ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

МЕТОДОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БОРОТЬБИ

Практичне заняття

Тема 2. Криптографічний захист інформації

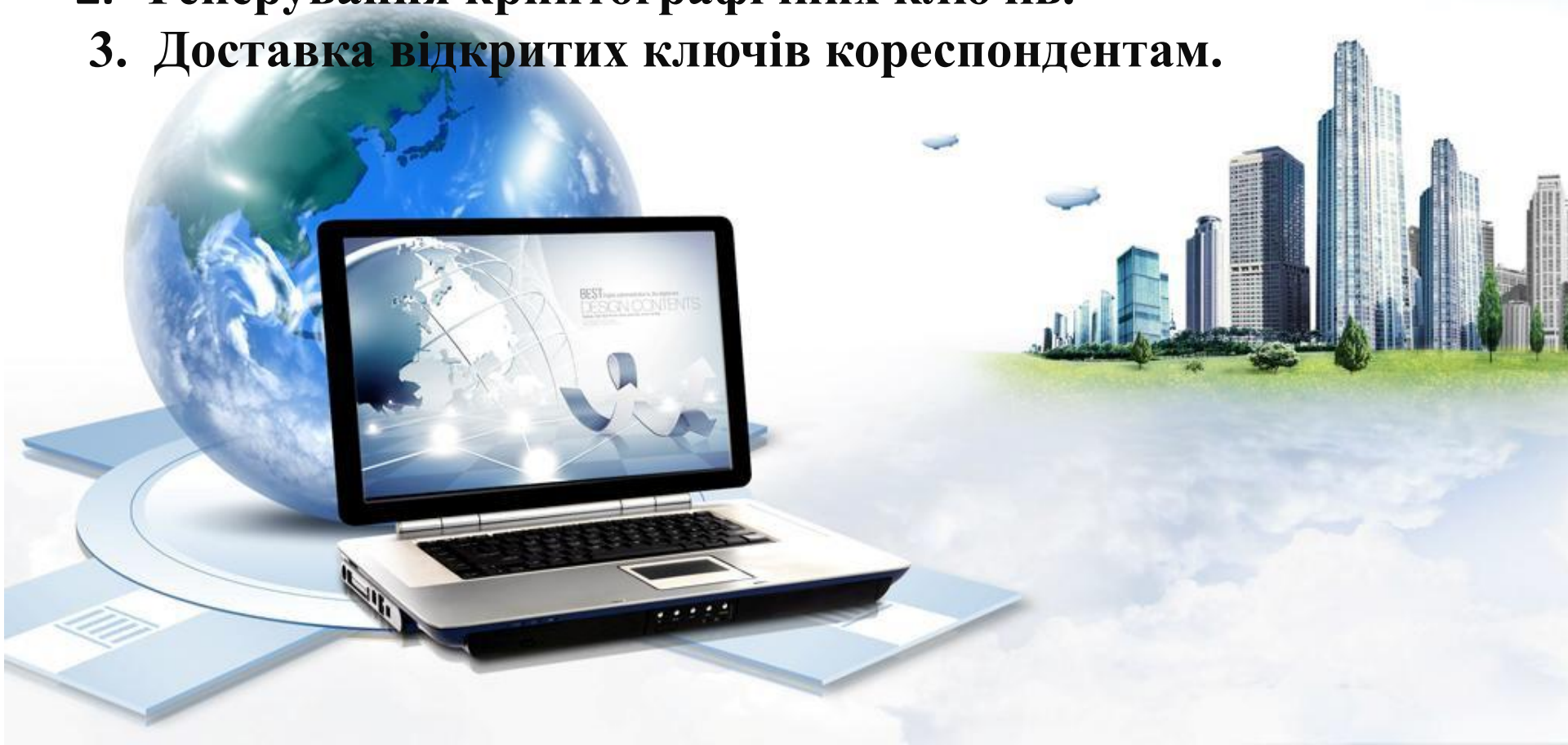
Заняття 2. Захист електронного листування за допомогою системи PGP.

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

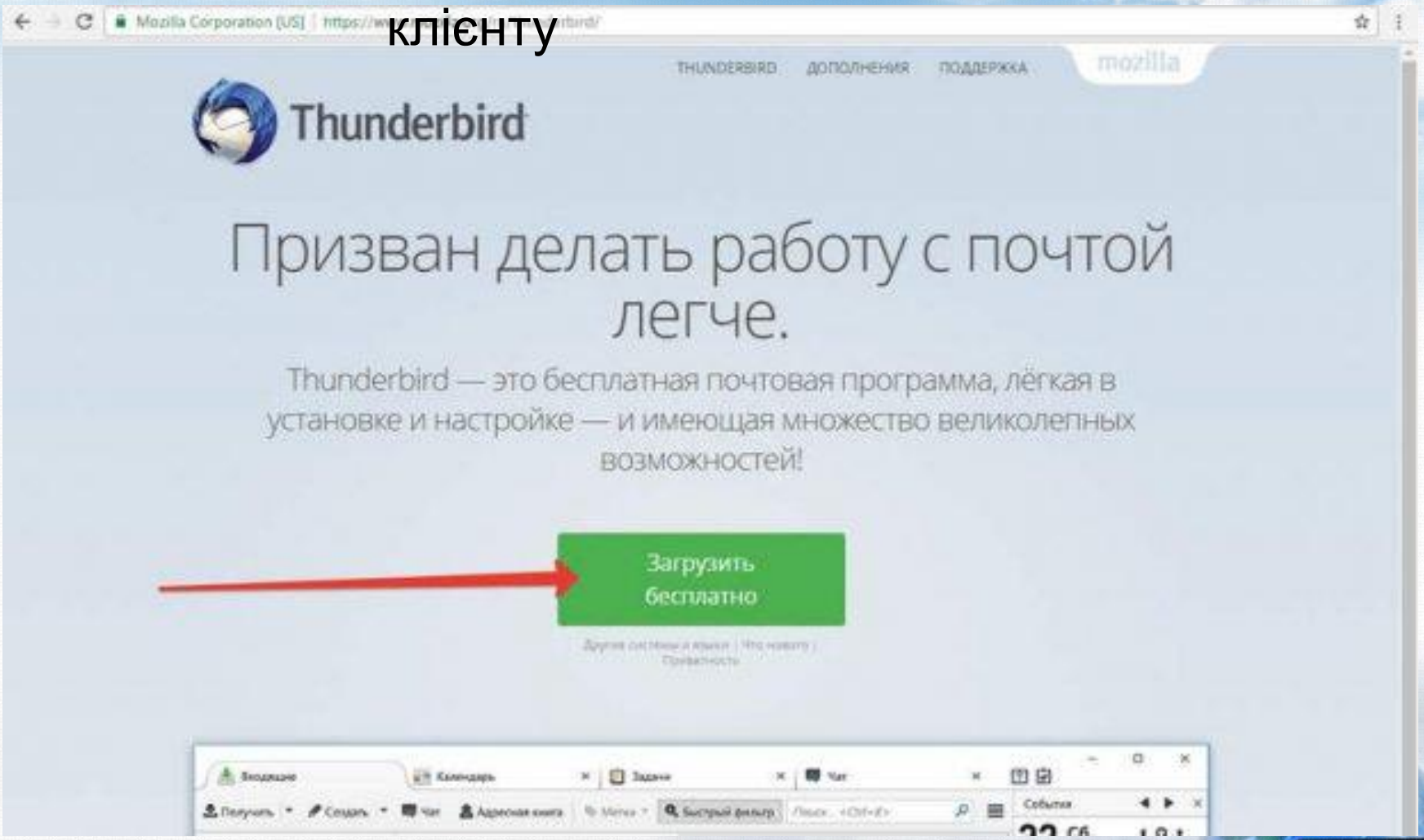
МЕТОДОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БОРОТЬБИ

Практичне заняття

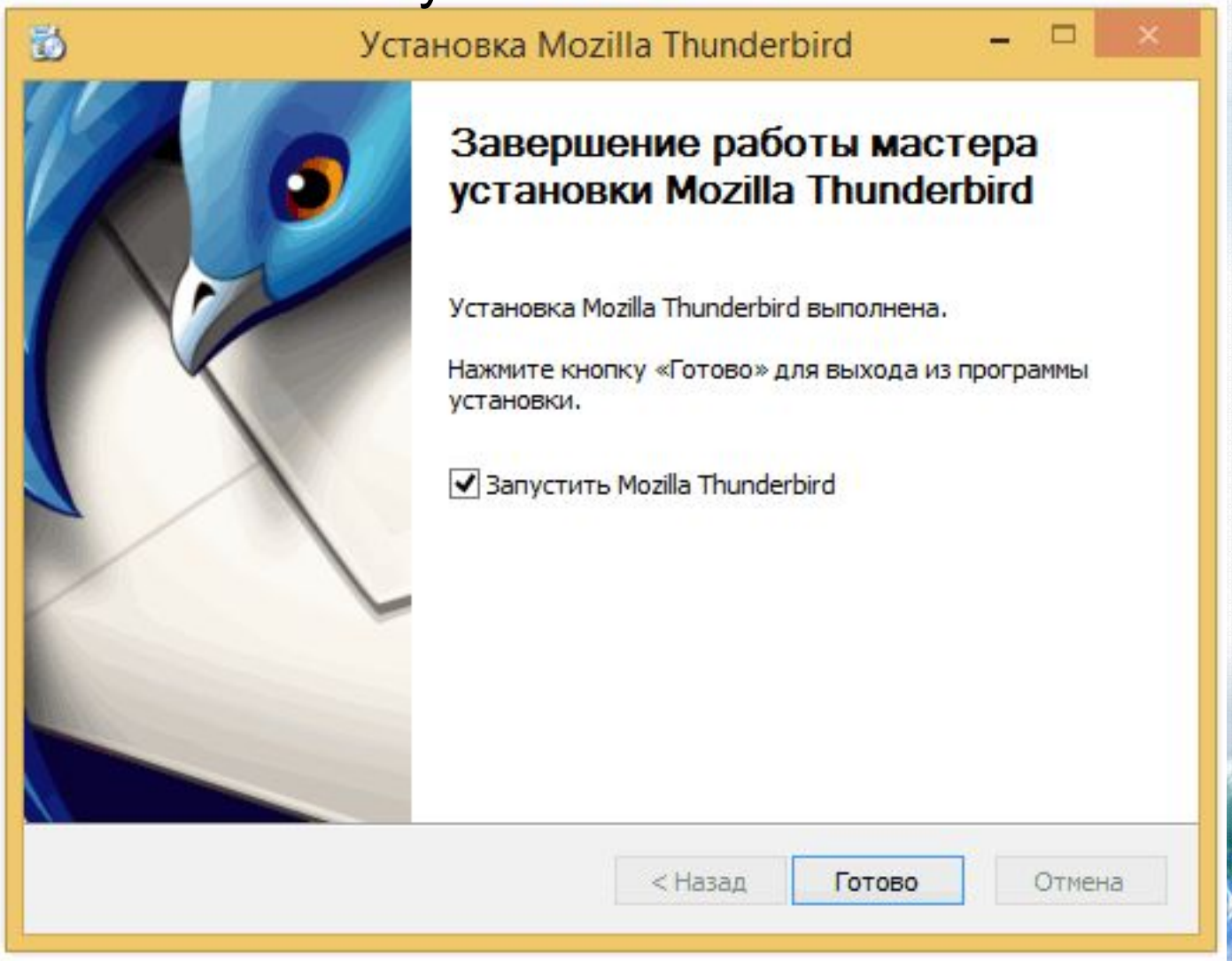
1. **Можливості та базові прийоми застосування системи PGP.**
2. **Генерування криптографічних ключів.**
3. **Доставка відкритих ключів кореспондентам.**



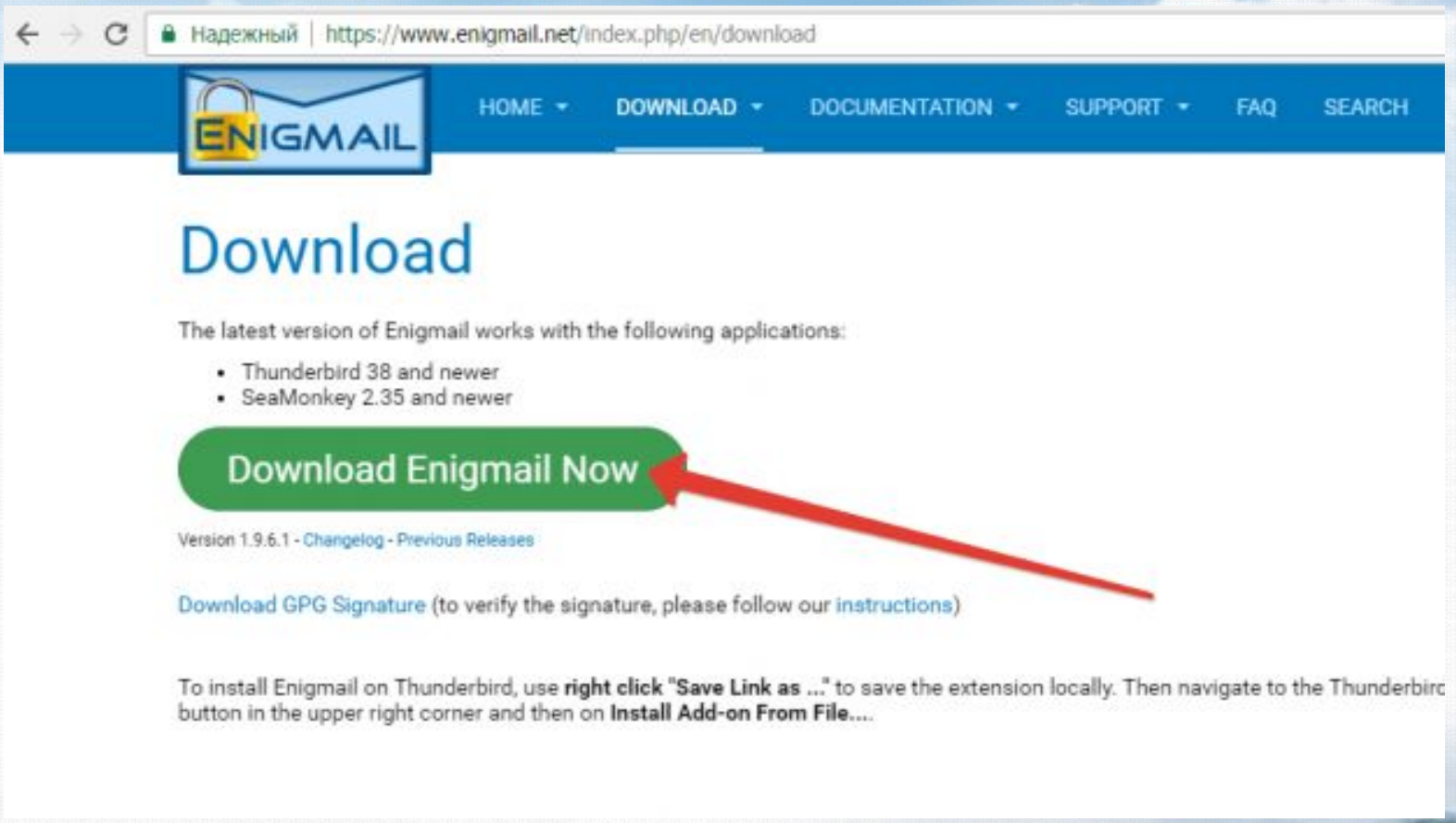
Установка поштового клієнту



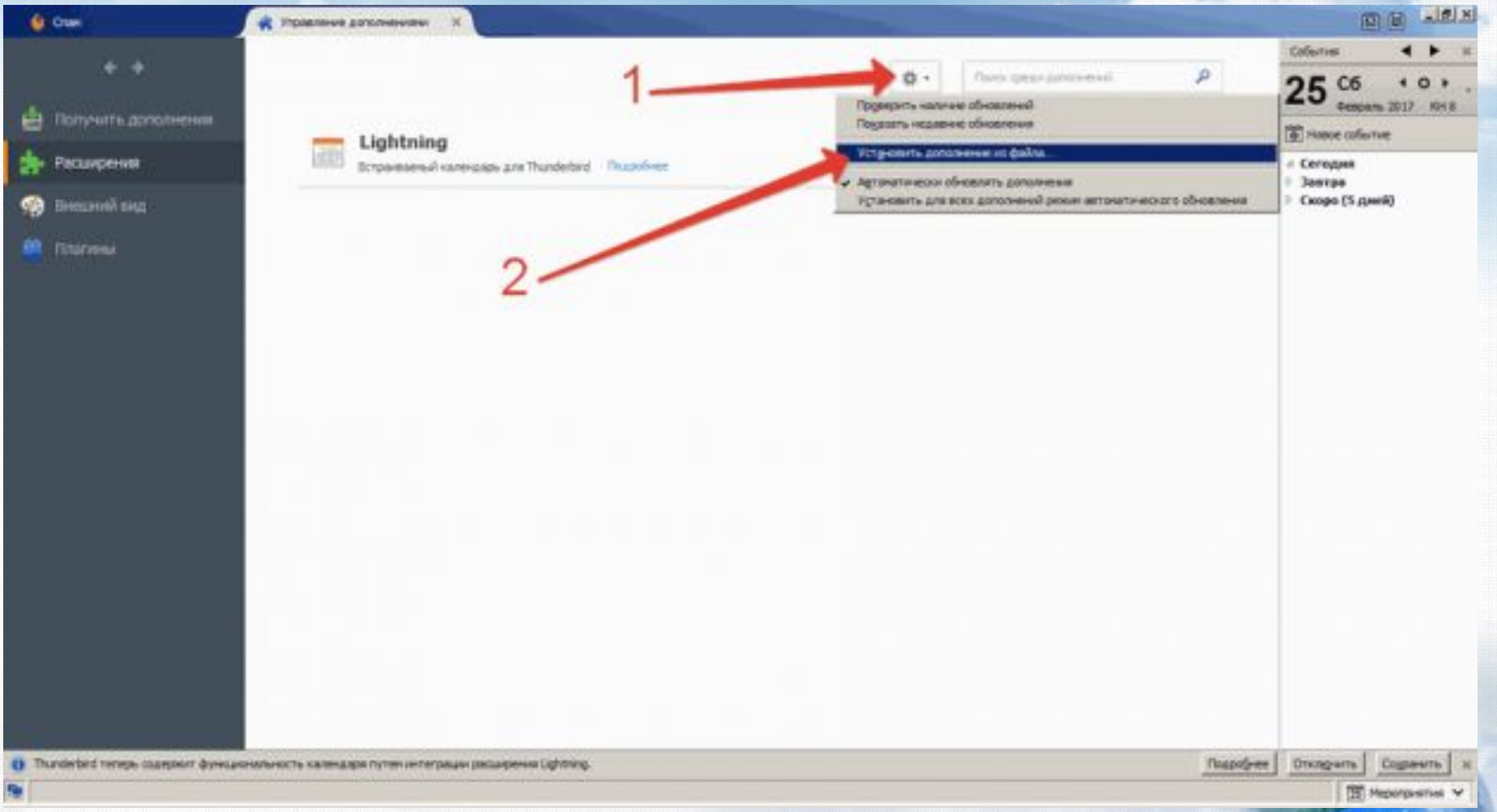
Установка поштового клієнту



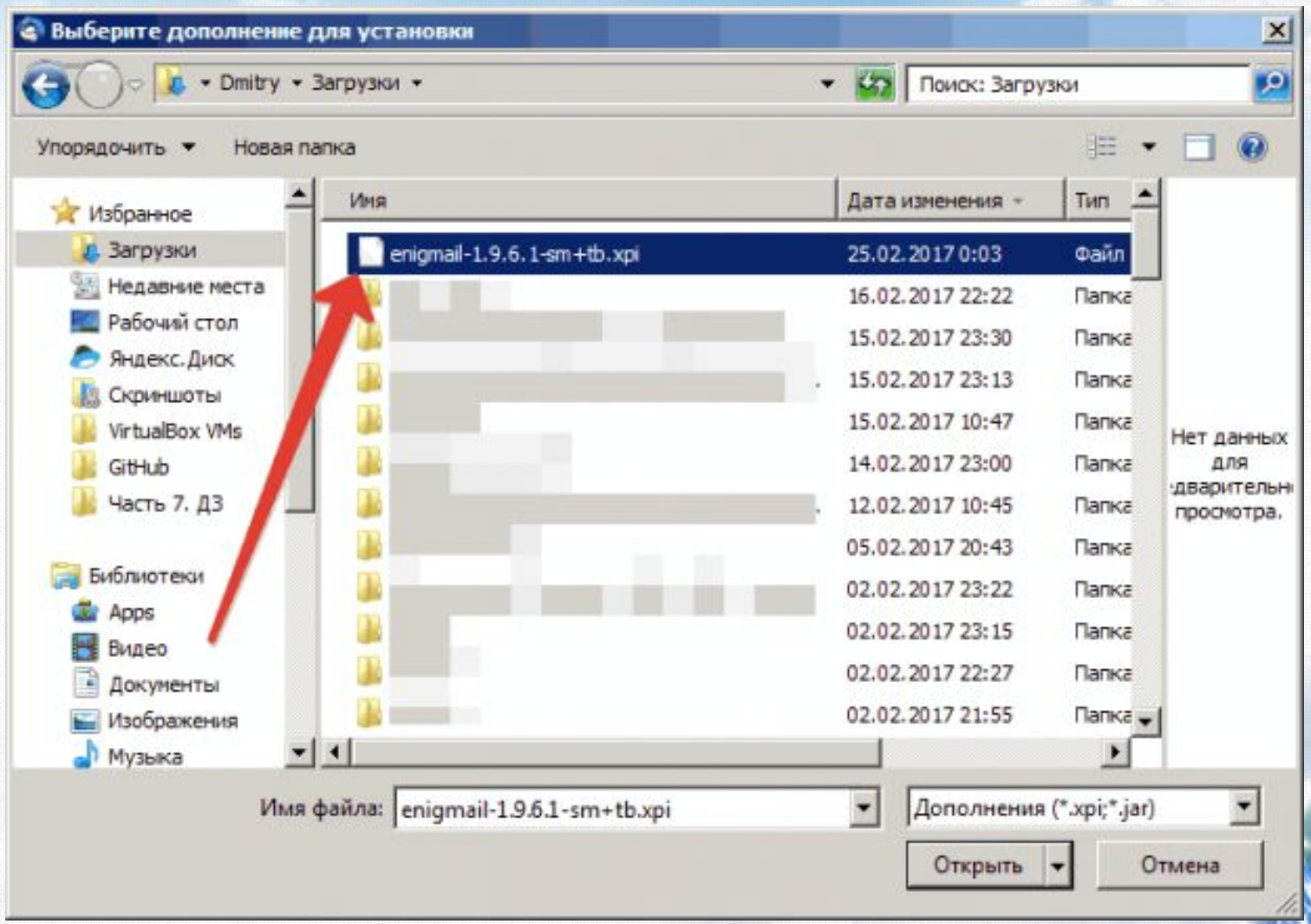
Установка плагіна PGP-шифрування **Enigmail**



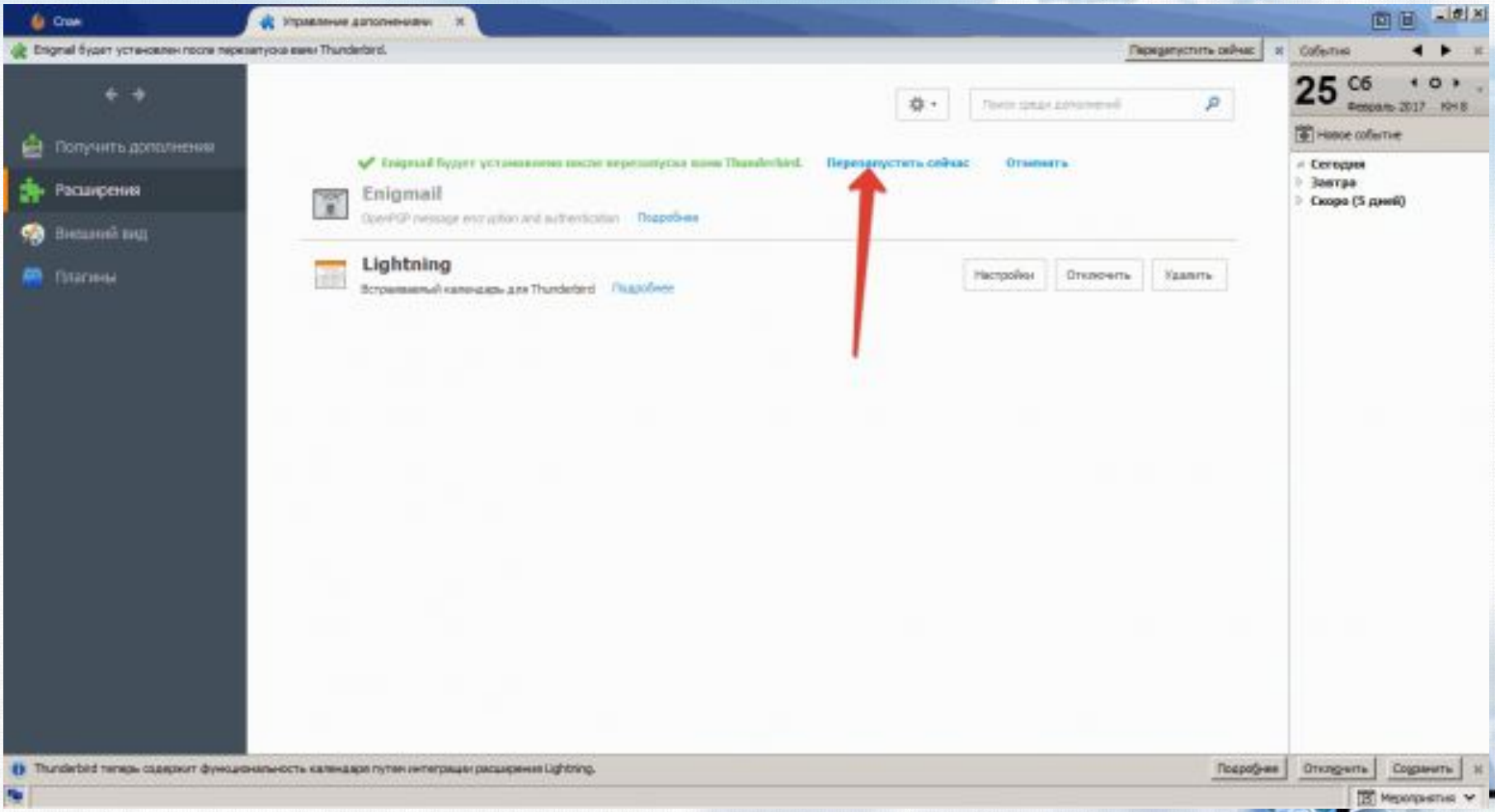
Установка плагіна PGP-шифрування **Enigmail**



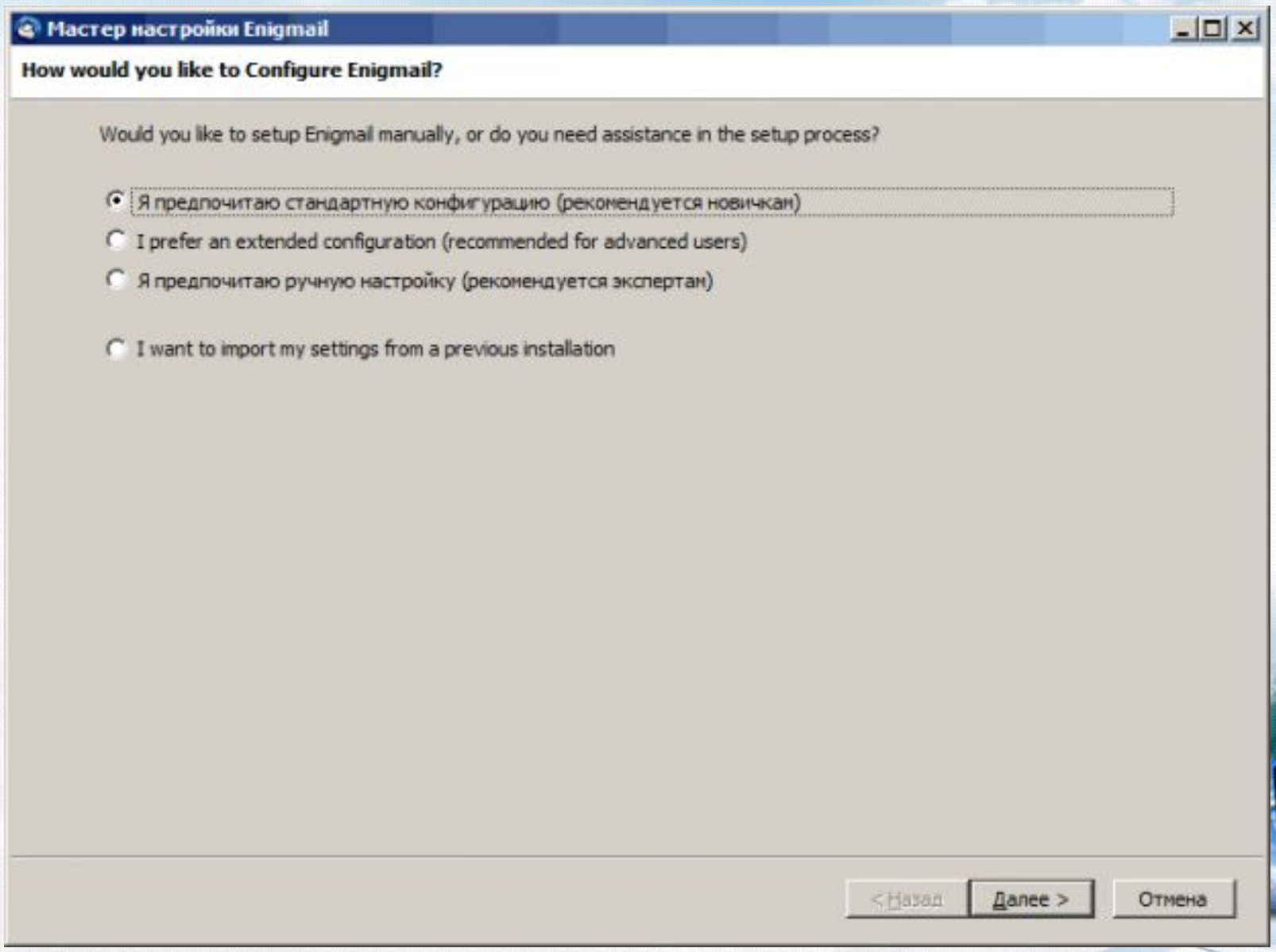
Установка плагіна PGP-шифрування **Enigmail**



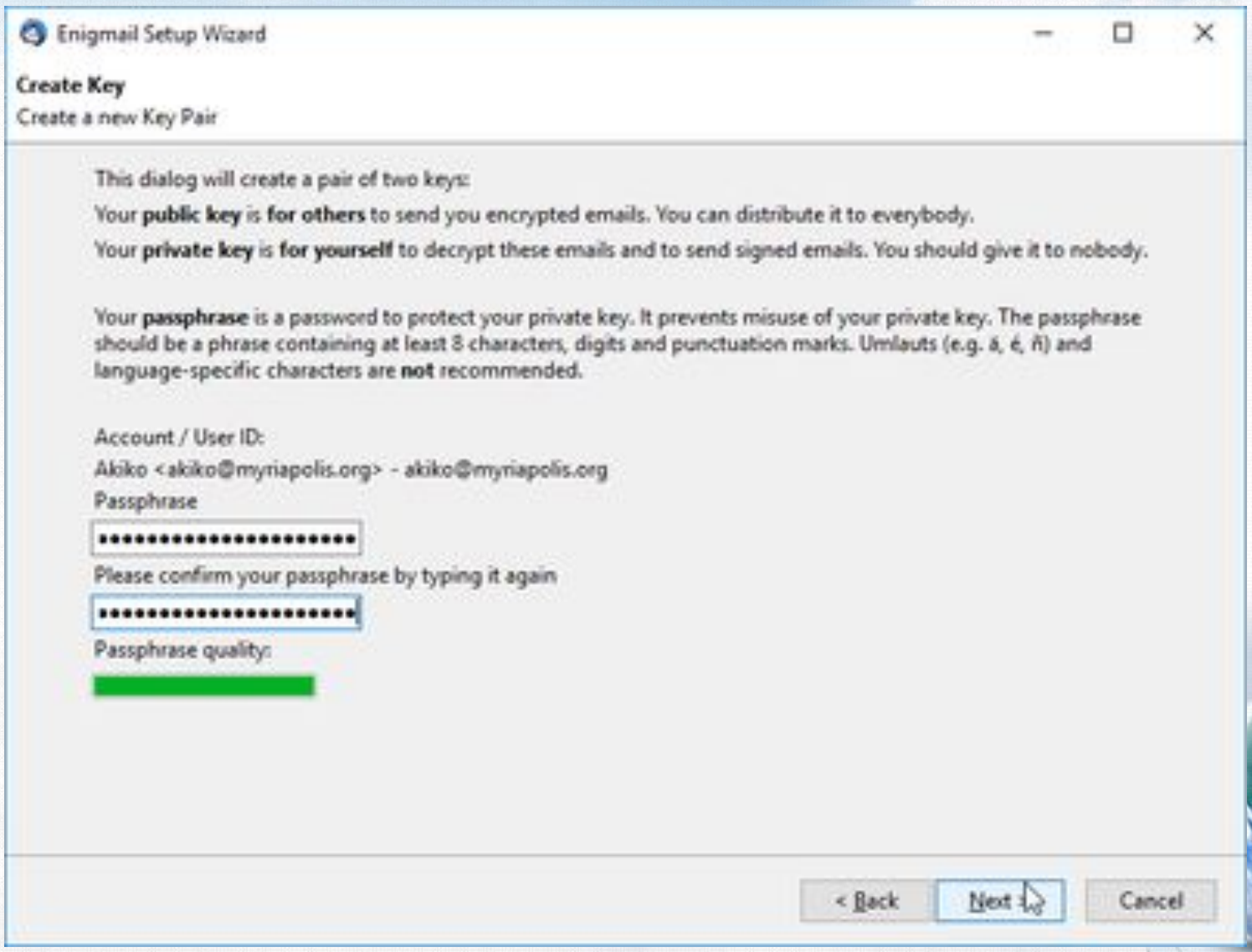
Установка плагіна PGP-шифрування **Enigmail**



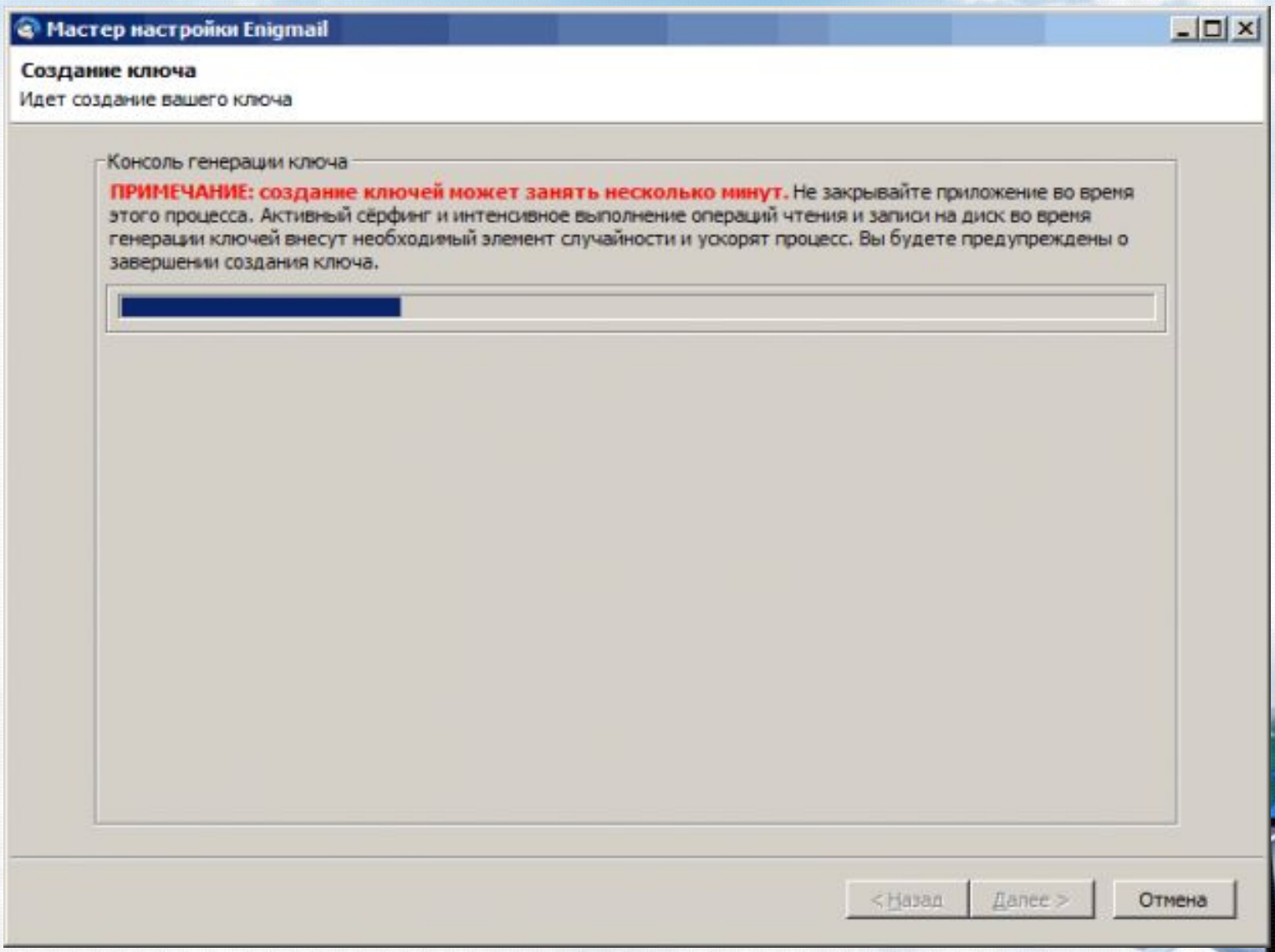
Налаштування плагіна PGP-шифрування **Enigmail**



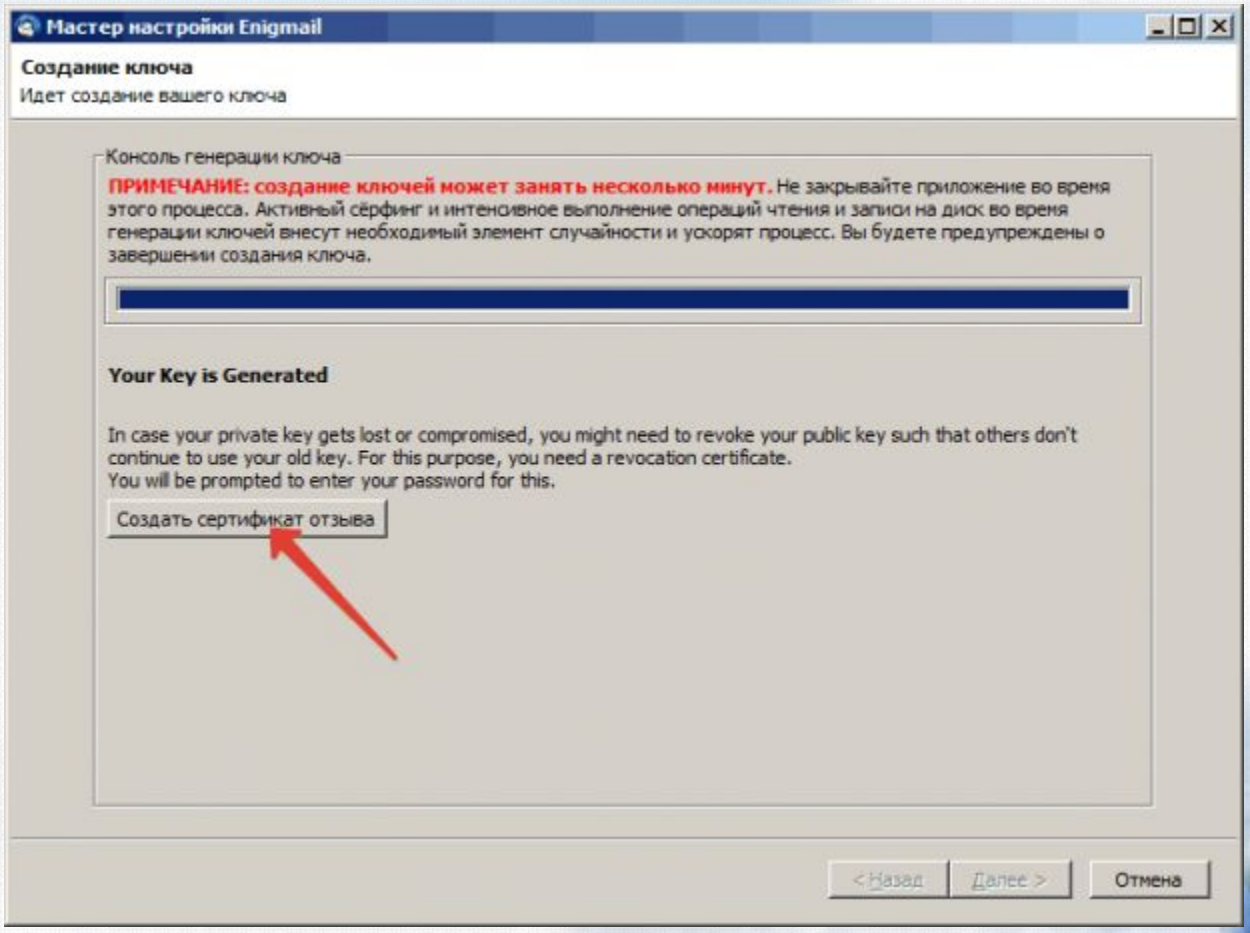
Створення **пари** ключів **Enigmail**



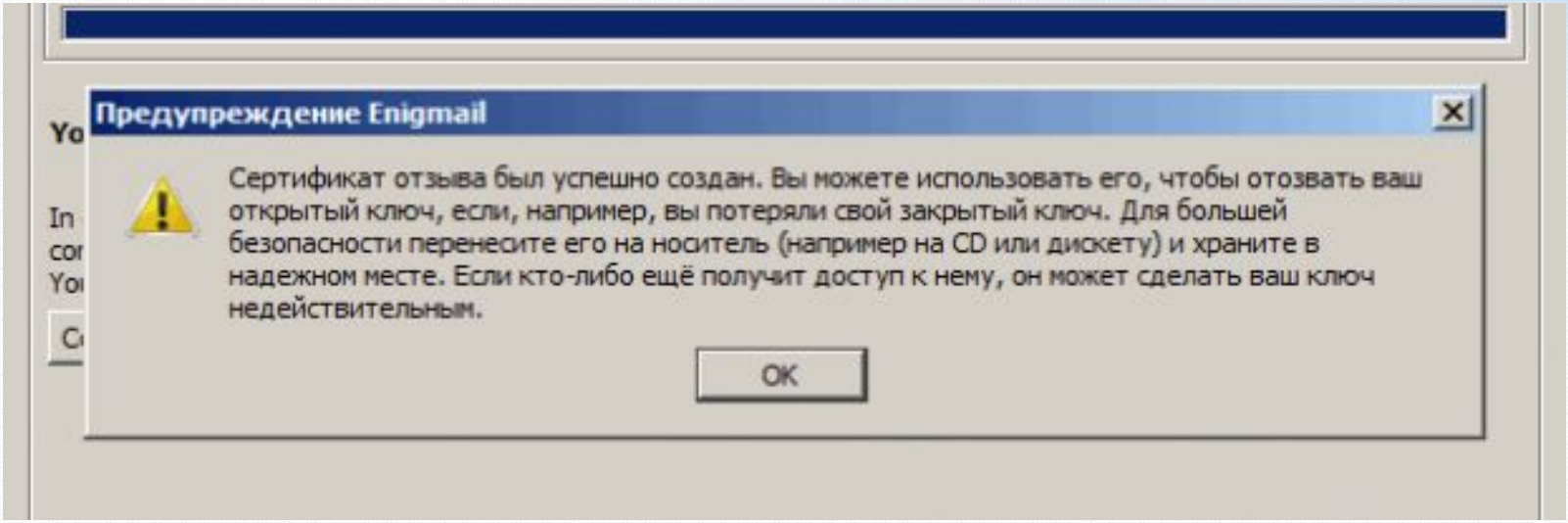
Створення **пари** ключів **Enigmail**



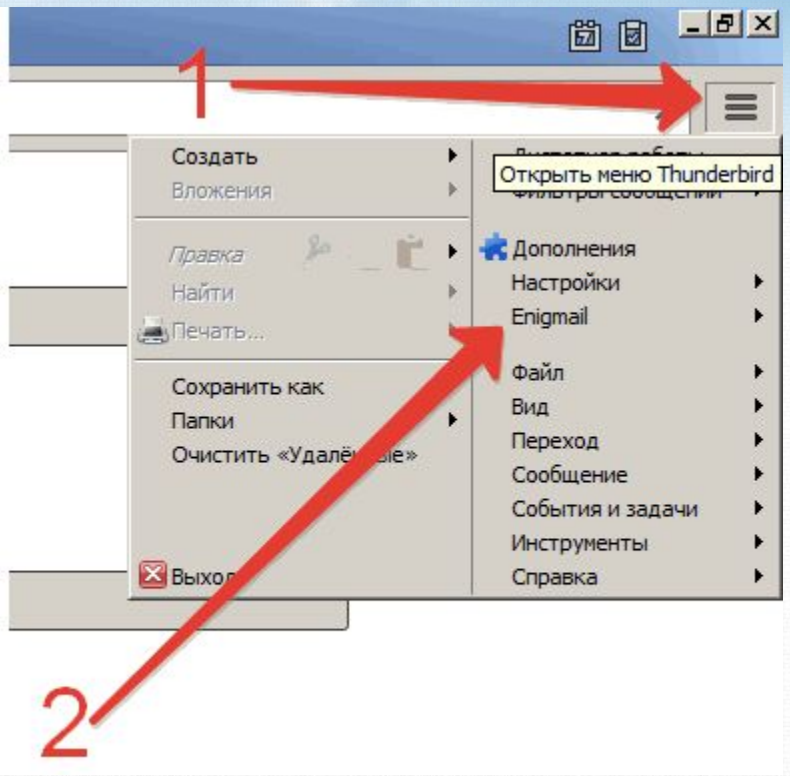
Створення **сертифікату відклику ключів**

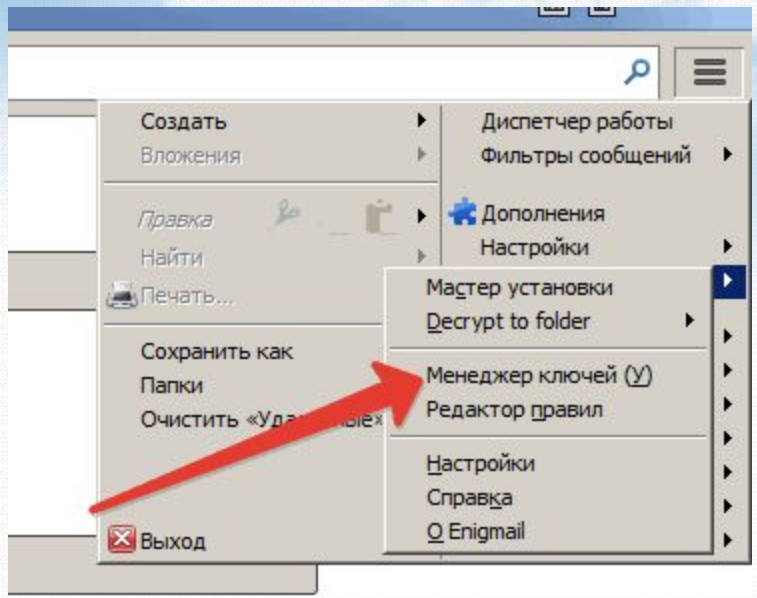


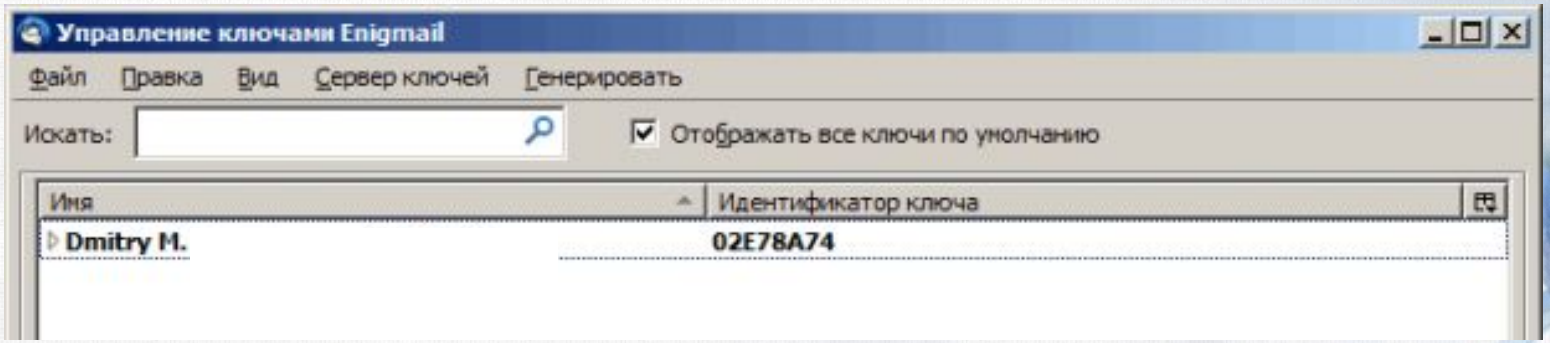
Створення **сертифікату відклику ключів**



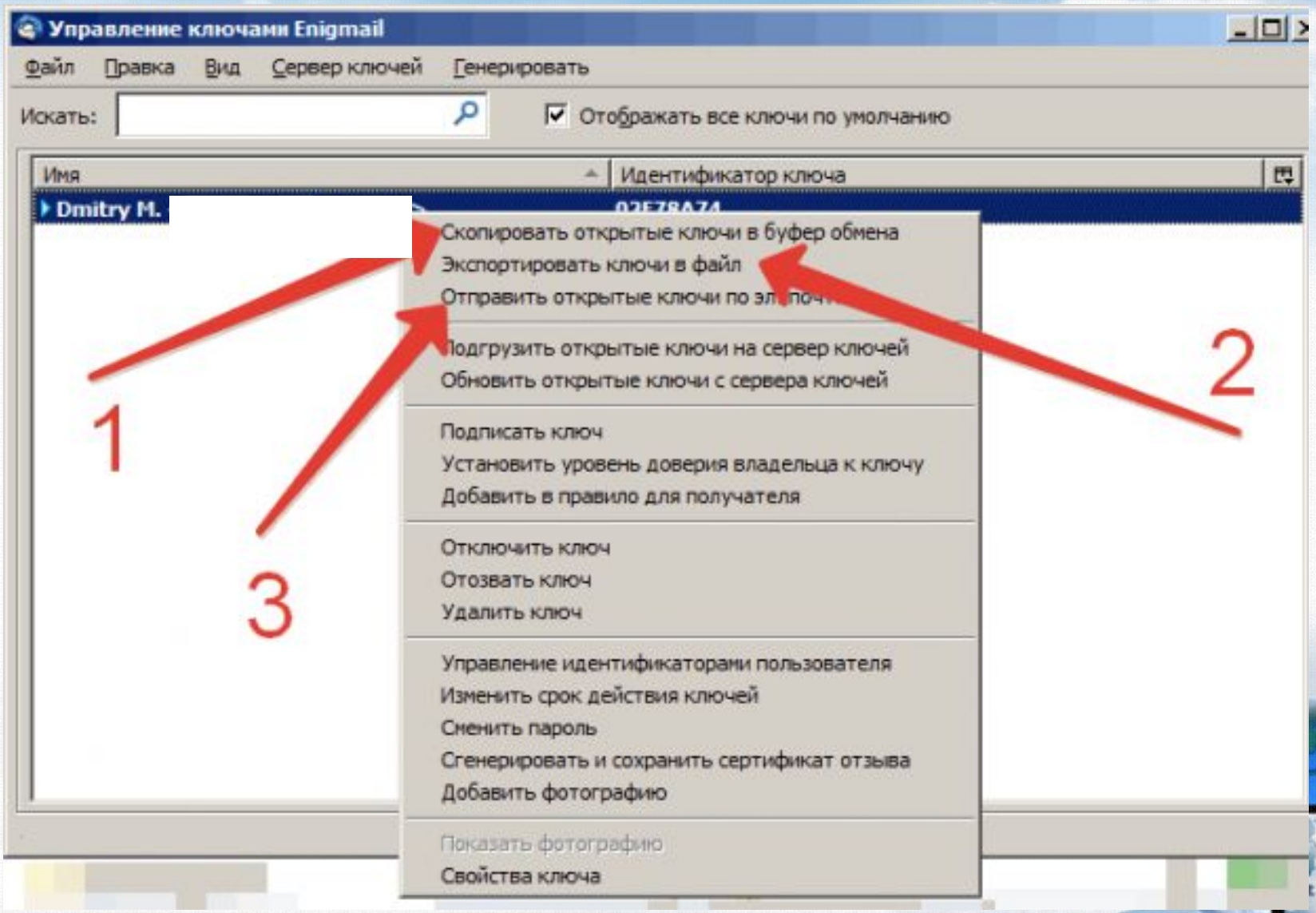
Створення **сертифікату відклику ключів**





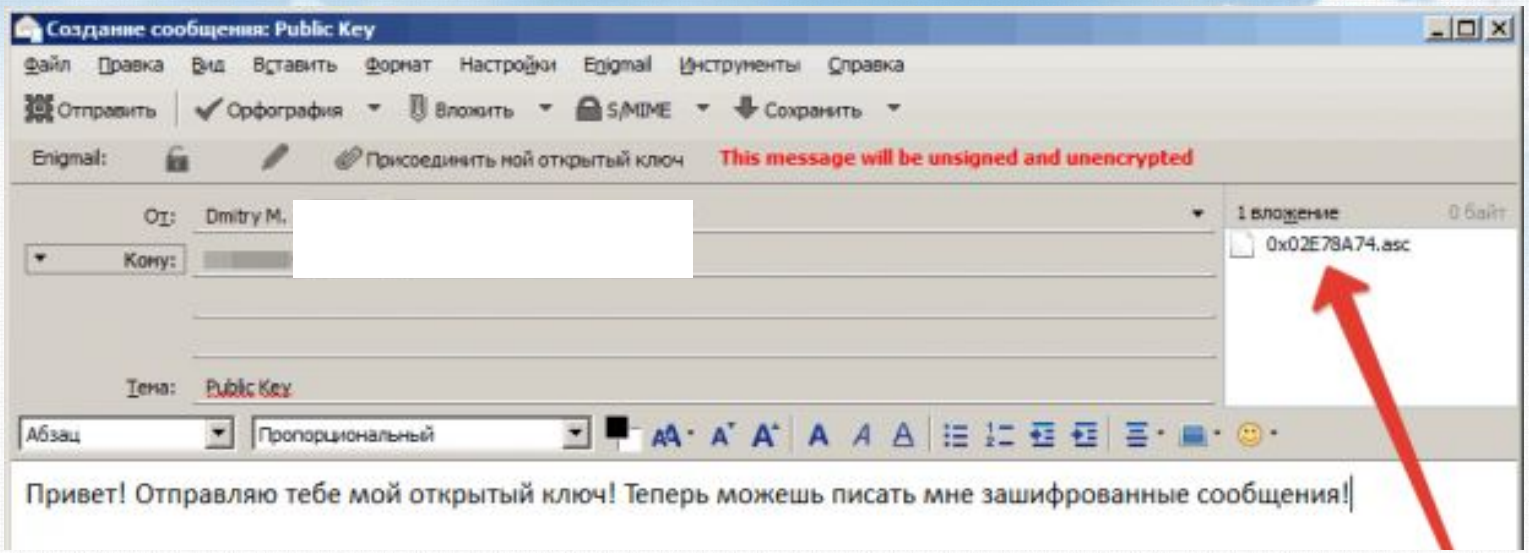


Обмін відкритими **ключами**

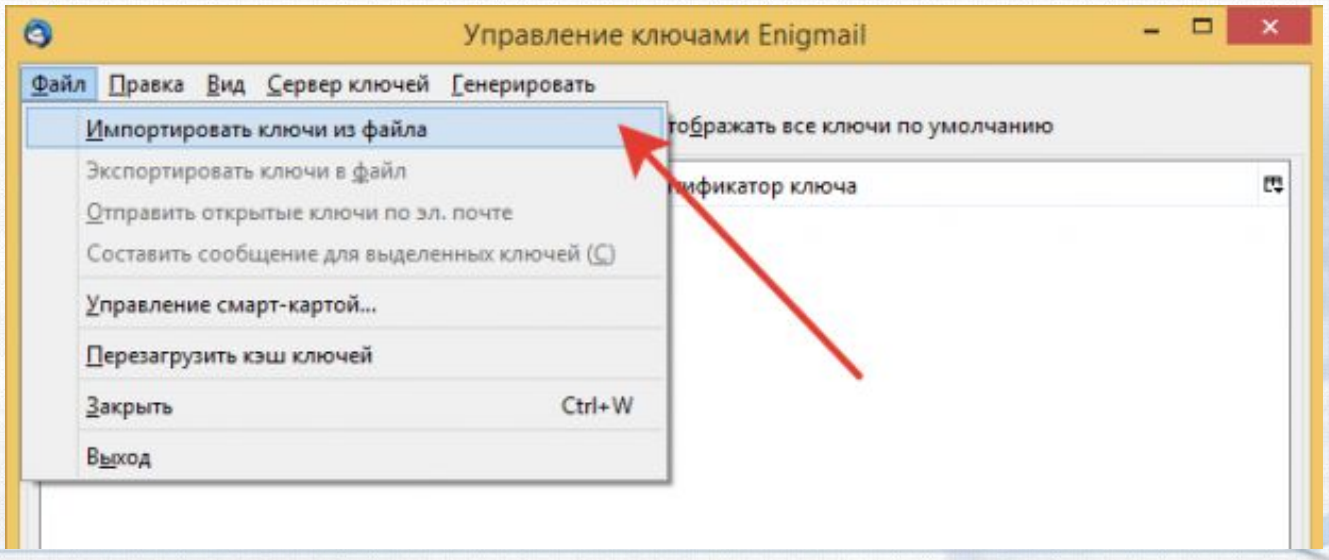


Обмін відкритими **ключами**

1:

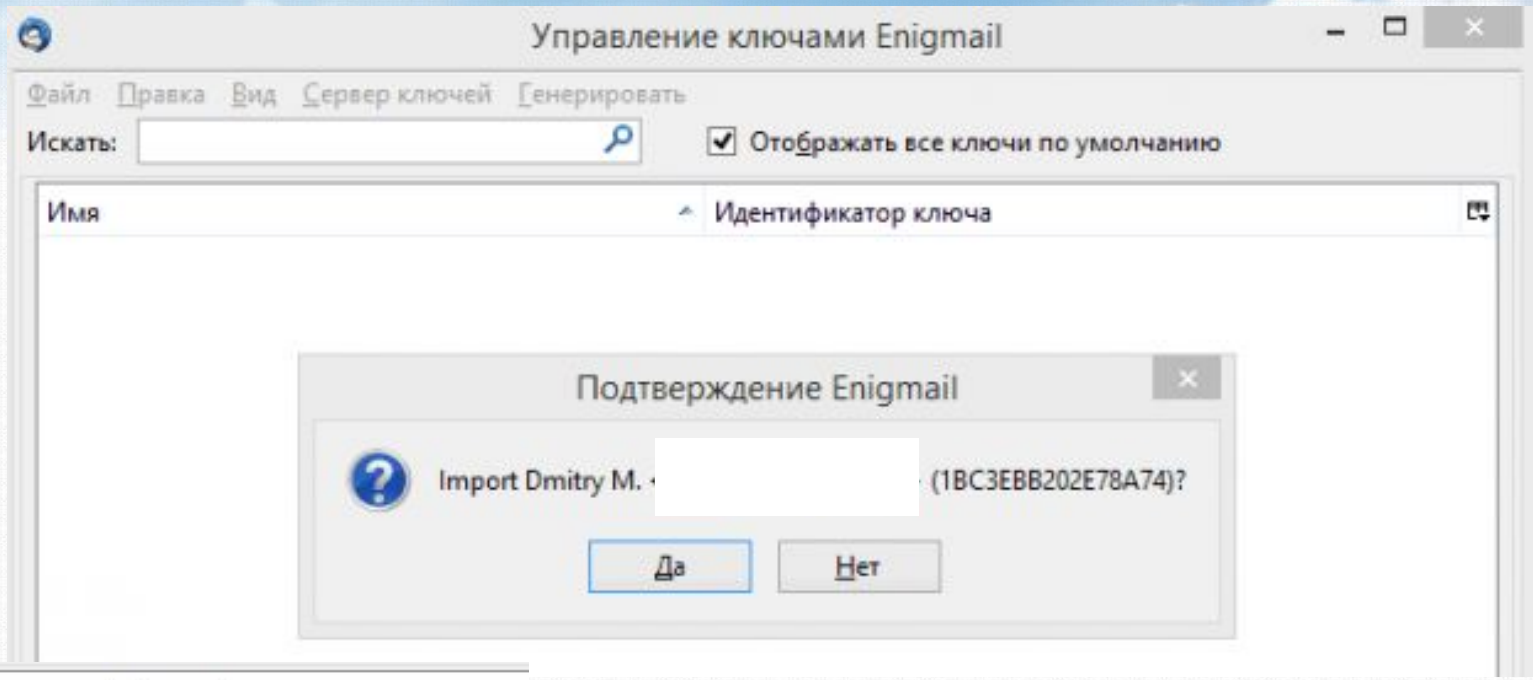


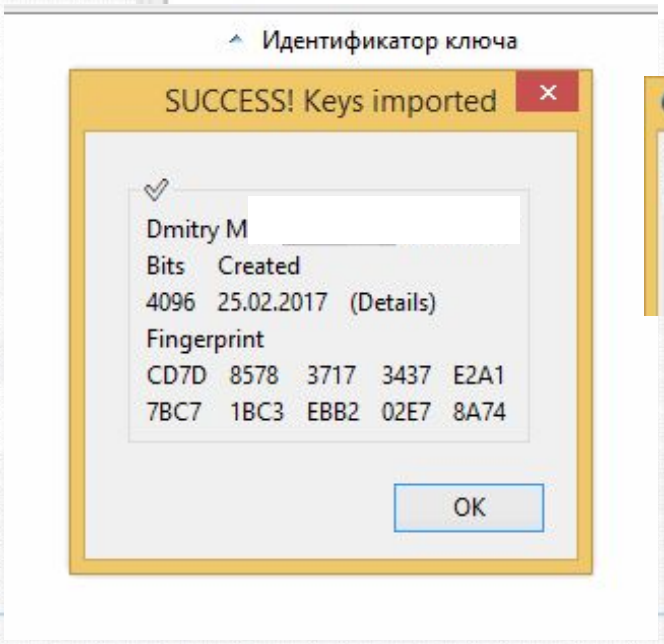
2:

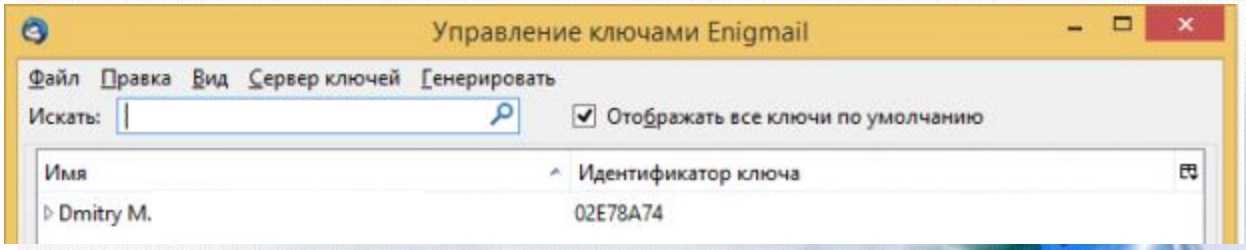


Обмін відкритими **ключами**

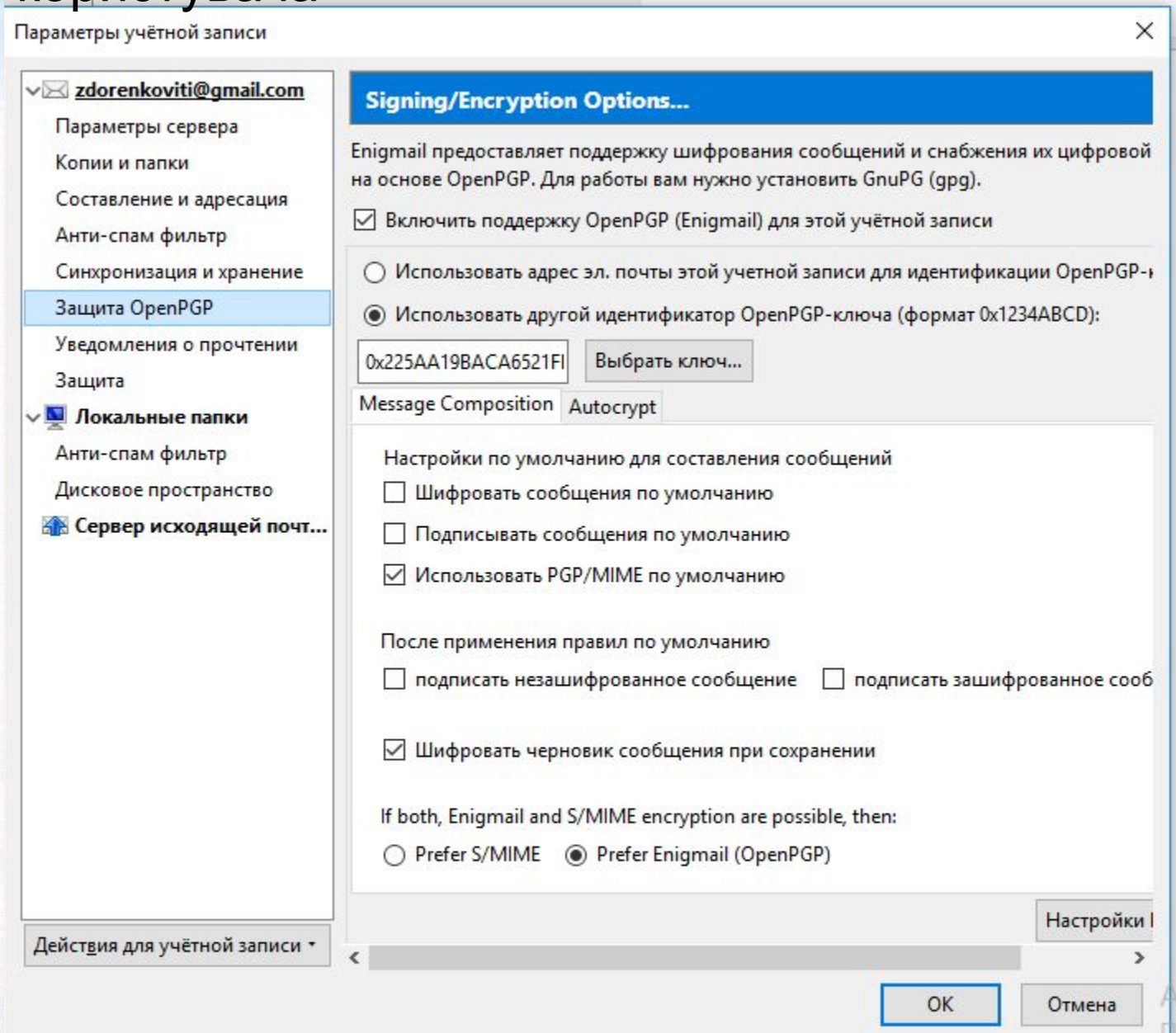
2:





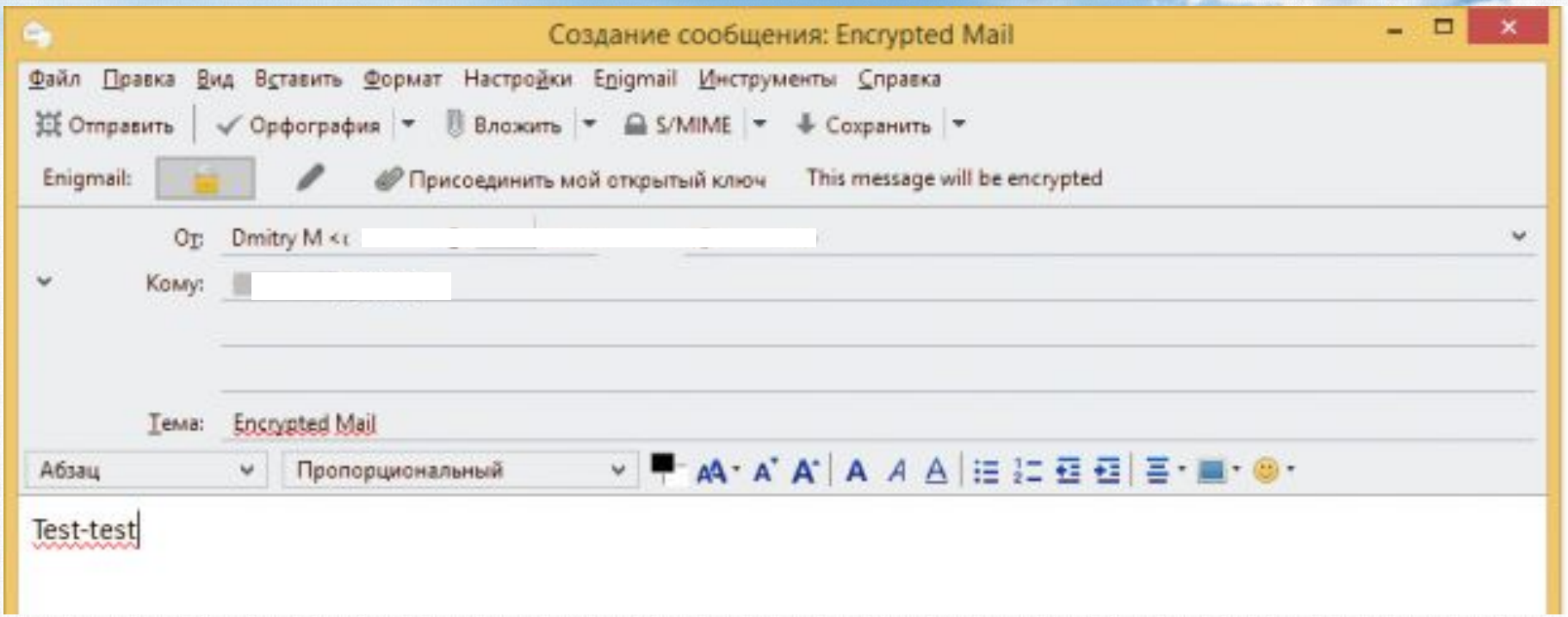


Застосування **Enigmail** до облікового запису користувача

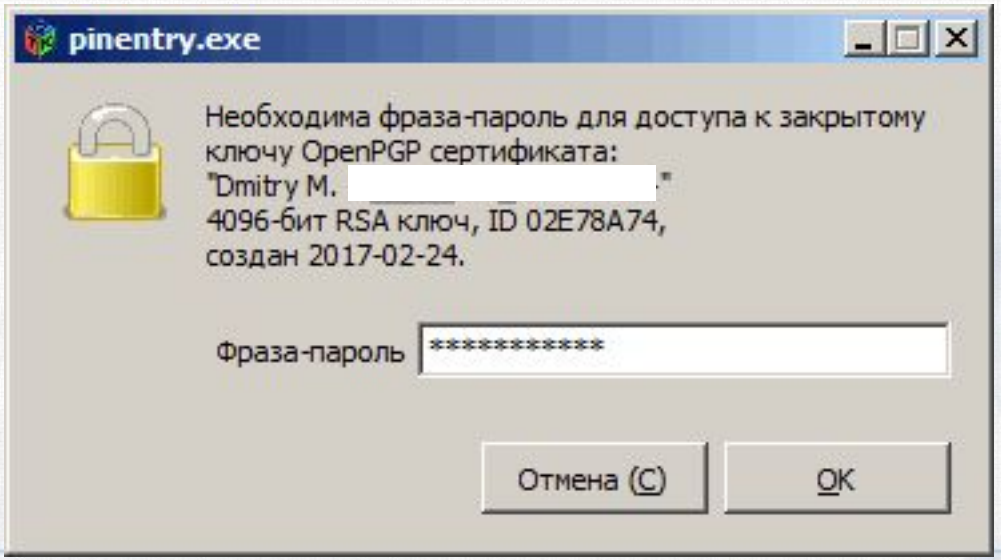


Створення та отримання захищеного повідомлення

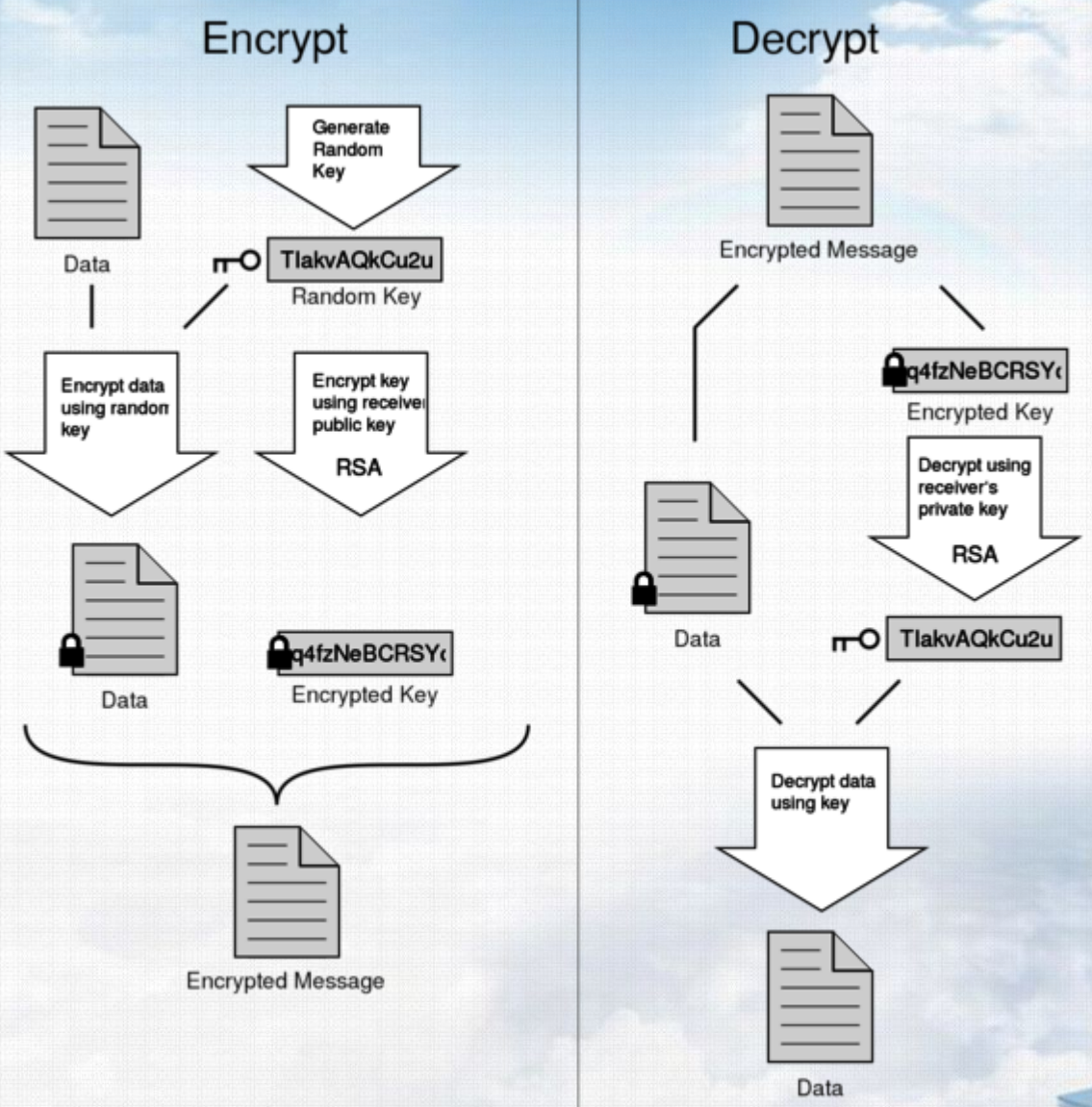
2:



1:



PGP(Pretty Good Privacy) система



ПРАКТИЧНЕ ЗАВДАННЯ

1. **Встановити поштові клієнти**
2. **Налаштувати облікові записи користувачів для відправки та отримання електронної пошти.**
3. **Обмінятися електронними листами з кореспондентом**
4. **Відстежити Wireshark його вміст.**
5. **Встановити криптоплагін PGP до поштового клієнту.**
6. **Згенерувати пари криптографічних ключів(відкритий та закритий)**
7. **Захистити закриті ключі паролем.**
8. **Створити сертифікати відклику ключів**
6. **Обмінятися відкритими ключами з кореспондентами.**
7. **Створити зашифрований лист. Обмінятися електронними листами з кореспондентом.**
8. **Відстежити Wireshark його вміст.**
9. **Зробити висновки.**

Використані джерела інформації:

- Богуш В.М., Довидьков О.А., Кривуца В. Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.
- Кузьменко Б.В., Чайковська О.А. Захист інформації. Навчальний посібник. Ч.1. (Організаційно-правові засоби забезпечення інформаційної безпеки) - К., 2009. – 83 с.
- Соколов В. Ю. Інформаційні системи і технології: Навчальний посібник. - К .: ДУІКТ, 2010.
  - 138 с.
- Чунарьова А.В., Зюбіна Р.В. Проблеми захисту інформації в сучасних інформаційно- комунікаційних системах та мережах [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com/6_PNI_2011/Informatica/4_80227.doc.htm. – Назва з екрану.
- Захист інформації - українське законодавство у сфері захисту інформації [Електронний ресурс]. – Режим доступу: http://library.detut.edu.ua/index.php/zahustinformacii. – Назва з екрану.