



ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА
ІНФОРМАТИЗАЦІЇ

МЕТОДОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БОРОТЬБИ

Практичне

Тема 2. Криптографічний захист інформації
Заняття 2. Захист електронного листування
за допомогою системи PGP.



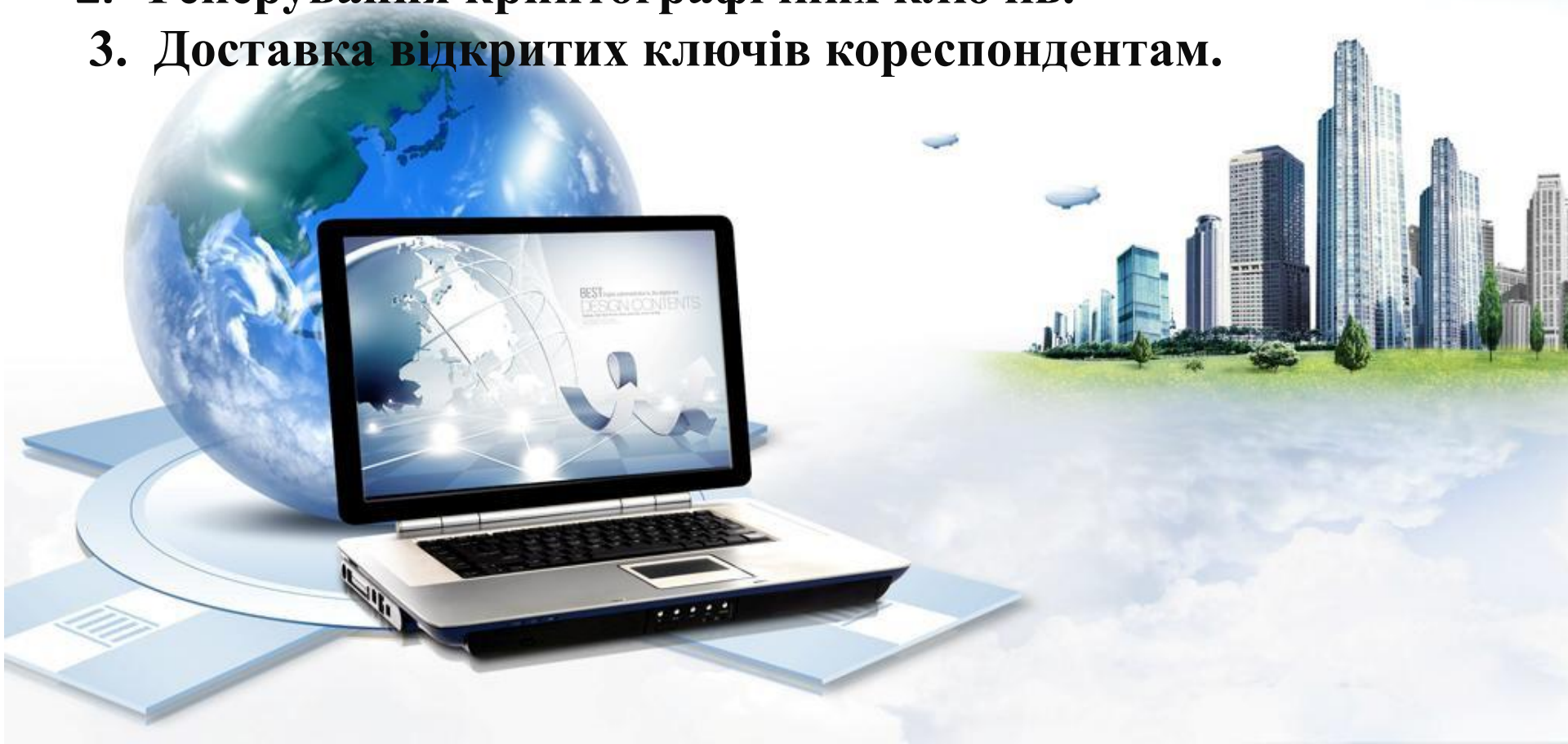


ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА
ІНФОРМАТИЗАЦІЇ

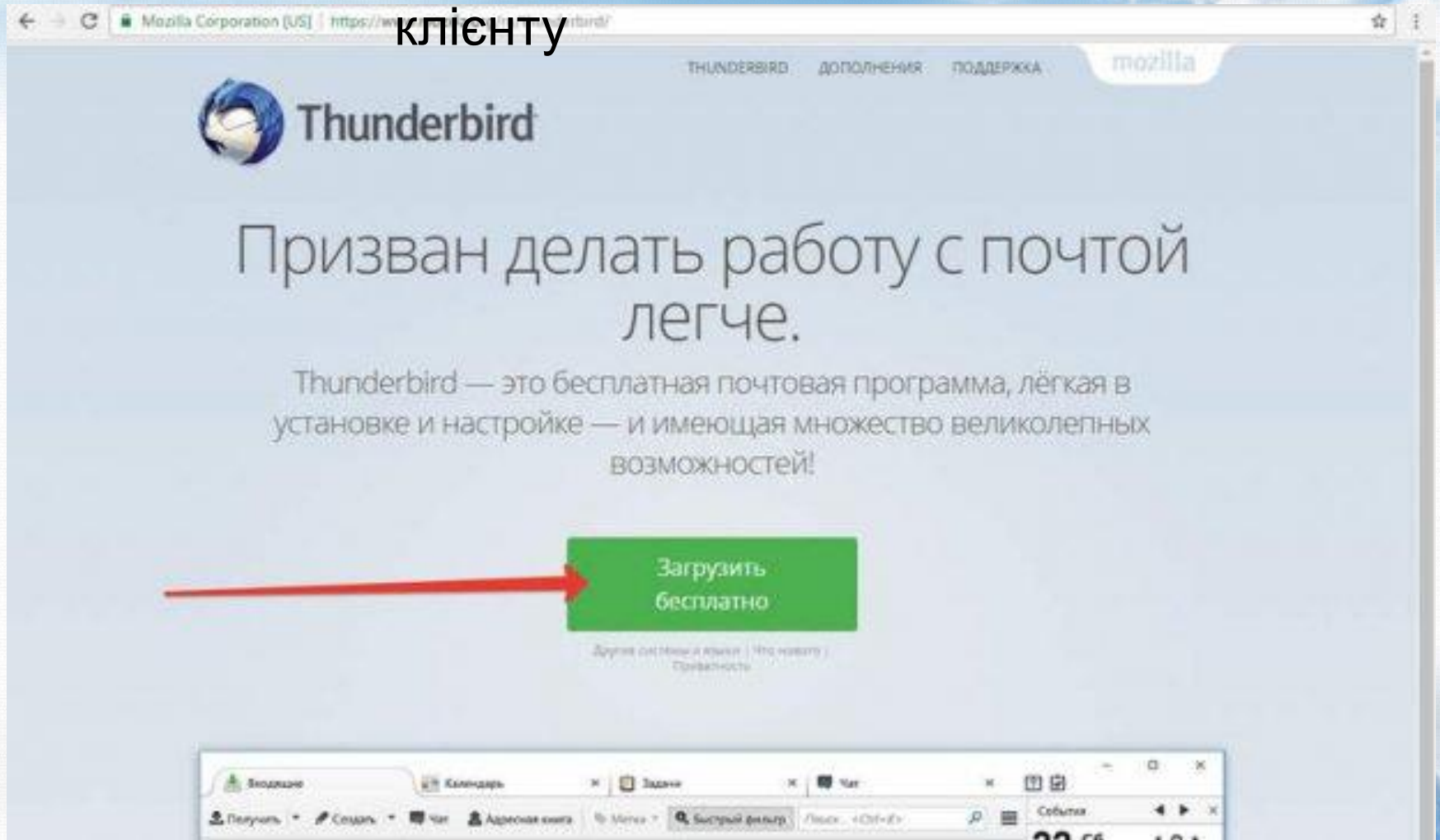
МЕТОДОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БОРОТЬБИ

Практичне
заняття


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



Установка поштового клієнту




THUNDERBIRD ДОПОЛНЕНИЯ ПОДДЕРЖКА mozilla

 **Thunderbird**

Призван делать работу с почтой легче.

Thunderbird — это бесплатная почтовая программа, лёгкая в
установке и настройке — и имеющая множество великолепных
возможностей!

 [Загрузить
бесплатно](#)

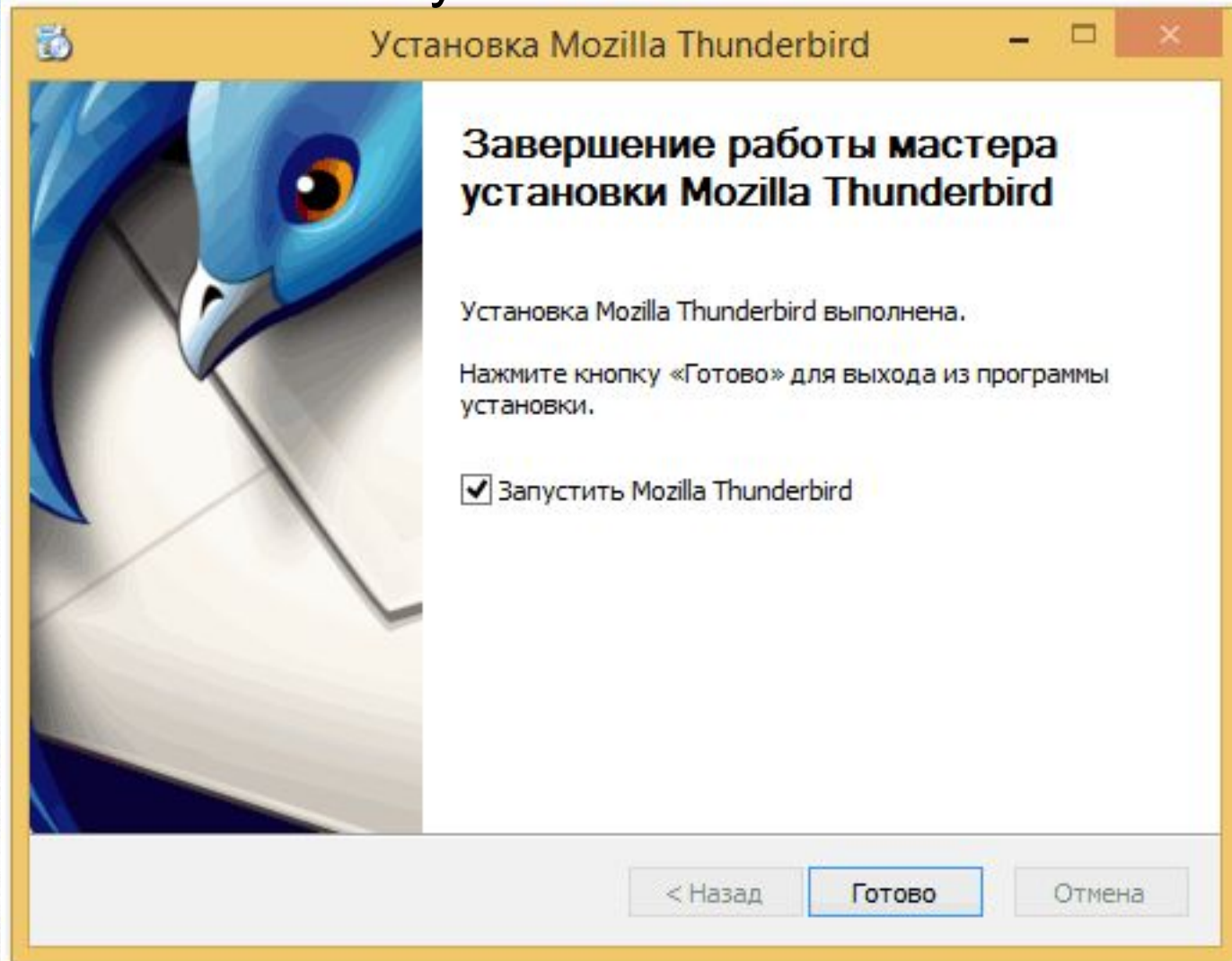
Другие сайты и ссылки | Что нового |
Конфиденциальность

Задание

Получить • Создать • Чат • Адресная книга • Поиск: «Быстрый фильтр»



Установка ПОШТОВОГО КЛІЄНТУ



Установка плагіна PGP-шифрування Enigmail

← → ↻ Надежный | https://www.enigmail.net/index.php/en/download

ENIGMAIL HOME ▾ DOWNLOAD ▾ DOCUMENTATION ▾ SUPPORT ▾ FAQ SEARCH

Download

The latest version of Enigmail works with the following applications:

- Thunderbird 38 and newer
- SeaMonkey 2.35 and newer

[Download Enigmail Now](#)

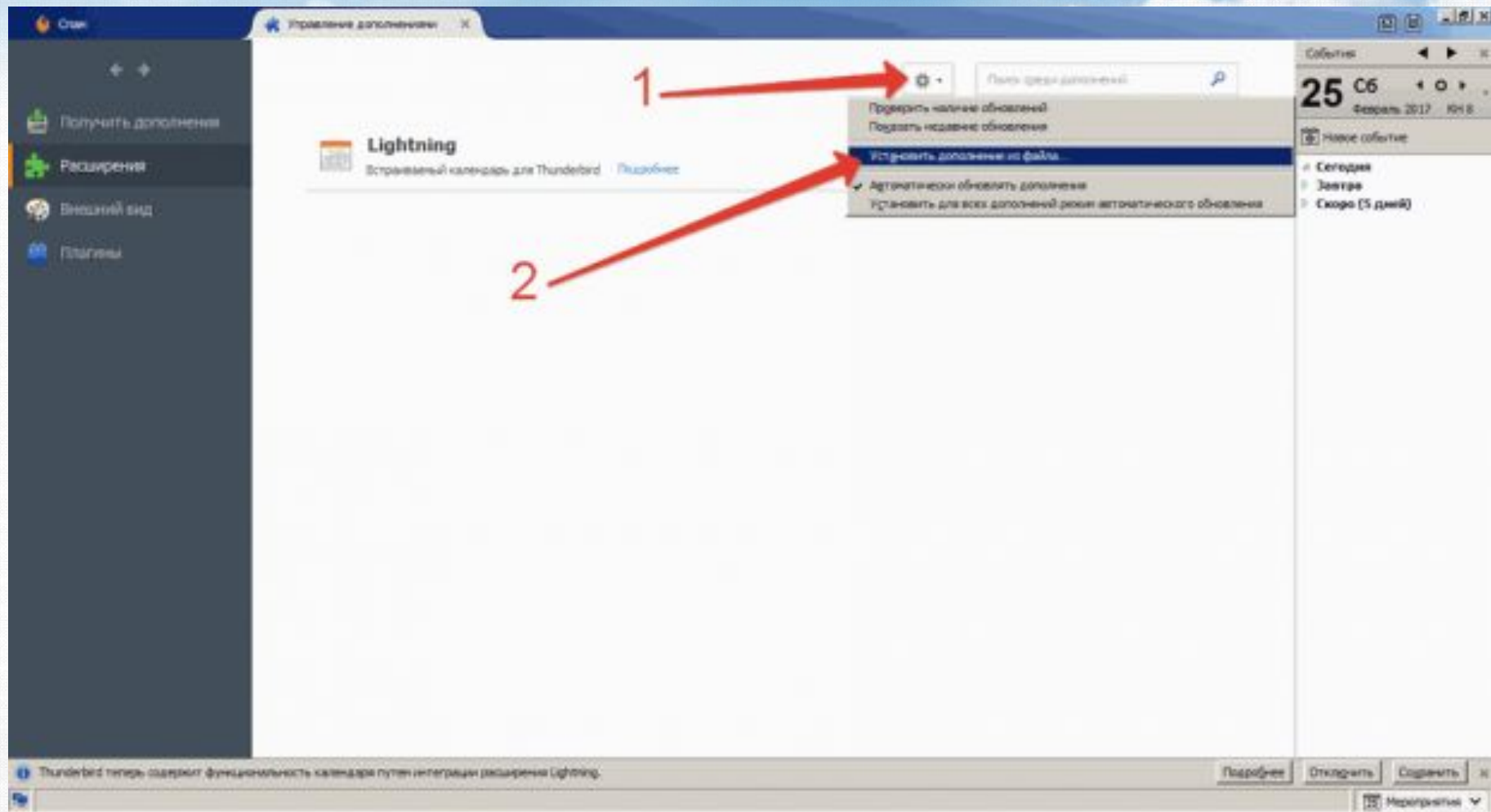
[Version 1.9.6.1 - Changelog - Previous Releases](#)

[Download GPG Signature](#) (to verify the signature, please follow our [instructions](#))

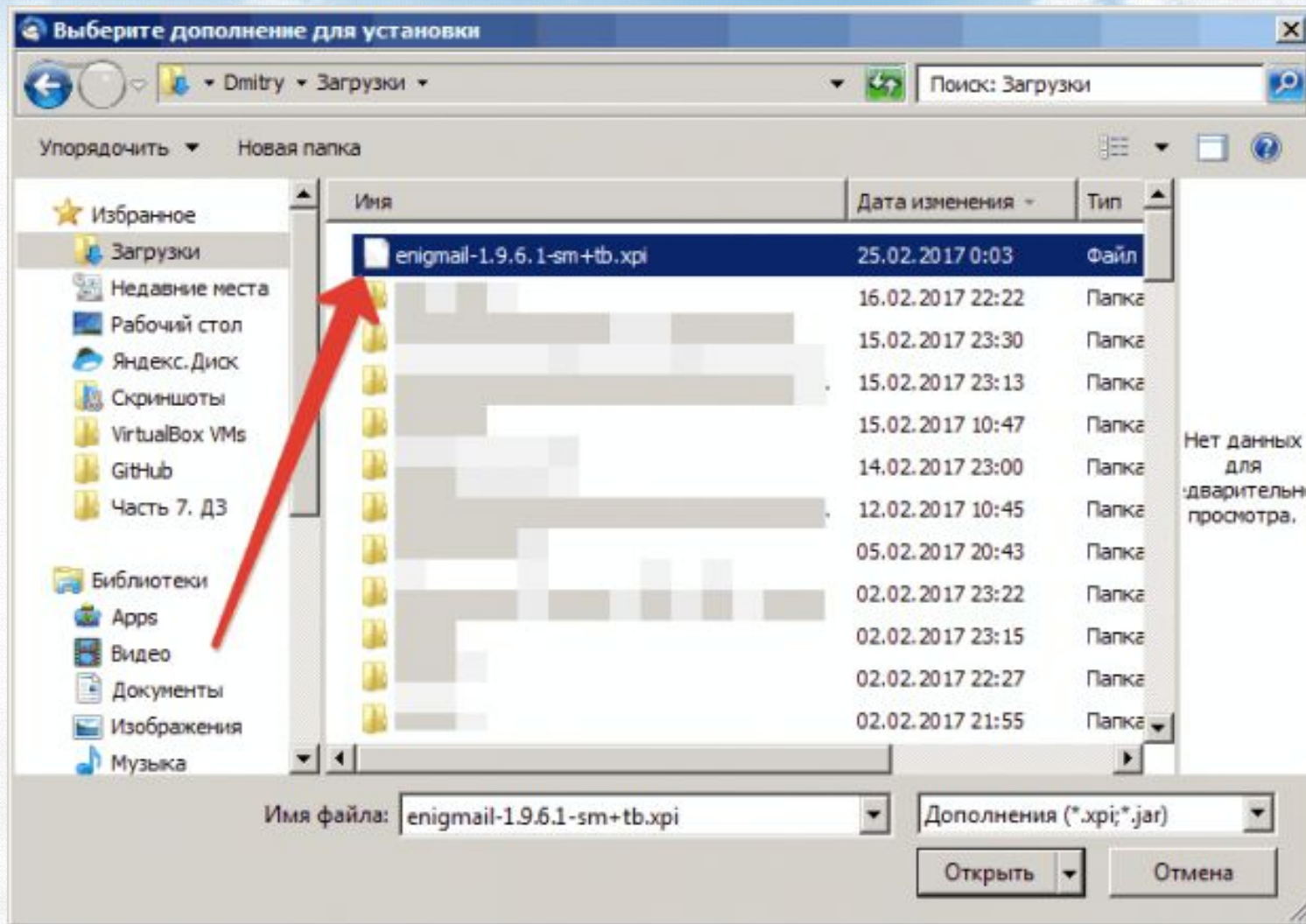
To install Enigmail on Thunderbird, use **right click** "Save Link as ..." to save the extension locally. Then navigate to the Thunderbird button in the upper right corner and then on **Install Add-on From File...**



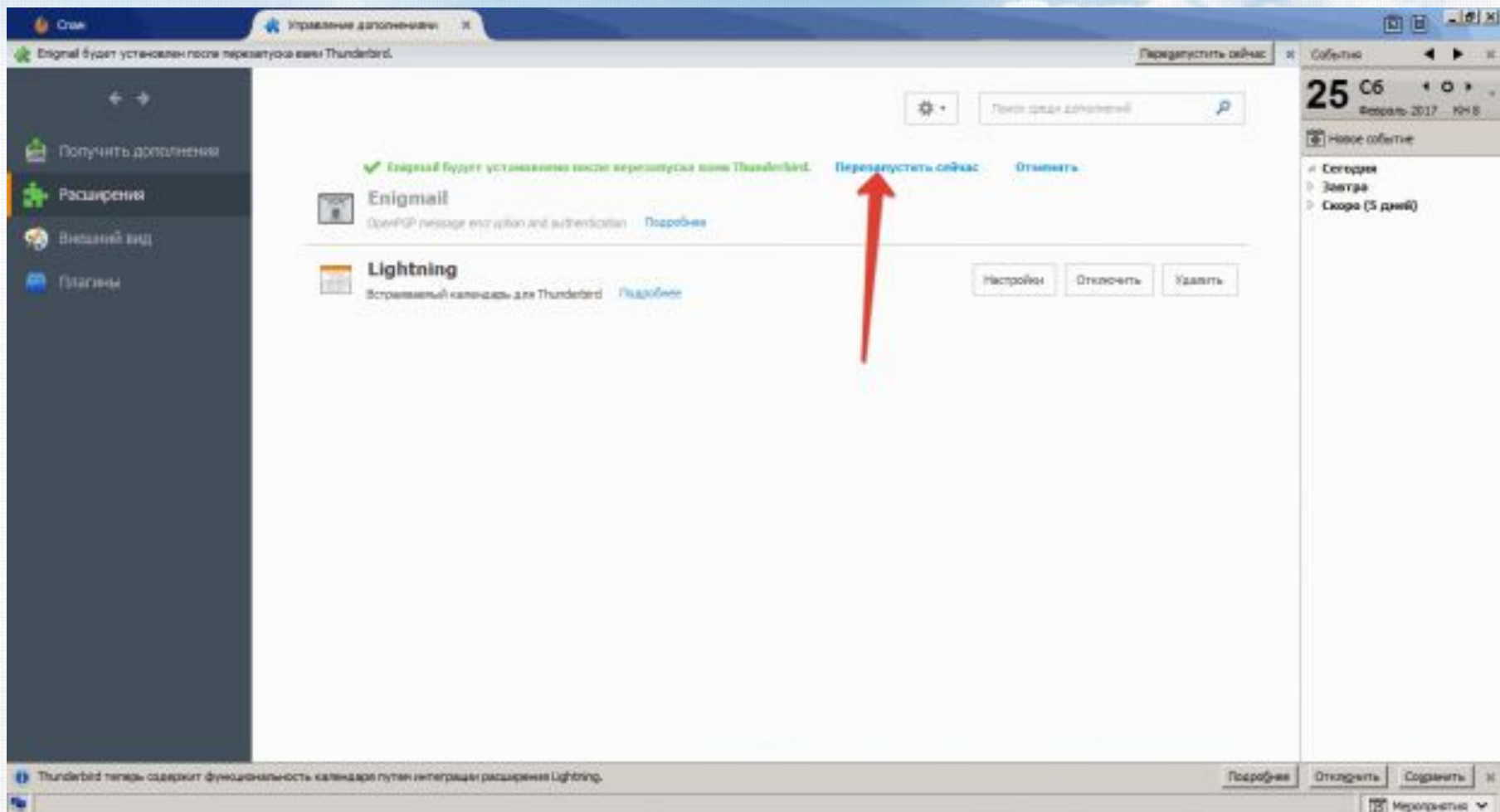
Установка плагіна PGP-шифрування Enigmail



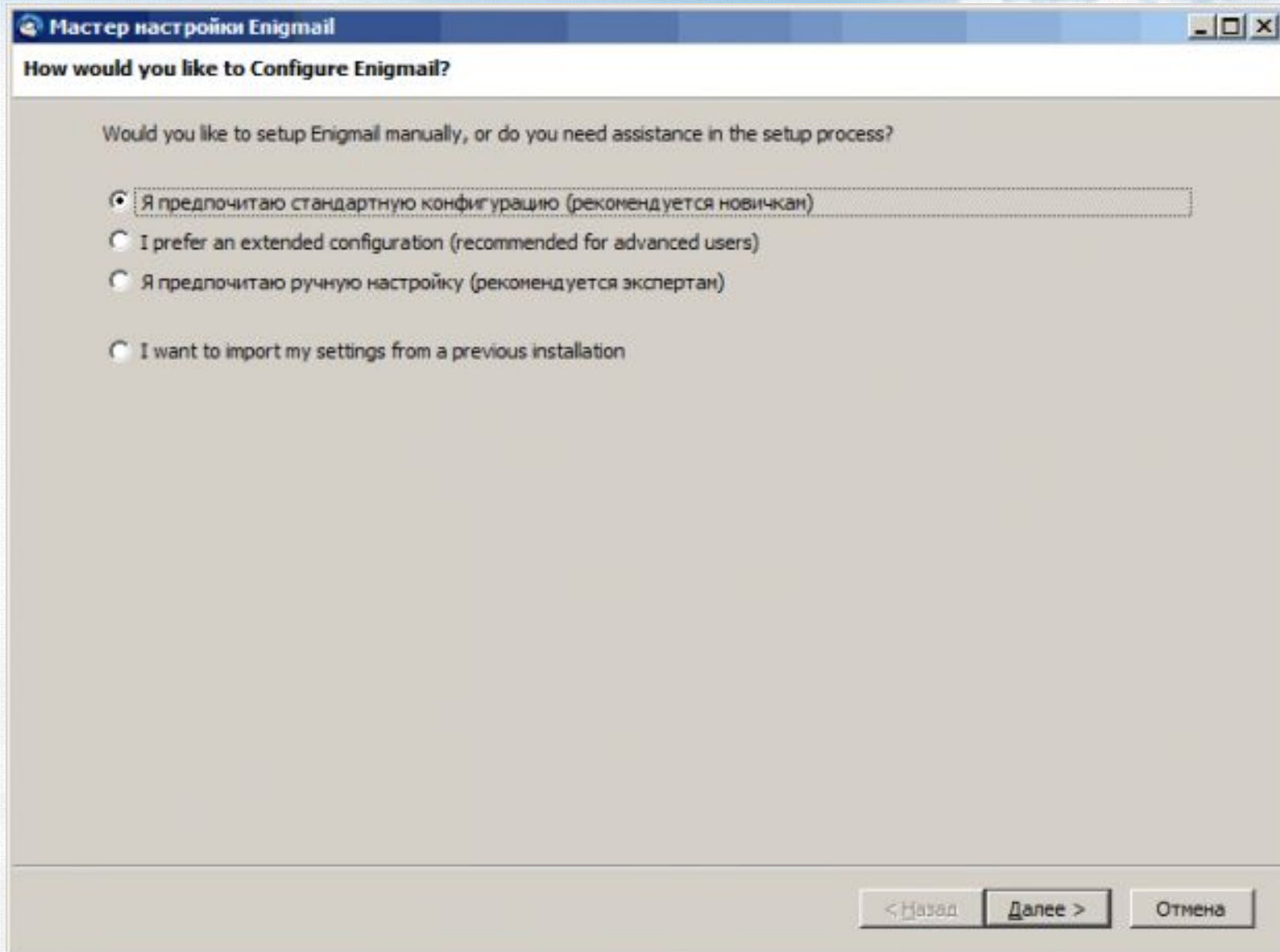
Установка плагіна PGP-шифрування Enigmail



Установка плагіна PGP-шифрування Enigmail



Налаштування плагіна PGP-шифрування Enigmail



Створення пари ключів Enigmail

Enigmail Setup Wizard

Create Key
Create a new Key Pair

This dialog will create a pair of two keys:
Your **public key** is **for others** to send you encrypted emails. You can distribute it to everybody.
Your **private key** is **for yourself** to decrypt these emails and to send signed emails. You should give it to nobody.

Your **passphrase** is a password to protect your private key. It prevents misuse of your private key. The passphrase should be a phrase containing at least 8 characters, digits and punctuation marks. Umlauts (e.g. ä, é, ñ) and language-specific characters are **not** recommended.

Account / User ID:
Akiko <akiko@myriapolis.org> - akiko@myriapolis.org

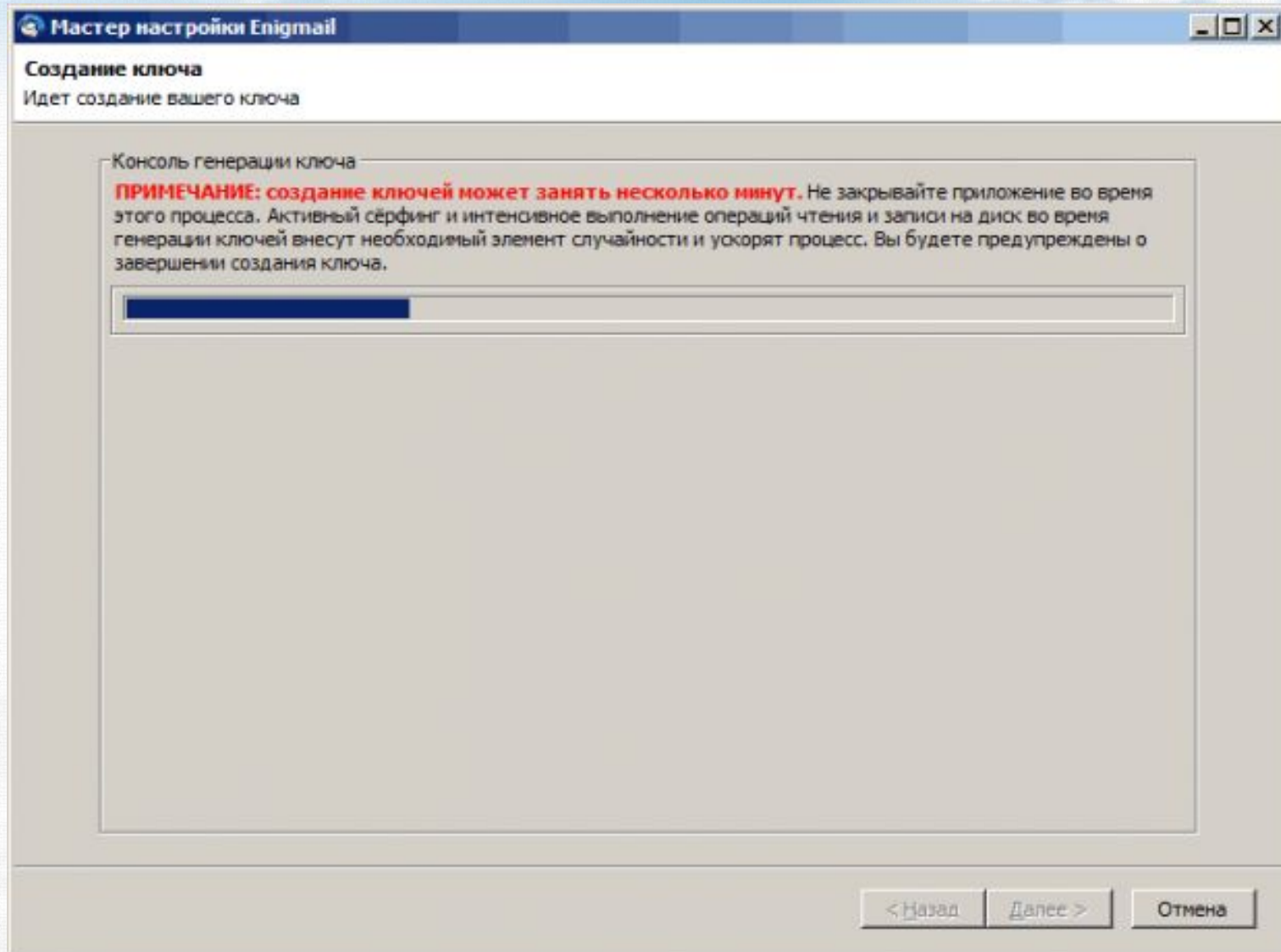
Passphrase
[.....]

Please confirm your passphrase by typing it again
[.....]

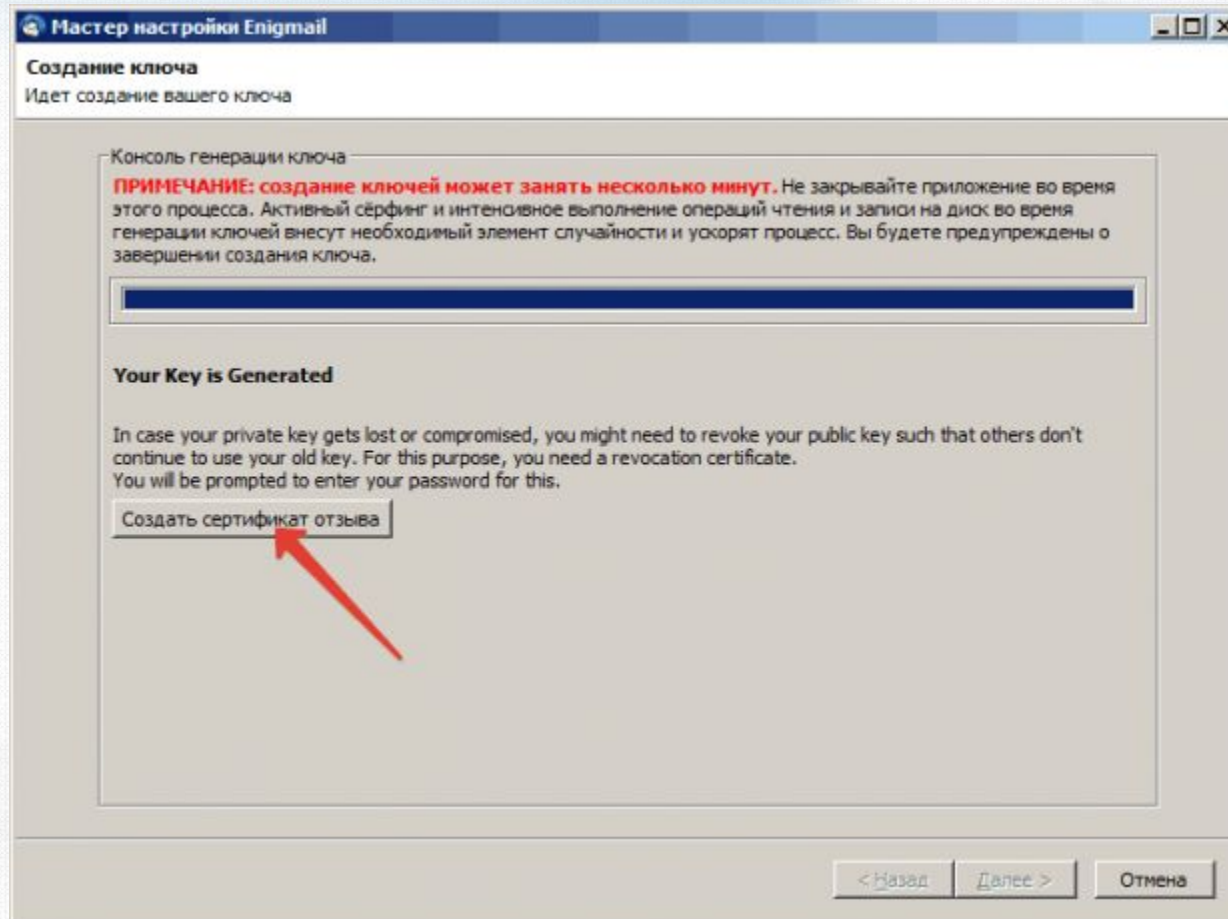
Passphrase quality:
[████████████████████]

< Back Next > Cancel

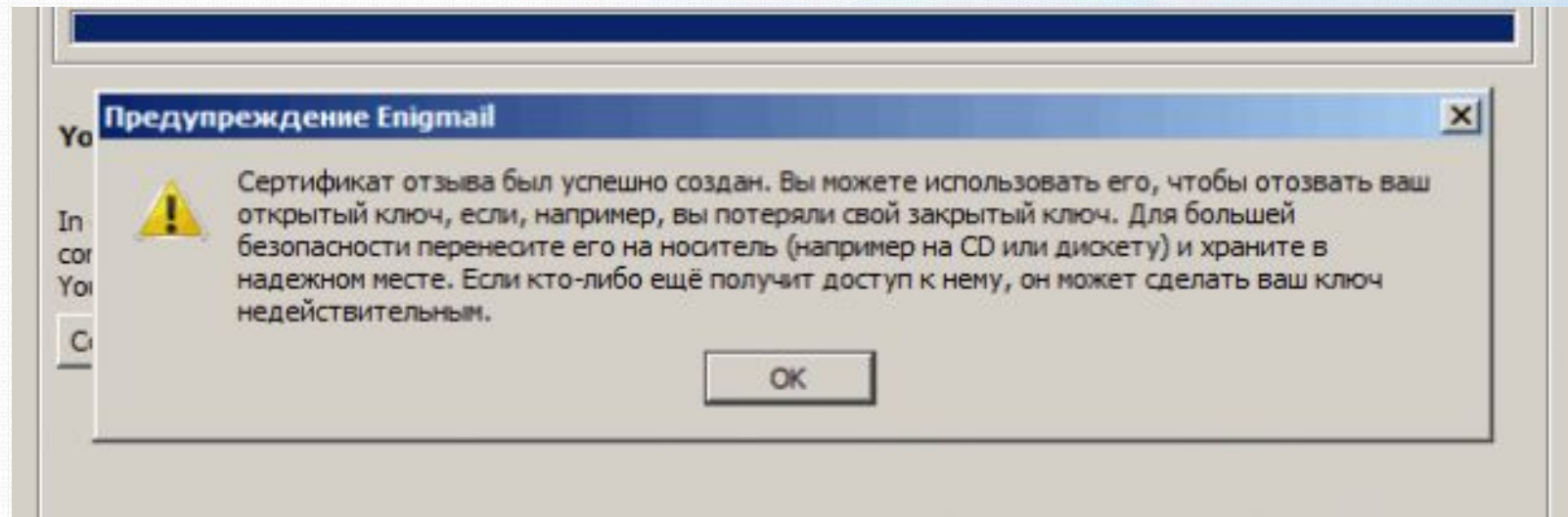
Створення пари ключів Enigmail



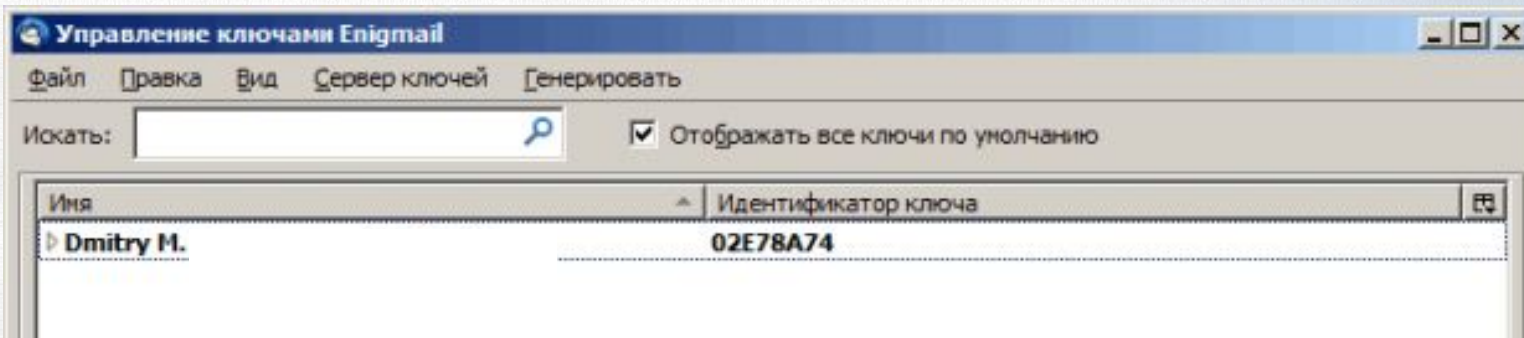
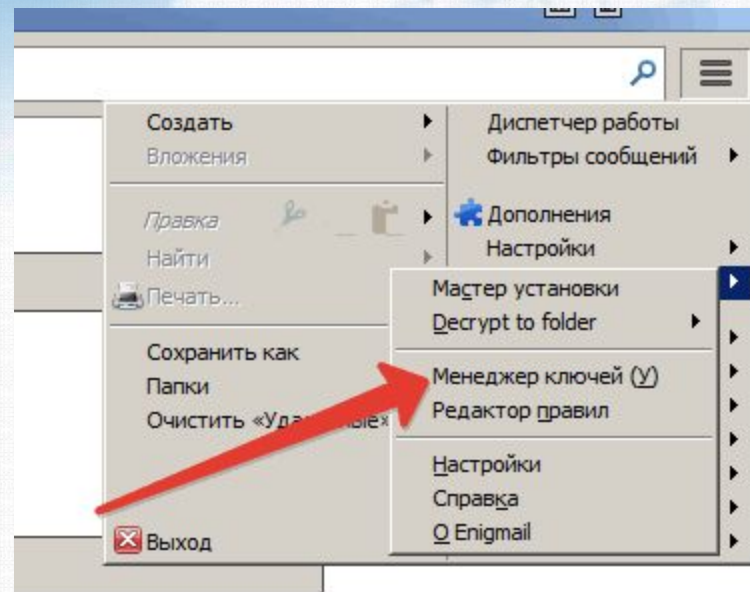
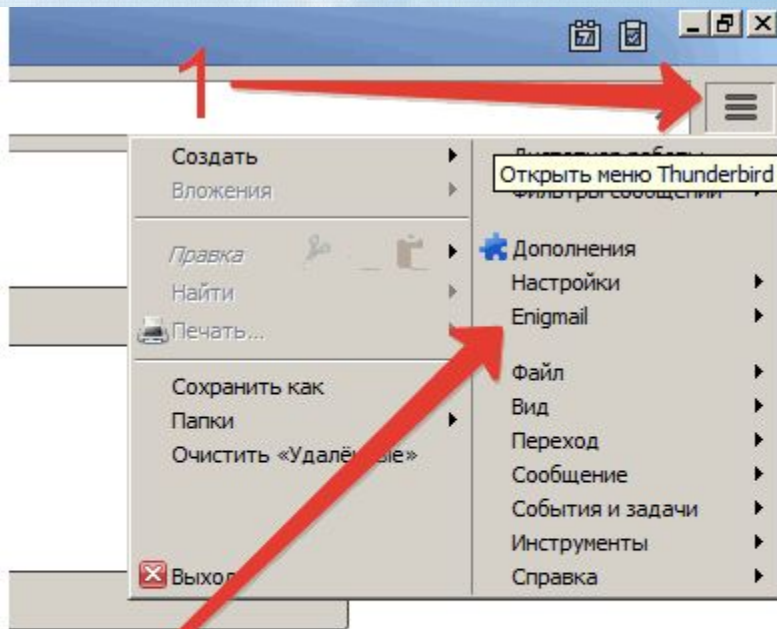
Створення сертифікату відклику ключів



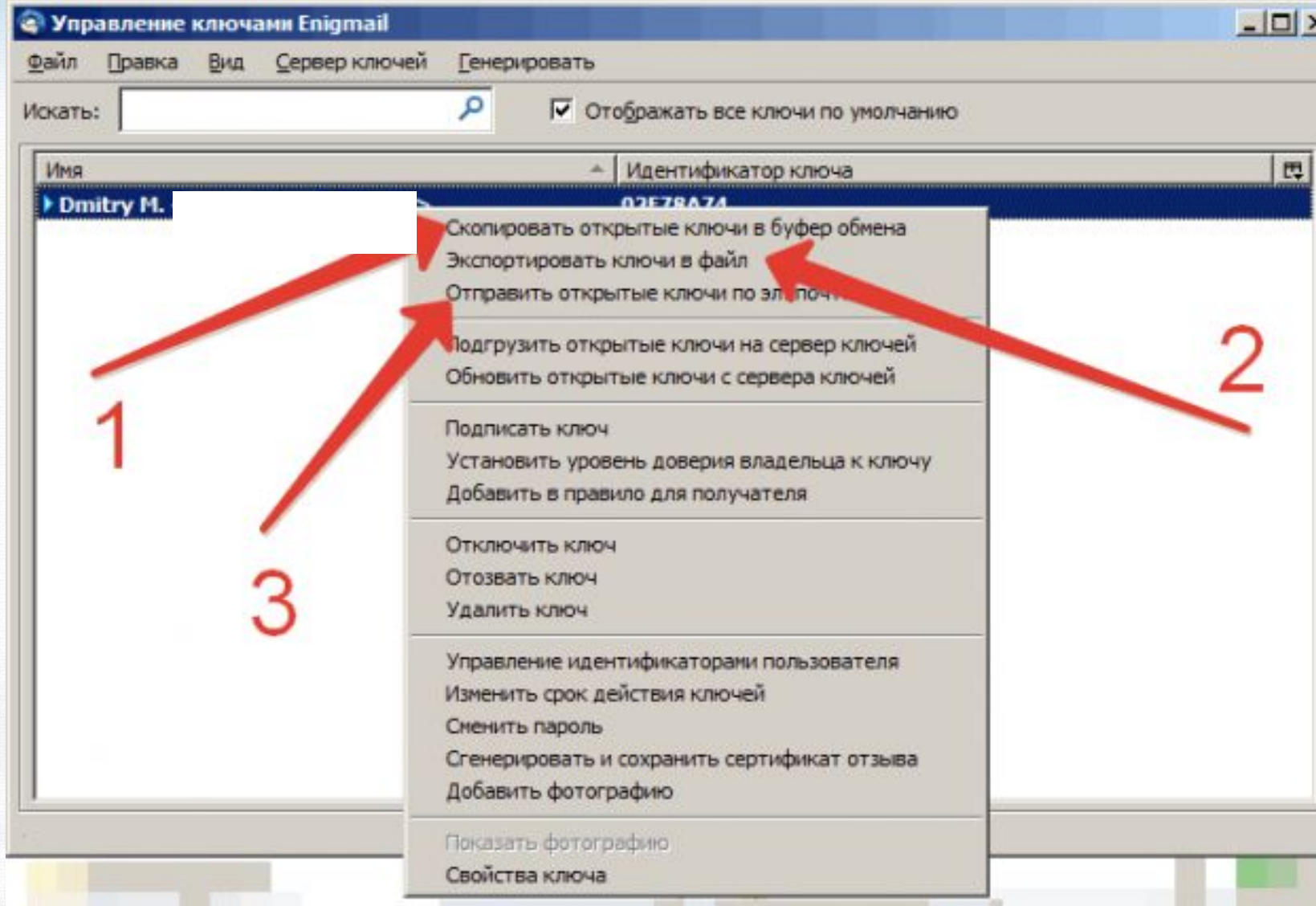
Створення сертифікату відклику ключів



Створення сертифікату відклику ключів

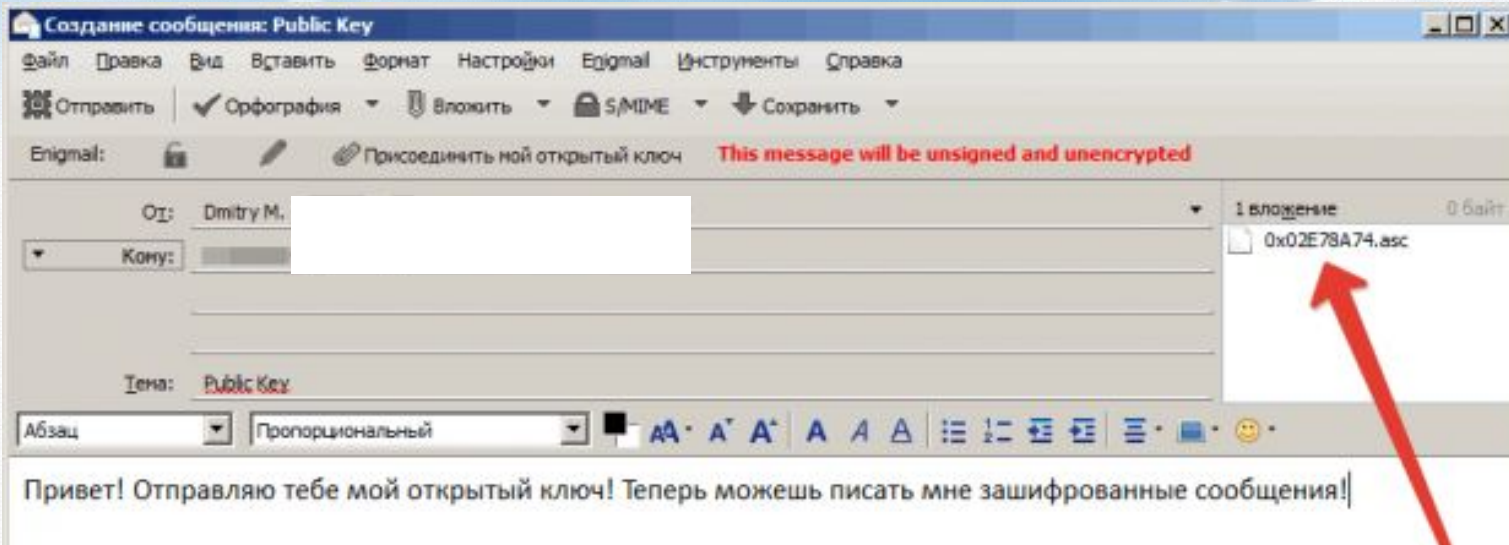


Обмін відкритими ключами

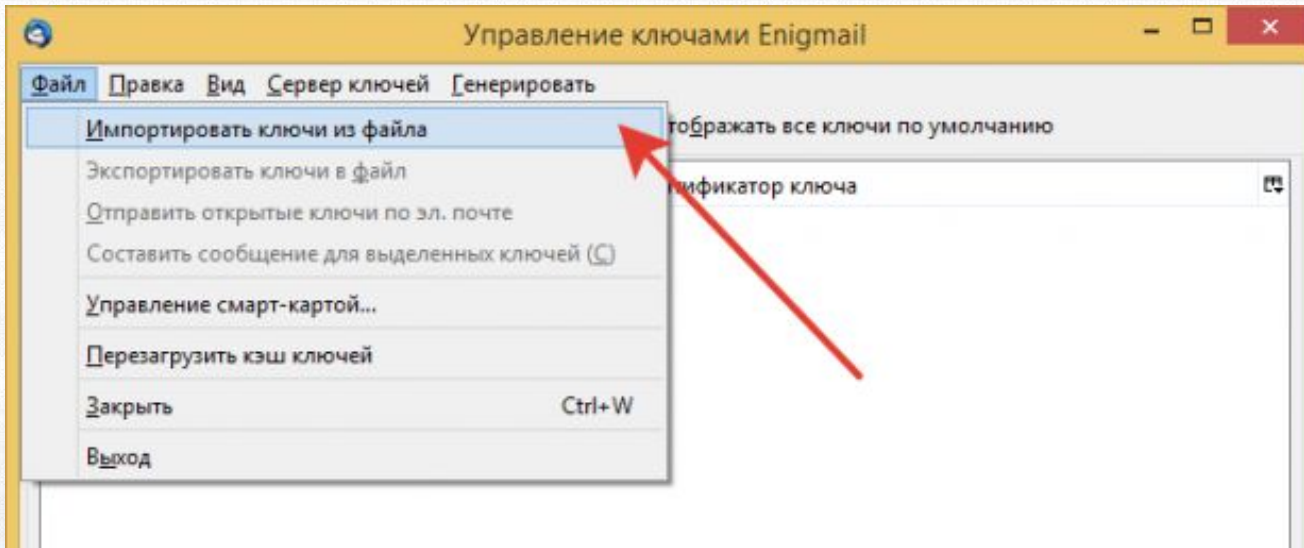


Обмін відкритими ключами

1:

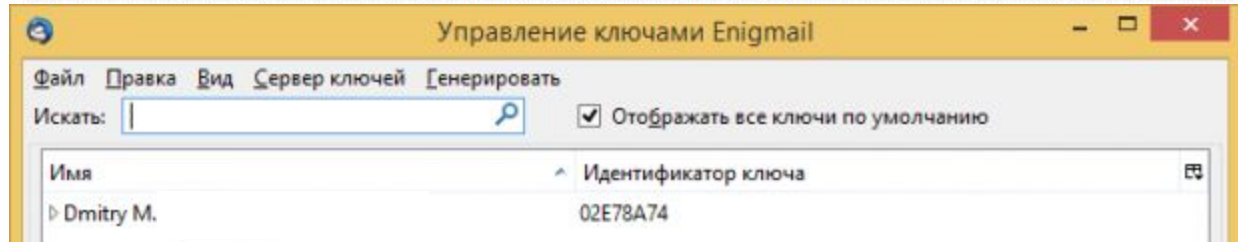
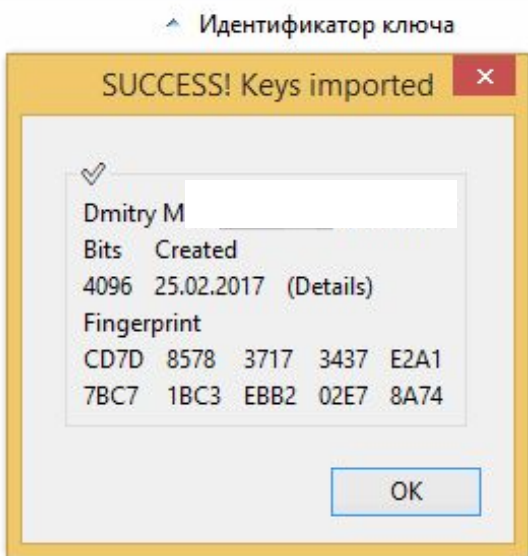
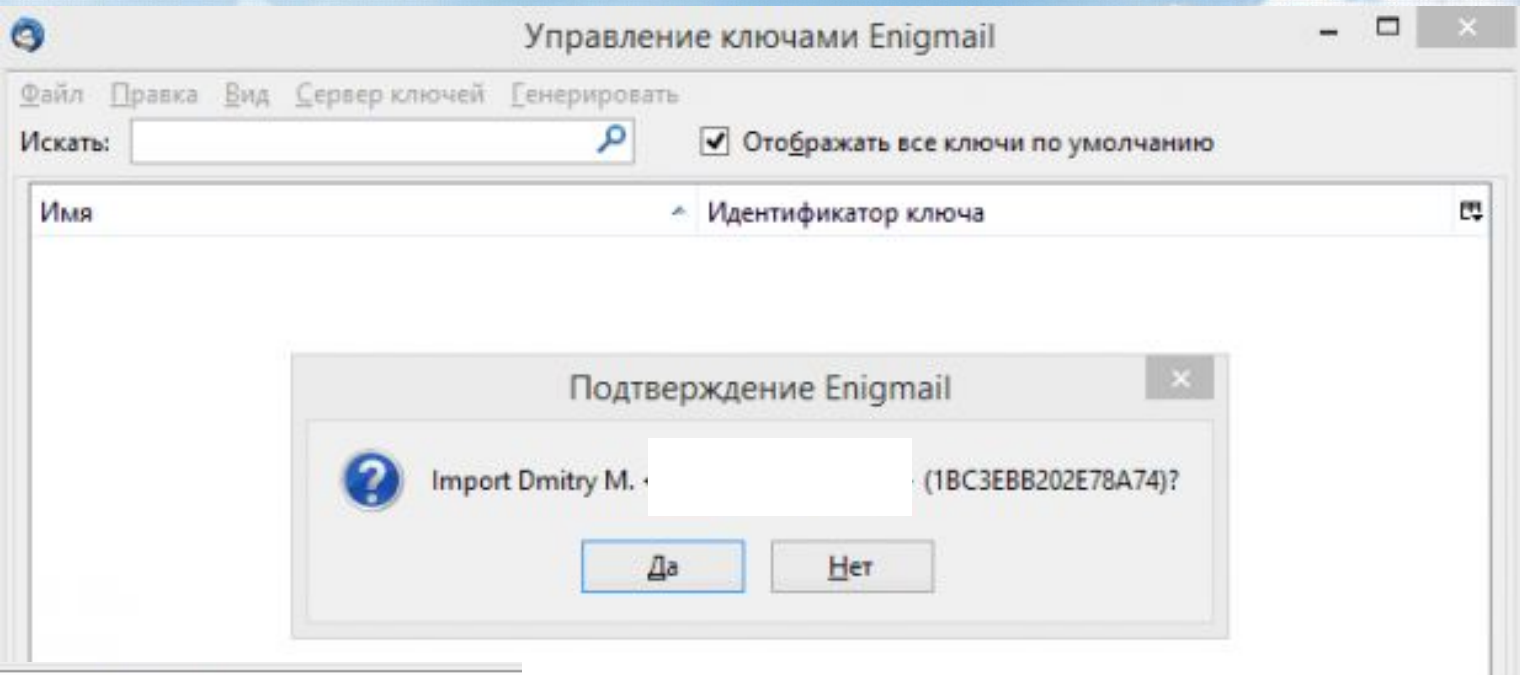


2:



Обмін відкритими ключами

2:



Застосування Enigmail до облікового запису користувача

Параметры учётной записи



✉ **zdorenkoviti@gmail.com**

- Параметры сервера
- Копии и папки
- Составление и адресация
- Анти-спам фильтр
- Синхронизация и хранение
- Защита OpenPGP**
- Уведомления о прочтении
- Защита

📁 **Локальные папки**

- Анти-спам фильтр
- Дисковое пространство

🏠 **Сервер исходящей почт...**

Signing/Encryption Options...

Enigmail предоставляет поддержку шифрования сообщений и снабжения их цифровой на основе OpenPGP. Для работы вам нужно установить GnuPG (gpg).

Включить поддержку OpenPGP (Enigmail) для этой учётной записи

- Использовать адрес эл. почты этой учетной записи для идентификации OpenPGP-и
 Использовать другой идентификатор OpenPGP-ключа (формат 0x1234ABCD):

0x225AA19BACA6521F1

Выбрать ключ...

Message Composition Autocrypt

Настройки по умолчанию для составления сообщений

- Шифровать сообщения по умолчанию
 Подписывать сообщения по умолчанию
 Использовать PGP/MIME по умолчанию

После применения правил по умолчанию

подписать незашифрованное сообщение подписать зашифрованное сооб

Шифровать черновик сообщения при сохранении

If both, Enigmail and S/MIME encryption are possible, then:

- Prefer S/MIME Prefer Enigmail (OpenPGP)

Действия для учётной записи ▾

Настройки |

OK

Отмена

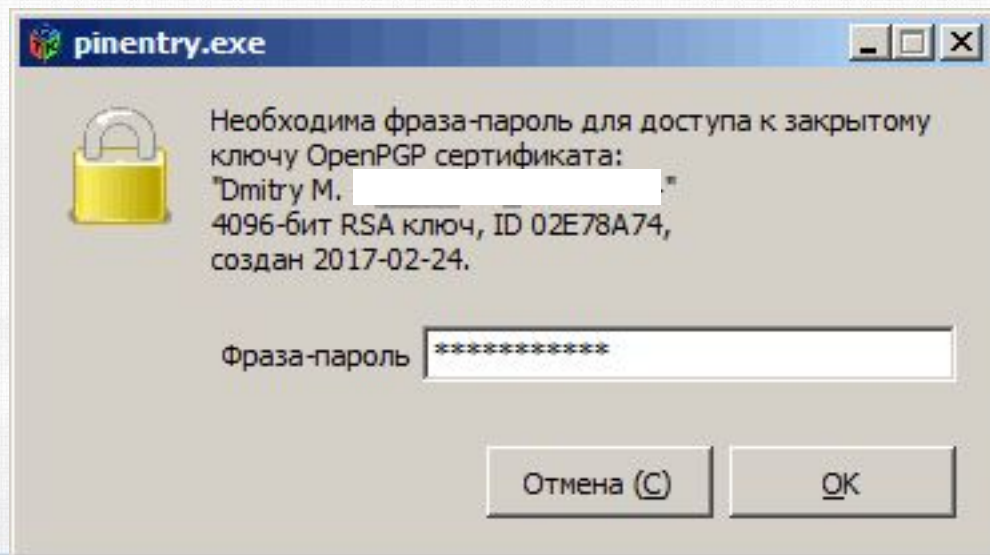


Створення та отримання захищеного повідомлення

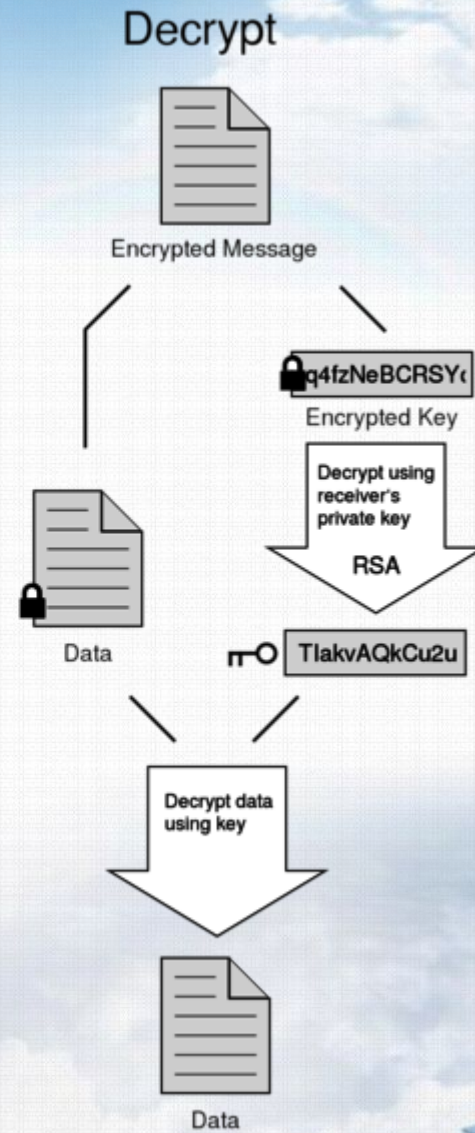
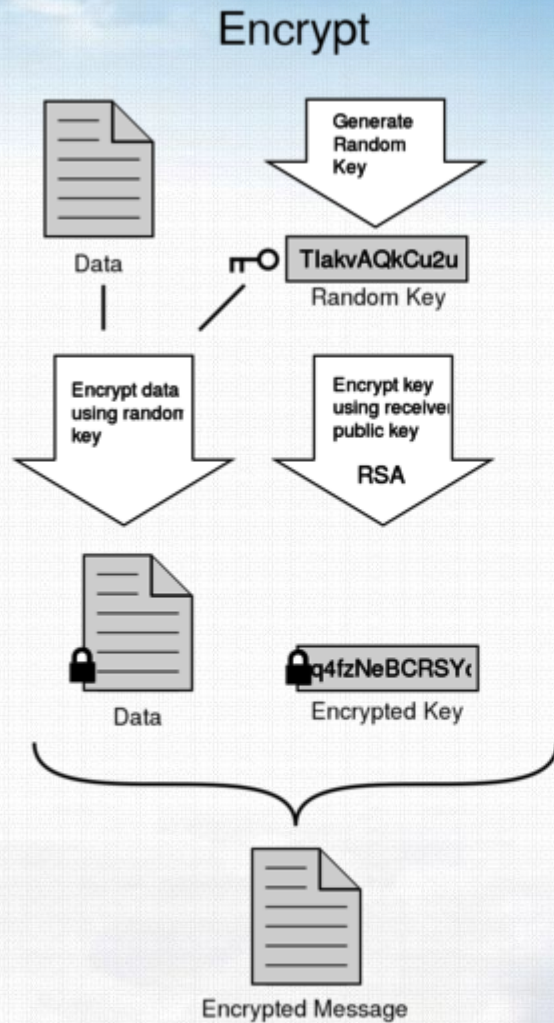
2:



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.

