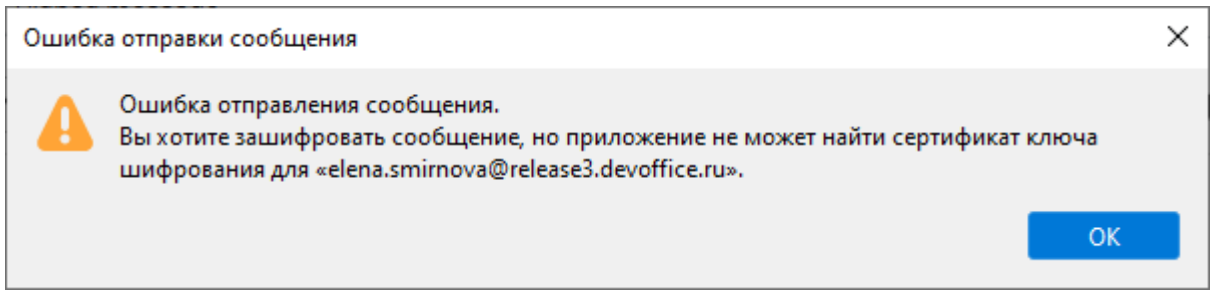

Рисунок 24 – Сообщение об отсутствии сертификата получателя

4.5 Проверка подписи и расшифровка письма

Чтобы проверить подпись и/или расшифровать письмо, откройте письмо, подписанное электронной подписью и/или зашифрованное. Проверка подписи и/или расшифровка письма начнется автоматически. В случае, если пароль контейнера не был сохранен ранее, на экране возникнет диалог подтверждения пароля (см. Рисунок 25):

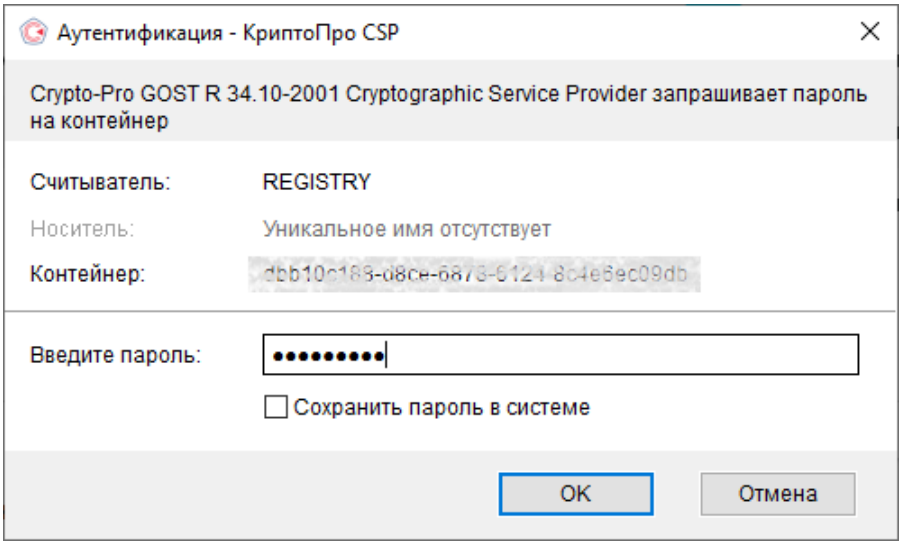

Рисунок 25 – Диалог подтверждения пароля

После окончания проверки в открытом письме отобразятся (см. Рисунок 26):

– текст письма;
– вложенные файлы, если они были прикреплены к этому письму;
– индикация шифрования и электронной подписи.

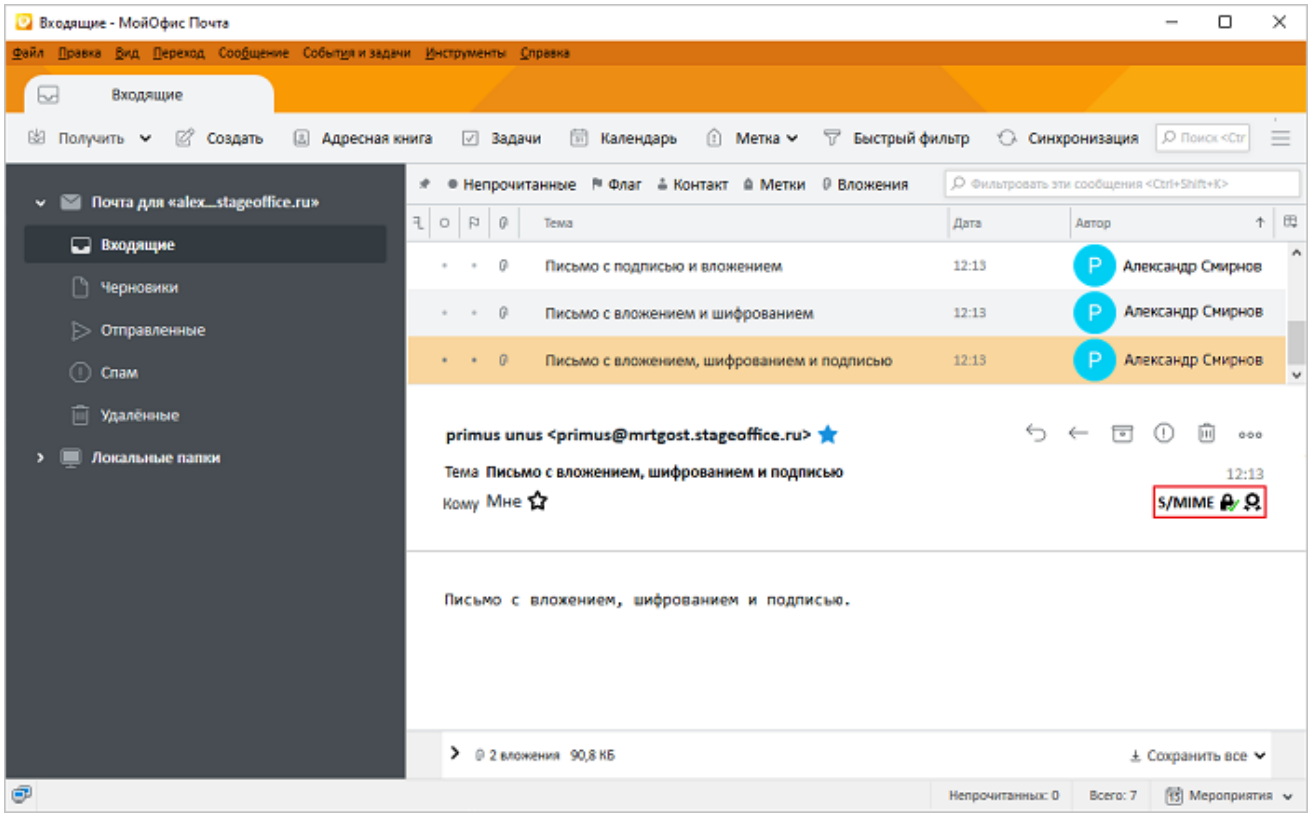

Рисунок 26 – Письмо с шифрованием и подписью

По нажатию на индикатор шифрования открывается информационная панель, содержащая данные о шифровании и подписи данного письма.

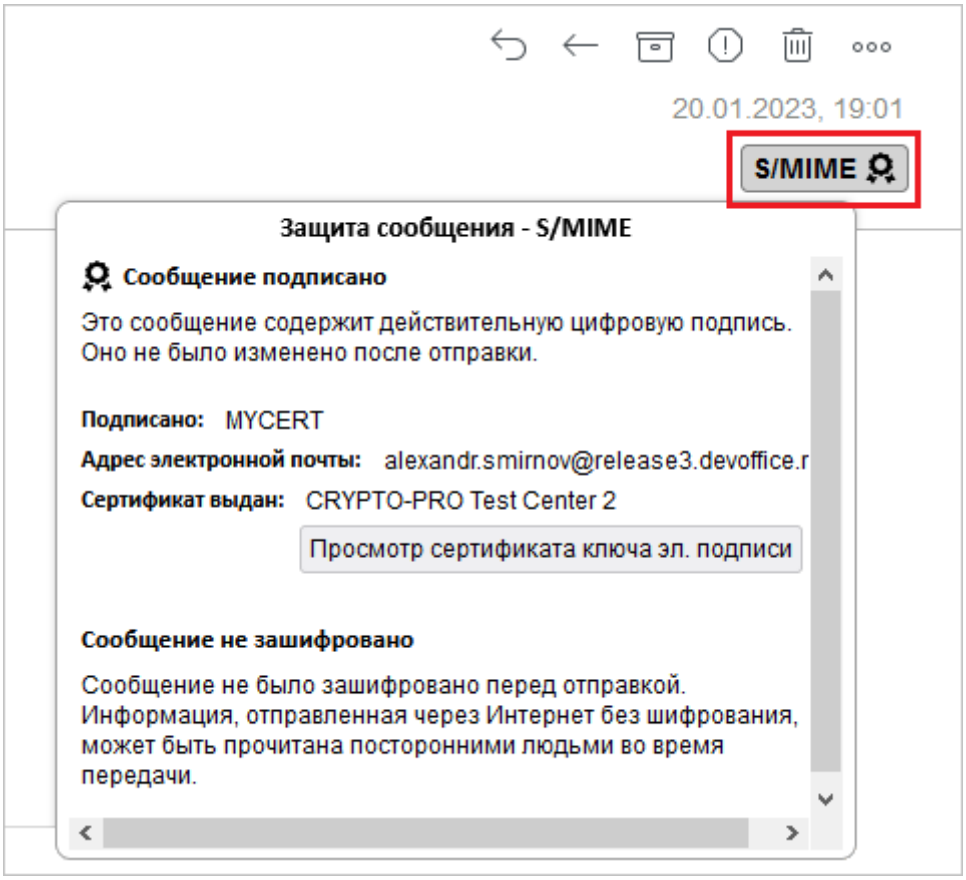

Рисунок 27 – Информация о подписи и шифровании письма

В случае возникновения проблем (например, просроченный сертификат) символ шифрования или подписи отобразится перечеркнутым 

.

В остальном работа в приложении «МойОфис Почта» для ОС Windows/Linux/macOS с поддержкой криптографической защиты данных описана в документе «МойОфис Почта, Настольные приложения. Руководство пользователя».