4.3.2 ЭЦП и шифрование почтовых сообщений в Microsoft Outlook

Выработка и проверка ЭЦП, а также шифрование почтовых сообщений играют важную роль при обеспечении информационной безопасности.

В общем случае у всех пользователей есть устройство Рутокен с сертификатом и ключевой парой (открытый и закрытый ключ).

Третья сторона (Центр сертификации, Удостоверяющий центр) удостоверяет по цифровому сертификату его законного владельца.

ЭЦП почтовых сообщений производится отправителем почтового сообщения с использованием своего закрытого ключа.

При помощи открытого ключа можно проверить правильность цифровой подписи, а также посмотреть информацию об отправителе.

Для шифрования почтовых сообщений два пользователя сначала должны обменяться подписанными сообщениями.

Почтовое сообщение шифруется отправителем при помощи открытого ключа получателя. Таким образом любой может зашифровать сообщение для пользователя при помощи открытого ключа, но только владелец закрытого ключа может расшифровать сообщение. Именно для сохранности цифрового идентификатора и ключевой пары следует хранить их на устройстве Рутокен.

При использовании устройства Рутокен только легальный получатель сможет прочесть зашифрованное для него сообщение.

Настройка ЭЦП и шифрования почтовых сообщений не зависит от почтового сервера и Центра сертификации, а сводится к настройке программы почтового клиента.

Эта инструкция помогает настроить электронную цифровую подпись и шифрование почтовых сообщений посредством сертификата, хранящегося на устройстве Рутокен, на примере **Microsoft Outlook 2013**.

Настройки выполняются с использованием почтового сервера Microsoft Exchange Server 2013 с Центром сертификации на **Microsoft Windows 2008 /2003/2000 Server**. Кроме того, необходимо, чтобы на компьютерах, где производится подпись и шифрование почты, были установлены **драйверы Рутокен**. Для примера используются учетные записи **Admin** и **User**.

1 этап: Настройка учетной записи электронной почты в Microsoft Outlook.

2 этап: Настройка параметров безопасности Microsoft Outlook.

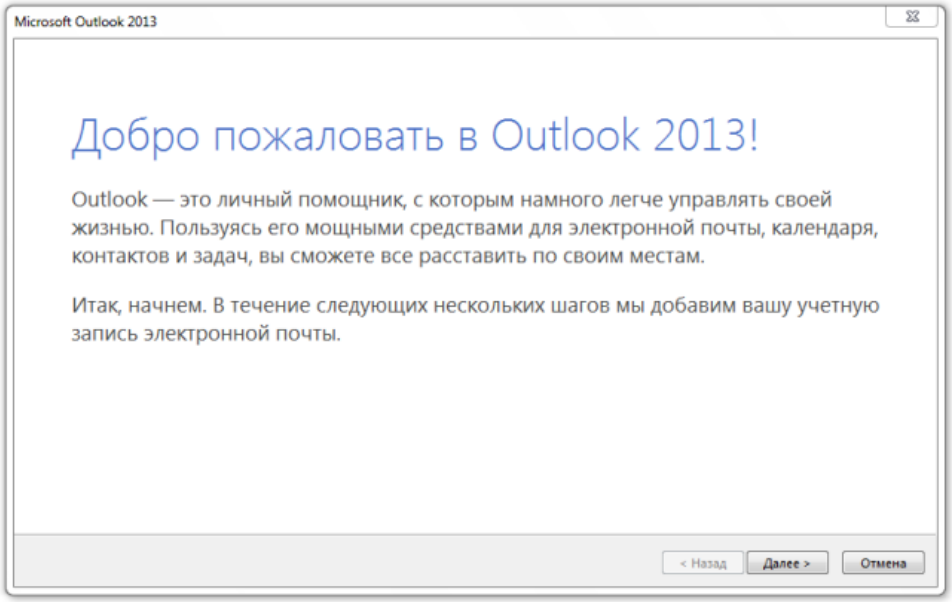
3 этап: Создание подписанного почтового сообщения.

4 этап: Шифрование почты посредством сертификата, хранящегося на устройстве Рутокен.

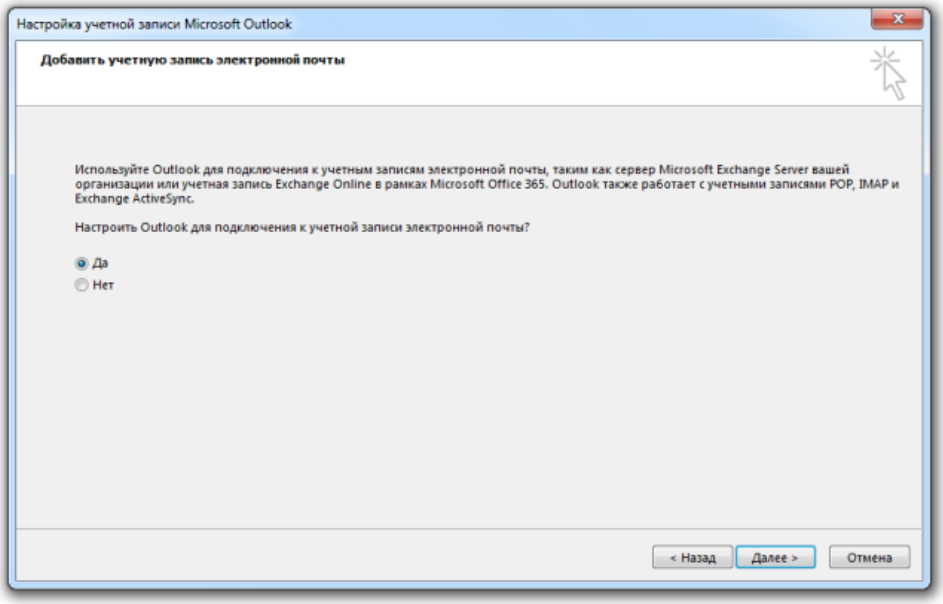
Настройка учетной записи электронной почты в Microsoft Outlook

Для настройки учетной записи электронной почты:

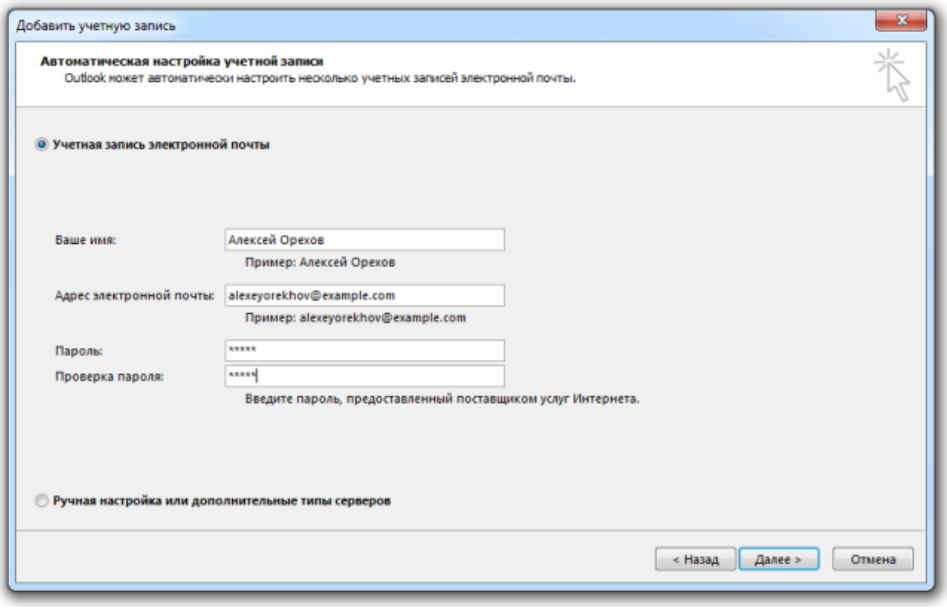
1. Запустите **Microsoft Outlook 2013**. Нажмите на кнопку **[Далее]**.



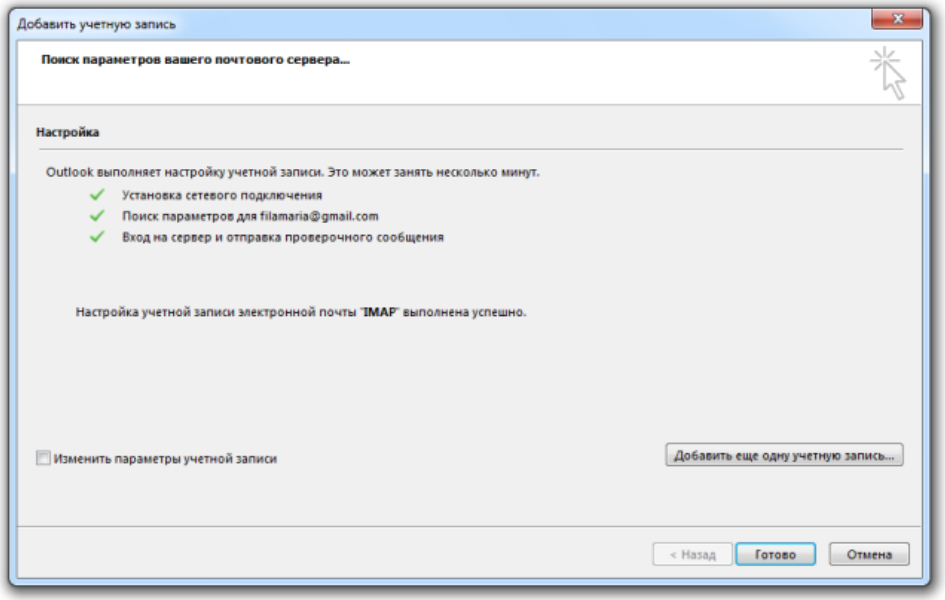
2. В окне **Настройка учетной записи Microsoft Outlook** установите переключатель в положение **Да** и нажмите на кнопку **[Далее]**.



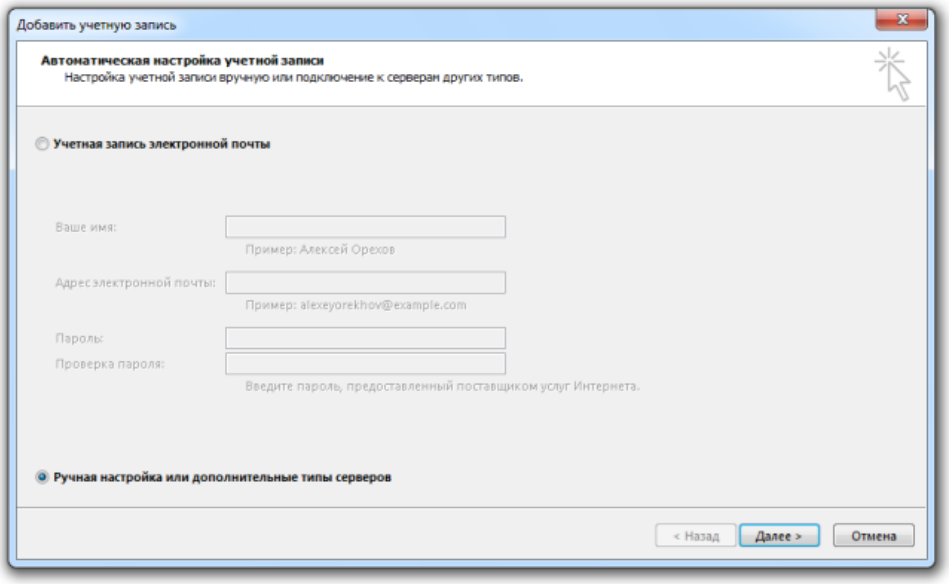
3. В окне **Добавить учетную запись** заполните необходимые поля и нажмите на кнопку **[Далее]**.



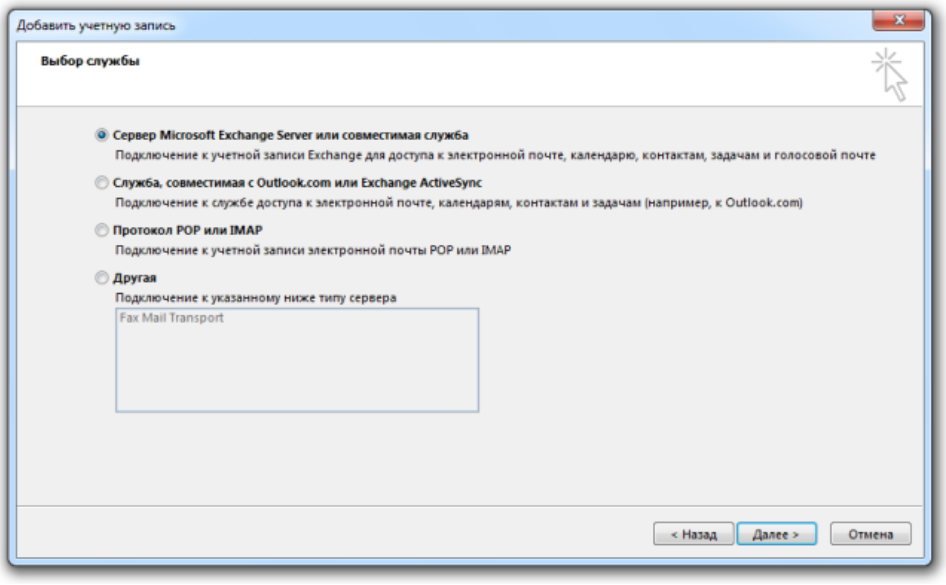
4. Дождитесь окончания процесса настройки учетной записи и нажмите на кнопку **[Готово]**.



5. Чтобы вручную настроить учетную запись пользователя, установите переключатель в положение **Ручная настройка или дополнительные типы серверов** и нажмите на кнопку **[Далее]**.

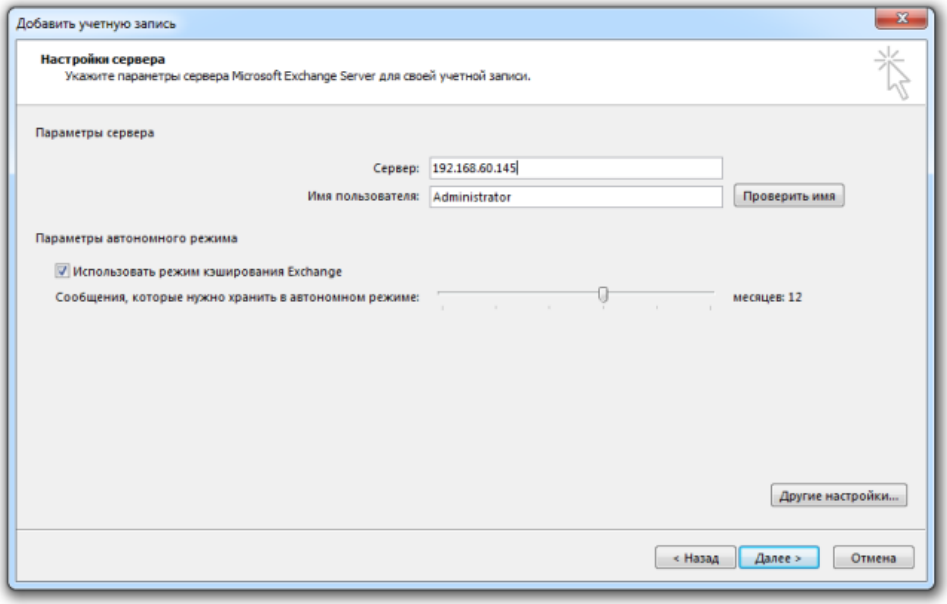


6. В примере в качестве почтового сервера используется **Microsoft Exchange Server 2010**, поэтому переключатель установлен в положение **Сервер Microsoft Exchange Server или совместимая служба** (в качестве почтового сервера может быть использован любой почтовый сервер). Настройки электронной цифровой подписи и шифрования почтовых сообщений относятся только к почтовому клиенту. Нажмите на кнопку **[Далее]**.

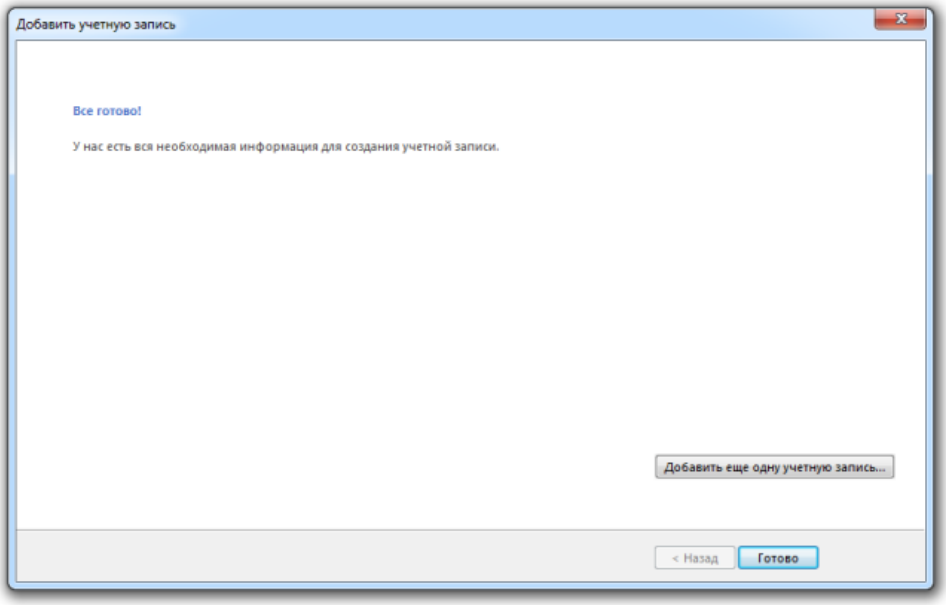


Если используется не Microsoft Exchange Server, то последующие настройки будут другими.

7. Введите IP-адрес или имя почтового сервера, а также имя пользователя. Нажмите на кнопку **[Проверить имя]**.



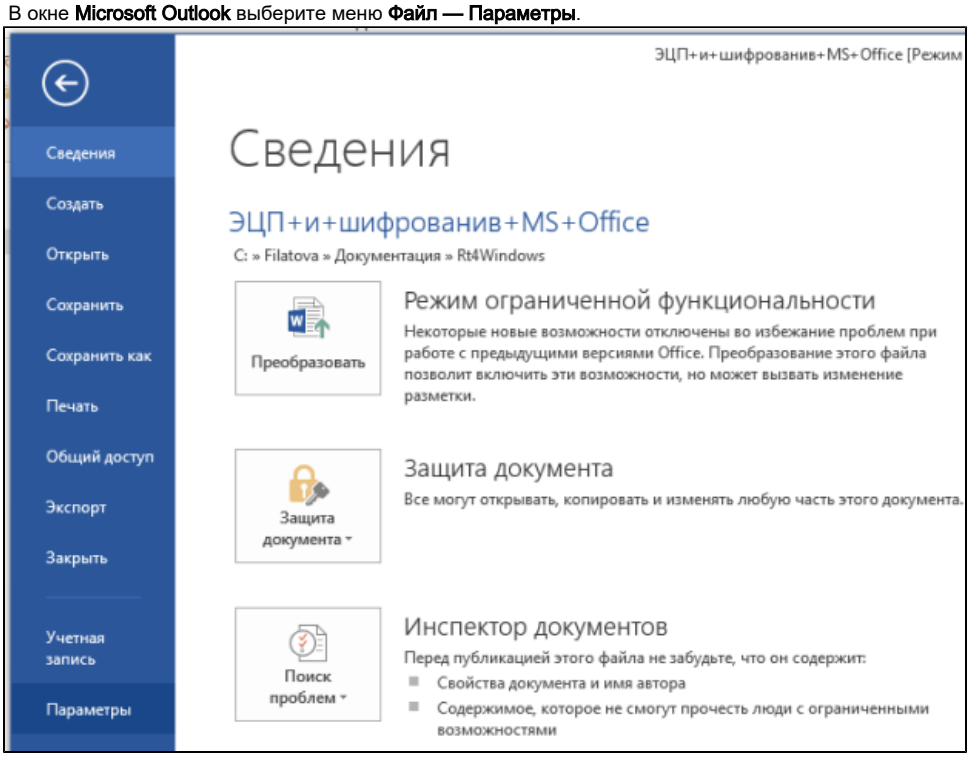
8. Нажмите на кнопку **[Далее]**.
9. В окне **Добавить учетную запись** ознакомьтесь с сообщением и нажмите на кнопку **[Готово]**.



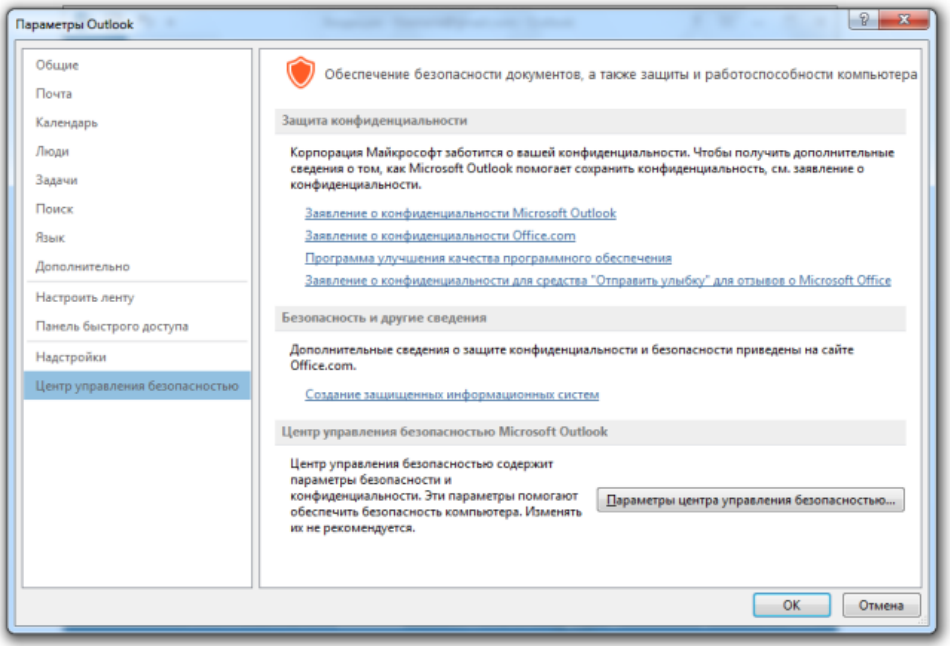
Настройка параметров безопасности Microsoft Outlook

Для настройки параметров безопасности:

1. В окне **Microsoft Outlook** выберите меню **Файл — Параметры**.

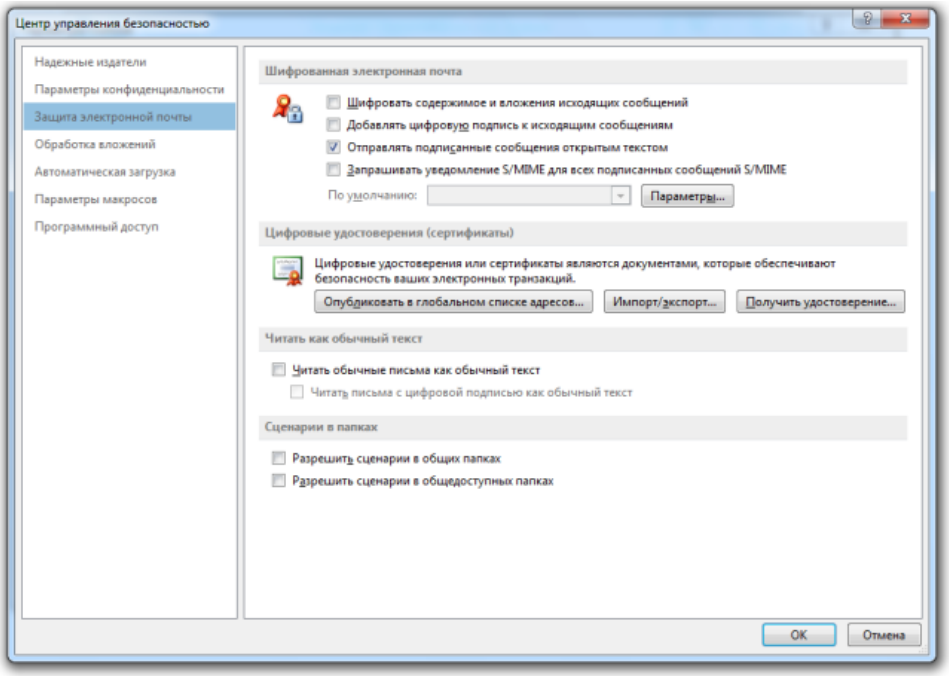


2. В окне **Параметры Outlook** выберите пункт меню **Центр управления безопасностью**.
3. Нажмите на кнопку **[Параметры центра управления безопасностью...]**.

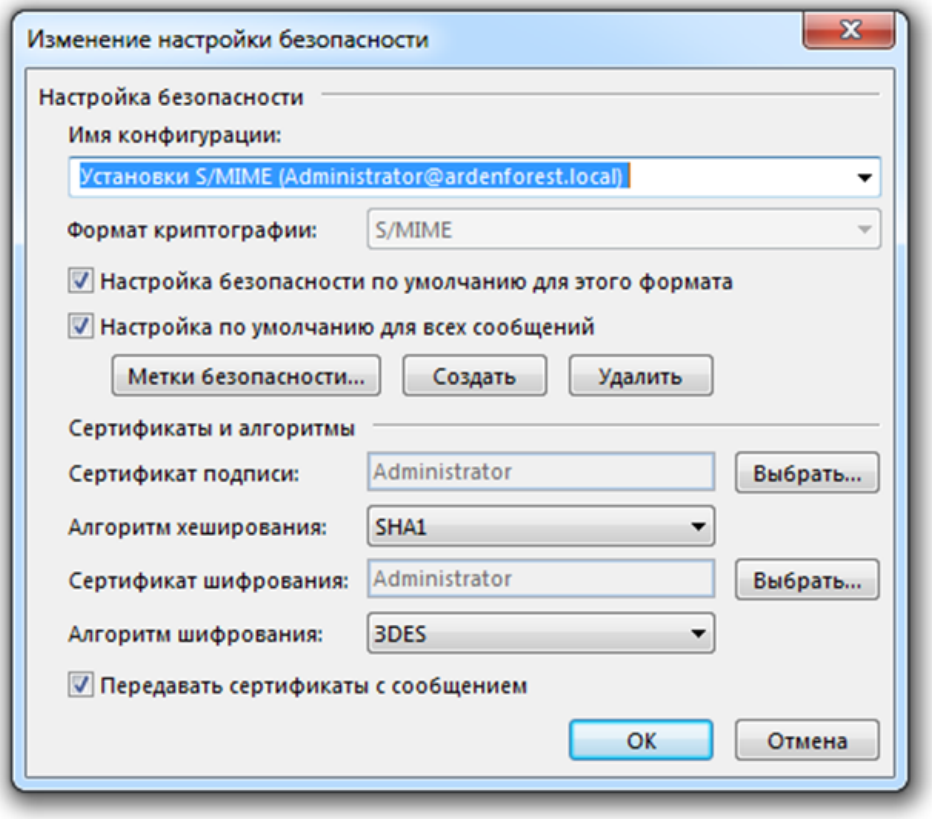


4. В окне **Центр управления безопасностью** выберите пункт **Защита электронной почты**.

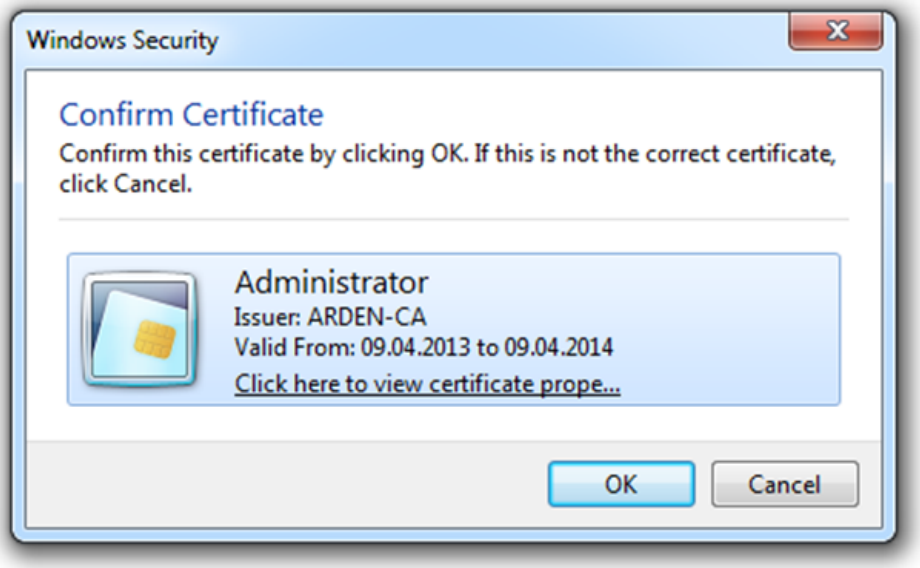
5. В разделе **Шифрованная электронная почта** нажмите на кнопку **[Параметры...]**.



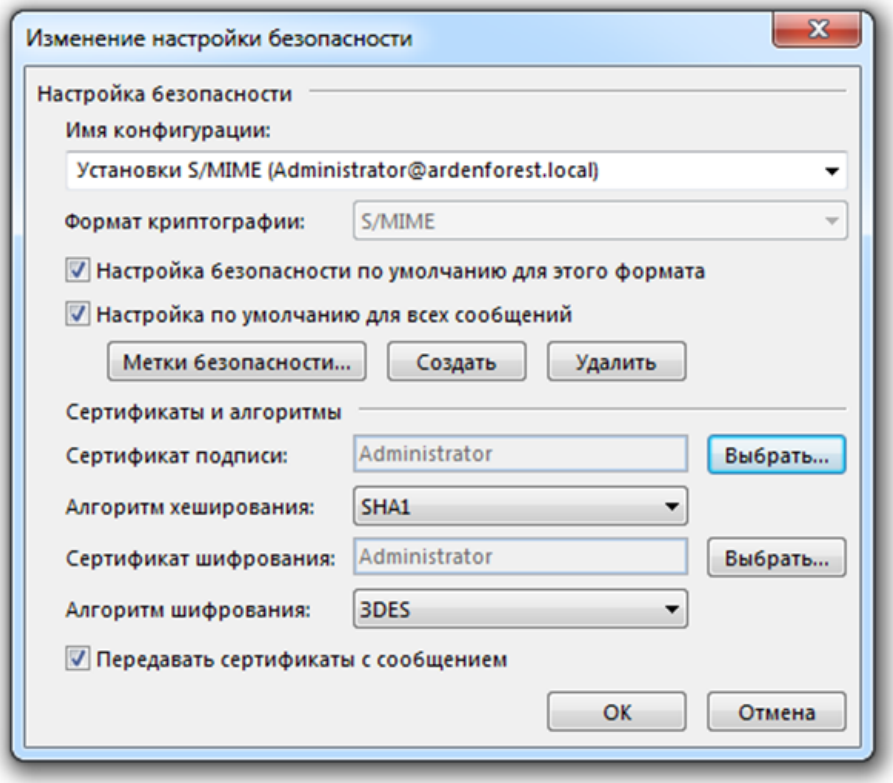
6. В окне **Изменение настройки безопасности** заполните необходимые поля.
7. Проверьте корректность данных в полях **Сертификат подписи** и **Сертификат шифрования**.
8. Чтобы изменить эти данные, нажмите на кнопку **[Выбрать...]** рядом с необходимым полем.



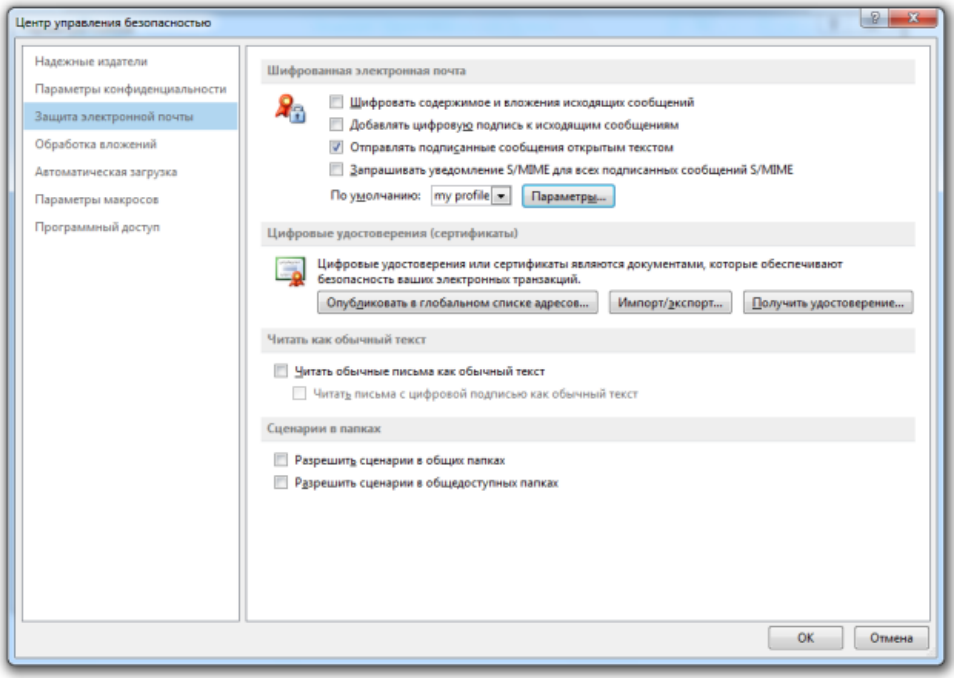
9. Щелкните по названию необходимого сертификата и нажмите на кнопку**[OK]**.



10. Убедитесь, что все необходимые поля в окне **Изменение настройки безопасности** заполнены.
11. Нажмите на кнопку **[OK]**.



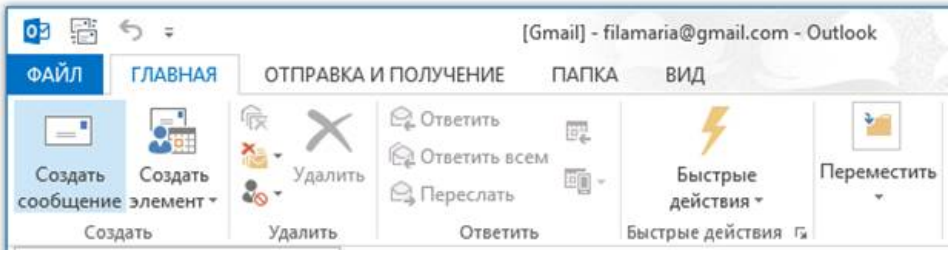
12. В окне **Центр управления безопасностью** нажмите на кнопку **[OK]**.



Создание подписанного почтового сообщения

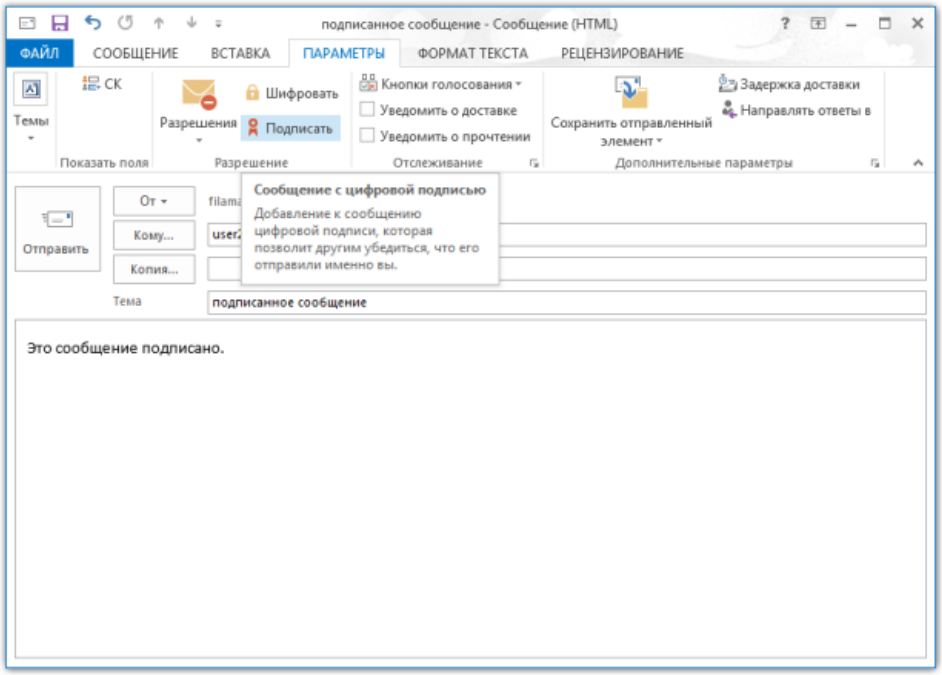
Для создания подписанного почтового сообщения:

1. В окне **Microsoft Outlook** нажмите на кнопку **[Создать сообщение]**.



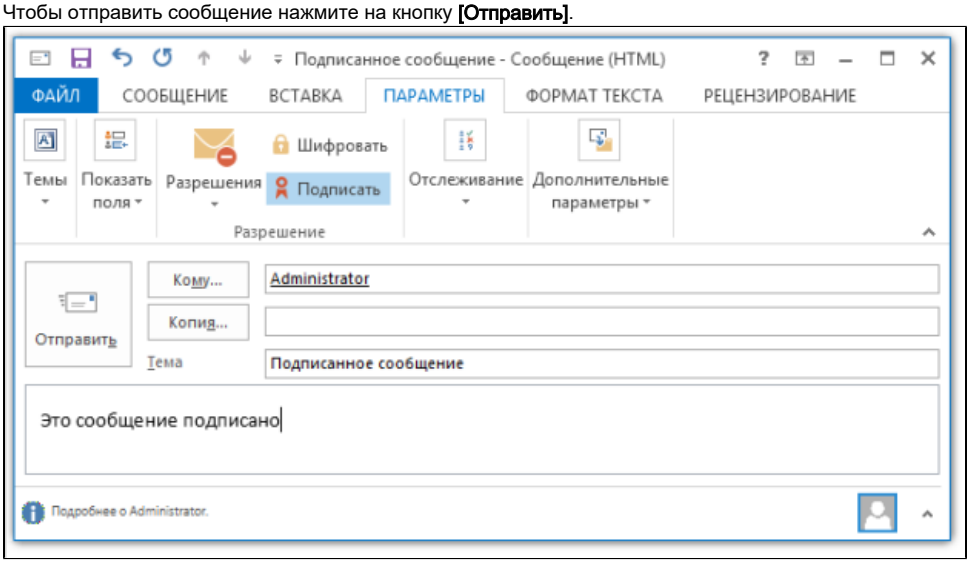
2. Введите адрес получателя, тему и текст сообщения.

3. Чтобы создать электронную цифровую подпись для сообщения, нажмите на кнопку **[Подписать]**.

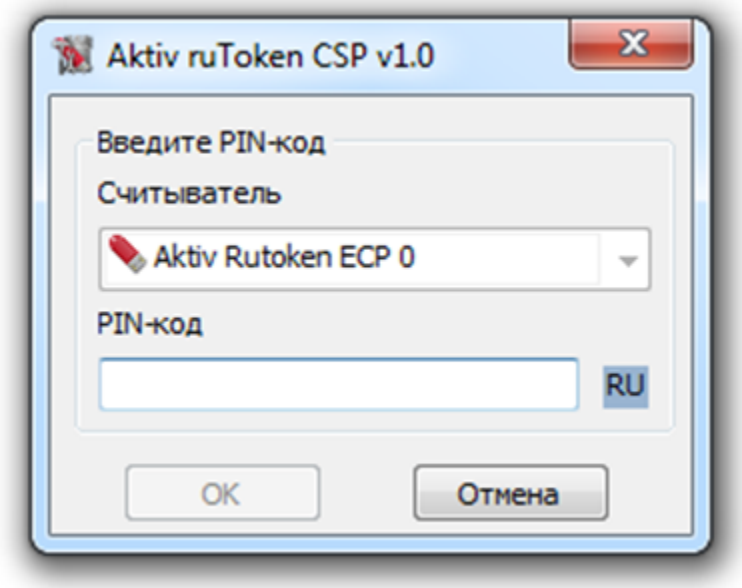


Кнопки **[Подписать]** и **[Шифровать]** доступны только после настроек параметров электронной цифровой подписи и шифрования почтовых сообщений. При нажатии на кнопку **[Подписать]** не происходит подписи сообщения, подпись происходит непосредственно перед отправкой сообщения. Если нажата кнопка **[Подписать]**, то сообщение до отправки можно править и даже сохранять в качестве черновика, но после отправки сообщение перестает быть доступным для редактирования.

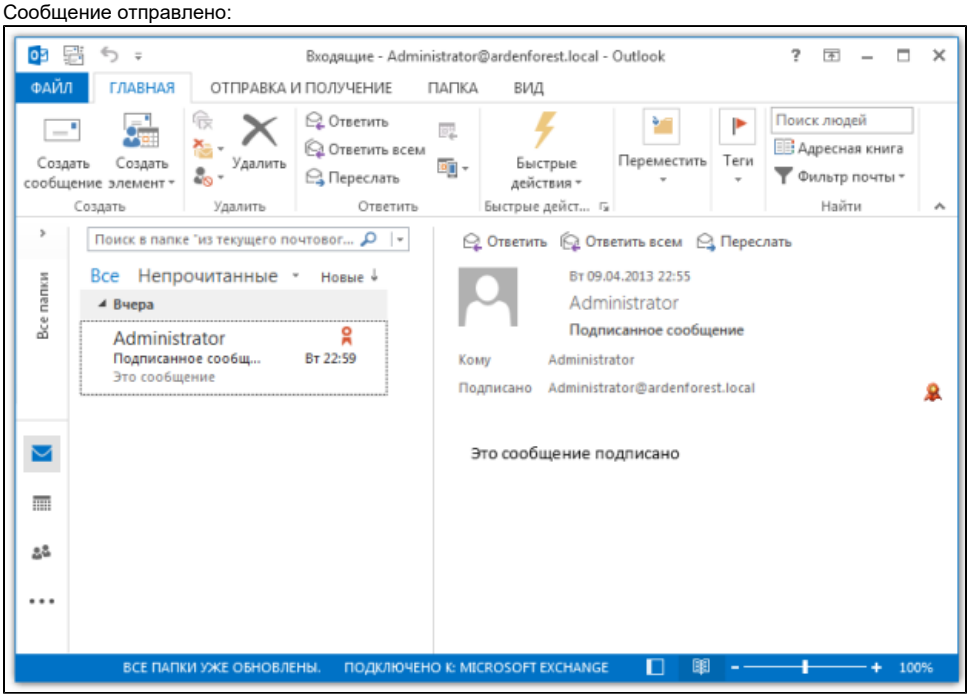
4. Чтобы отправить сообщение нажмите на кнопку **[Отправить]**.



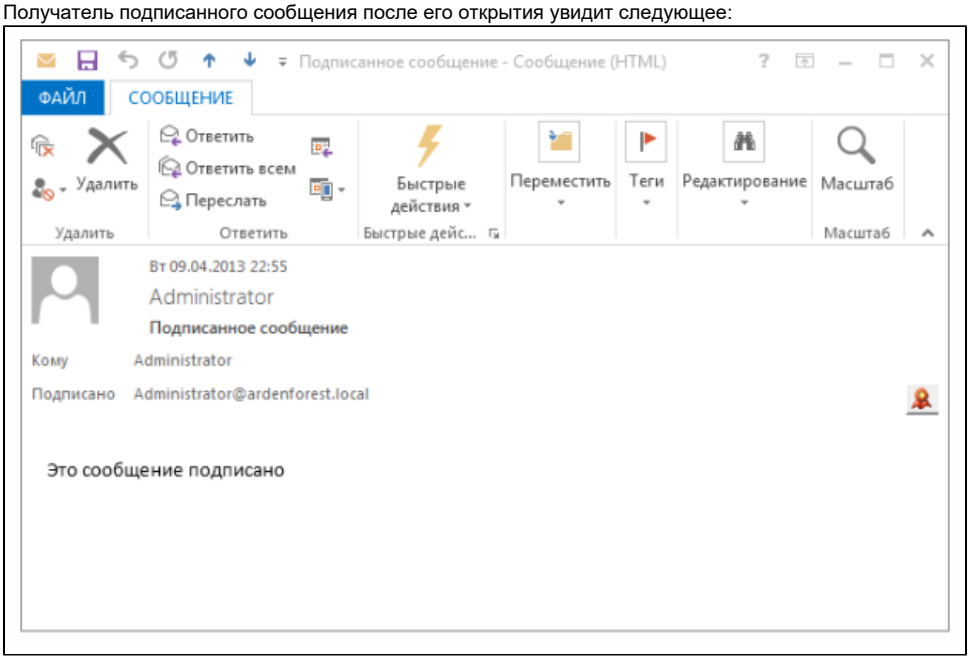
5. Введите PIN-код Пользователя и нажмите на кнопку **[OK]**.



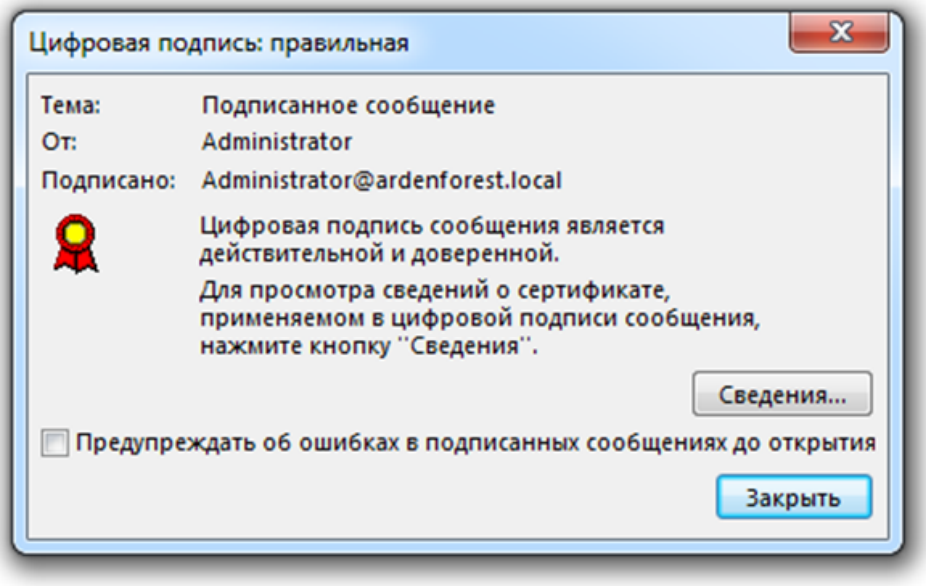
6. Сообщение отправлено:



7. Получатель подписанного сообщения после его открытия увидит следующее:

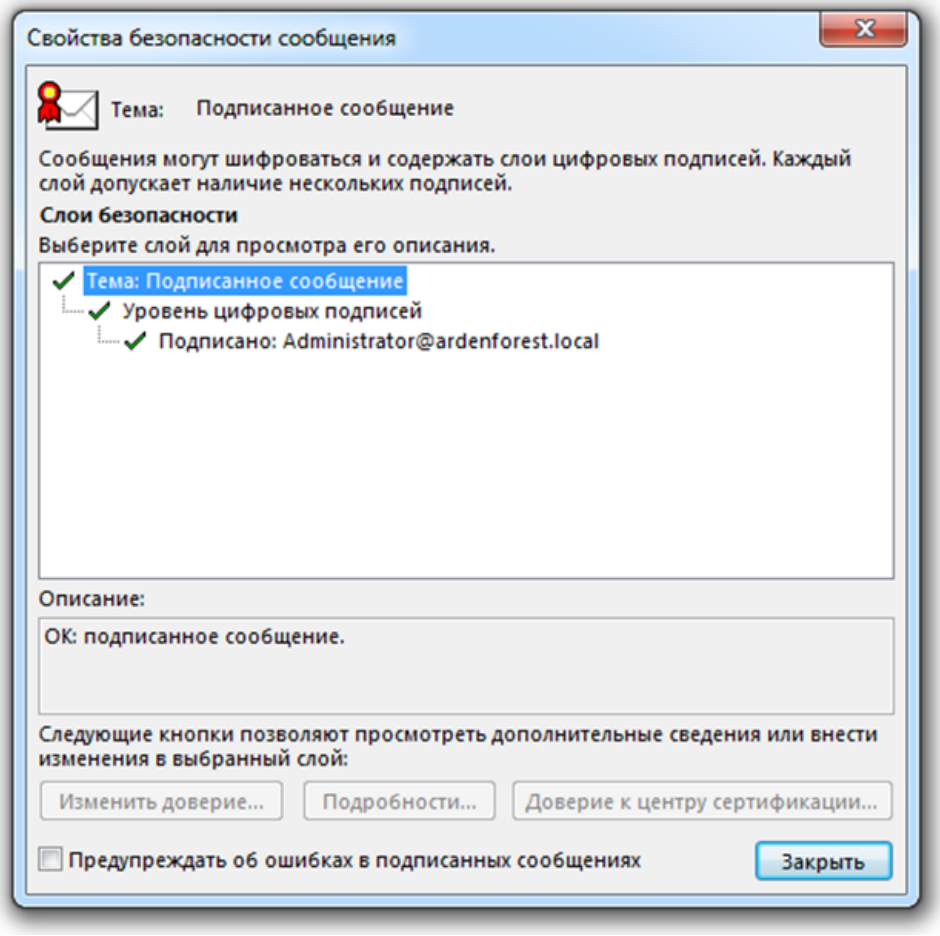


8. Чтобы посмотреть более подробную информацию о подписи этого сообщения, щелкните по иконке  напротив поля **Подписано**.
9. В окне **Цифровая подпись: правильная** ознакомьтесь с информацией.
10. Для просмотра более подробной информации нажмите на кнопку **[Сведения...]**.

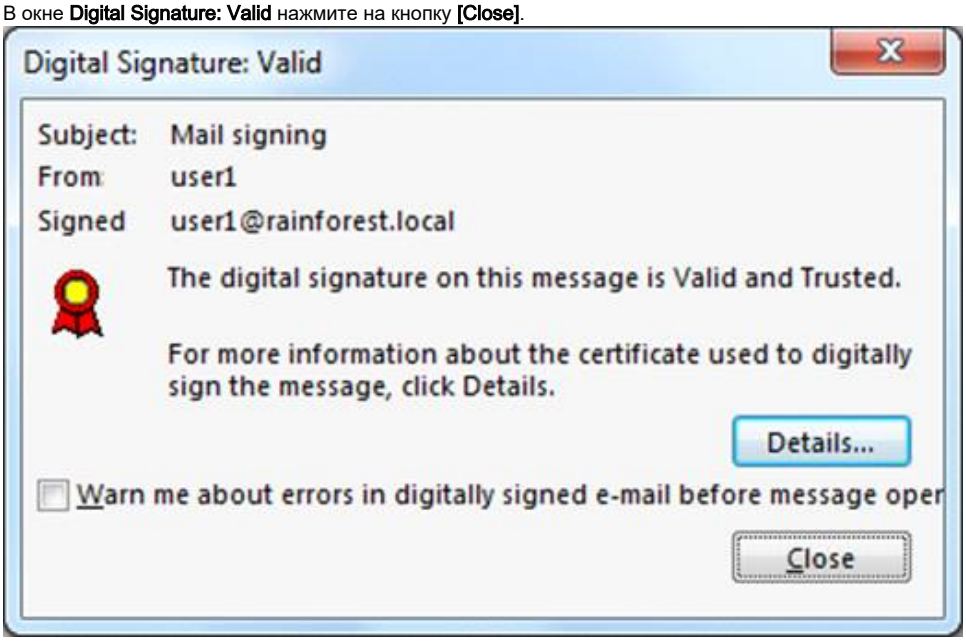


11. Кликните по имени пользователя, подписавшего сообщение.

12. В окне **Свойства безопасности сообщения** нажмите на кнопку **[Закрыть]**.



13. В окне **Digital Signature: Valid** нажмите на кнопку **[Close]**.

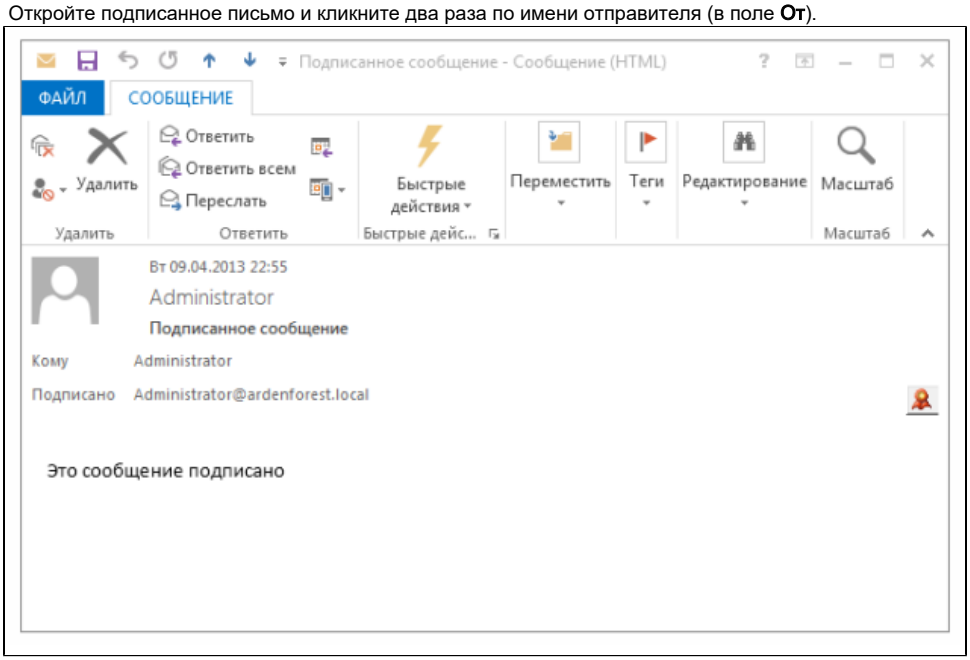


Шифрование почты посредством сертификата, хранящегося на устройстве Рутокен

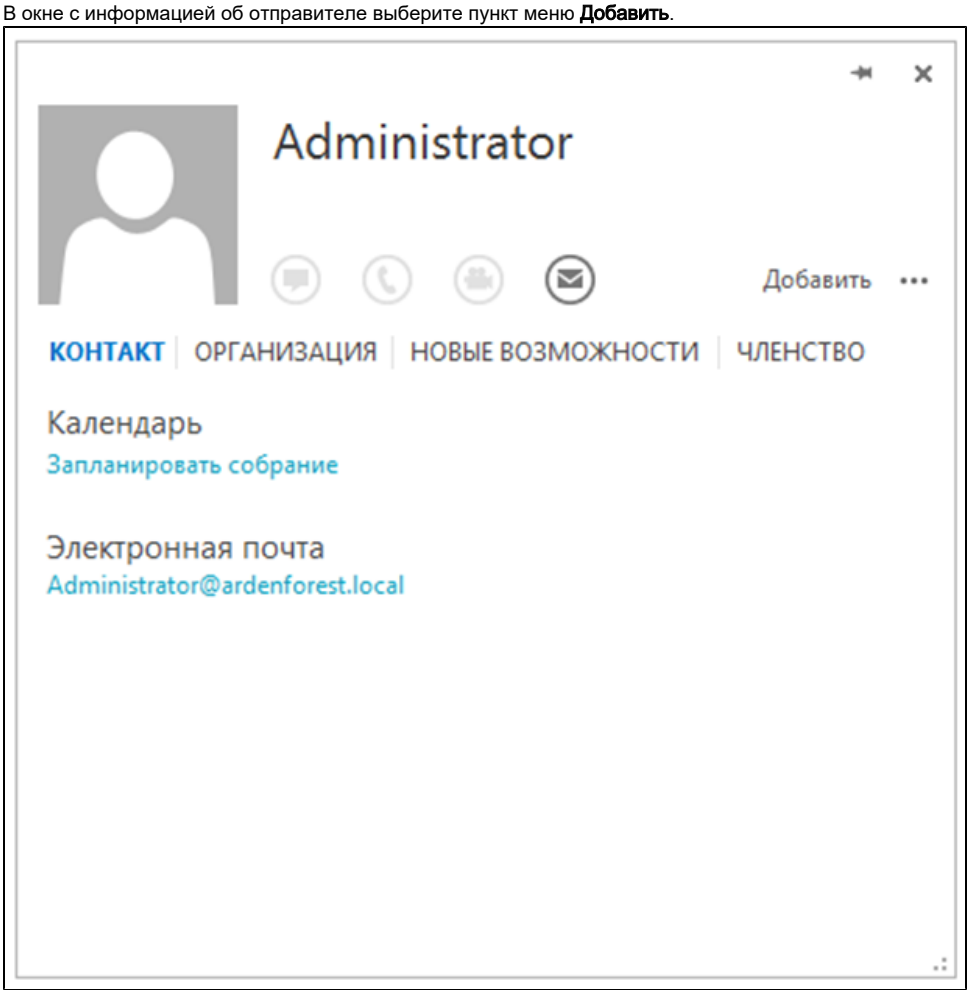
Для того чтобы пользователи могли зашифровывать почтовые сообщения друг для друга, им необходимо сначала обменяться подписанными сообщениями и создать контакты в адресной книге **Microsoft Outlook** со своими адресами и соответствующими сертификатами.

Для того, чтобы зашифровать почту с помощью сертификата, хранящегося на устройстве Рутокен:

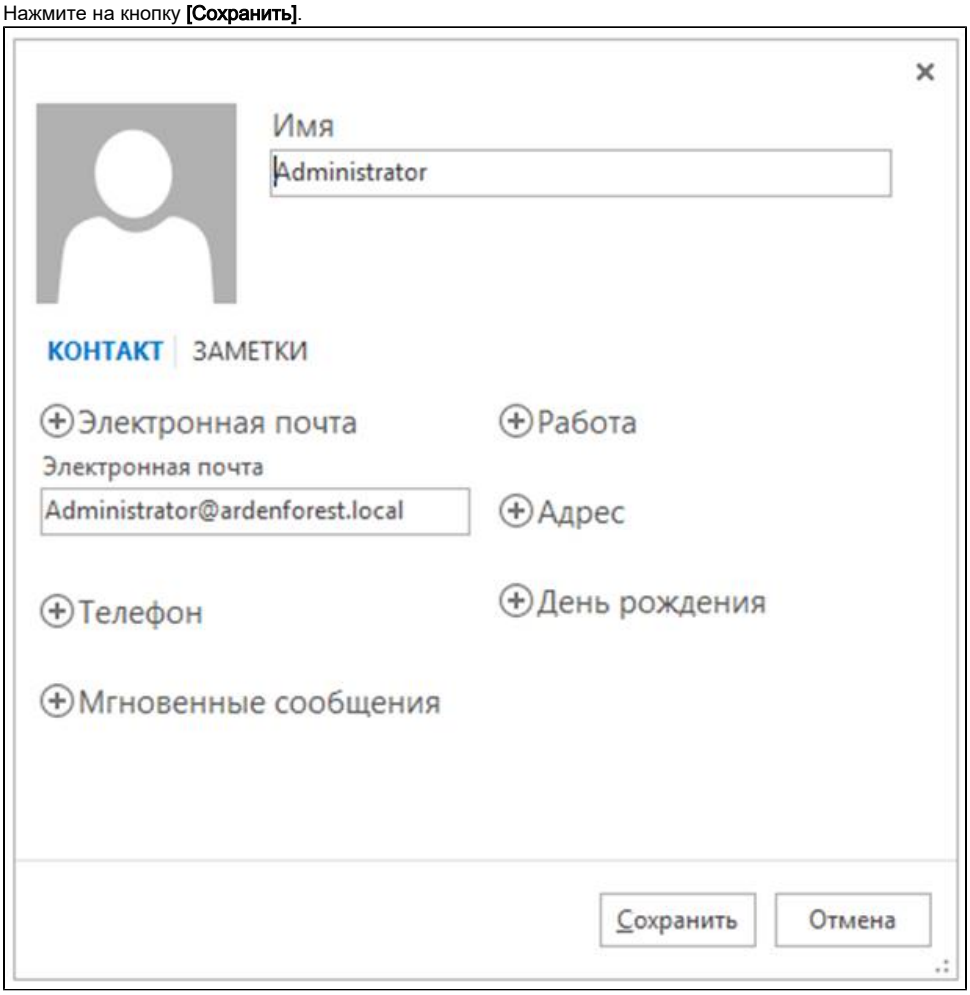
1. Откройте подписанное письмо и кликните два раза по имени отправителя (в поле **От**).



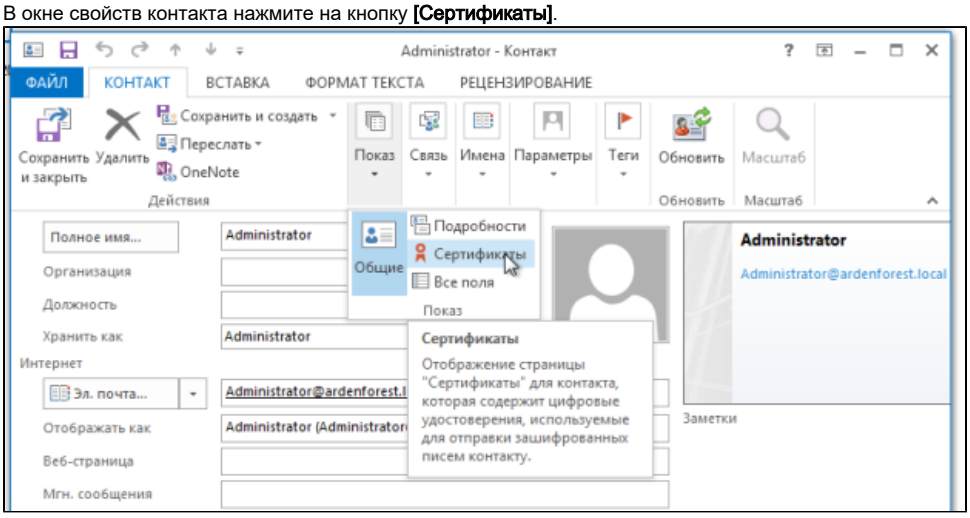
2. В окне с информацией об отправителе выберите пункт меню **Добавить**.



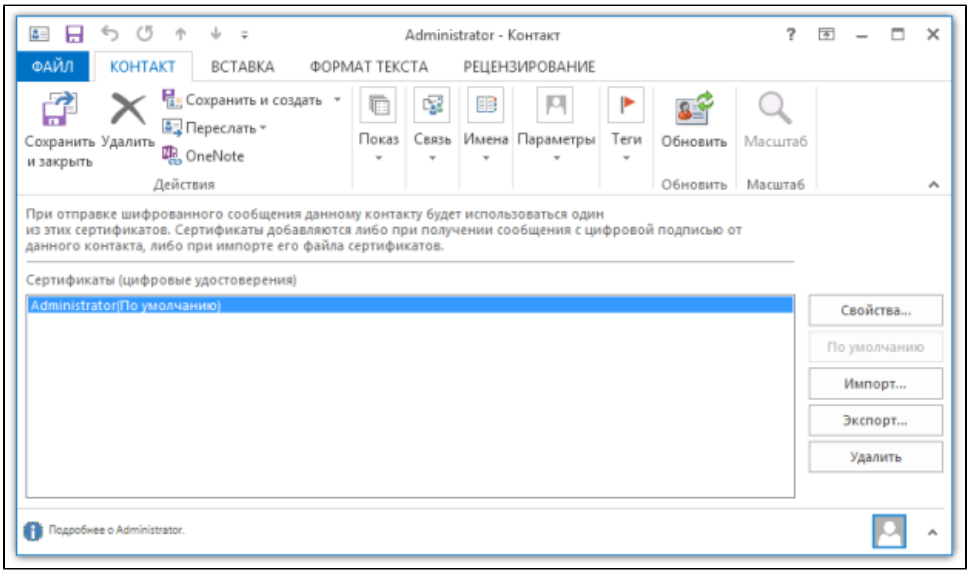
3. Нажмите на кнопку **[Сохранить]**.



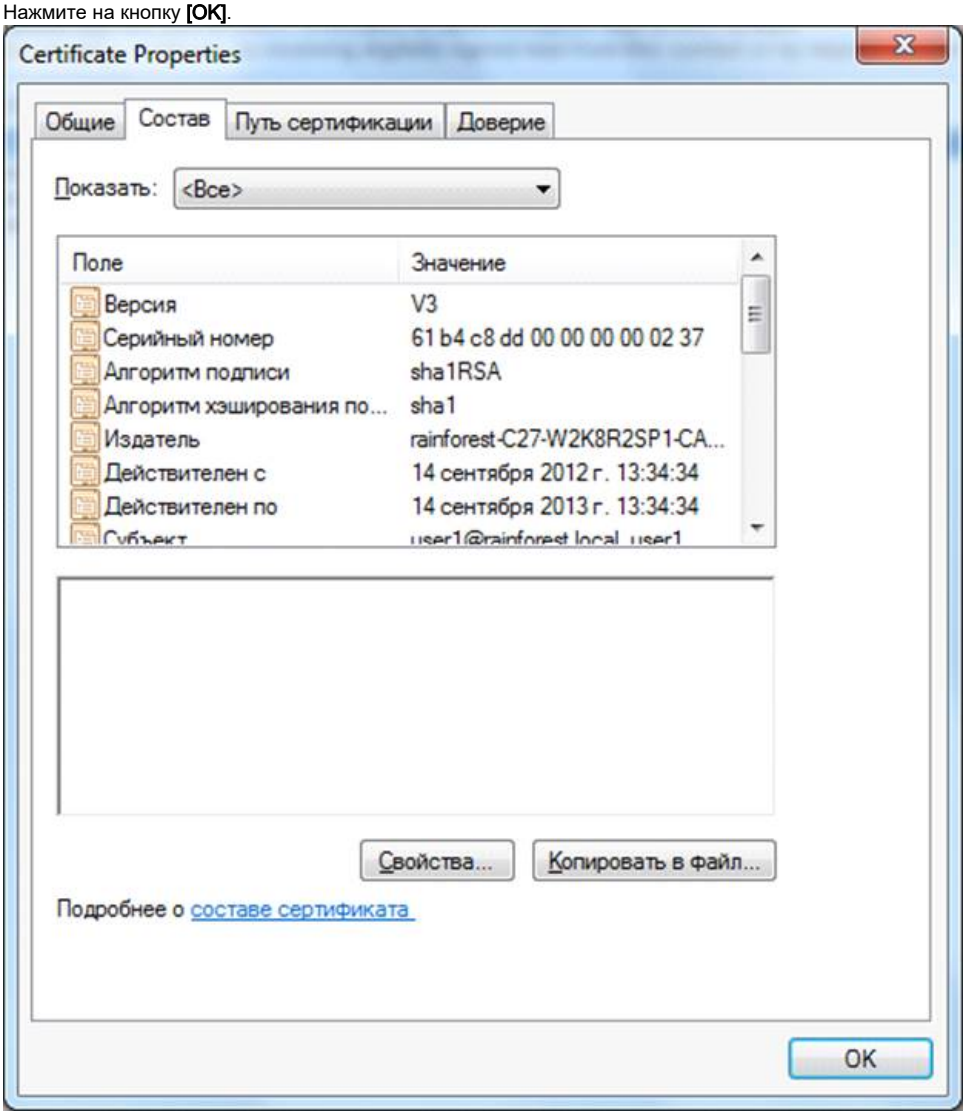
4. В окне свойств контакта нажмите на кнопку **[Сертификаты]**.



5. Один из сертификатов отправителя отмечен как сертификат по умолчанию. Щелкните по его названию и нажмите на кнопку **[Свойства...]**.

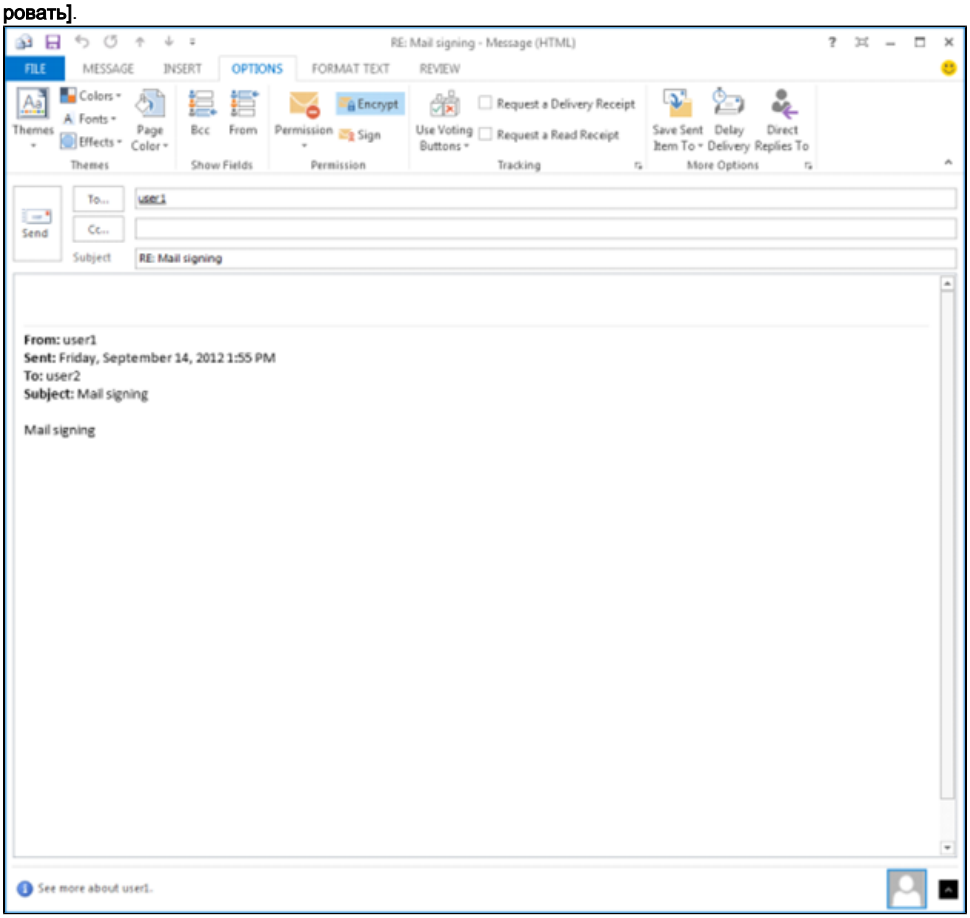


6. Проверьте, что это тот сертификата, с помощью которого вы хотите шифровать почтовые сообщения для этого контакта.
7. Нажмите на кнопку **[OK]**.



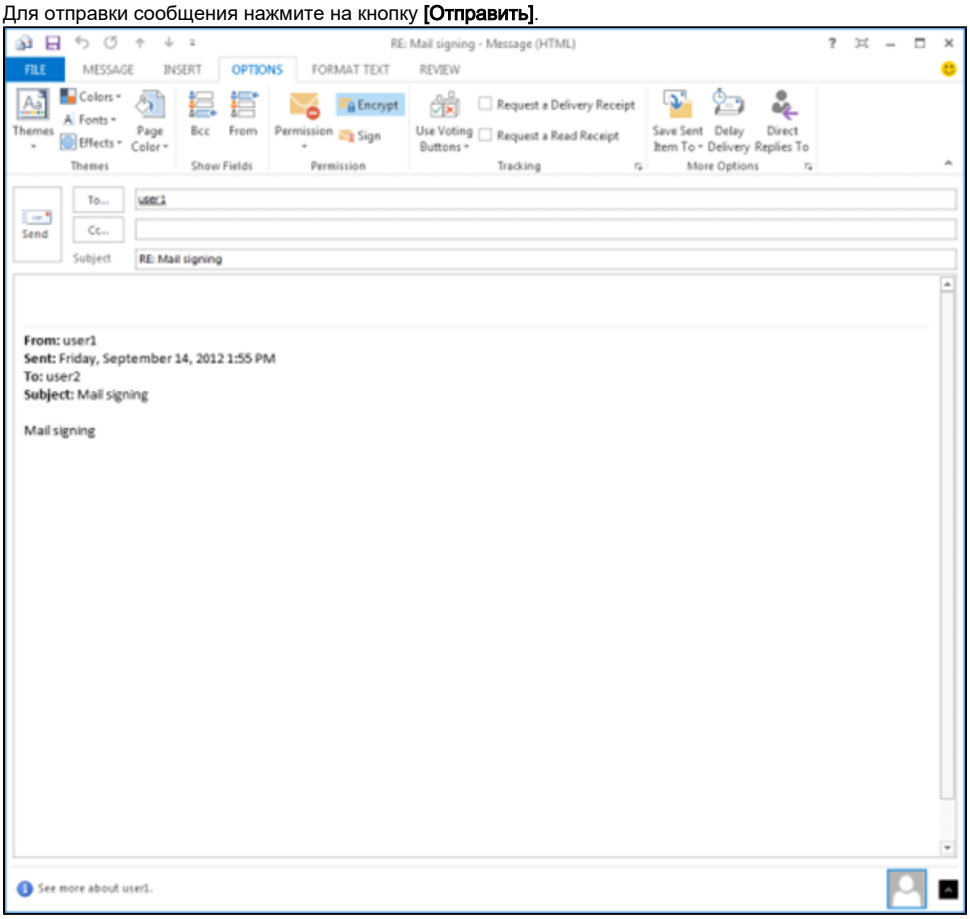
8. Закройте окно контакта.

9. При создании нового почтового сообщения для заведенного ранее контакта, перейдите на вкладку **Параметры** и нажмите на кнопку **[Шифровать]**.

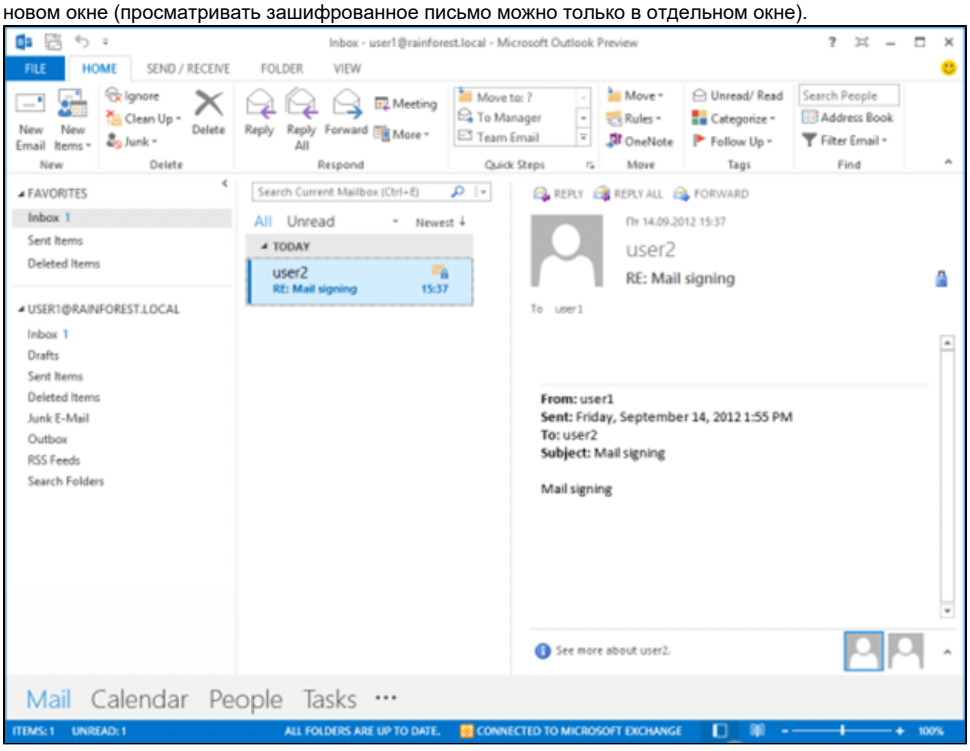


Можно настроить **Outlook 2013** таким образом, чтобы все создаваемые почтовые сообщения автоматически подписывались и шифровались при отправлении. Для этого в главном окне **Outlook 2013** зайдите в меню **Файл**, выберите пункт **Параметры**. В окне **Центр управления безопасностью** выберите пункт **Защита электронной почты**. В разделе **Защита электронной почты** выберите опции **Шифровать содержимое и вложения исходящих сообщений** для шифрования всех исходящих почтовых сообщений **Добавлять цифровую подпись к исходящим сообщениям** для создания электронной цифровой подписи исходящих сообщений соответственно.

10. Для отправки сообщения нажмите на кнопку **[Отправить]**.

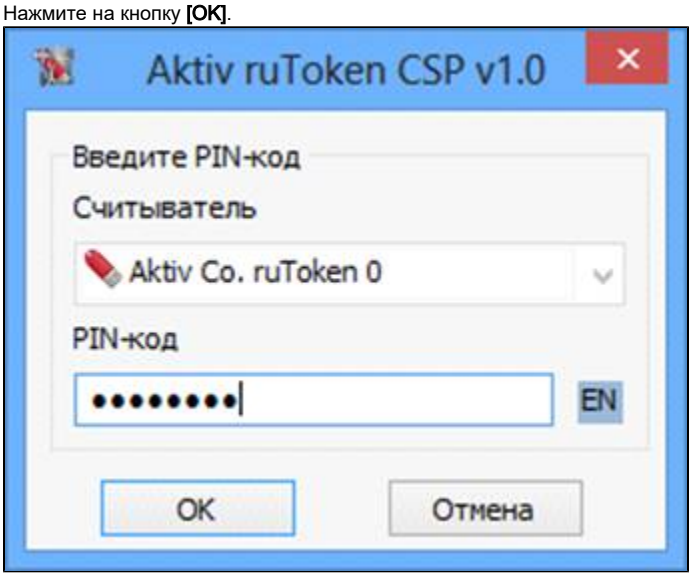


11. Для получения зашифрованного сообщения кликните дважды по его значку в папке **Входящие**. Полученное сообщение откроется в новом окне (просматривать зашифрованное письмо можно только в отдельном окне).



12. Введите PIN-код Пользователя устройства Рутокен.

13. Нажмите на кнопку **[OK]**.



14. Зашифрованное сообщение будет расшифровано и доступно для прочтения:

