

Робота із сертифікатом від Globalsign

Отримання сертифікату

Підписування документів MS Word

*Надсилання підписаних та шифрованих повідомлень з
допомогою The Bat*

Зміст

Отримання сертифікату від Globalsign	3
Експорт сертифікату у файл.....	19
Імпорт сертифіката від GlobalSign	30
Здійснення імпорту сертифікату від GlobalSign в Internet Explorer	30
Здійснення імпорту сертифікату від GlobalSign в TheBat.....	36
Використання сертифікату від GlobalSign для накладання електронного цифрового підпису в документах MS Word.....	46
Підпис документів MS Word 2013	46
Підпис документів MS Word 2010	54
Підпис документів MS Word 97-2003.....	60
Використання сертифікату від GlobalSign для надсилання підписаних, зашифрованих, підписаних/зашифрованих листів з допомогою TheBat.....	70
Підписування листів сертифікатом від GlobalSign.....	70
Шифрування листів із використанням сертифікату від GlobalSign	75
Імпорт ключа в адресну книгу	76
Надсилання зашифрованого листа	82
Шифрування та накладання підпису із використанням сертифікату від GlobalSign	87
Надсилання підготованих до відправки листів.....	93

Отримання сертифікату від Globalsign

Для отримання сертифікату від Globalsign спершу слід зайти на сайт <https://www.globalsign.com/> (Див. Рис. 1, а.). При генерації сертифікату має значення яким саме браузером користуватися, тому процес генерації слід розпочати і закінчити на одному і тому ж комп'ютері із використанням одного і того ж браузера. Ми будемо використовувати **Google Chrome**¹. Процес генерації сертифікату для інших браузерів може дещо відрізнятись, тому їх можна використовувати більш досвідченим користувачам. Крім того рекомендується використовувати поштову скриньку на сервері **Gmail**.

Стартова сторінка Globalsign матиме приблизно такий вигляд (Див. Рис. 1):



Рис. 1 Приклад стартової сторінки Globalsign

Організація доволі часто міняє інтерфейс свого Web-сайту, тому з часом сторінка матиме інший вигляд.

Підведемо вказівник мишки до меню Products, для того, щоб перегляну перелік послуг (Див. Рис. 1, б). Серед запропонованого списку обираємо [Digitally Sign and Encrypt Email](#) (Див. Рис. 2), тобто обираємо можливість використання сертифікату для створення цифрового підпису та шифрування

¹ На момент опитування у групі заочників браузером Google Chrome користувалося найбільше студентів, тому він був вибраний в якості прикладу.

повідомлень електронної пошти. Проте, отриманий сертифікат також дасть можливість накладати електронний цифровий підпис і документам MS Office.



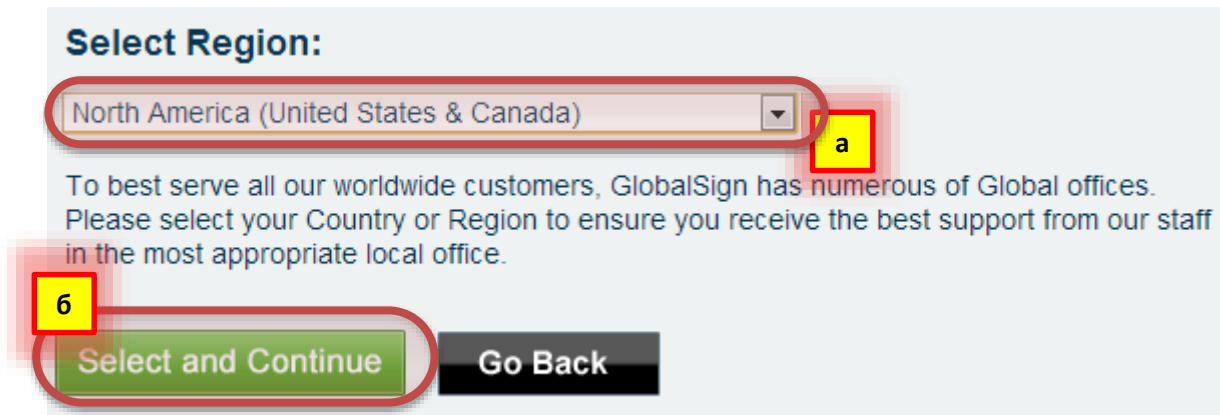
Рис. 2 Фрагмент. Меню "Products"

Після переходу за посиланням з'являється можливість згенерувати пробний сертифікат. Для цього слід натиснути кнопку "Free Trial" (Рис. 3).



Рис. 3 Кнопка "Free Trial"

Наступна сторінка, яка завантажиться матиме поле зі списком у якому слід вибрати регіон. Найчастіше пробний сертифікат можна отримати, якщо скористатися в якості регіону North America (United States & Canada) (Рис. 4, а). В інших регіонах сервіс використання пробних сертифікатів може не надаватися. Після вибору регіону слід натиснути кнопку "Select and Continue" (Рис. 4, б).



Select Region:

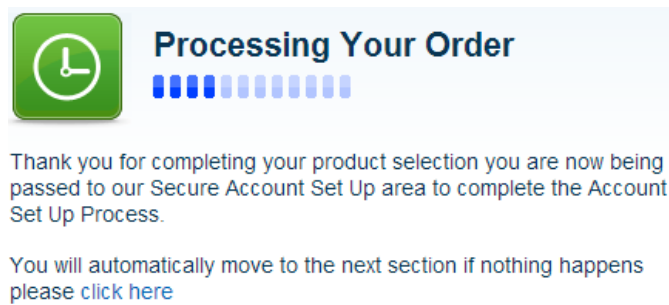
North America (United States & Canada) ▾

To best serve all our worldwide customers, GlobalSign has numerous of Global offices. Please select your Country or Region to ensure you receive the best support from our staff in the most appropriate local office.

6 Select and Continue **Go Back**

Рис. 4 Вибір регіону

Буде розпочато процес обробки замовлення (Рис. 5).



Processing Your Order

Thank you for completing your product selection you are now being passed to our Secure Account Set Up area to complete the Account Set Up Process.

You will automatically move to the next section if nothing happens please [click here](#)

Рис. 5 Процес замовлення

Для отримання пробного сертифікату спочатку потрібно зареєструватися на сайті заповнивши реєстраційну форму. При заповненні інформації користувача слід вводити ім'я та прізвище латинкою (Рис. 6). Дозволяється заповнювати лише "необхідні" поля.

Certificate Application

1. Account Setup 2. Product Details 3. Completed

Account Details >> Confirm Details

Account Details

Please specify details for your account. Your account contact will receive notices regarding your Certificate application and will be the main contact associated with your GlobalSign Certificate Center (GCC) account. If you are applying on behalf of someone else, enter their details, and you can specify an additional Technical Contact for yourself later in the application process.

■ User Information	
First Name <small>Required</small>	<input type="text" value="Vasyl"/>
Middle Name or Initial	<input type="text"/>
Last Name <small>Required</small>	<input type="text" value="Ivanov"/>
Email Address <small>Required</small>	<input type="text" value="ivanov.vasyl@gmail.com"/> <small>Please check email is accurate, this email address will be used in the application process</small>

Рис. 6 Форма. Інформація про користувача

Нижче наведено приклад заповнення інформації про організацію (Рис. 7). Її також слід заповнювати латинкою.

■ Primary Organization Details	
Organization Name <small>Required</small>	<input type="text" value="OA"/> <small>Specify the Organization Registered Name in full, including Inc, Ltd, NV, Plc etc Enter "Personal" if this Certificate is for personal use</small>
Department	<input type="text"/>
Street Address 1 <small>Required</small>	<input type="text" value="Seminarska, 2"/> <small>e.g. Two International Drive</small>
Street Address 2	<input type="text"/> <small>e.g. Suite 330</small>
City <small>Required</small>	<input type="text" value="Ostroh"/>
State / County <small>Required</small>	<input type="text" value="Ukraine"/>
Zip / Postal Code	<input type="text" value="35800"/>
Country <small>Required</small>	<input type="text" value="Ukraine - UA"/>
Phone Number <small>Required</small>	<input type="text" value="380365430258"/> <small>e.g. 603-570-7060 or 01622 766766</small>
Fax Number	<input type="text"/> <small>e.g. 603-570-7059 or 01622 662255</small>
Business Directory ID / Number	<input type="text"/> <small>DUNs (D&B) Number</small> <small>If you have a Business Directory ID or Number (such as a DUNs number) please enter it here</small>
Organization Category	<input type="text" value="-- Select Business type --"/>
Your TimeZone	<input type="text" value="GMT+02:00 Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius"/>

Do you wish to register a trading address?

No Yes

Рис. 7 Інформація про організацію

Після заповнення блоку "Деталі логіну" слід натиснути кнопку "Next" (Рис. 8). В якості "Username" найкраще вибрати ваше ім'я та прізвище латинкою без крапки та без пробілу. Дозволяється використовувати лише символи латинського алфавіту чи цифри. Мінімальна довжина "username" – 8 символів. Ті ж вимоги стосуються й пароля. Пароль слід ввести двічі однаковий.

GlobalSign Certificate Center (GCC) Login Details

Your GCC account allows you to manage all your GlobalSign Certificates and provides fast access to ordering additional products and renewing, reissuing and revoking current Certificates. Please create a memorable Username and Password.

Username Required	<input type="text" value="ivanowasyl"/> <small>Username is case sensitive and must be 8 - 64 characters. Alpha-numeric values only (A-Z, 0-9)</small>
Password Required	<input type="password" value="....."/> <small>Password is case sensitive and must be 8 - 64 characters. Alpha-numeric values only (A-Z, 0-9)</small>
Password(re-enter) Required	<input type="password" value="....."/>



Рис. 8 Деталі логіну

На наступній сторінці слід уважно перевірити введену на попередньому кроці інформацію, прочитати умови надання сервісу, погодитися з ними та натиснути кнопку "Next" (Рис. 9)

16.4 The section titles in the GCC T&C are for convenience only and have no legal or contractual effect.

I AGREE TO TERMS OF SERVICE



Рис. 9 Фрагмент умов надання сервісу

Наступний крок дозволяє задіяти додаткові можливості досвідченим користувачам, проте користувачі цієї інструкції до таких не належать, тому слід просто натиснувши кнопку "Next" перейти до наступного кроку (Рис. 10).

Certificate Application

1. Account Setup 2. Product Details 3. Completed

Product Details >> Certificate Identity Details >> Confirm Details

Product Details - PersonalSign 30 Day Demo

I have an externally generated CSR Check only if you are an Advanced User and have an externally generated Certificate Signing Request (CSR) Otherwise click Next...	<input type="checkbox"/> Yes, I have an externally generated CSR (advanced users only)
PKCS12 Option This option will create the public and private key on behalf of the subscriber. This is an alternative to the key generation taking place in the Subscriber's browser later in the application process.	<input type="checkbox"/> Yes, use PKCS#12 Option
TOTAL COST (inc. Tax)	\$ 0

Back Next

Рис. 10 Деталі продукту

Наступний крок дозволяє вказати яка mail-адреса буде використовуватися для ідентифікації сертифіката. Найпростіше використати електронну адресу вказану на одному з попередніх кроків. Зручно буде також використати пароль вказаний на одному з попередніх кроків. Пароль вказаний на цьому кроці буде використано для того, щоб "забрати" новостворений сертифікат (Рис. 11).

Certificate Application

1. Account Setup

2. Product Details

3. Completed

Product Details >>
Certificate Identity Details
>> Confirm Details

Certificate Identity Details

These details will be vetted and included as the certified identity within your issued Certificate. Make sure the details entered are correct - we will vet the details you include. To assist you, some details will be pre-populated from previous pages or from your GCC account details, you may overwrite these if needed.

Email Address Required	<input style="width: 90%;" type="text" value="ivanov.vasyl@gmail.com"/> <small>The specified email will be visible within the issued Certificate in the Common Name field</small>
--	--

Create Temporary Pickup Password

Please create a temporary pickup password. You will only need this during the installation process. This is not the same as your account password.

If you forget this password you will need to resubmit your order. Please copy it somewhere safe.

Pickup Password Required	<input style="width: 90%;" type="password" value="....."/> <small>Password must be a minimum of 8 characters. Alpha-numeric values only (A-Z, 0-9)</small>
Pickup Password (re-enter) Required	<input style="width: 90%;" type="password" value="....."/>

Рис. 11 Деталі ідентифікації сертифіката

Крім того доведеться заповнити невеличку анкету (невеличка плата за безплатність ;)). Приклад заповнення анкети зображено нижче (Рис. 12).

Please complete the below questions to help us understand your digital certificate requirements

How did you hear about GlobalSign? <i>Required</i>	<input checked="" type="radio"/> Referred by friend or Coworkers <input type="radio"/> Referred by Microsoft Outlook/Website <input type="radio"/> Researched Search Engine <input type="radio"/> Researched Search Engine Advertisement (Side Advertisement) <input type="radio"/> Informed by Advertisement/Campaign/Others <input type="radio"/> I am a n. existing Customer/Partner <input type="radio"/> I am a n. existing Test Cert User
Please specify the number of employees within your Organization. <i>Required</i>	<input type="radio"/> 1-10 employees <input type="radio"/> 11-100 employees <input checked="" type="radio"/> 101+ employees
Please specify your purpose for trialing a PersonalSign certificate. <i>Required</i>	<input checked="" type="checkbox"/> For Demonstration/Test to your Client <input type="checkbox"/> To evaluate if PersonalSign works for our Services/Products <input type="checkbox"/> For Personal Use <input type="checkbox"/> To evaluate PersonalSign for my Organization/Team
What do you intended using this test certificate for? <i>Required</i>	<input checked="" type="checkbox"/> To Test Email Encryption <input checked="" type="checkbox"/> To Test Digital Signature on Email <input type="checkbox"/> To Test Authentication to secure network or devices <input checked="" type="checkbox"/> To Test Digital Signature on Document <input type="checkbox"/> Others (Free writing) <div style="border: 1px solid black; height: 40px; width: 100%;"></div>
On completion of your 30 days trial do you plan to upgrade to a full PersonalSign certificate? <i>Required</i>	<input type="radio"/> Yes, I will be purchasing a full certificate from GlobalSign <input type="radio"/> Yes, I will be purchasing but unsure from which provider <input type="radio"/> Yes, I will be purchasing multiple certificates <input type="radio"/> No, I will be applying for another demo certificate <input checked="" type="radio"/> No, it was for test purposes only
What factors would influence your decision to buy a digital certificate? <i>Required</i>	<input checked="" type="checkbox"/> Support <input type="checkbox"/> Sales/Relationship <input type="checkbox"/> Choice/Function/Option <input type="checkbox"/> Issuance Speed <input type="checkbox"/> Ease of Business <input type="checkbox"/> Price <input type="checkbox"/> Design of Website <input type="checkbox"/> Preferred Service Provider
Who is your current certificate provider? <i>Required</i>	<input type="checkbox"/> GlobalSign <input type="checkbox"/> Verisign <input type="checkbox"/> Thawte <input type="checkbox"/> Comodo <input checked="" type="checkbox"/> None/Others (Free writing) <div style="border: 1px solid black; height: 20px; width: 100%;"></div>

Рис. 12 Приклад заповнення анкети

Після заповнення анкети слід підтвердити, що пароль, який використовуватиметься для отримання сертифікату було збережено в надійному місці натиснути кнопку "Next" (Рис. 13).

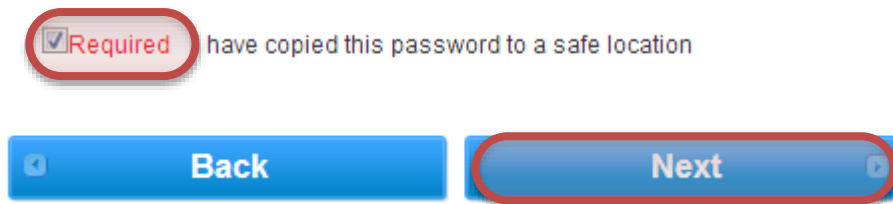


Рис. 13 Збереження пароля у безпечному місці

На етапі "Підтвердження Деталей" (Рис. 14), слід лише погодитися з угодою і натиснути кнопку "Next" (Рис. 15).



Рис. 14 Підтвердження деталей (а)

Certificates to Users in a Digital Certificate Hierarchy. GlobalSign is subscriber's CA hereunder. Digital Signature Information encrypted with a Private Key which is appended to electronic data to identify the owner of the Private Key and verify the integrity of the electronic data. Digitally Signed shall refer to electronic data to which a Digital Signature has been appended.

I AGREE TO THE SUBSCRIBER AGREEMENT



Рис. 15 Підтвердження деталей (б)

При успішній реєстрації на наступній сторінці повинен з'явитися такий фрагмент (Рис. 16):

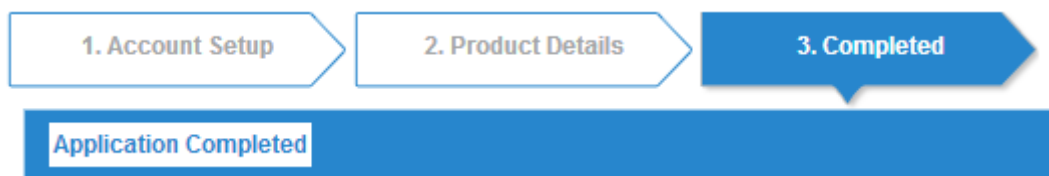


Рис. 16 Завершення процесу реєстрації

Наступний етап – перевірка електронної пошти. Якщо все було зроблено правильно, то згодом на електронну пошту прийде три листи (Рис. 17).

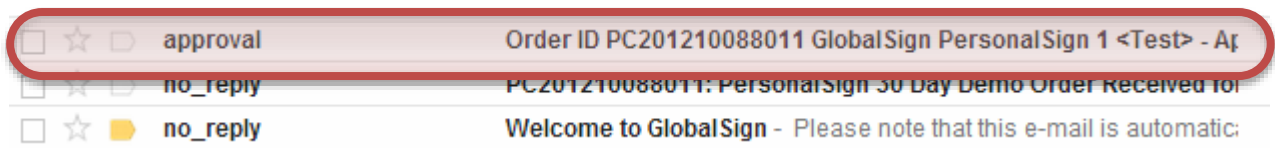


Рис. 17 Перших три листа від Globalsign

Лист який був отриманий останній слід відкрити і використати для підтвердження введеної на першому етапі інформації. Для цього слід скористатися посиланням, що розміщене у листі (Рис. 18).

Dear Customer,

An application for a PersonalSign 1 <Test> Certificate has been placed with GlobalSign for ivanov.vasyl@gmail.com (-) and Order ID PC201210088011.

In order for GlobalSign to issue the Certificate, the email address must be validated. Please follow the below link to choose to APPROVE or NOT APPROVE the application.

Only if you approve the application will the Certificate be issued.

<https://reqist.globalsign.com/ra/arrivalMailApproval/arrivalMailApproval/ArrivalMailApproval.do?r=8791bb86&e=600e84f89855&c=0a57da559db84478d2ffe53ed274fbfb00a2f58a>

Рис. 18 Фрагмент листа з посиланням підтвердження

Після того як буде здійснено перехід за посиланням відобразиться сторінка підтвердження справжності електронної скриньки, на якій слід натиснути кнопку "APPROVE" (Рис. 19).

APPROVE or DO NOT APPROVE Certificate Application

An application for a PersonalSign 1 <Test> Certificate for ivanov.vasyl@gmail.com (-) has been received.

In order to issue the Certificate, the right of the applicant to apply for the Certificate must be validated.

The following Applicant details were submitted during the ordering process.
Please review the Applicant details below, and then:

Click I APPROVE to authorize the order, or;
 Click I DO NOT APPROVE to reject the order, the Certificate WILL NOT be issued.

Application Details

Order ID	PC201210088011
Common Name	ivanov.vasyl@gmail.com
Contact First Name	Vasyl
Contact Middle Name	-
Contact Last Name	Ivanov
Contact Phone	380365430258
Contact Email	ivanov.vasyl@gmail.com
Organization (O)	-
Locality (L)	-
State (S)	-
Country (C)	-
Application Email	ivanov.vasyl@gmail.com
Application Date	2012-10-08 20:16:04.351

I APPROVE I DO NOT APPROVE

Рис. 19 Підтвердження інформації

Після підтвердження електронної скриньки слід знову перевірити електронну пошту. Повинен надійти ще один лист (Рис. 20).

<input type="checkbox"/>	☆	<input type="checkbox"/>	no_reply	Certificate Download Ready - PC201210088011: PersonalSign 30 Day Demc
<input type="checkbox"/>	☆	<input type="checkbox"/>	approval	Order ID PC201210088011 GlobalSign PersonalSign 1 <Test> - Approve App
<input type="checkbox"/>	☆	<input type="checkbox"/>	no_reply	PC201210088011: PersonalSign 30 Day Demo Order Received for ivanov.va
<input type="checkbox"/>	☆	●	no_reply	Welcome to GlobalSign - Please note that this e-mail is automatically sent

Рис. 20 Лист для завантаження сертифікату

Відкривши лист слід скористатися посиланням для завантаження сертифікату (Рис. 21).

HOW TO PICK UP & INSTALL YOUR CERTIFICATE

IMPORTANT:

For assistance please visit the appropriate support site:

Code Signing Certificate Support Site: <https://www.globalsign.com/support/codesign.php>

PersonalSign Certificate Support Site: <https://www.globalsign.com/support/personalsign.php>

You must complete this process on the machine from which you intend to use the Certificate.

* Windows 2000 & XP Users: We recommend you use the Internet Explorer or Firefox browsers.

* Windows Vista Users: We recommend you do NOT use Internet Explorer. Please use Firefox (available free of charge from www.mozilla.com) to complete the process. If you have to use Internet Explorer, please click on the link below for detailed instructions on preparing the browser: www.globalsign.com/support/keygen/microsoft.php

Click on the link below to initiate the Certificate generation and installation process.

<https://system.globalsign.com/pc/public/certificate/install.do?p=8beb3e5f504286d25892dbfce33bb41aadf7bc3f>

Make sure the above link is unbroken and complete. Copy and Paste the entire link into your browser if necessary.

Рис. 21 Фрагмент листа із посиланням для завантаження сертифікату

Після переходу за посиланням з'явиться можливість встановити сертифікат. Для цього потрібно ввести пароль, призначений для отримання сертифікату (він був створений Вами на одному з попередніх етапів) та натиснути кнопку "Next" (Рис. 22)

Install Certificate

You will now go through the Certificate generation and installation process.
Note that if you continue on this computer, your Certificate will be installed on this computer.

Step One: Enter your Pickup Password

Your Pickup Password will have been set by the applicant during the application.

Enter the Pickup Password to continue.

Forgotten the Pickup Password? [Click Here](#) for instructions.

Next

Рис. 22 Встановлення сертифікату

Вибір провайдера криптографічного сервісу (Рис. 23). Після погодження необхідних моментів натисніть кнопку "Next".

Install Certificate

Step Two: Select the Cryptographic Service Provider (CSP)

The CSP is used to generate the cryptographic keys within your Certificate.

We have listed the CSPs found on your computer. For further assistance on using CSPs and which may be appropriate if you are installing your Certificate onto a hardware device such as crypto USB, view the [CSP Support Guide](#).

Please note! Depending on your browser / Operating System setup, there may be a information bar or Pop Up asking you to install "Microsoft Certificate Enrolment Control" displayed at the top of this page.

If so, you MUST allow this to run. It is a safe program that your browser uses to install your certificate. To run it, click on the information bar or Pop Up and follow the instructions.

Cryptographic Service Provider: 2048 (Високий рівень)

GlobalSign Subscriber Agreement for PersonalSign Certificates Version 1.3

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE DIGITAL CERTIFICATE ISSUED TO YOU OR YOUR ORGANISATION. BY USING THE DIGITAL CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED DIGITAL CERTIFICATE OR CANCEL THE ORDER WITHIN 7 DAYS OF ISSUANCE TO GLOBALSIGN FOR A FULL REFUND. IF YOU HAVE PROBLEMS UNDERSTANDING THIS AGREEMENT, E-MAIL US AT legal@globalsign.com

This GlobalSign PersonalSign Subscriber Agreement ("Agreement") is effective as of the

I AGREE TO THE SUBSCRIBER AGREEMENT

Please click Next and wait. Do not click Next again and do not close the browser, the process may take a few seconds.

Next

Рис. 23 Вибір провайдера криптографічного сервісу

Наступне вікно дозволить встановити два сертифікати (Рис. 24):

1. Ваш особистий сертифікат (він буде розміщений у сховищі сертифікатів Google Chrome) (Рис. 25).
2. Сертифікат проміжного центру сертифікації (він буде необхідний для організації ланцюжка довіри і його слід зберегти на змінний носій) (Рис. 26).

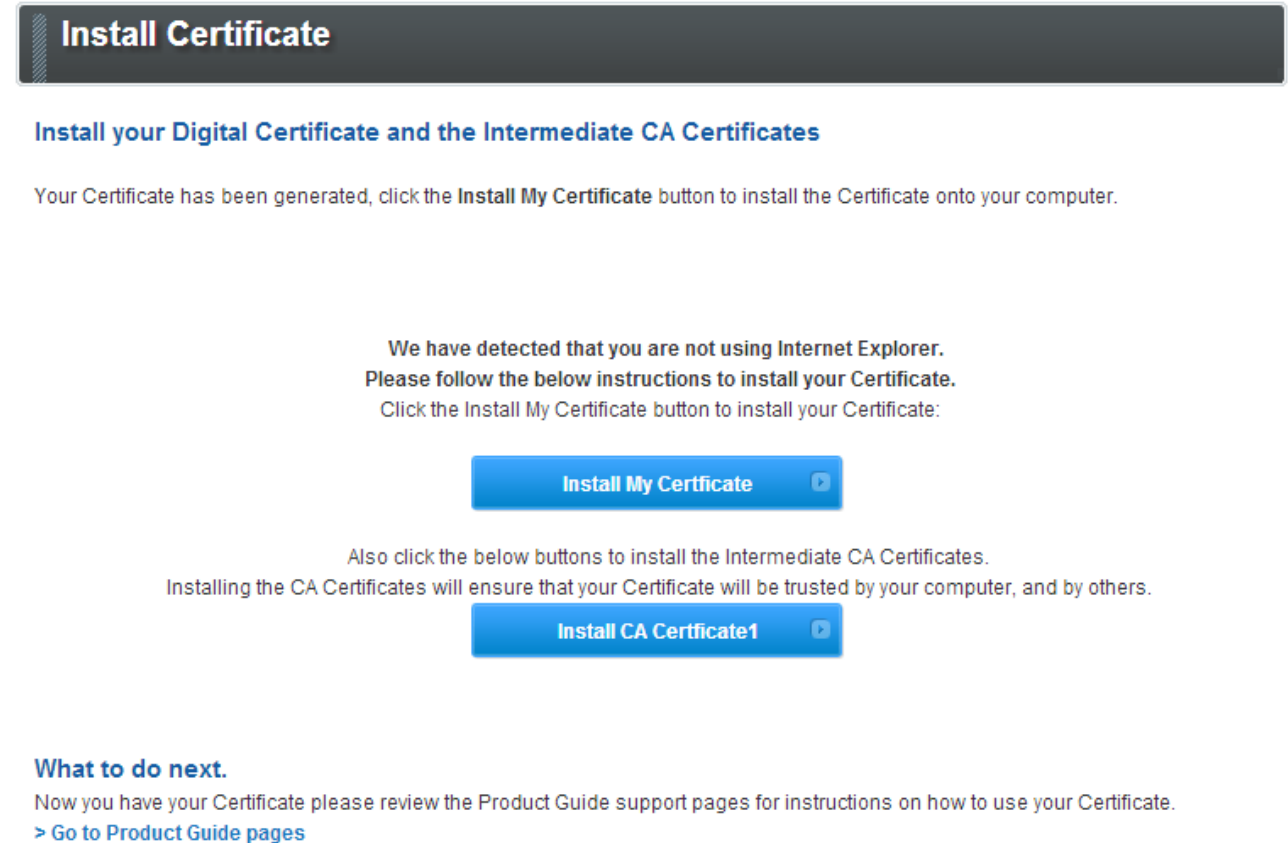


Рис. 24 Встановлення сертифікатів

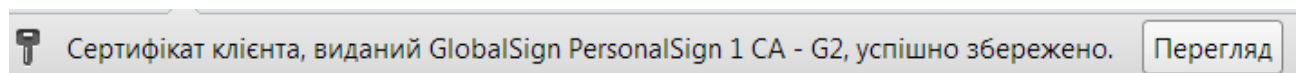


Рис. 25 Повідомлення про успішне збереження персонального сертифікату

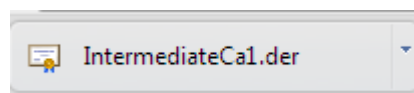


Рис. 26 Повідомлення про успішне збереження сертифіката проміжного центру сертифікації

Експорт сертифікату у файл

Для здійснення експорту сертифікату у файл слід пройти таку послідовність кроків на комп'ютері на якому було здійснено встановлення сертифікату:

1. Перейти до налаштувань Google Chrome

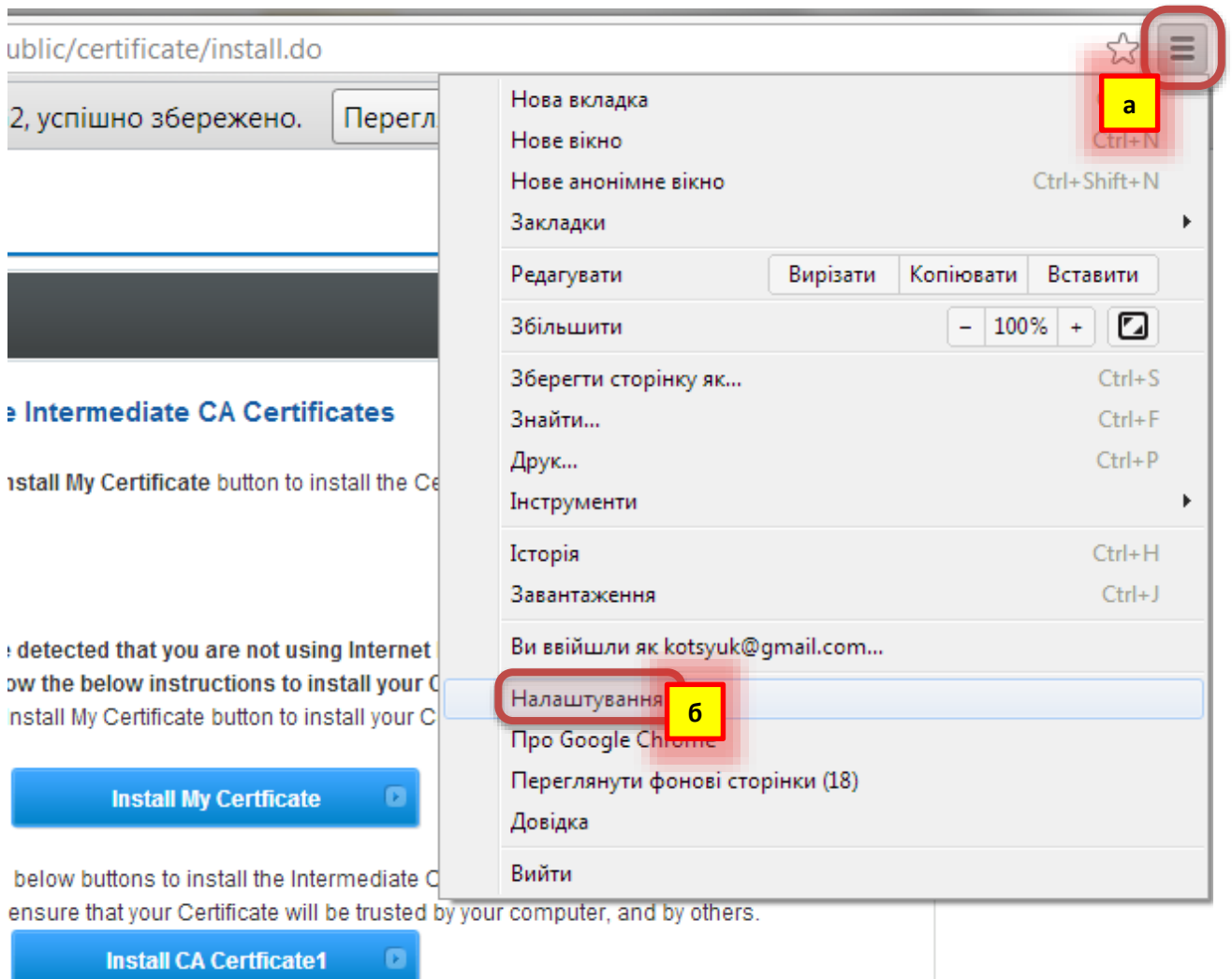


Рис. 27 Вхід у налаштування Google Chrome

2. Внизу сторінки знайти розширені налаштування

Веб-переглядач за умовчанням

Наразі переглядачем за умовчанням є Google Chrome.

[Показати розширені налаштування...](#)

Рис. 28 Розширені налаштування

3. Перейти до підрозділу HTTPS/SSL, та скористатися кнопкою "Керувати сертифікатами"

HTTPS/SSL

[Керувати сертифікатами...](#)

Перевірити відкликання сертифіката сервера

Рис. 29 Розділ HTTPS/SSL

4. Вибрати власний сертифікат та натиснути кнопку "Експорт..."

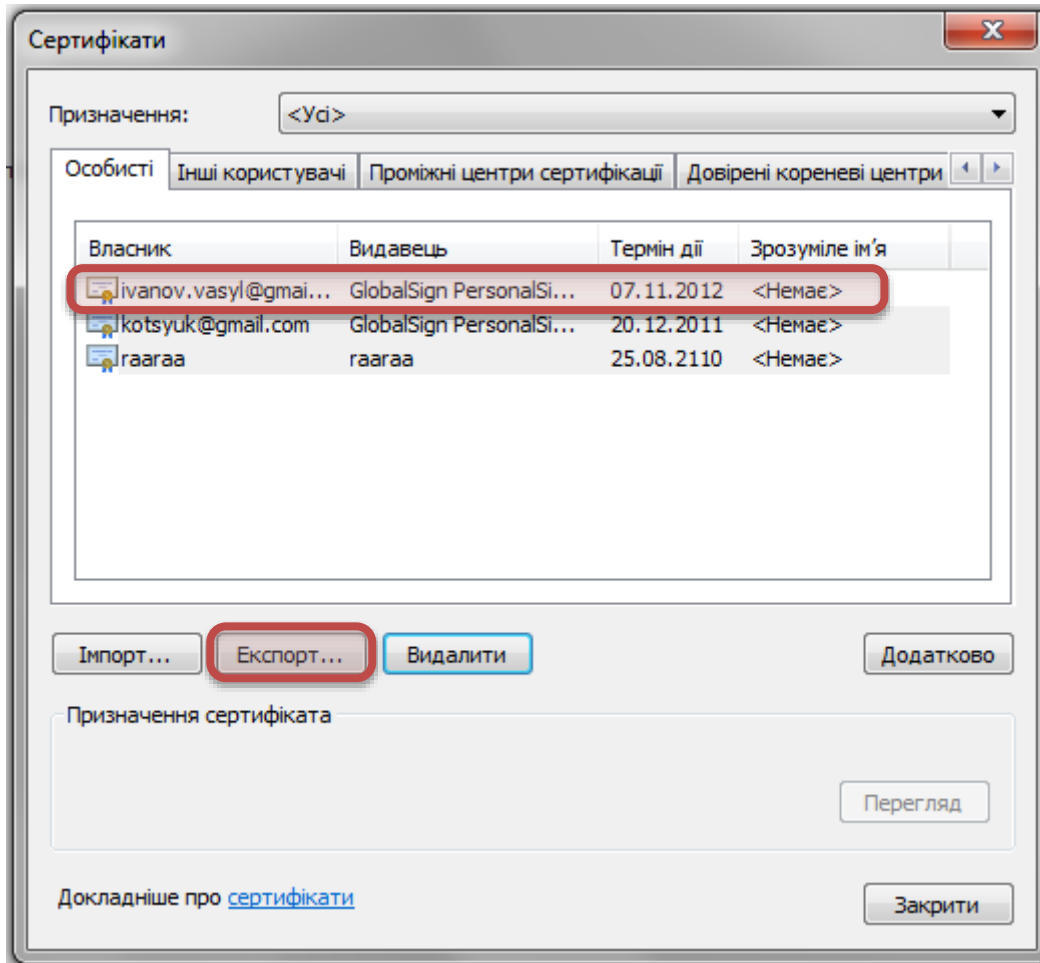
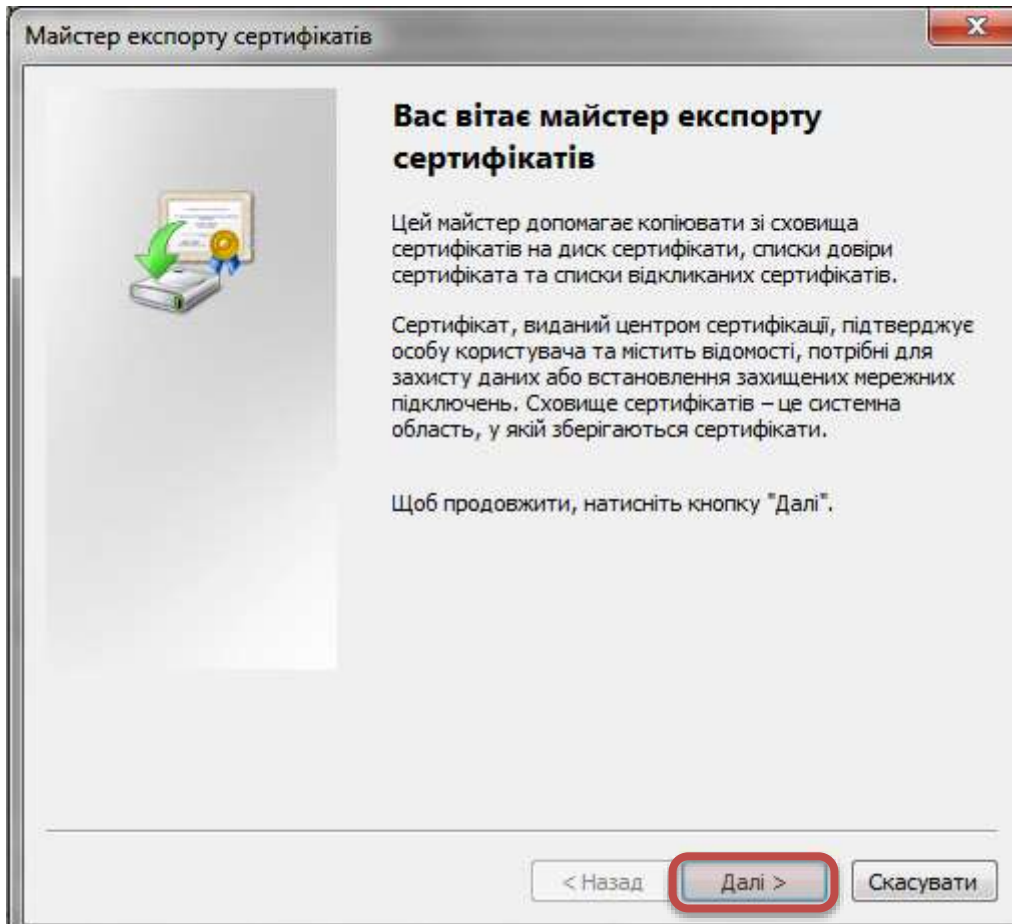


Рис. 30 Діалогове вікно "Сертифікати"

5. Запуск майстра сертифікатів, слід натиснути кнопку "Далі".



6. Експортування закритого ключа, слід вибрати можливість "Так" та натиснути кнопку "Далі"

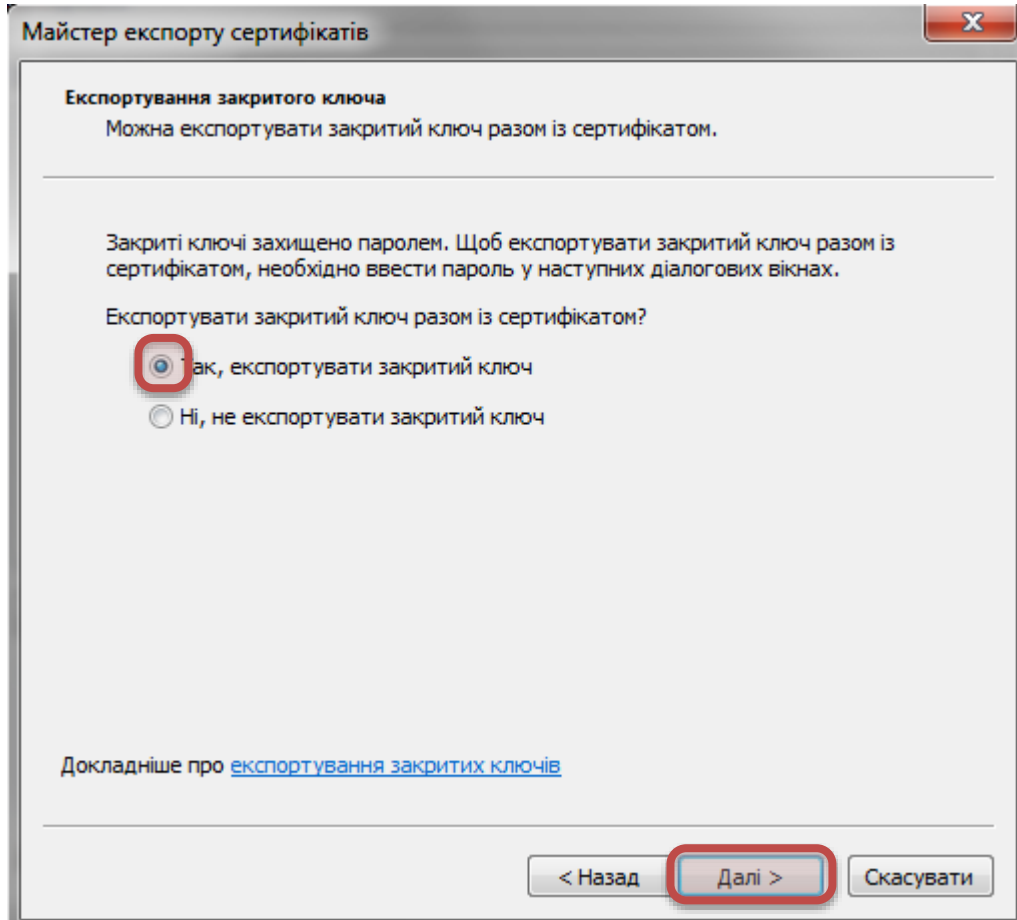


Рис. 31 Експортування закритого ключа

7. Формат експорту. Використайте можливість додати всі сертифікати до шляху сертифікації. Решту прапорців не варто ставити.

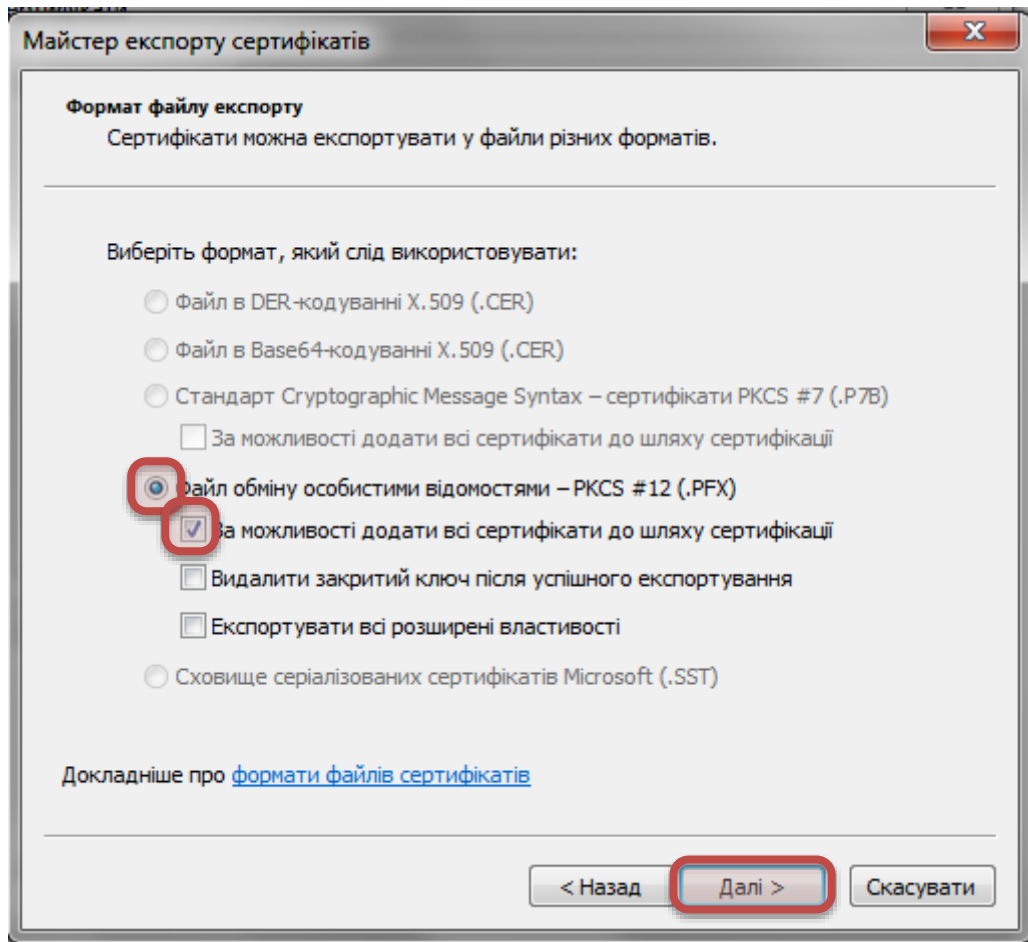


Рис. 32 Формат експорту

8. Захист приватного ключа паролем. Використайте той самий пароль, який використовували протягом генерації сертифікату. Пароль слід ввести двічі однаковий.

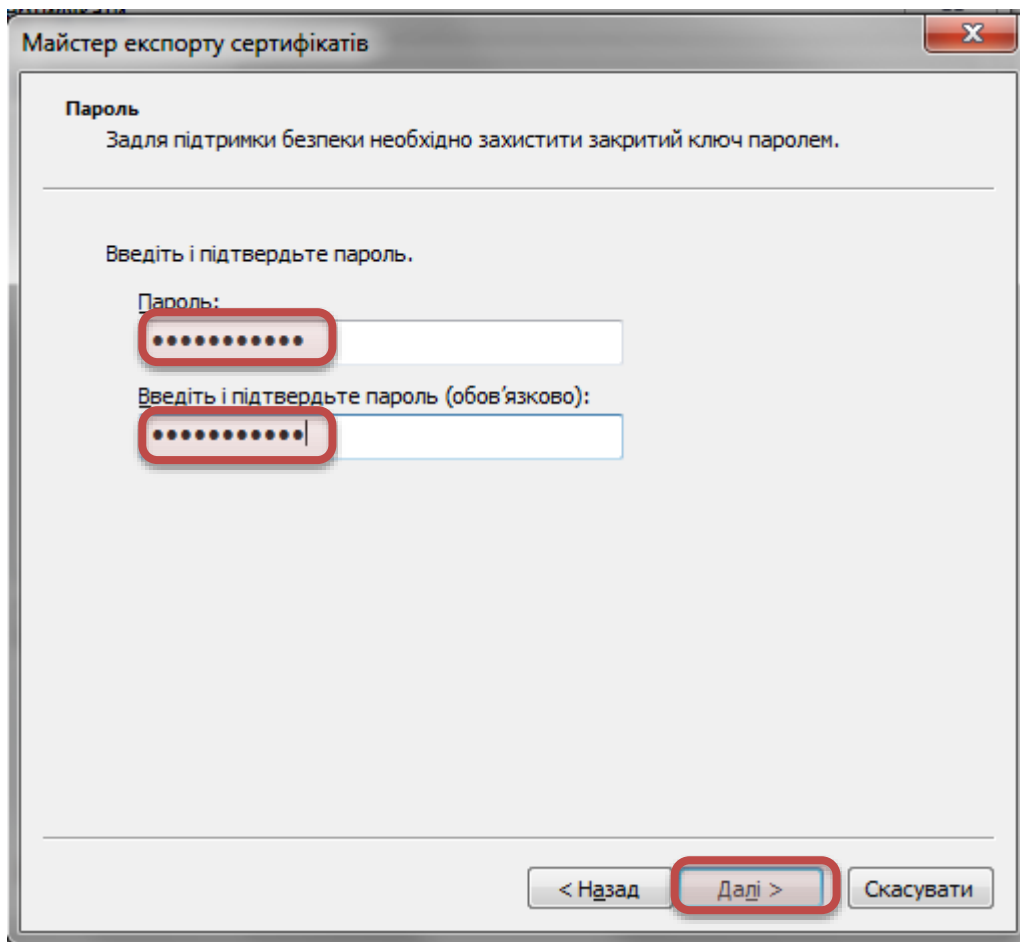


Рис. 33 Захист приватного ключа паролем

9. Скористайтесь кнопкою "Огляд..." для вказання місця розташування та імені файлу експорту.

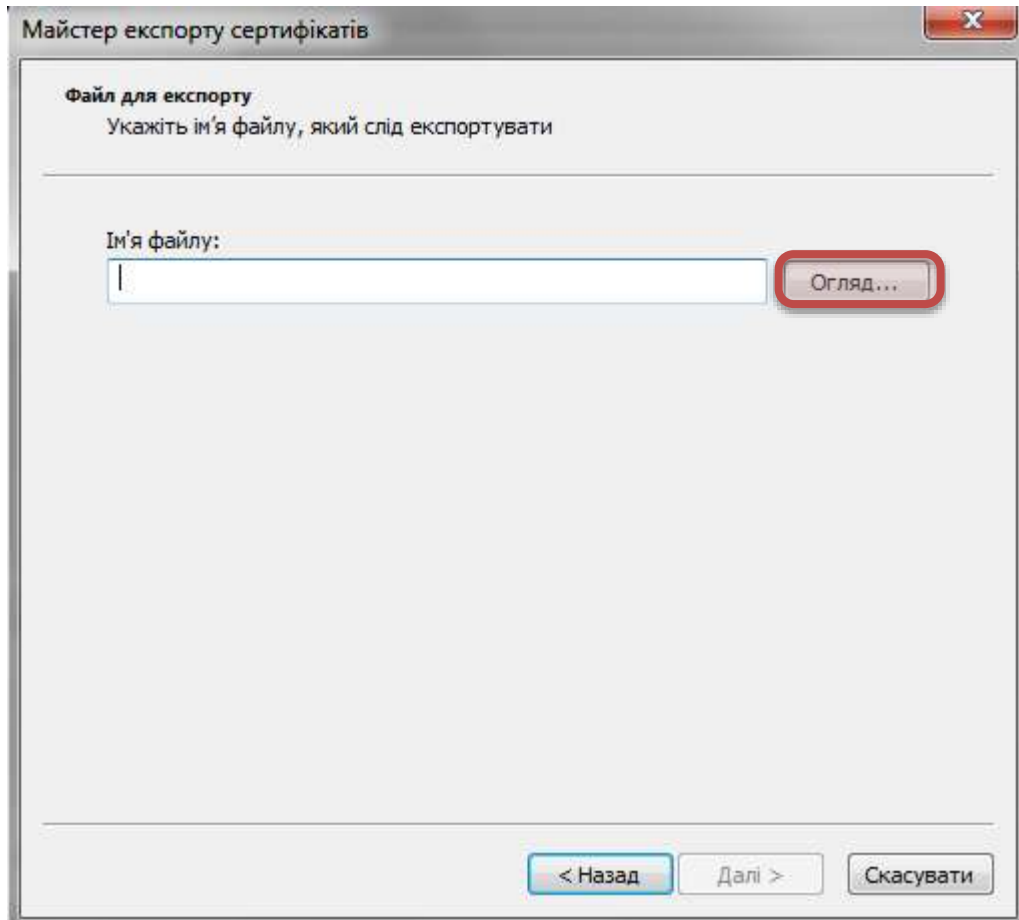


Рис. 34 Ім'я та розташування файлу експорту

10. Назва файлу експорту. Виберіть розташування файлу таким чином, щоб його легко було знайти (наприклад створіть на змінному носію папку **keys\global**) давши йому ім'я згідно зразка. Після виконання вимог натисніть кнопку "**Зберегти**".

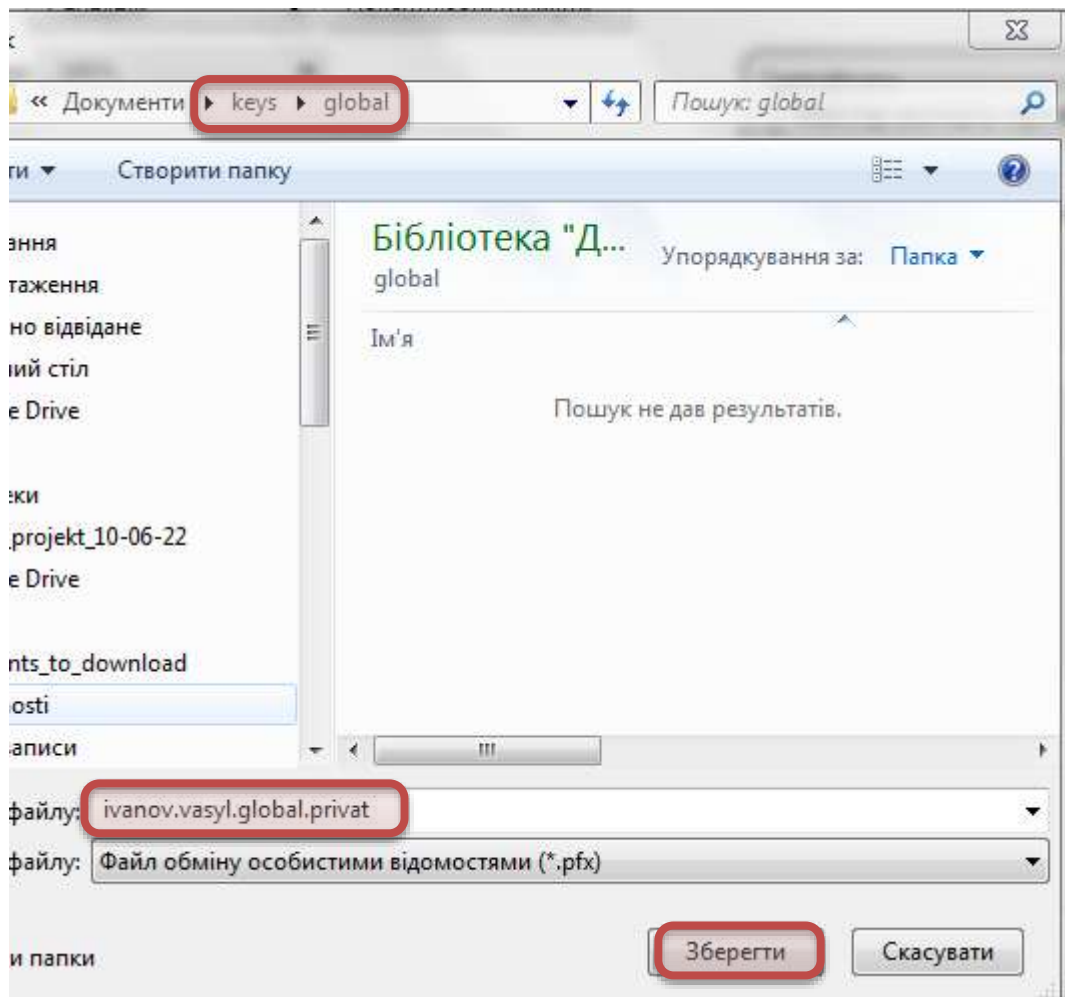


Рис. 35 Назва файлу та розташування

11. Після вказання шляху до файлу експорту слід натиснути кнопку "Далі"

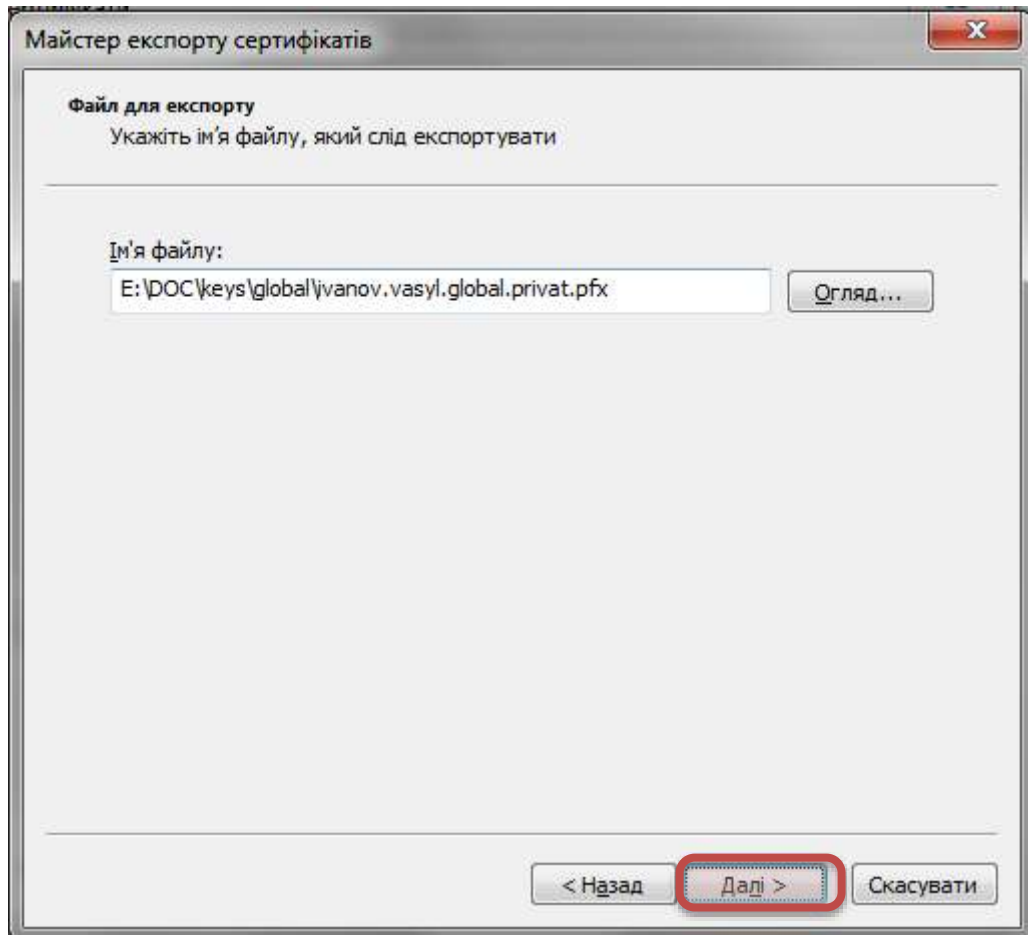


Рис. 36 Шлях до файлу експорту

12. Завершення роботи майстра – натисніть кнопку "Готово".

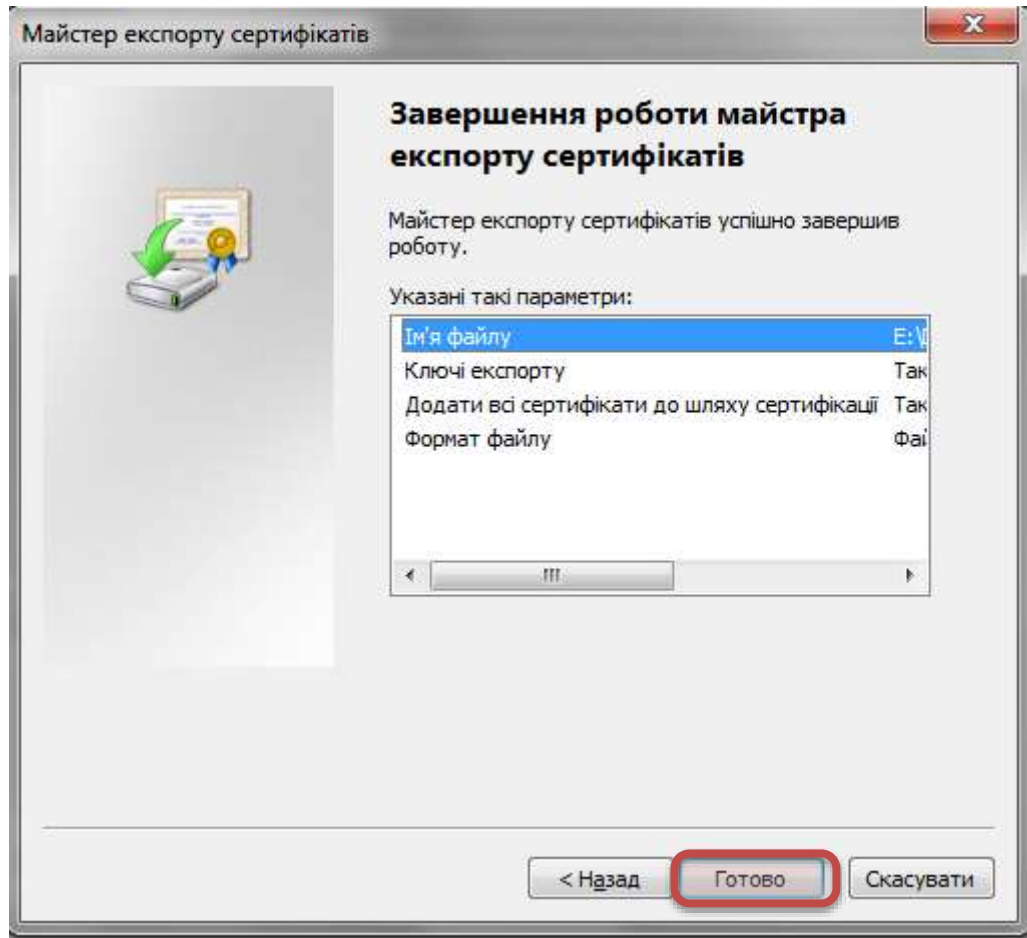
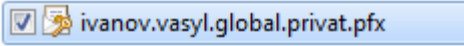


Рис. 37 Завершення роботи майстра

Після повідомлення про успішний експорт закрийте модальне вікно та діалогове вікно "Сертифікати".

Перевірте чи дійсно вдалося експортувати файл. За вказаним Вами шляхом повинен бути приблизно

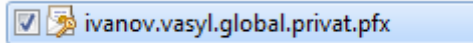
такий файл:



Імпорт сертифіката від Globalsign

Здійснення імпорту сертифікату від Globalsign в Internet Explorer

Сертифікат від Globalsign дозволяє здійснювати операцію підписування документів MS Office. Для того, щоб реалізувати цю можливість потрібно в операційній системі встановити власне сам сертифікат. Встановити сертифікат можливо з допомогою операції імпорту. Для імпорту сертифікату в Internet Explorer слід просто зробити подвійний клік на файлі експорту



Подальший процес імпорту описаний у вигляді сукупності ілюстрованих кроків¹:

1. Запуск майстра імпорту сертифікатів (Рис. 38).

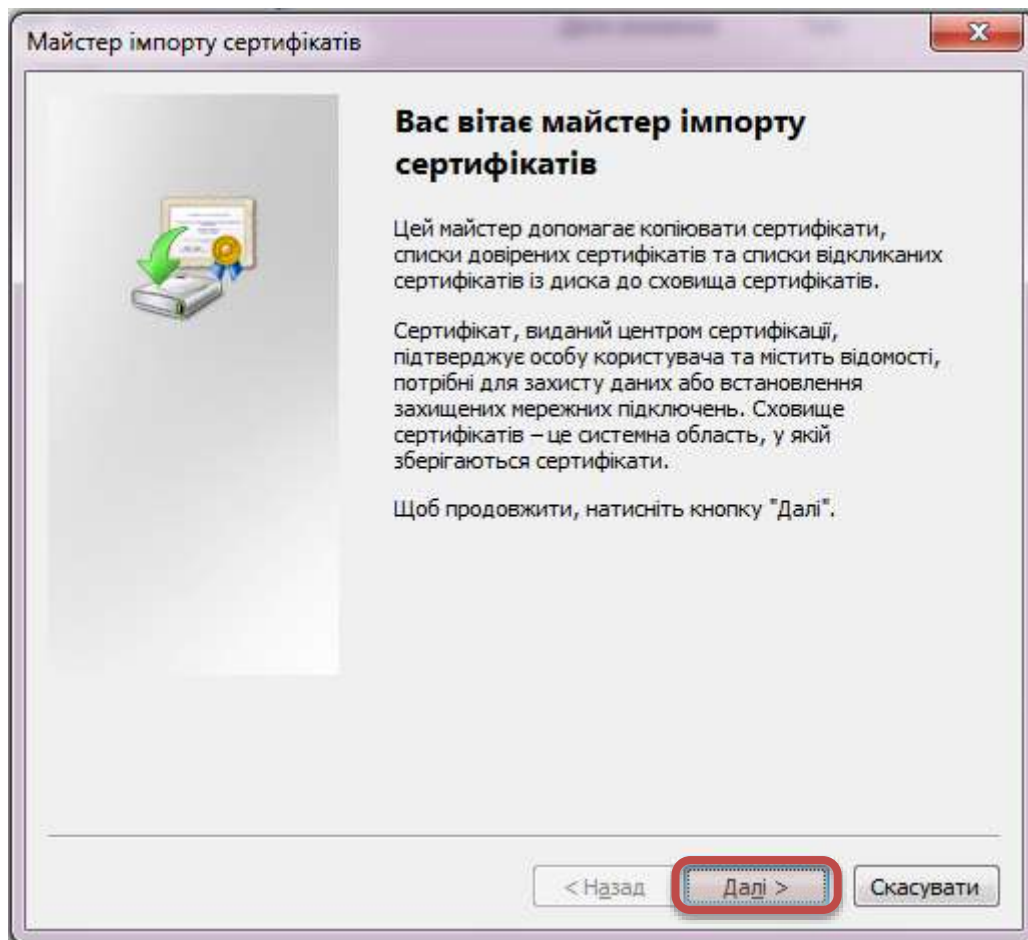


Рис. 38 Стартове вікно майстра імпорту сертифікатів

¹ В залежності від операційної системи та її версії послідовність кроків майстра може дещо відрізнятись.

2. Вказання файлу для здійснення імпорту (Рис. 39). Насправді файл вказувати не потрібно, так як він був вибраний автоматично в момент подвійного кліка на файлі.

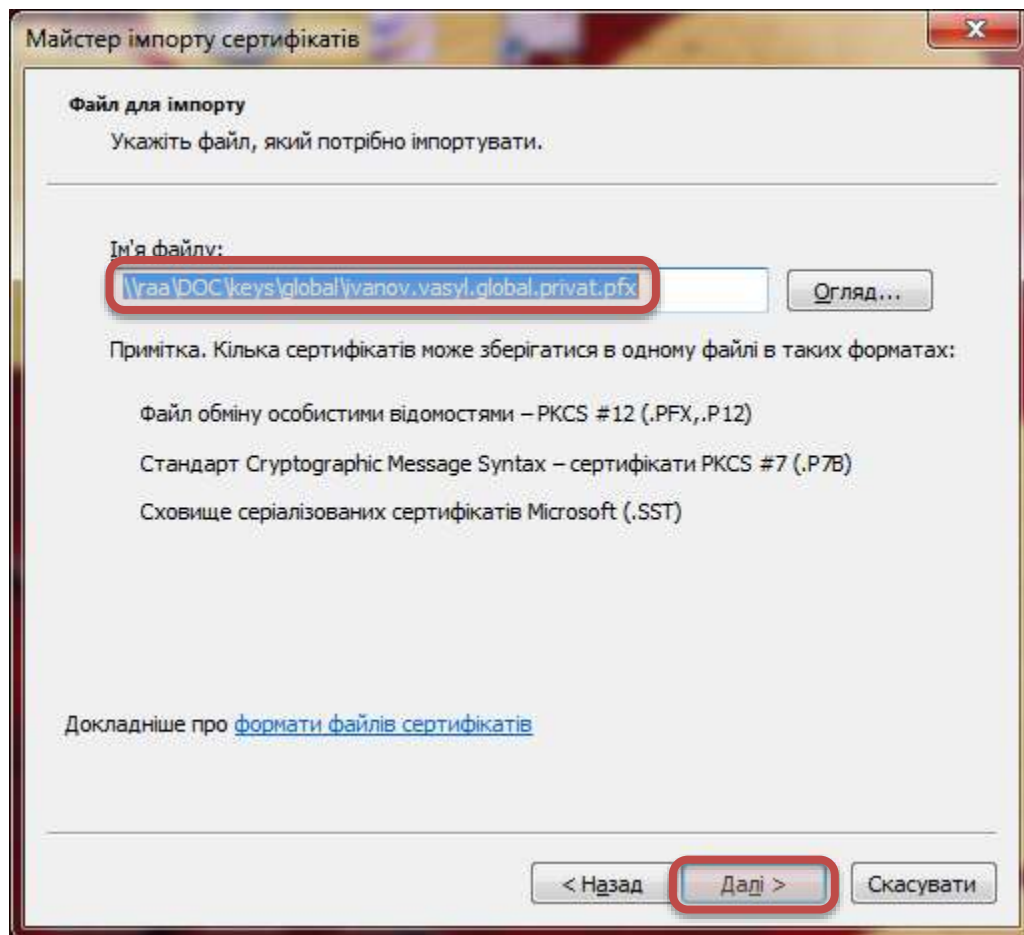


Рис. 39 Вказання імені файлу

3. Ввід пароля таємного ключа (Рис. 40).
 - a. Для здійснення імпорту слід ввести пароль доступу до таємного ключа.
 - b. Встановити прапорець «Увімкнути сильний захист закритого ключа». Це дасть можливість навіть на публічному комп'ютері здійснювати підпис, при цьому, під час кожного використання закритого ключа буде запитано пароль доступу до нього.
 - c. Встановити прапорець «Позначити цей ключ як придатний до експорту». Це дасть можливість і надалі здійснювати операції імпорту з допомогою цього ж файлу.

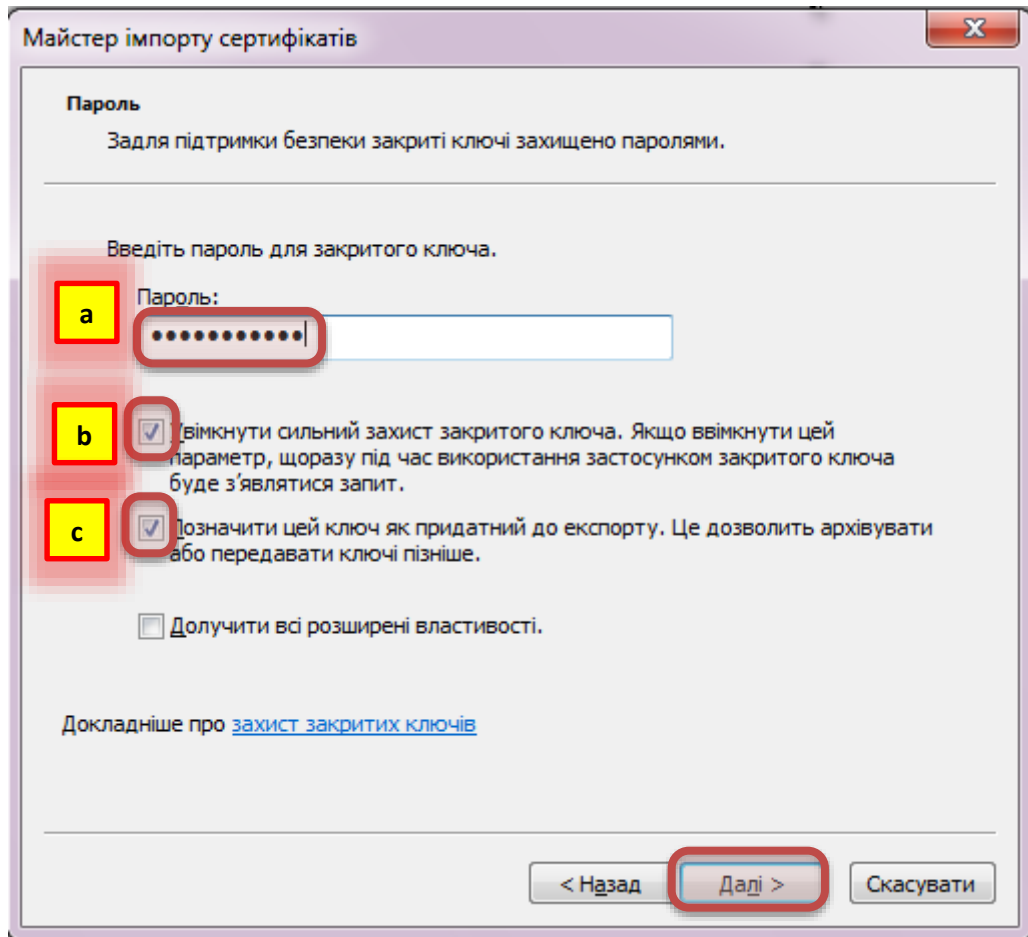


Рис. 40 Майстер імпорту ввід пароля таємного ключа

4. Вибір сховища сертифікатів. На цьому кроці слід скористатися функцією автоматичного вибору сховища на основі типу сертифікату (Рис. 41).

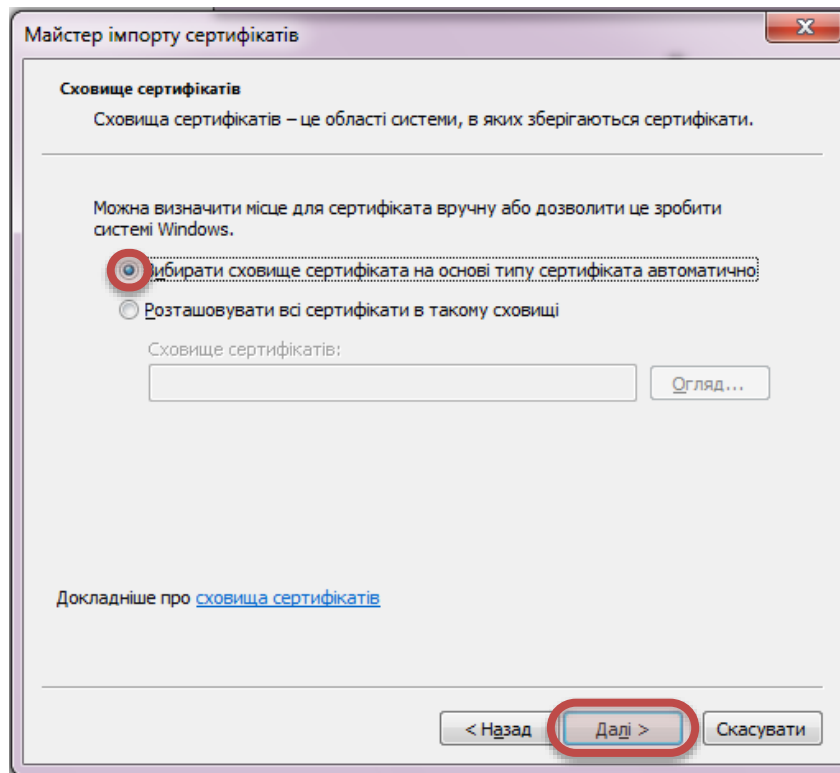


Рис. 41 Сховище сертифікатів

5. Завершальний крок налаштування майстра (Рис. 42).

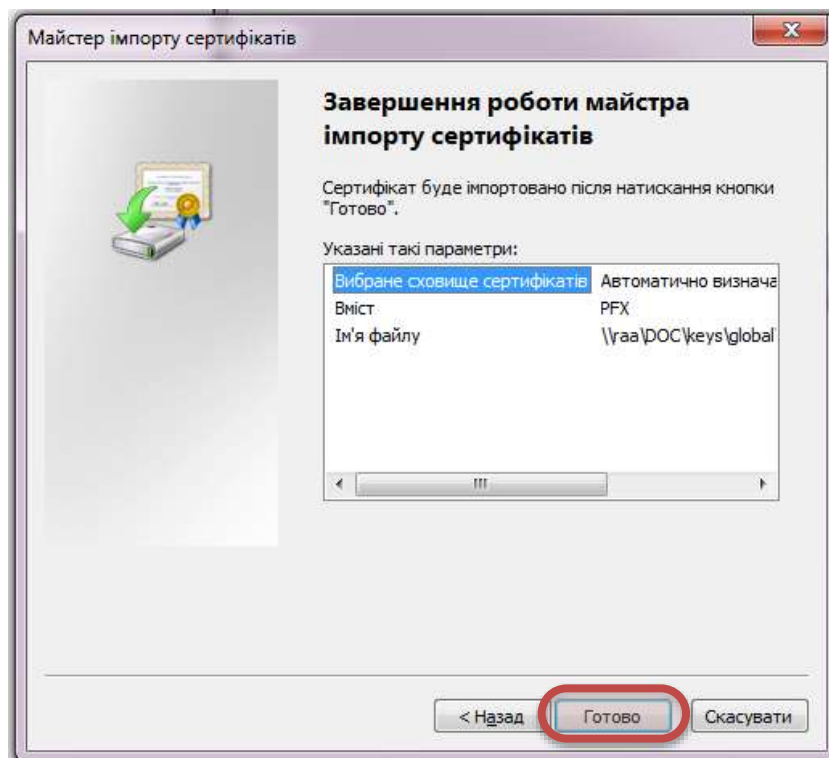


Рис. 42 Завершення налаштування майстра

- Початкове вікно імпорту сертифікату в Internet Explorer (Рис. 43). Слід вибрати високий рівень безпеки.

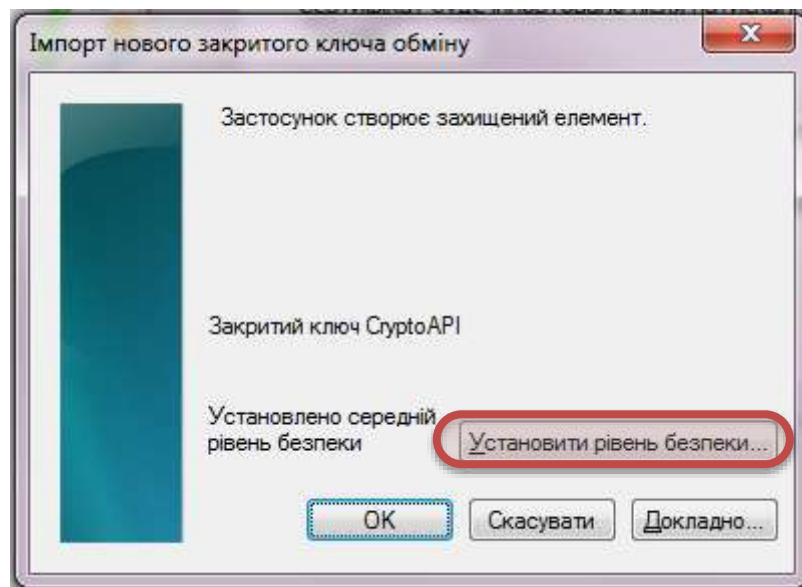


Рис. 43 Початкове вікно імпорту

- Вибрати високий рівень безпеки (Рис. 44).

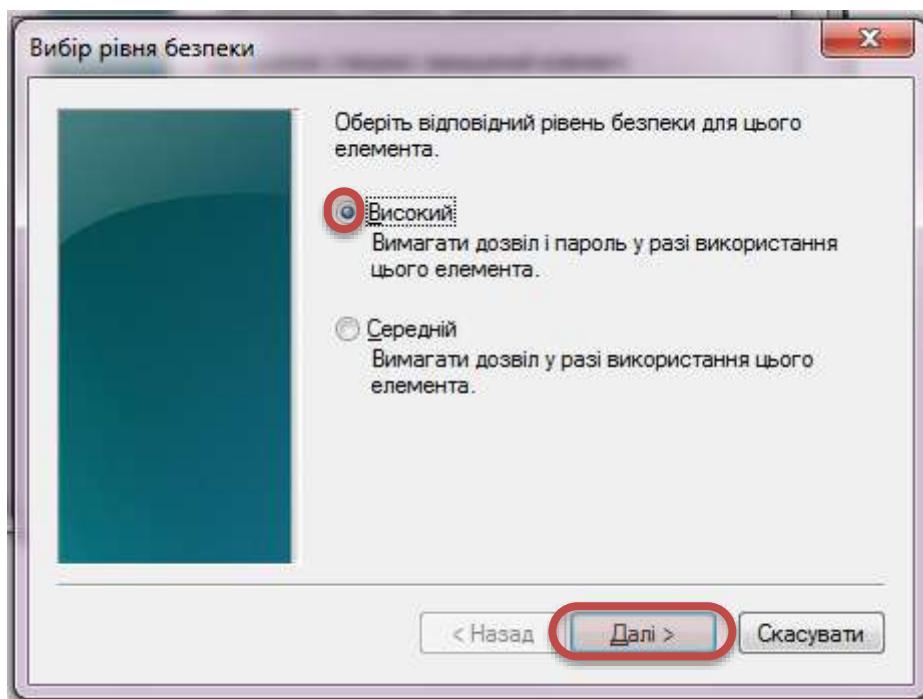


Рис. 44 Вибір рівня безпеки

8. Захист таємного ключа паролем (Рис. 45). На цьому етапі можна встановити інший пароль для доступу до таємного ключа, проте, рекомендується ввести такий же як і на попередніх кроках, щоб не заплутатися. Пароль слід ввести двічі однаковий, щоб система змогла переконатися, що Ви не зробили помилки під час вводу його першого разу.

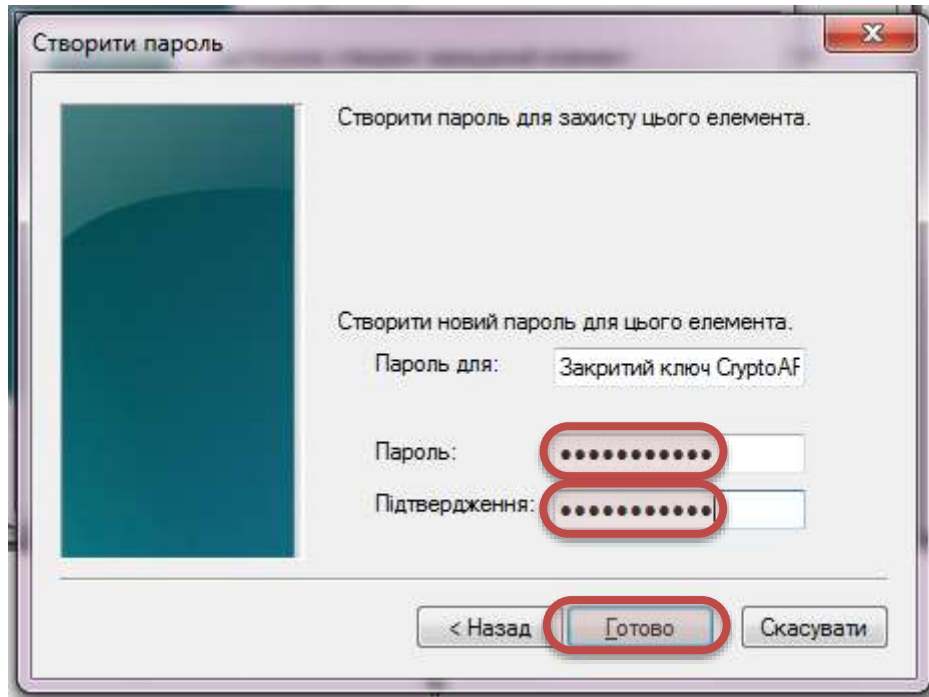


Рис. 45 Створення пароля таємного ключа

9. Підтвердження імпорту (Рис. 46).

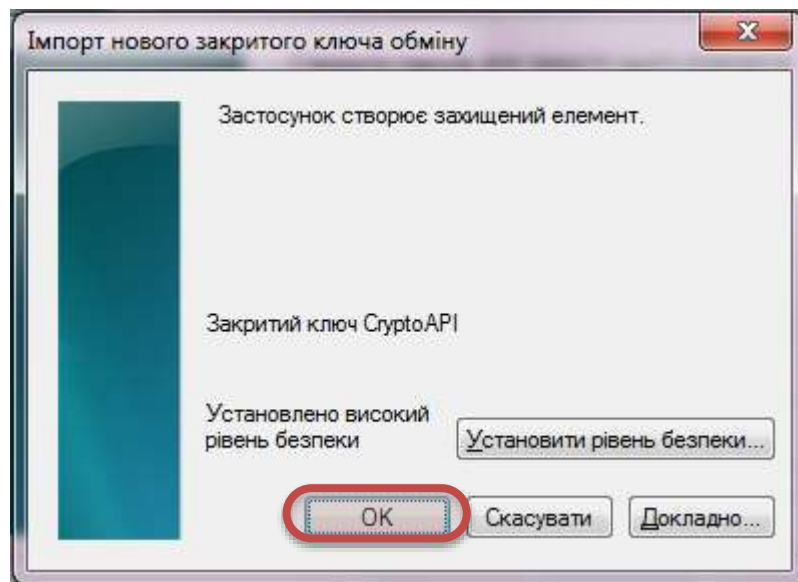


Рис. 46 Підтвердження імпорту ключа

10. Повідомлення про успішний імпорт ☺ (Рис. 47).

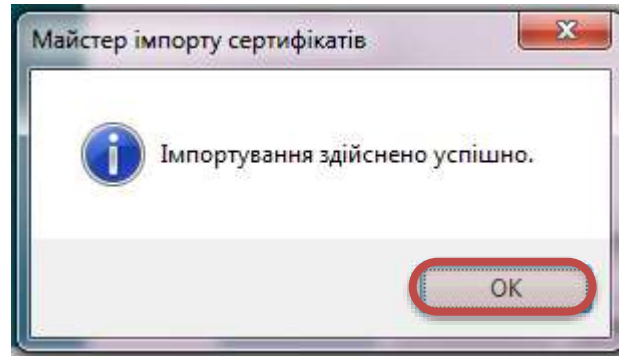


Рис. 47 Повідомлення про успішний імпорт

Тепер на комп'ютері, на якому щойно було здійснено імпорт сертифікату можна виконати [підпис документа MS Word](#).

Здійснення імпорту сертифікату від Globalsign в The Bat

Для того, щоб здійснити імпорт експортованого сертифікату від Globalsign слід завантажити поштовий клієнт The Bat з налаштованою скринькою та виконати низку ілюстрованих кроків, наведених нижче.

1. Відкрийте властивості скриньки (Рис. 48).
 - a. Виберіть свою власну скриньку, якщо їх більше ніж одна, як показано на рисунку.
 - b. Відкрийте меню «Скринька».
 - c. Виберіть підпункт «Властивості».

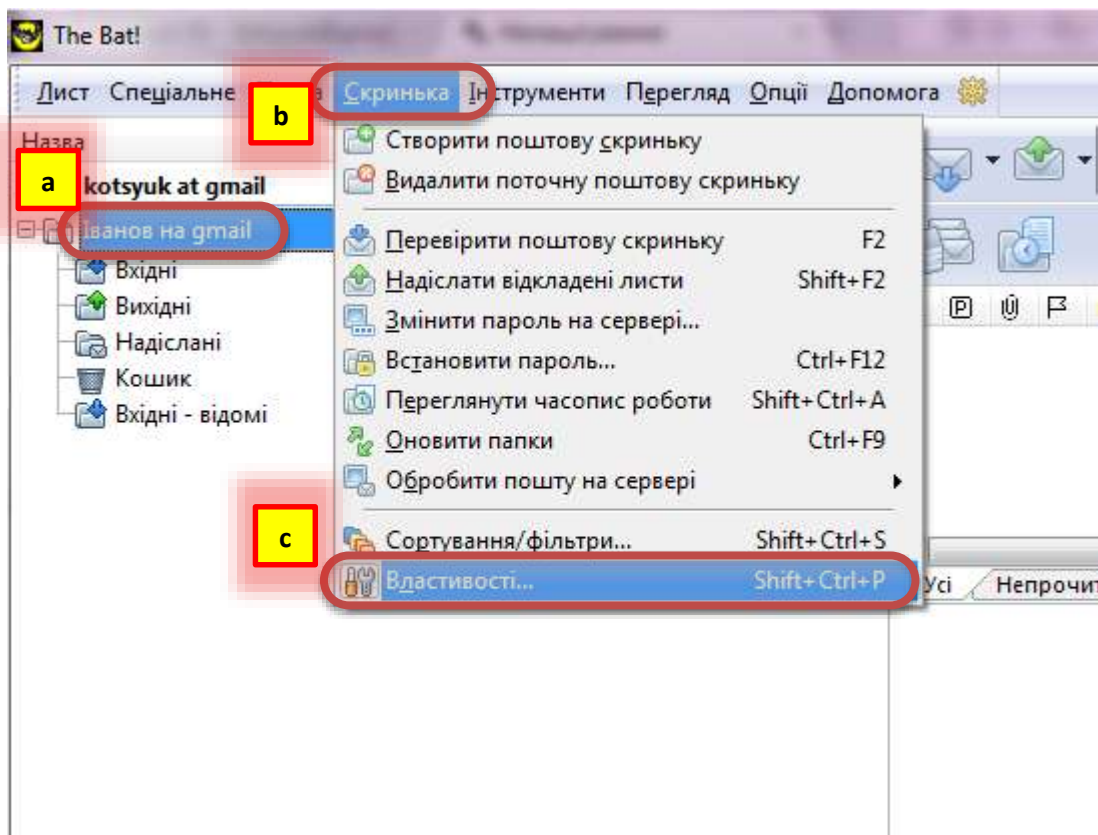


Рис. 48 Властивості скриньки

2. Відкрити можливість редагувати сертифікати (Рис. 49).
 - a. Виберіть розділ «Загальні відомості».
 - b. Натисніть кнопку «Редагувати сертифікати».

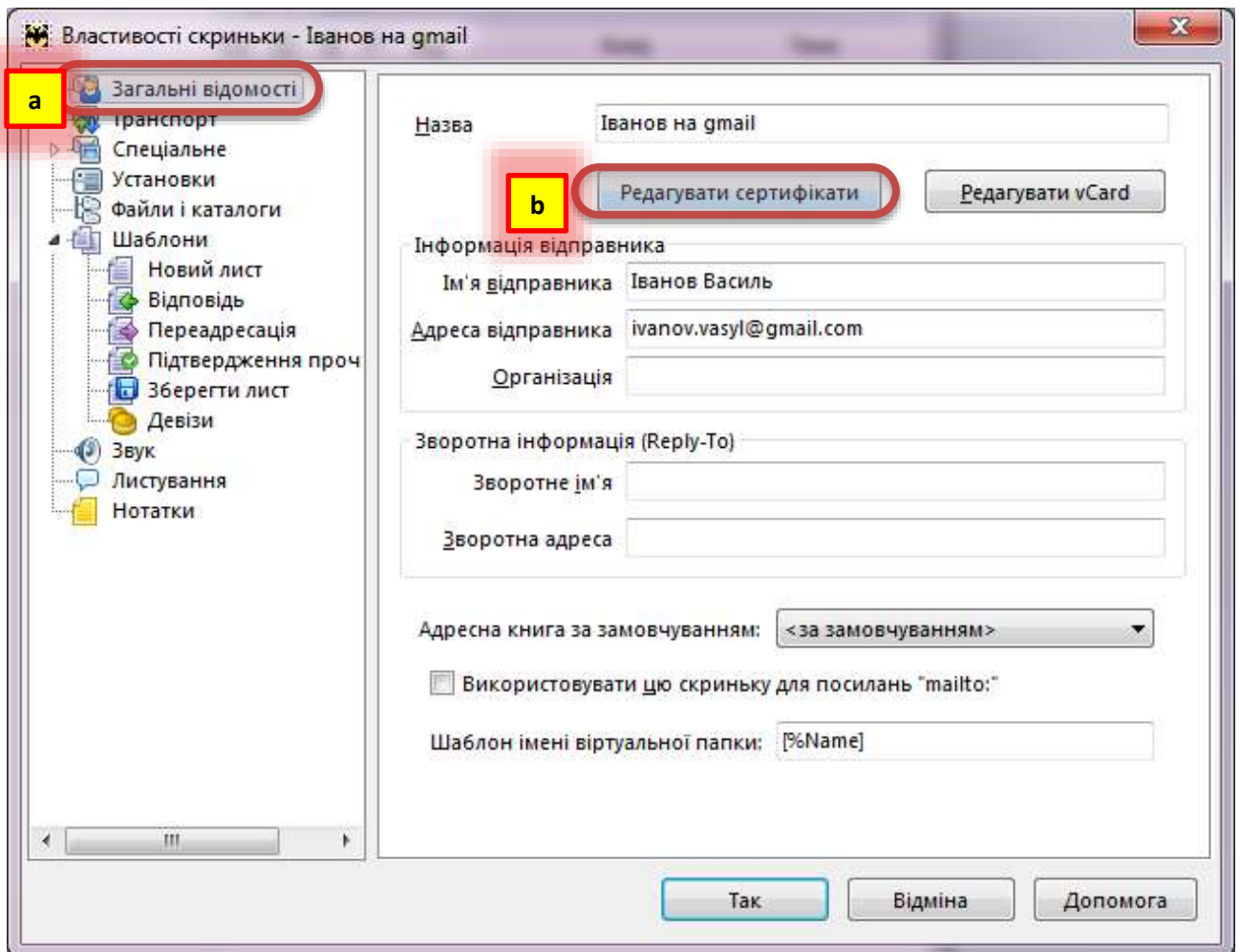


Рис. 49 Властивості скриньки, Загальні відомості

3. Розпочати процес імпорту (Рис. 50).
 - a. Переконайтеся, що відкрита вкладка сертифікат.
 - b. У переліку сертифікатів можуть існувати попередні сертифікати. Так на рисунку такий сертифікат існує. Це сертифікат, який Іванов Василь згенерував собі сам. Разом з тим такого сертифікату може не існувати (якщо одне з попередніх завдань виконано не було).
 - c. Натиснути кнопку «Імпортування».

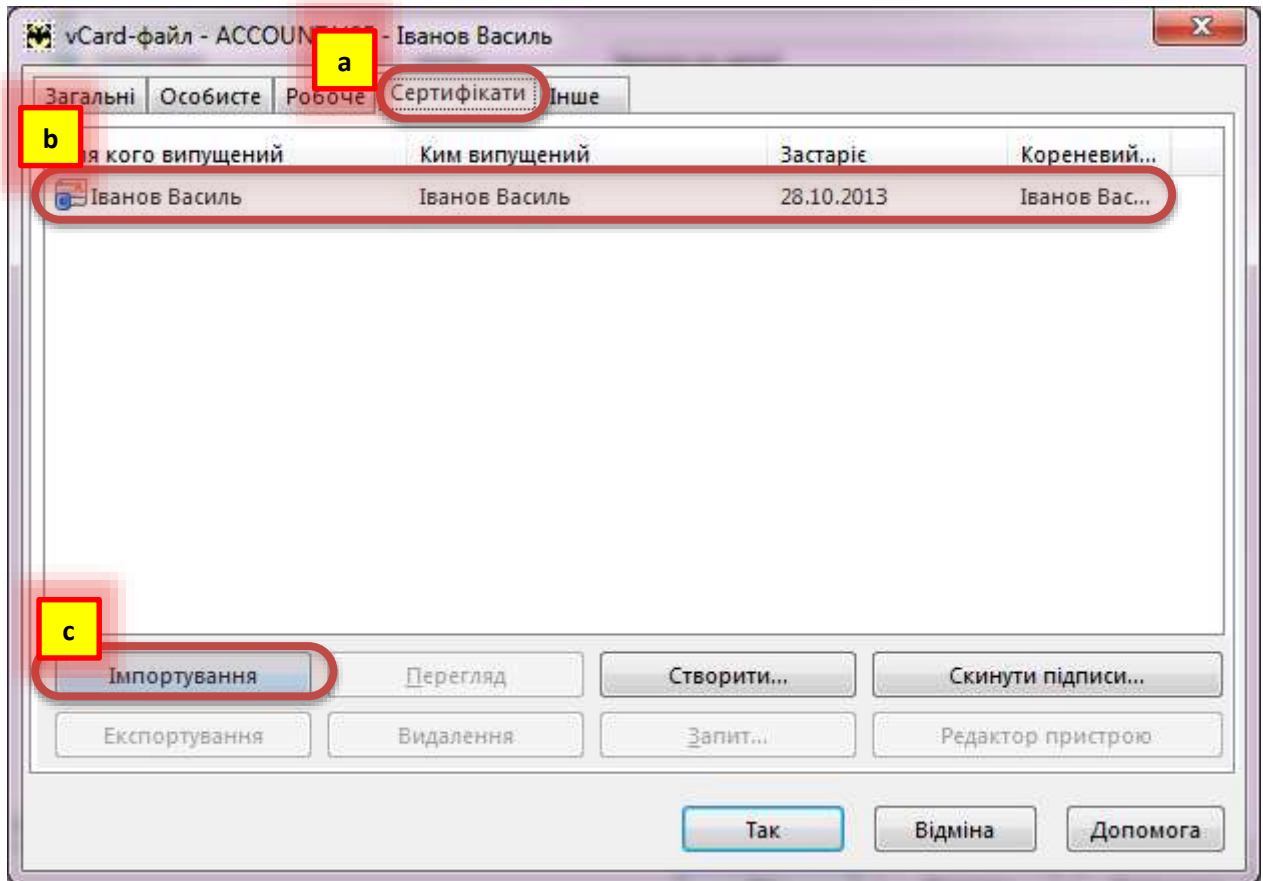


Рис. 50 vCard, вкладка "Сертифікати"

4. Вибір файлу експорту для здійснення імпорту (Рис. 51).
 - a. Вкажіть шлях до файлу з якого буде здійснювати імпорт. (Якщо експорт здійснювався у паку `..\keys\global`, то саме до неї слід вказати шлях).
 - b. Виберіть файл у який Ви екпортували сертифікат від Globalsign.
 - c. Переконайтеся, що у полі «Ім'я файлу» вибрано потрібний файл.
 - d. Натисніть кнопку «Відкрити».

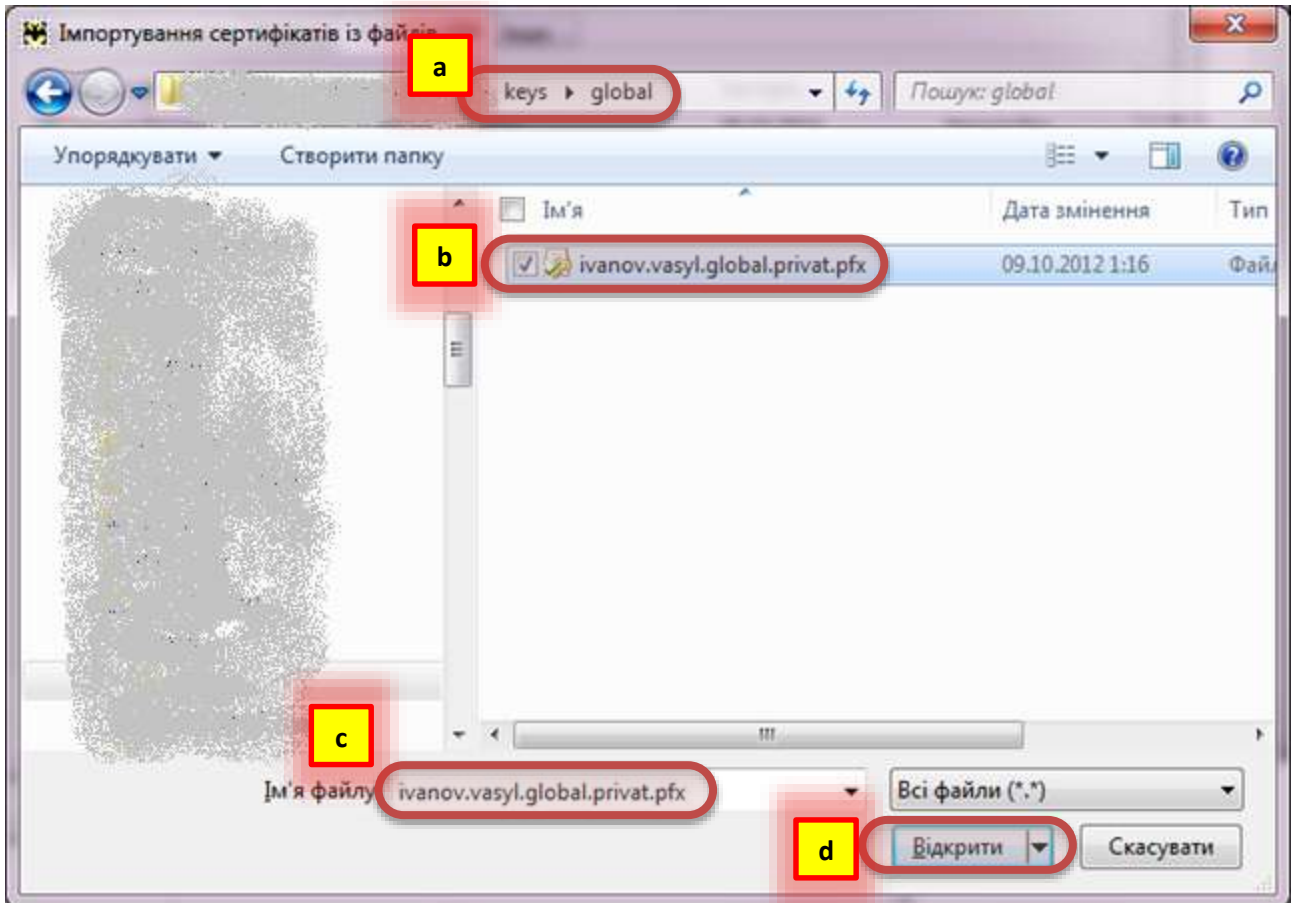


Рис. 51 Вибір файлу для імпорту

5. Введіть пароль для розшифрування особистого ключа та натисніть кнопку «Так» (Рис. 52)

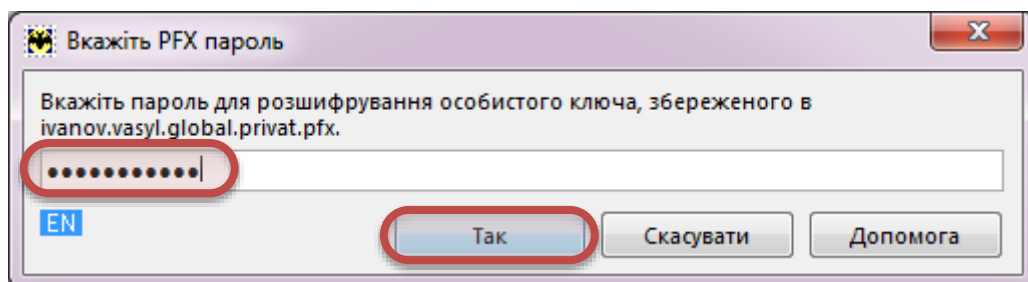


Рис. 52 Ввід пароля для розшифрування закритого ключа

- Повторно введіть пароль для розшифрування особистого ключа та натисніть кнопку «Так» (Рис. 53).

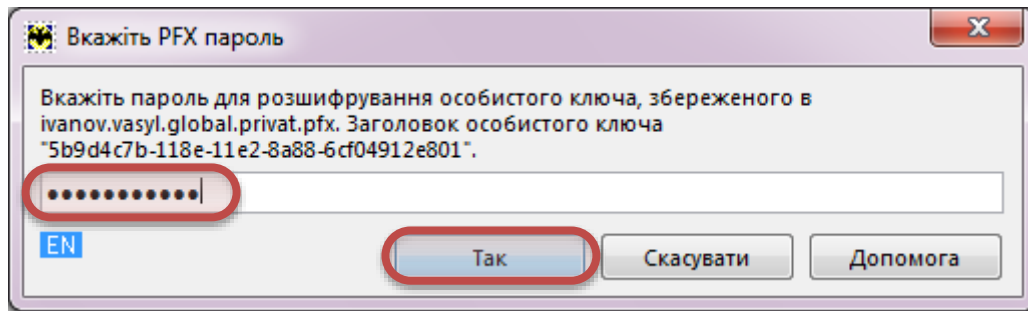


Рис. 53 Повторний ввід пароля

- В результаті імпорту з'явиться від одного до трьох сертифікатів. Слід зробити подвійний клік на Вашому сертифікаті від GlobalSign, щоб перевірити його справжність (Рис. 54).

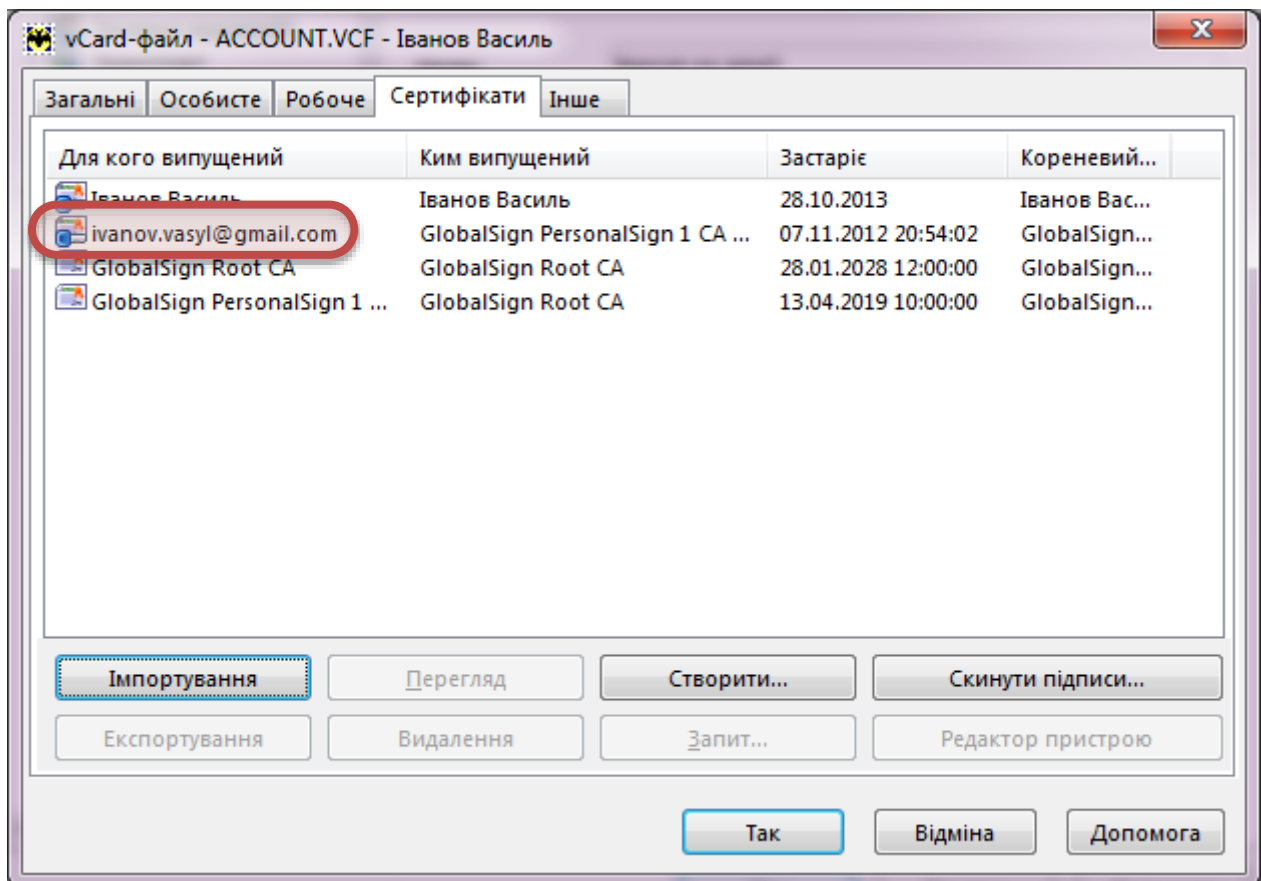


Рис. 54 Перегляд нового сертифікату

8. Слід перевірити дійсність сертифікату (Рис. 55).
 - a. Якщо піктограма сертифікату має зелений кружок з прапорцем й існує напис «Цей сертифікат є дійсним», можна одразу натиснути кнопку «Так» і перейти до кроку № 10. Якщо ж сертифікат недійсний:
 - b. Слід перейти у вкладку «Шлях».

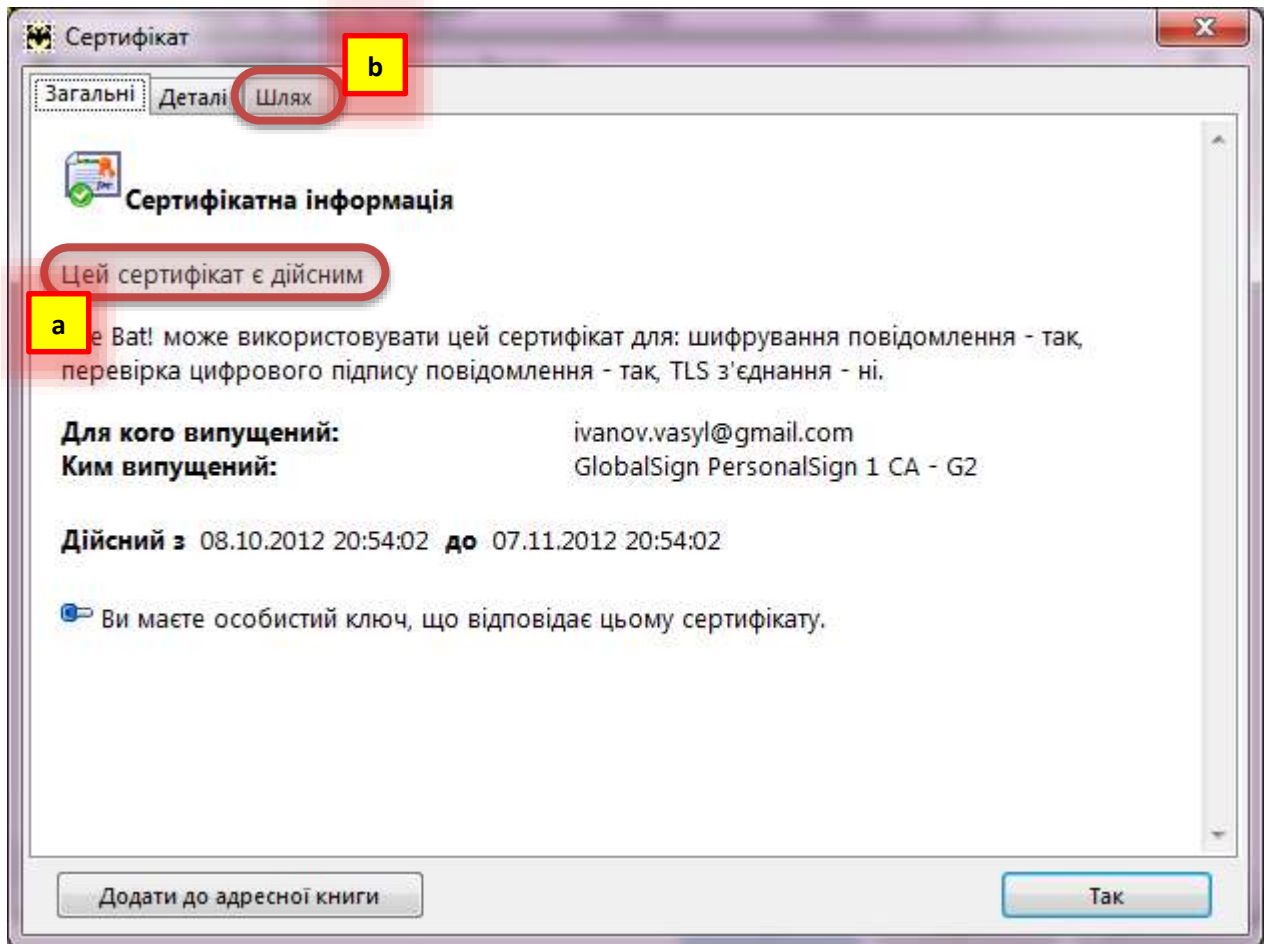


Рис. 55 Перевірка дійсності сертифіката

9. Додайте сертифікат до довірчих (Рис. 56).
 - a. Виберіть кореневий сертифікат.
 - b. Натисніть кнопку «Додати до Довірчих (Trusted)».
 - c. Після цього натисніть кнопку «Так».

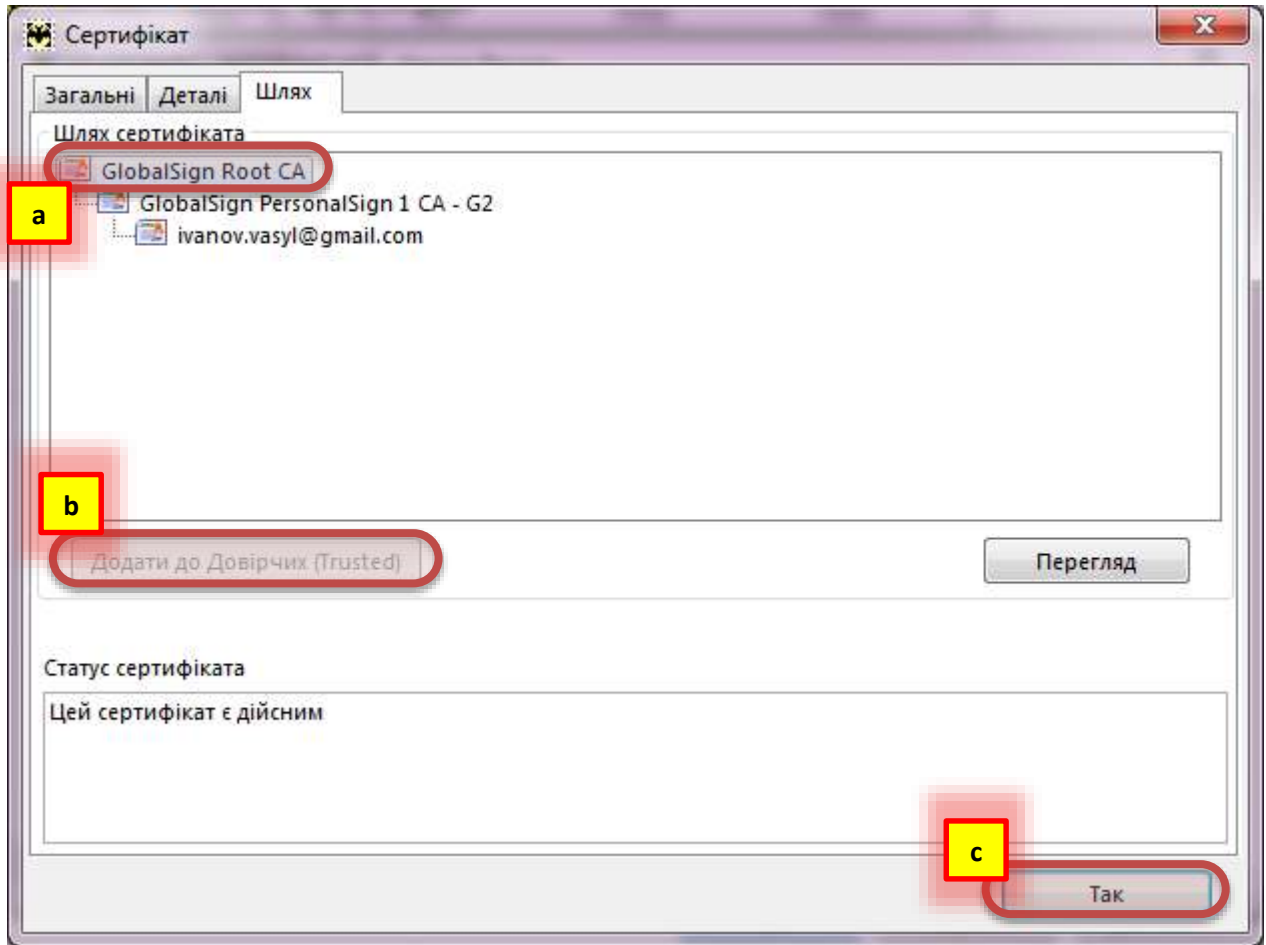


Рис. 56 Ланцюжок сертифікатів

10. Натисніть кнопку «Скинути підписи...» (Рис. 57). Це потрібно для вибору потрібного сертифікату при наступному доступі до таємного ключа. Якщо цього не зробити, то автоматично буде використано попередній ключ. Якщо Ви бажаєте кожен раз під час підписування документів використовувати інший ключ, цю операцію потрібно буде повторювати постійно.

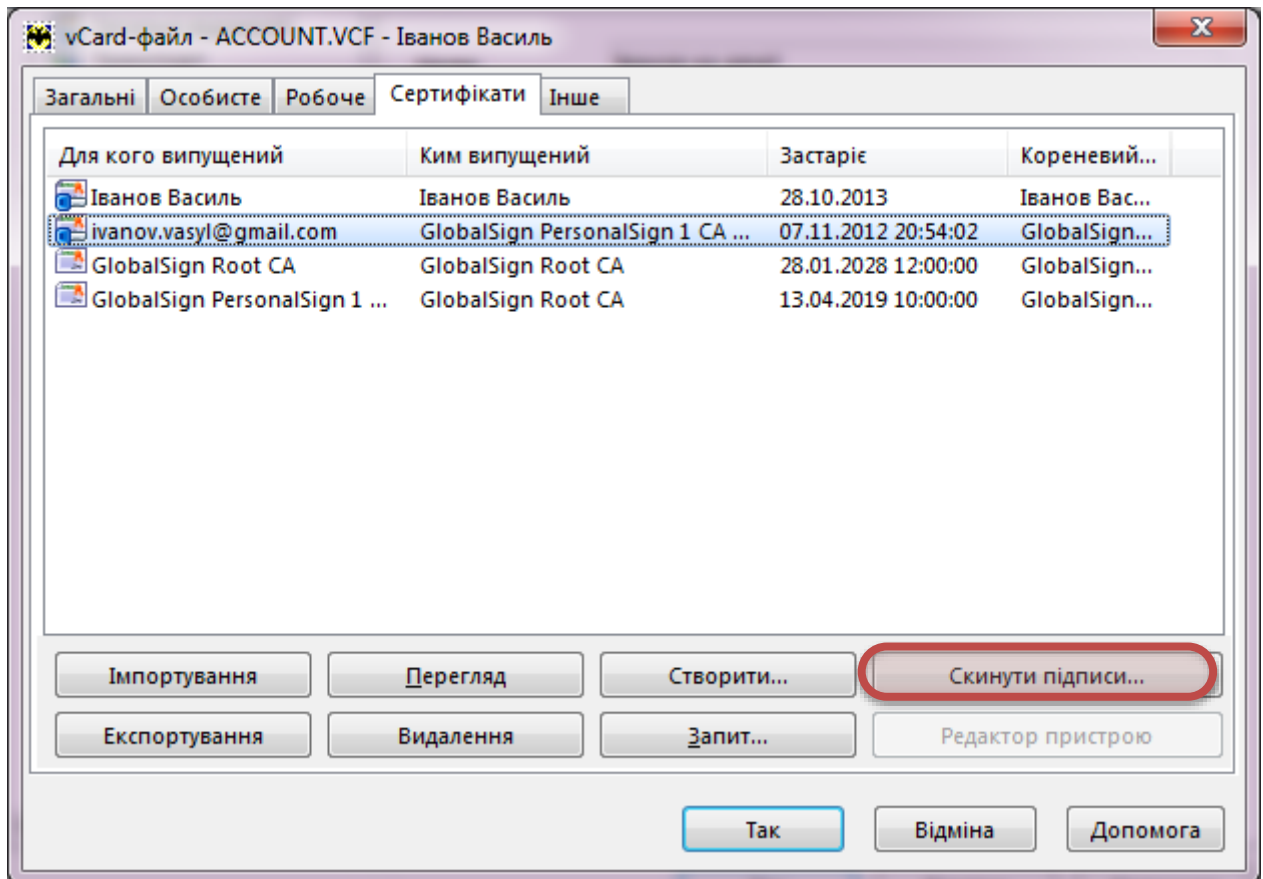


Рис. 57 Скидання підписів

11. Підтвердіть операцію скидання підписів, натиснувши «ОК».

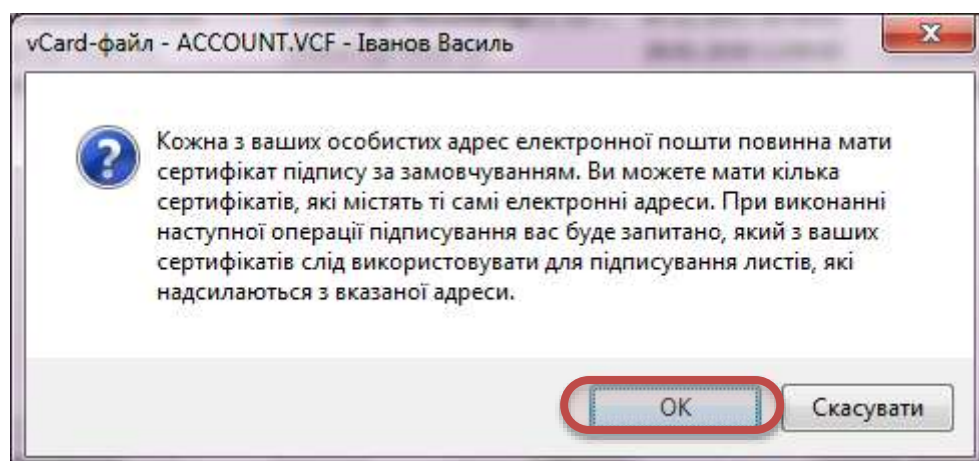


Рис. 58 Підтвердження операції скидання підписів

12. Підтвердіть виконані дії натиснувши кнопку «Так» (Рис. 59).

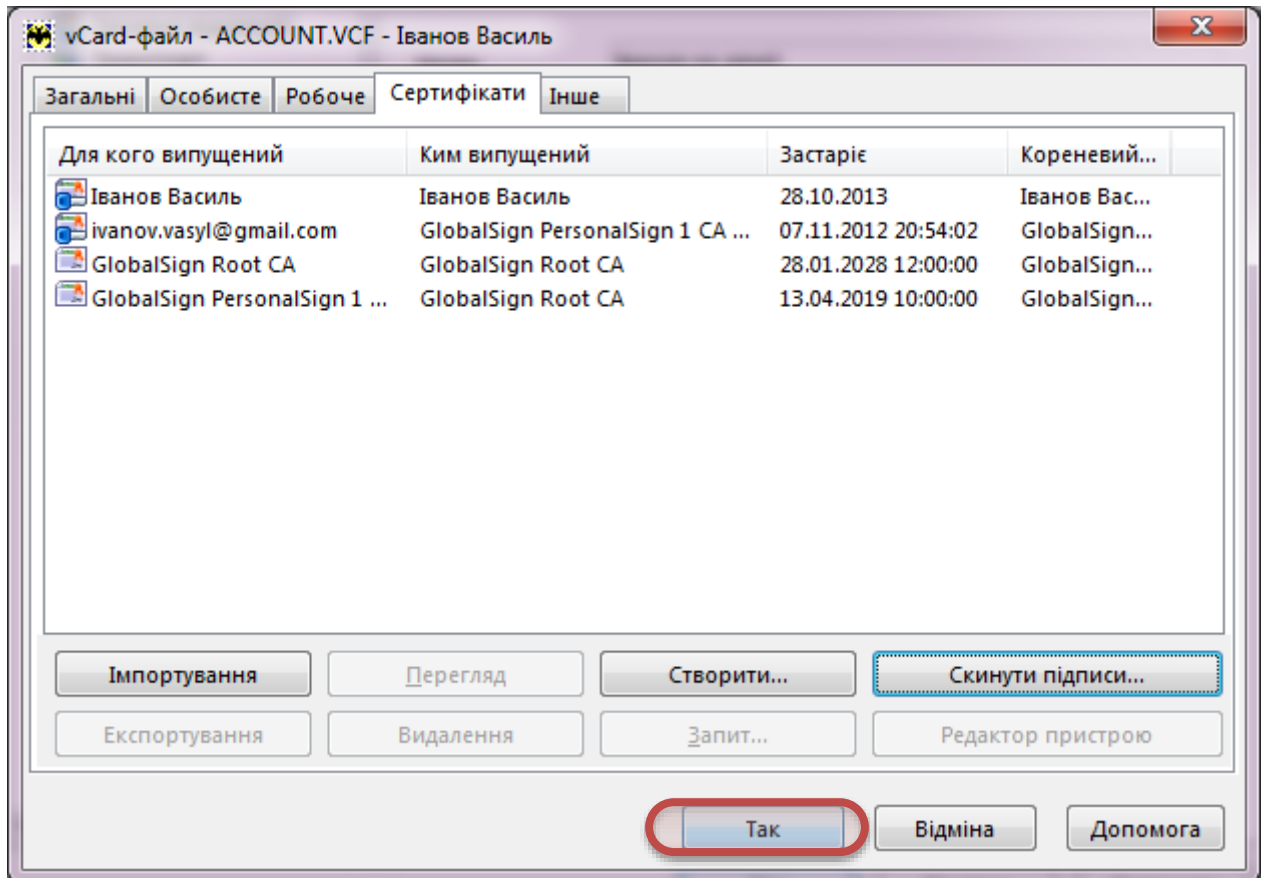


Рис. 59 Діалогове вікно "Сертифікати"

13. Підтвердіть виконані дії натиснувши кнопку «Так» (Рис. 60).

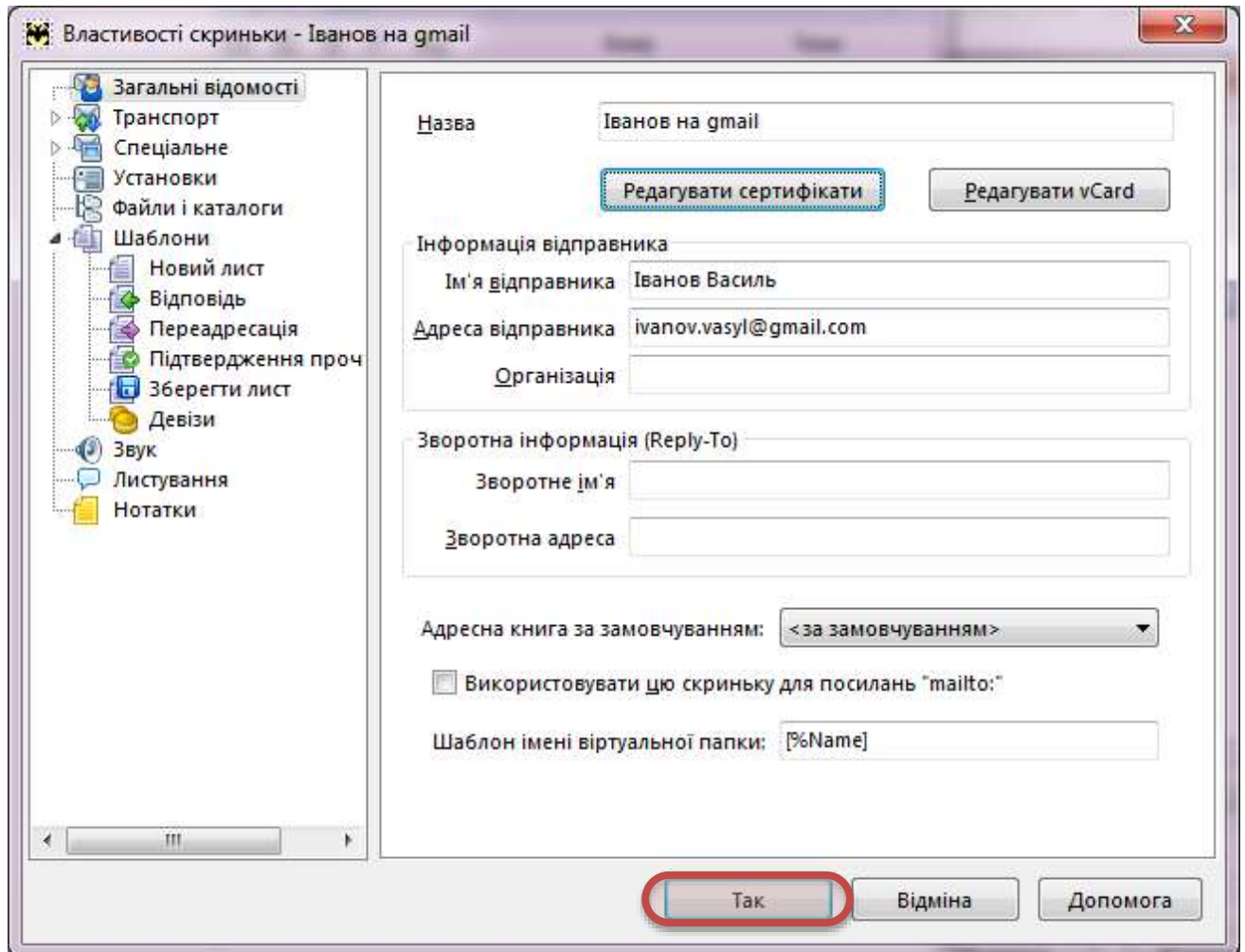


Рис. 60 Підтвердження імпорту та налаштувань

Використання сертифікату від Globalsign для накладання електронного цифрового підпису в документах MS Word

Перш ніж виконувати накладання цифрового підпису в документі MS Word, слід здійснити [імпорт сертифікату в Internet Explorer](#).

Накладати підпис можна на документ який вже названий та збережений. Тому, перш ніж розпочати процедуру підписування, слід створити документ MS Word та зберегти його з певною назвою. Пропонується дати таку назву документа: «Прізвище Ім'я підпис» де замість Прізвища та Імені вставити своє прізвище та ім'я¹.

Підпис документів MS Word 2013

1. Відкрийте підготований документ MS Word у текстовому процесорі MS Word (Рис. 61).

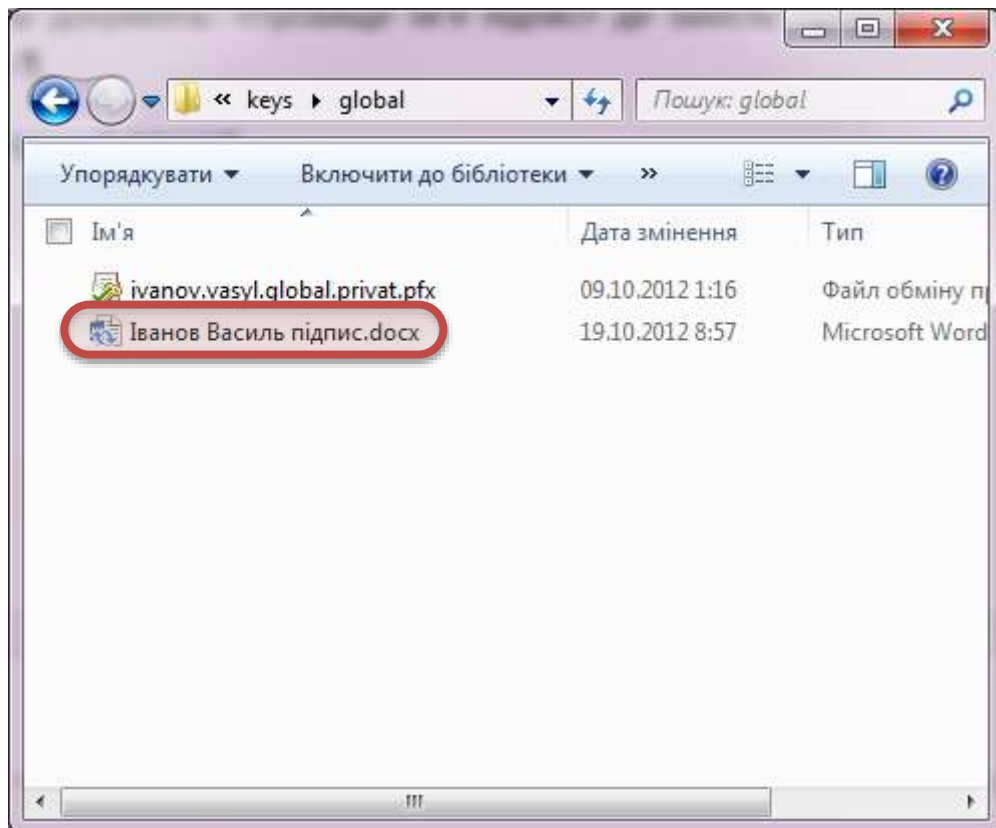


Рис. 61 Документ MS Word у папці

¹ В залежності від операційної системи та її версії процес підписування документа MS Office може дещо відрізнятися.

2. Перейдіть у меню FILE (Рис. 62).

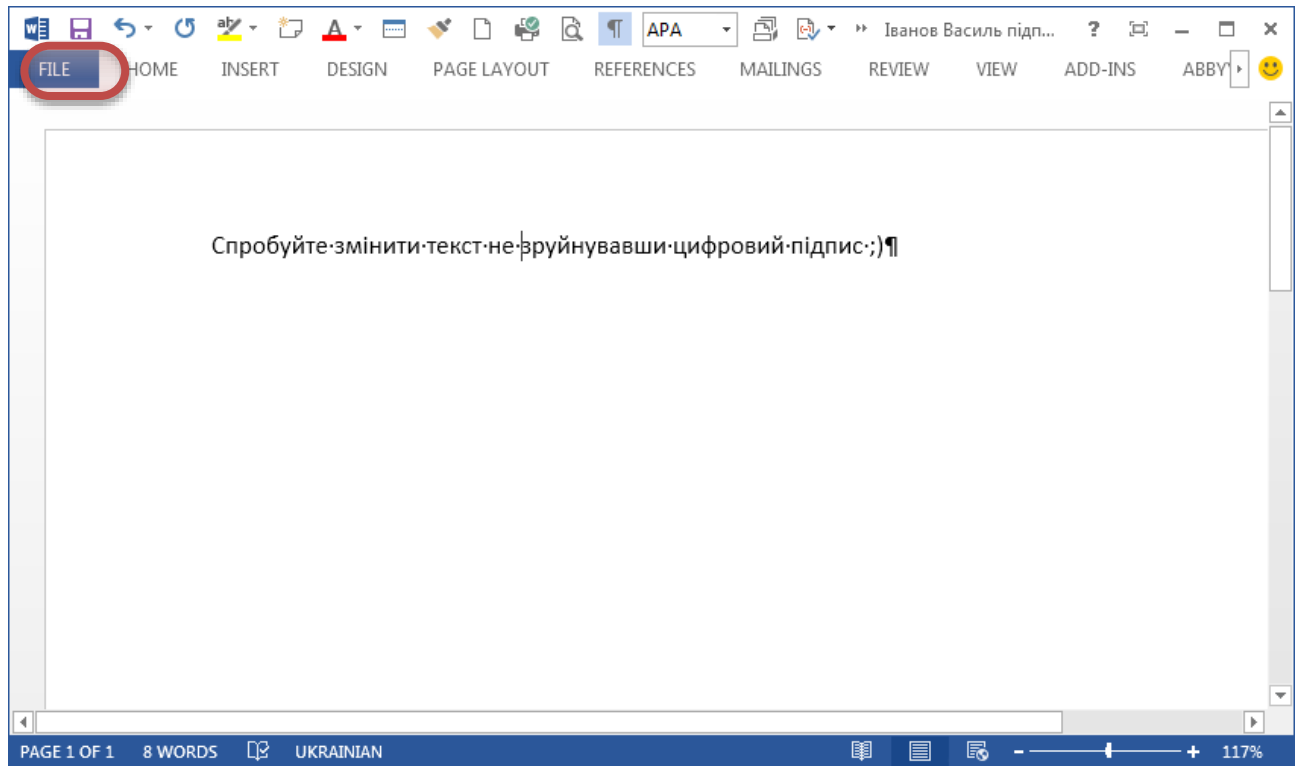


Рис. 62 Документ MS Word перед накладанням підпису

- У розділі «Info» відкрийте великою кнопкою «Protect Document» випадаюче меню та виберіть пункт «Add a Digital Signature» (Рис. 63).

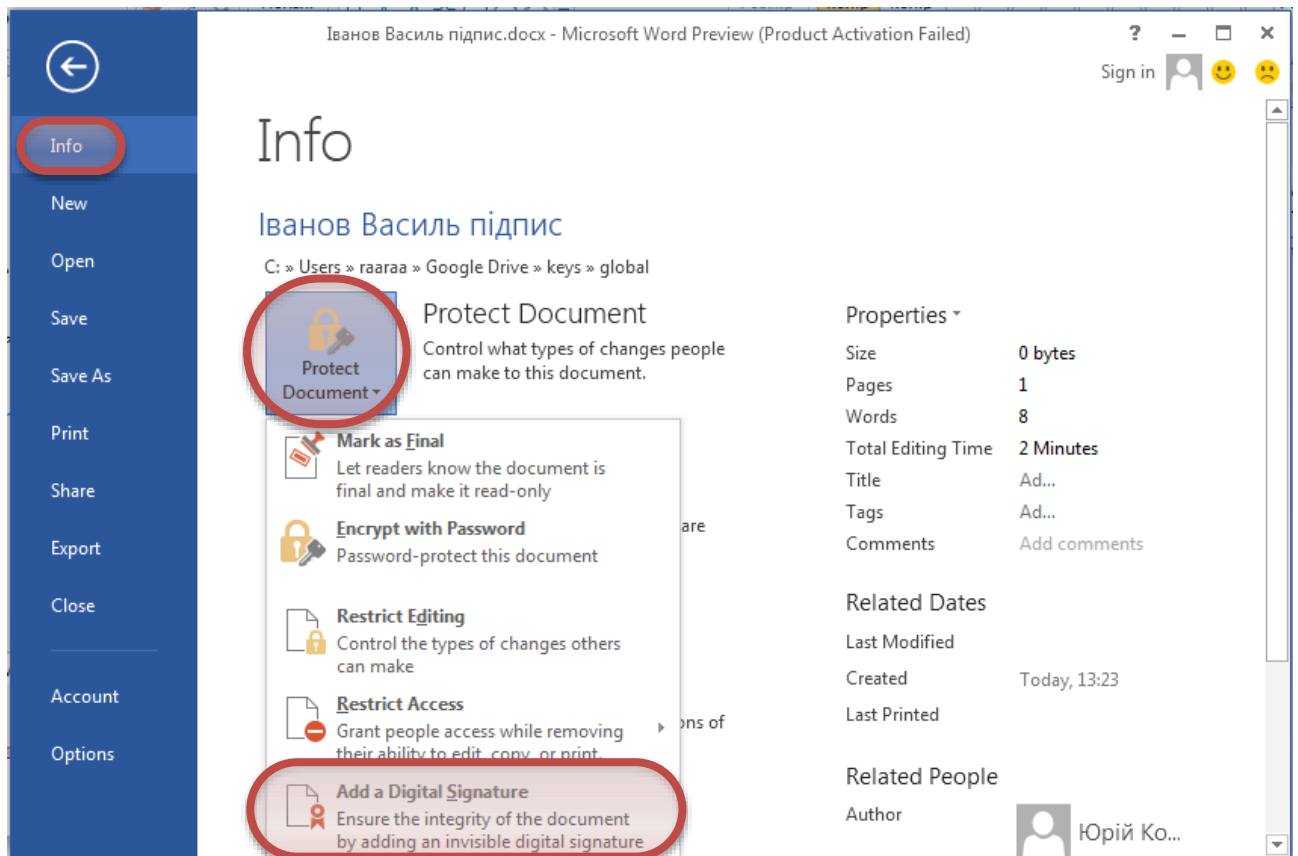


Рис. 63 Розділ "Info"

4. Вибір підпису¹ (Рис. 64).
 - a. Вкажіть тип відповідальності.
 - b. Вкажіть причину підписування.
 - c. Натисніть кнопку «Change...» для того, щоб вибрати серед існуючих підписів свій.

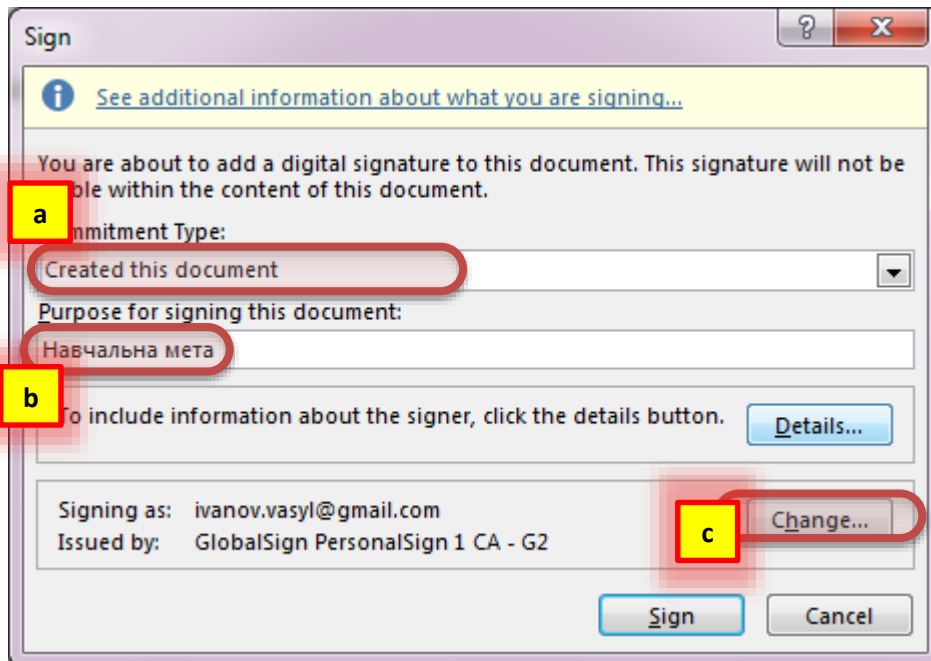


Рис. 64 Діалогове вікно "Підпис"

¹ Перш ніж виконувати накладання цифрового підпису в документі MS Word, слід здійснити [імпорт сертифікату в Internet Explorer](#).

5. Виберіть свій підпис та натисніть кнопку «ОК» (Рис. 65).

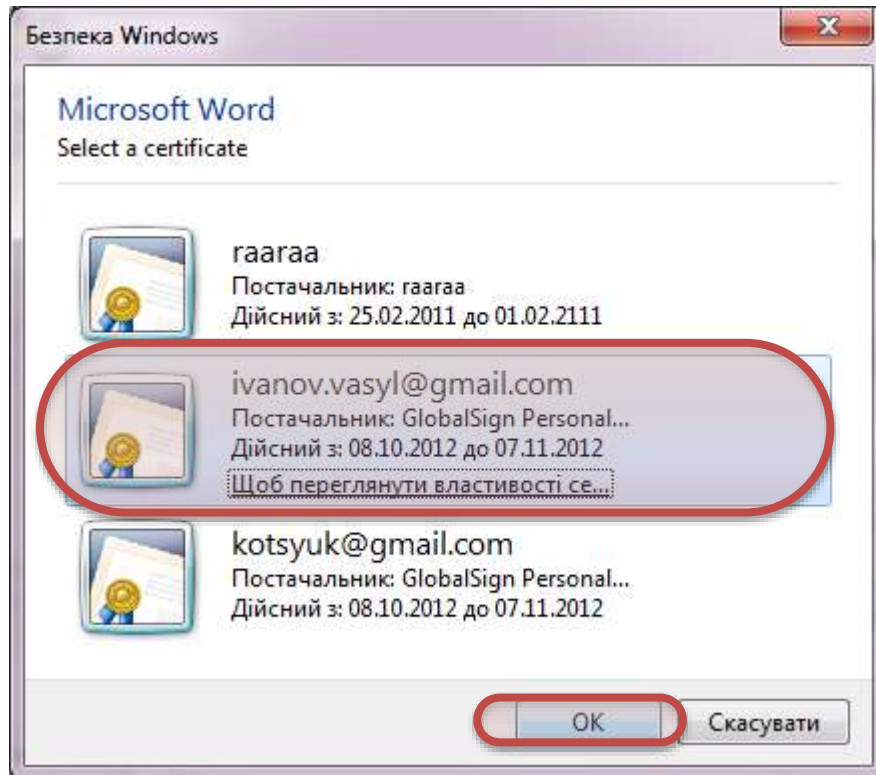


Рис. 65 Вибір сертифікату

6. Натисніть кнопку «Sign», для накладання підпису (Рис. 66).

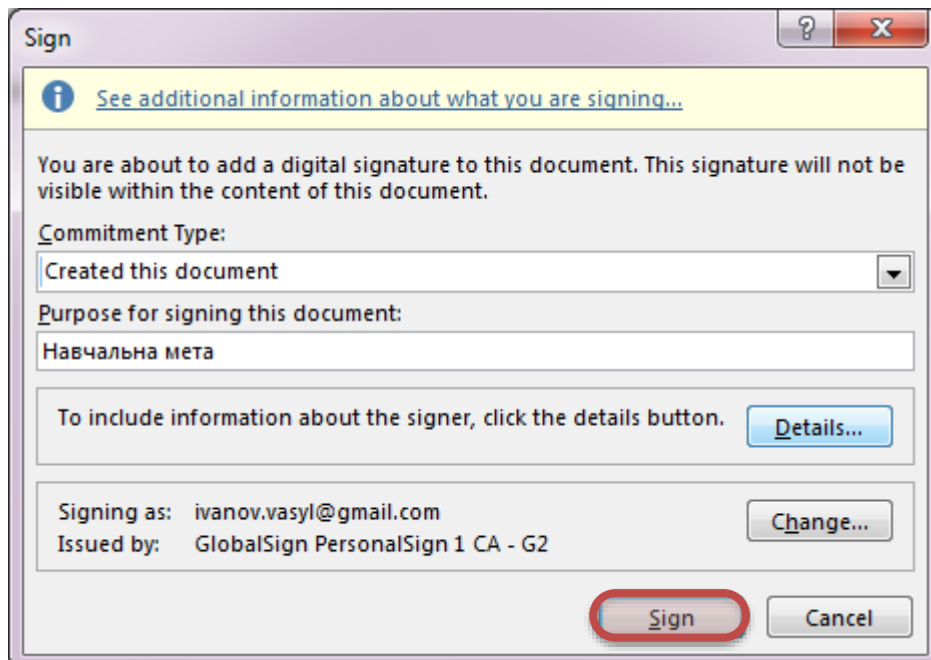


Рис. 66 Накладання підпису

7. Надіть дозвіл на використання таємного ключа та підтвердіть свій вибір паролем (Рис. 67).

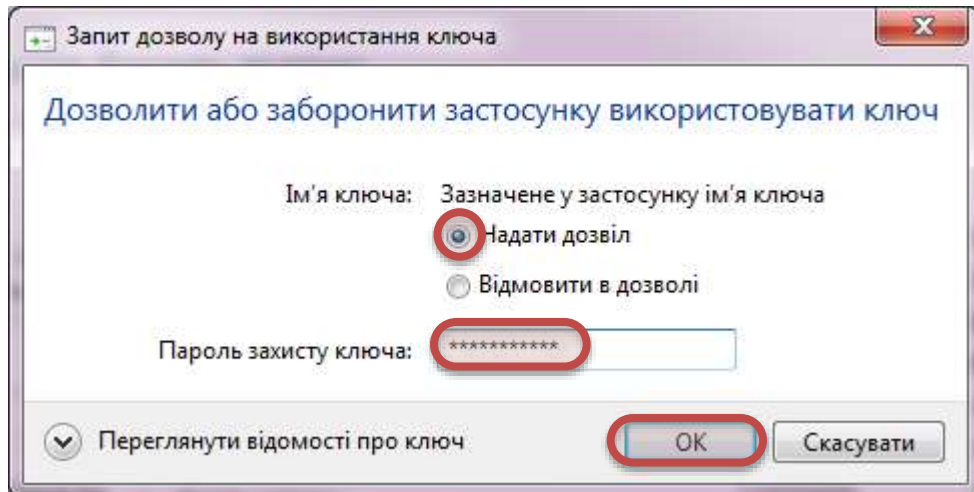


Рис. 67 Пароль доступу до закритого ключа

8. У повідомленні про успішне накладання підпису просто натисніть «ОК» (Рис. 68).



Рис. 68 Підтвердження успішності накладання підпису

9. В результаті операції підписування з'явиться позначка «Signed Document» (Рис. 69). Для перегляду підпису слід клацнути кнопку «View Signatures».

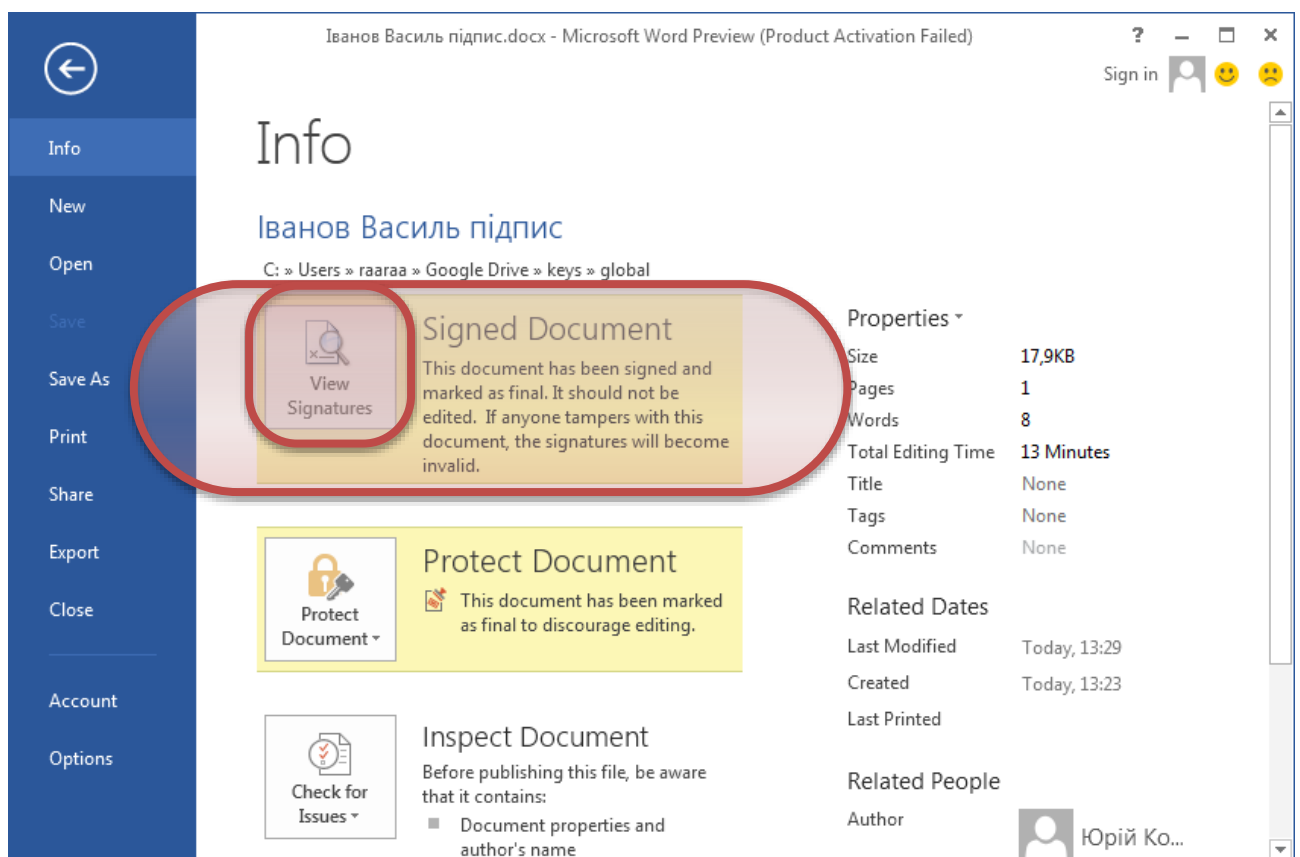


Рис. 69 Позначка про підпис документа

10. На завершальному рисунку показано як можна переглянути підпис (Рис. 70).

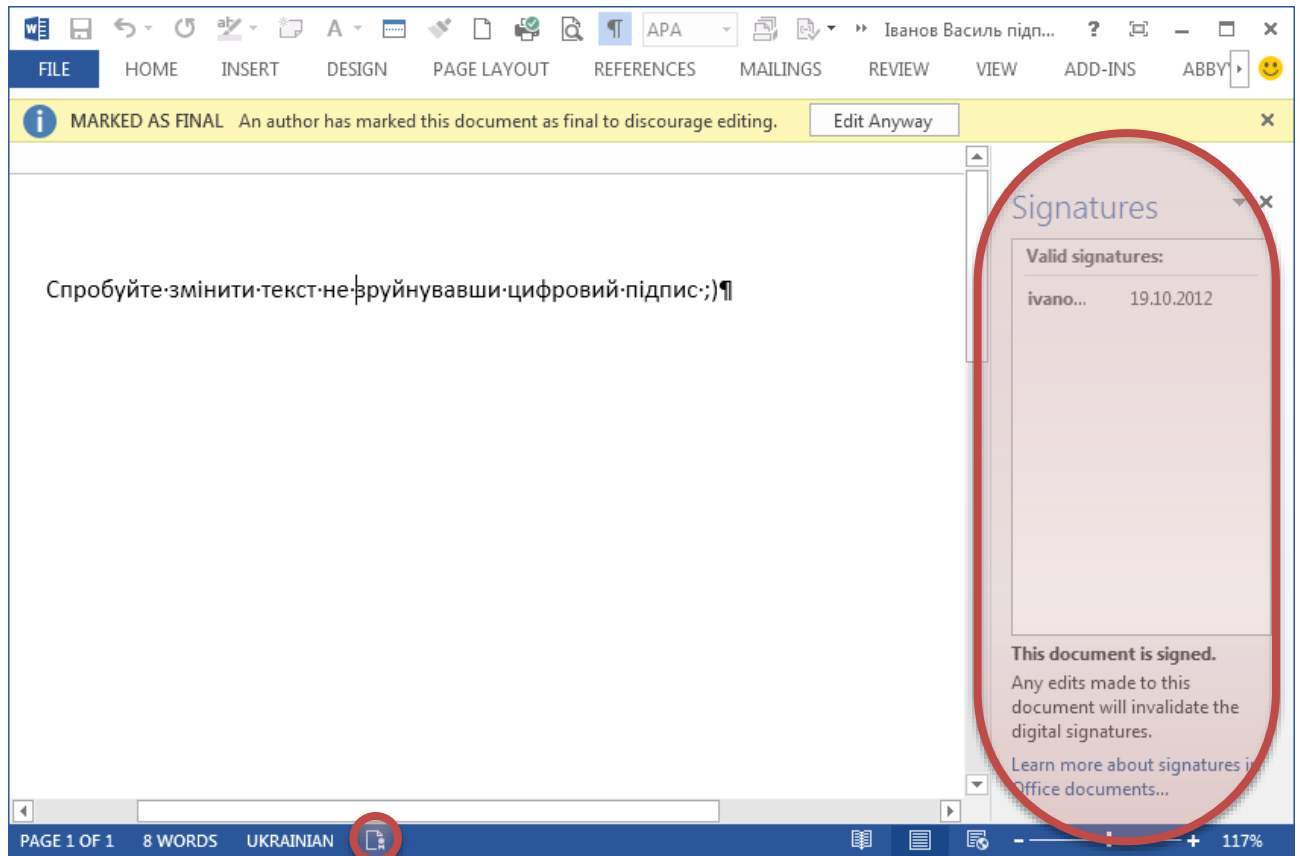


Рис. 70 Перегляд підпису

Підпис документів MS Word 2010

1. Відкрийте підготований документ MS Word у текстовому процесорі MS Word (Рис. 71).

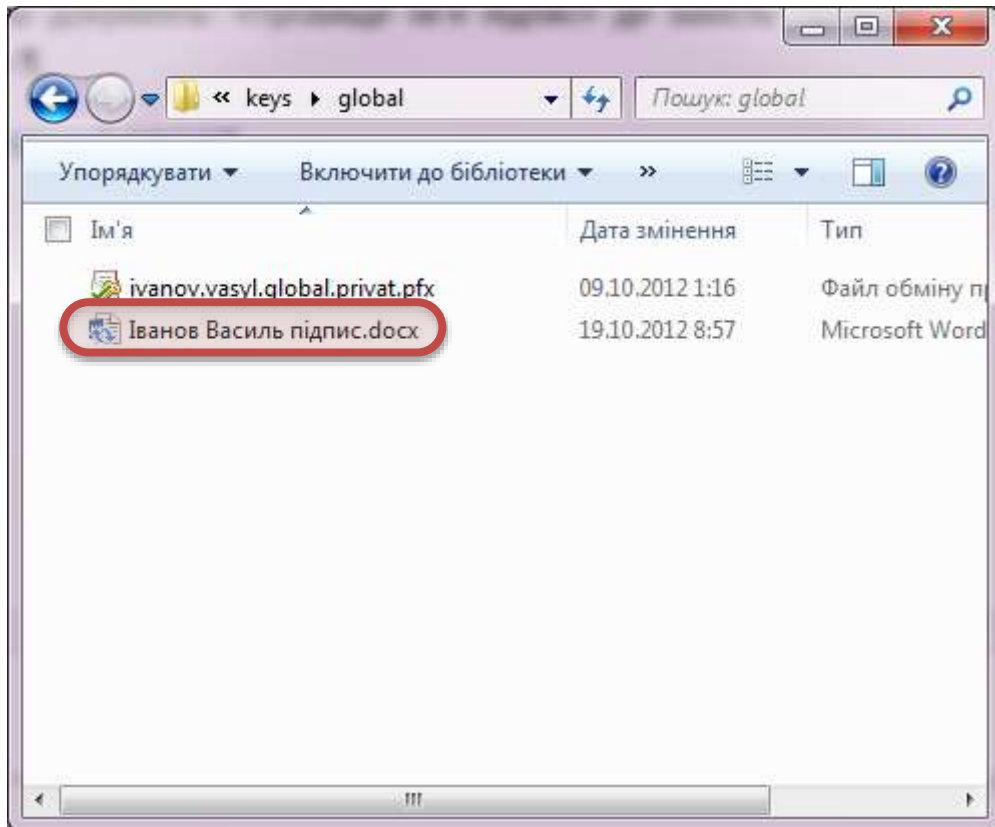


Рис. 71 Документ MS Word у папці

2. Перейдіть у меню «Файл» для накладання електронного цифрового підпису (Рис. 72).

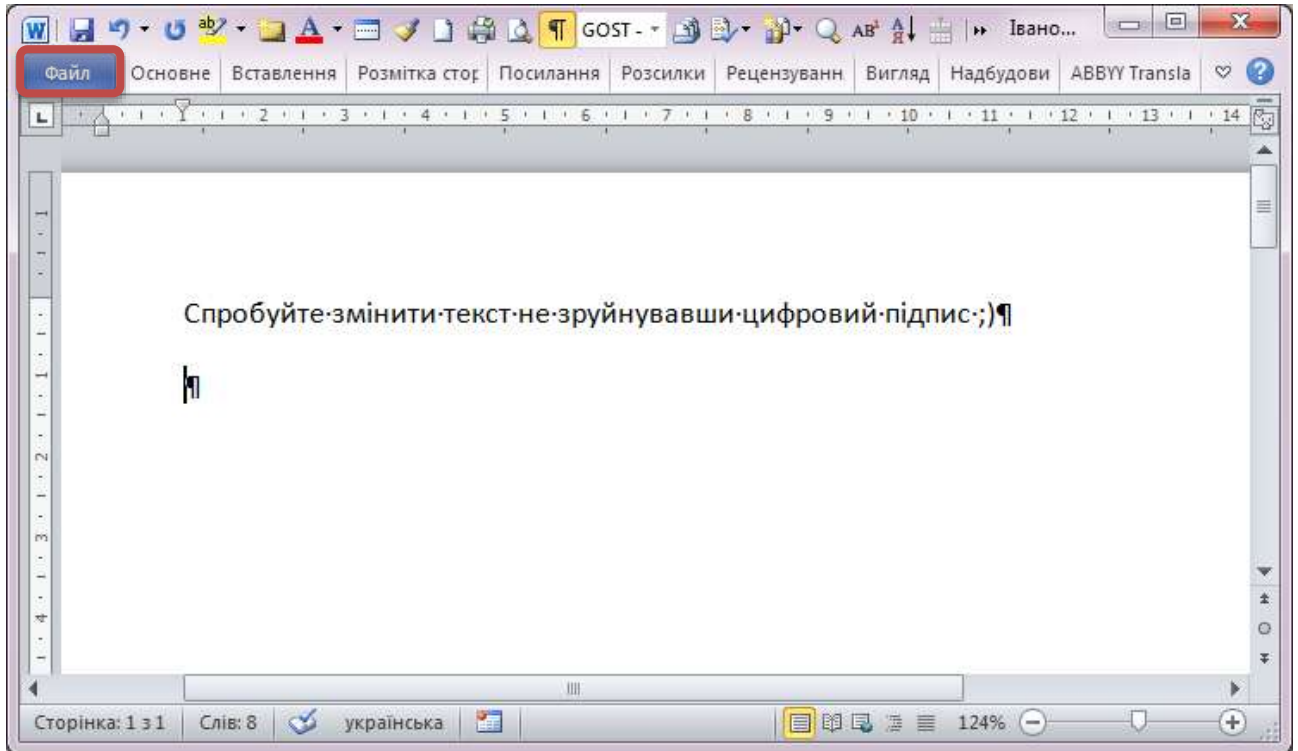


Рис. 72 Відкриття меню файл

3. У розділі «Відомості» скористайтеся кнопкою «Установити захист» та виберіть можливість «Додати цифровий підпис» (Рис. 73).

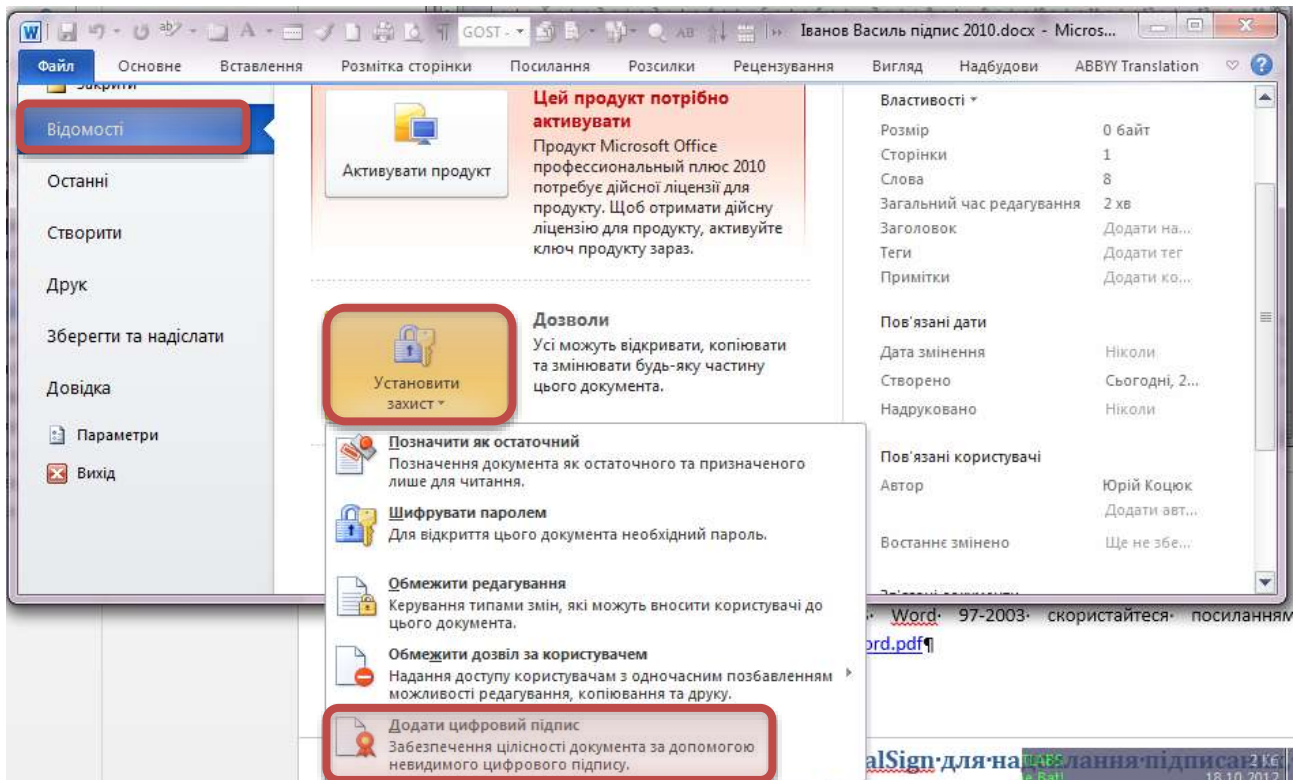


Рис. 73 Меню додавання цифрового підпису

4. Встановіть причину підпису та натисніть кнопку «Змінення...», для того, щоб вибрати серед існуючих сертифікатів свій¹ (Рис. 74).

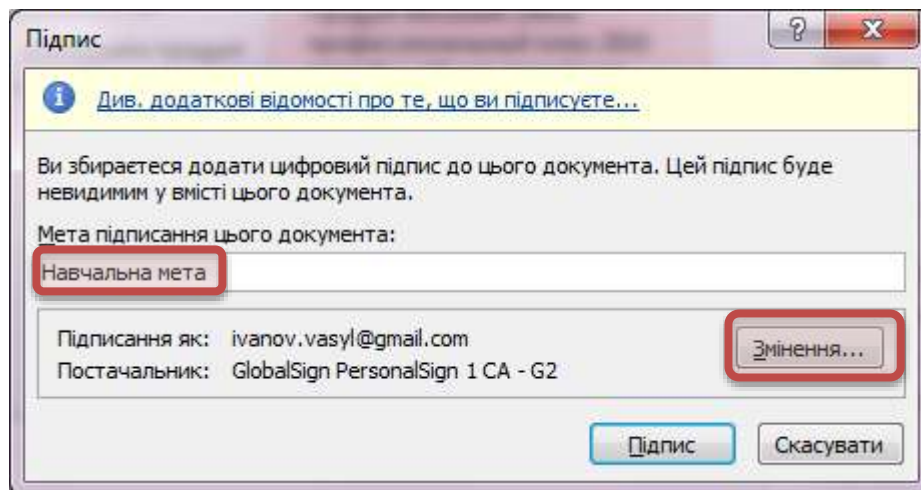


Рис. 74 Встановлення причини підпису

5. Серед існуючих сертифікатів виберіть свій сертифікат від Globalsign та натисніть кнопку «ОК» (Рис. 75).

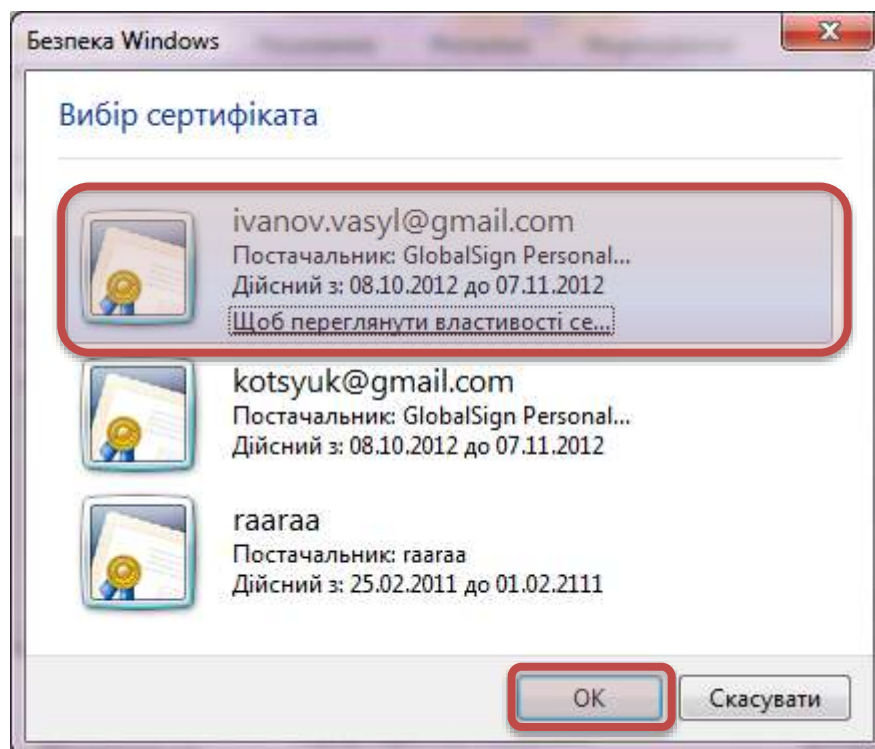


Рис. 75 Перелік існуючих сертифікатів

¹ Перш ніж виконувати накладання цифрового підпису в документі MS Word, слід здійснити [імпорт сертифікату в Internet Explorer](#).

6. Натисніть кнопку «Підпис» для початку процесу накладання Вашого підпису (Рис. 76).

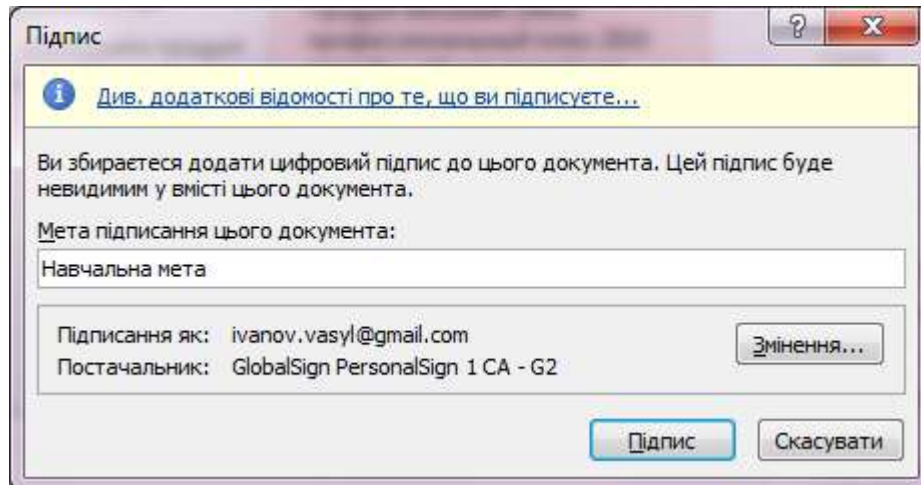


Рис. 76 Підпис

7. Надайте дозвіл на використання таємного ключа та підтвердіть свій вибір паролем (Рис. 77).

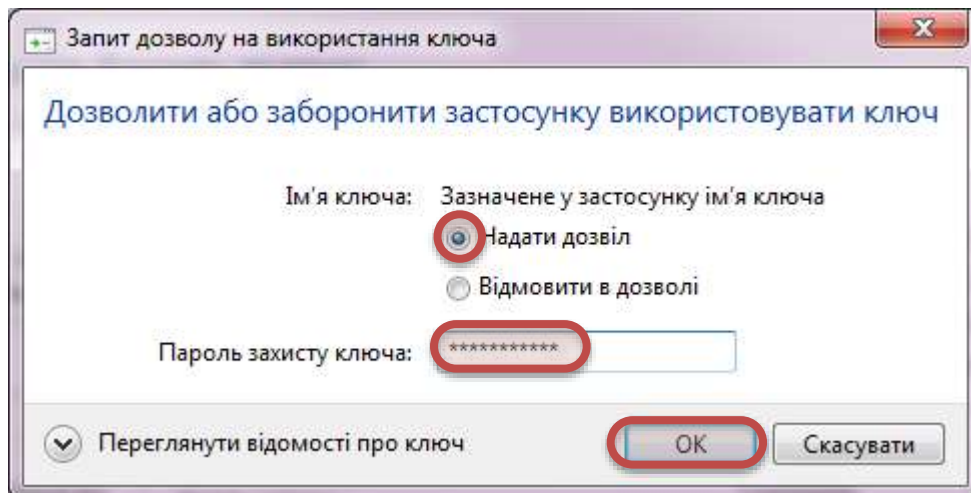


Рис. 77 Пароль доступу до закритого ключа

8. У повідомленні про успішне накладання підпису просто натисніть «ОК» (Рис. 78).



Рис. 78 Підтвердження успішності накладання підпису

9. В результаті операції підписування з'явиться позначка «Підписаний документ» (Рис. 79). Для перегляду підпису слід клацнути кнопку «Перегляд підписів».

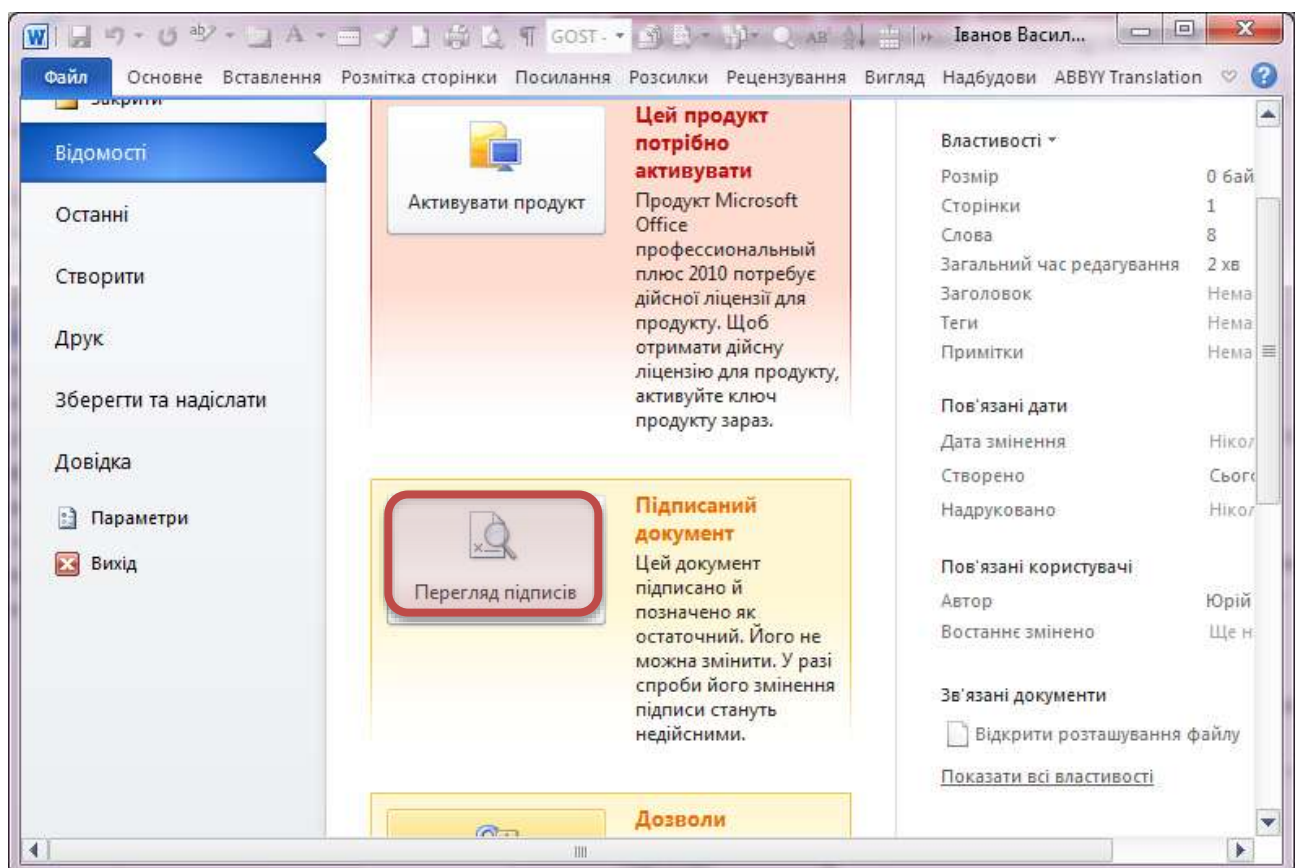


Рис. 79 Ініціація перегляду підпису

10. На завершальному рисунку показано як можна переглянути підпис (Рис. 80).

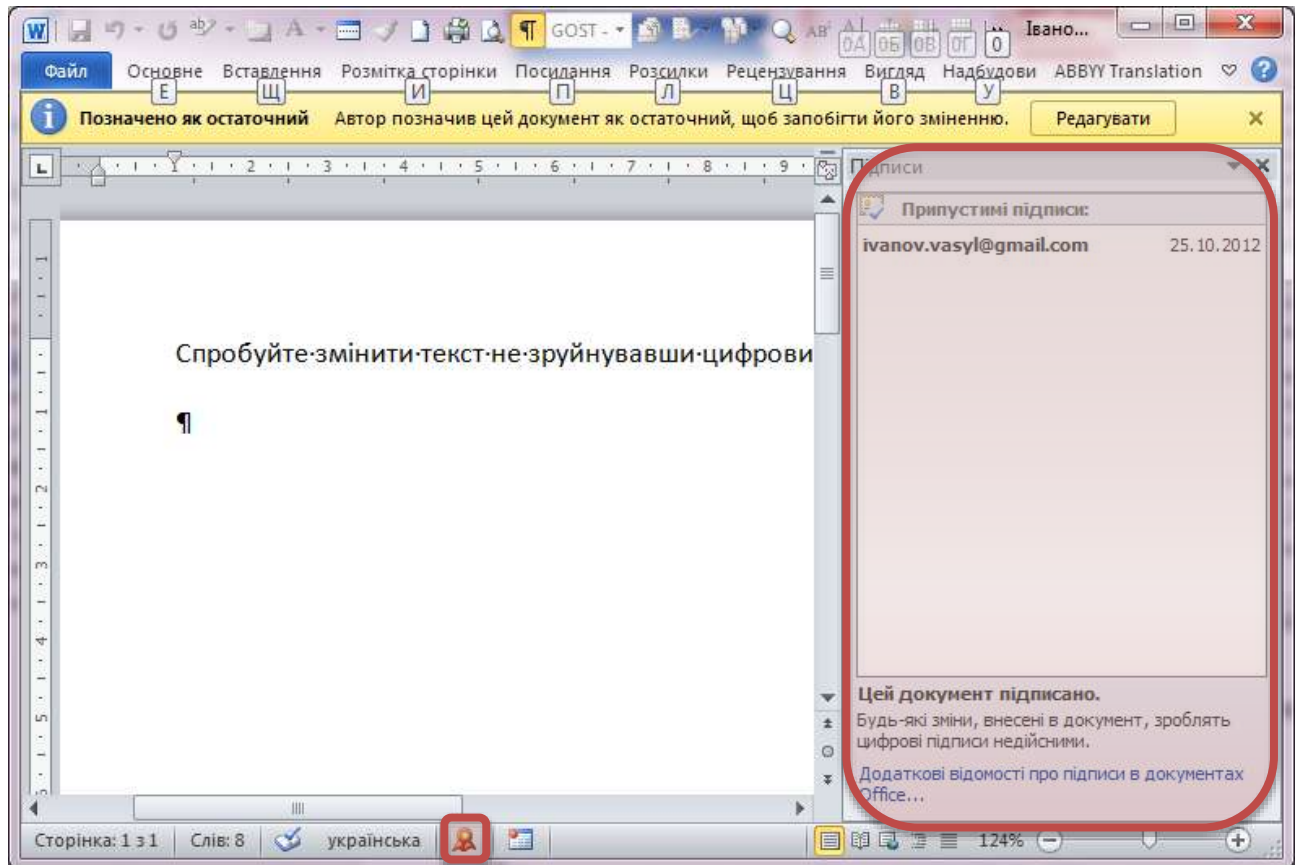


Рис. 80 Перегляд підпису

Підпис документів MS Word 97-2003

Для довідки щодо підпису документів MS Word 97-2003 скористайтеся посиланням: <http://www.acsk.uss.gov.ua/download/manual/MSWord.pdf>, або ж виконайте послідовність кроків у вигляді графічних зображень¹.

1. Відкрийте заздалегідь підготований документ MS Word (Рис. 81).

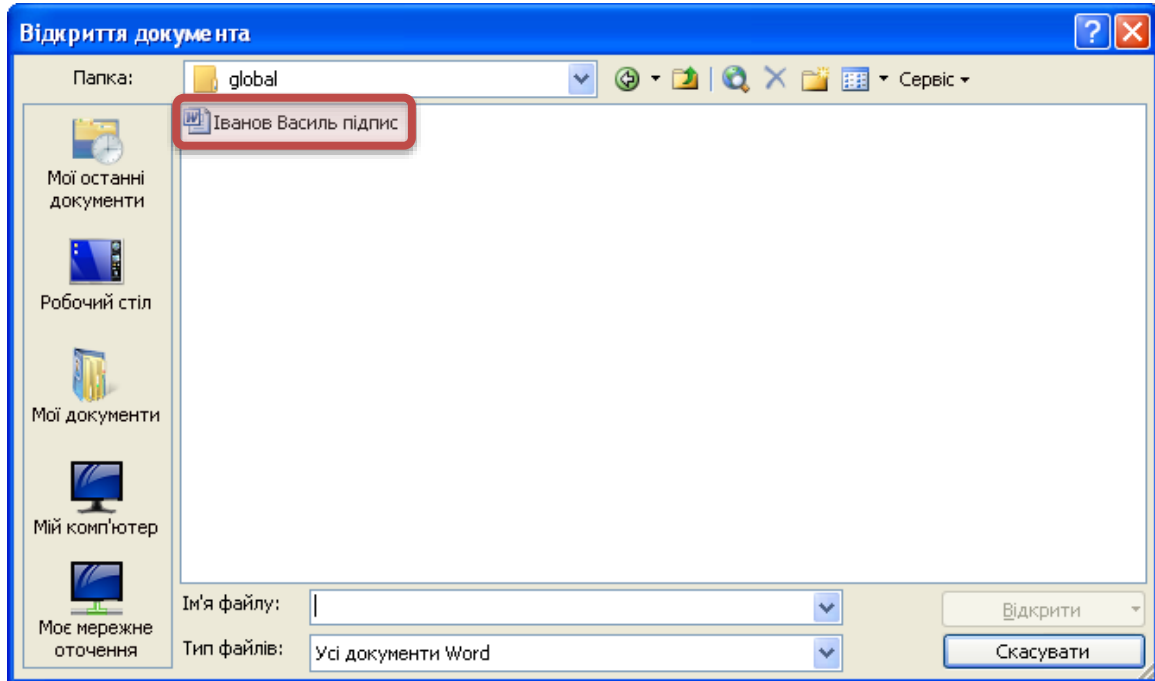


Рис. 81 Відкриття документа для підпису

¹ Увага, в залежності від версії операційної системи чи версії MS Office послідовність кроків може незначно відрізнятися

2. Скористайтесь меню «Сервіс», та виберіть підменю «Параметри» (Рис. 82).

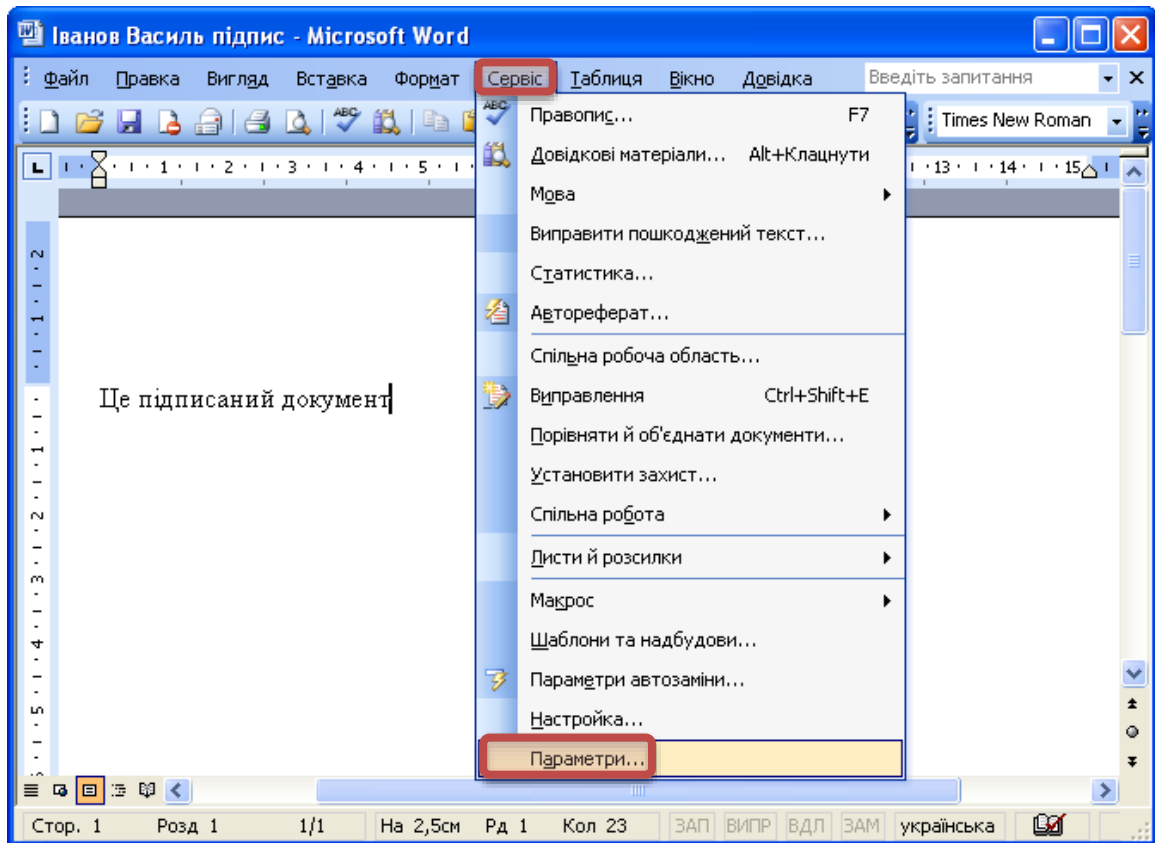


Рис. 82 Відкриття меню "Параметри"

- У діалоговому вікні «**Параметри**» виберіть вкладку «**Безпека**», і натисніть кнопку «**Цифрові підписи...**» (Рис. 83).

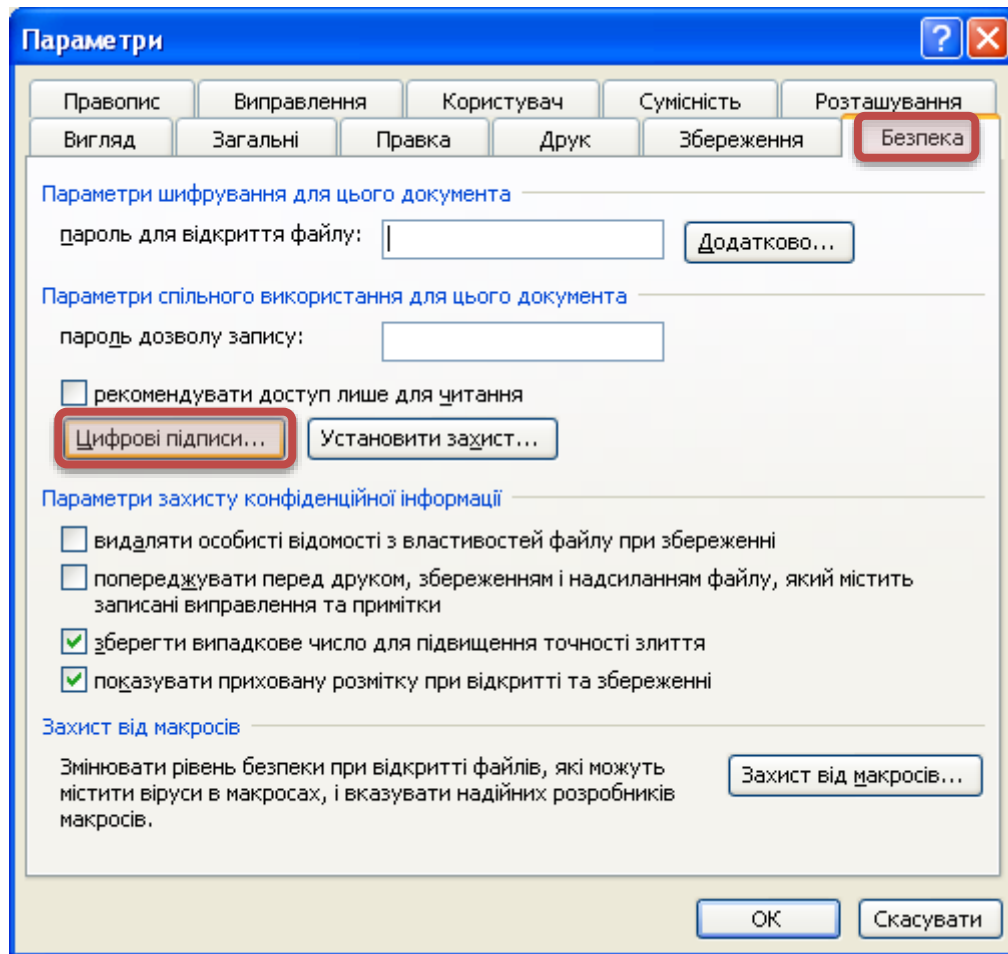


Рис. 83 Доступ до кнопки "Цифрові підписи..."

- Для того, щоб додати Ваш підпис до цифрових підписів документа у діалоговому вікні «Цифровий підпис» вкладки «Підписи» натисніть кнопку «Додати...» (Рис. 84).

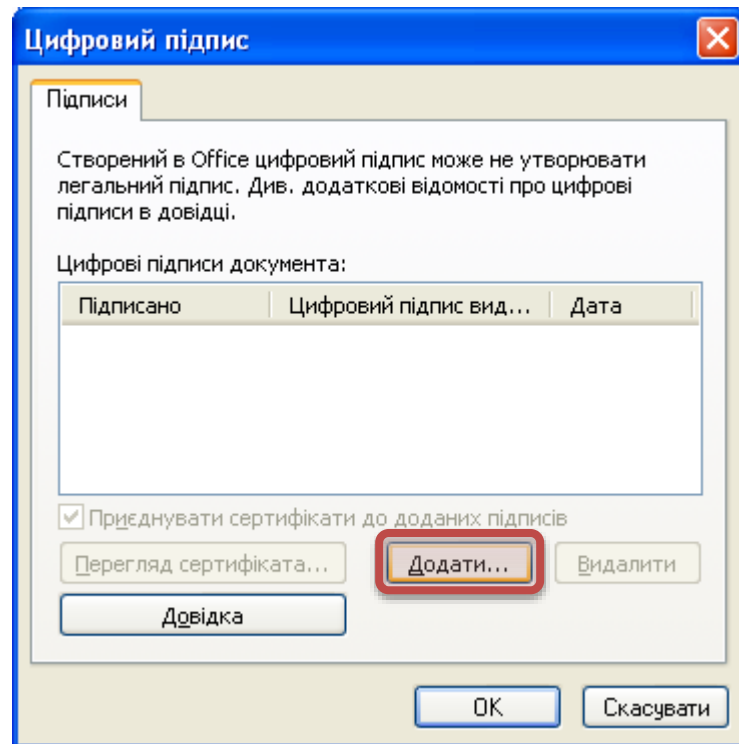


Рис. 84 Додавання цифрового підпису

- У діалоговому вікні «**Select Certificate**» виберіть власний сертифікат¹ та натисніть кнопку «ОК» (Рис. 85).

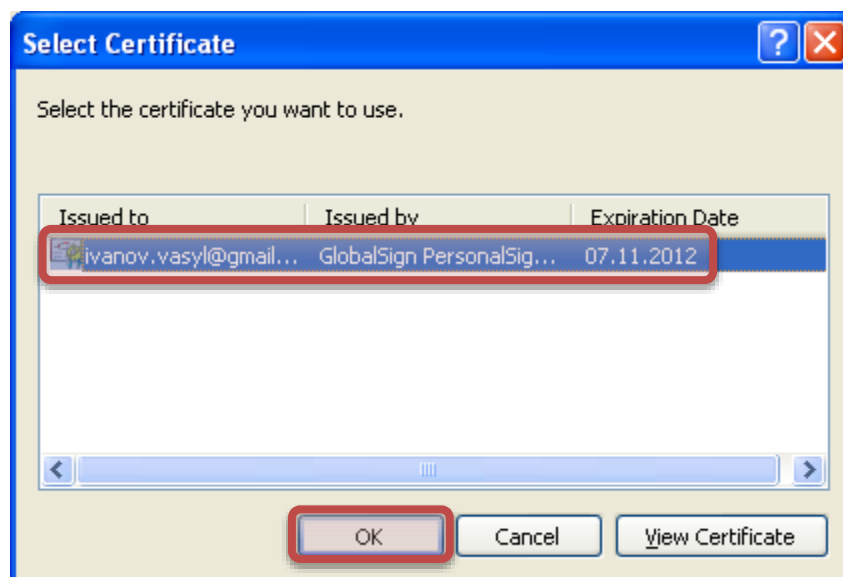


Рис. 85 Вибір сертифікату

¹ Якщо серед переліку сертифікатів Вашого сертифікату немає, Вам потрібно повторно [здійснити імпорт сертифікату в Internet Explorer](#).

6. У наступному діалоговому вікні слід ввести пароль, яким було захищено Ваш приватний ключ на етапі імпорту та натиснути кнопку «**OK**». Не слід ставити прапорець «**Remember password**», інакше накладати підпис від Вашого імені зможе будь-хто, хто працюватиме за цим же комп'ютером.



Рис. 86 Підпис даних Вашим приватним ключем

7. Для того щоб накласти підпис натисніть кнопку «**OK**» (Рис. 87).

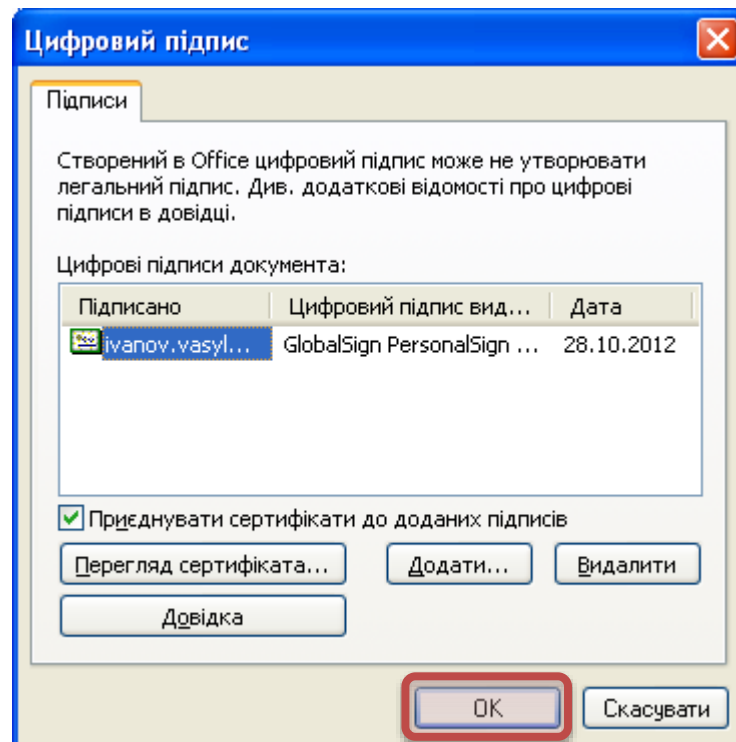


Рис. 87 Цифровий підпис

8. Для того щоб закрити діалогове вікно «**Параметри**» натисніть кнопку «**ОК**» (Рис. 88).

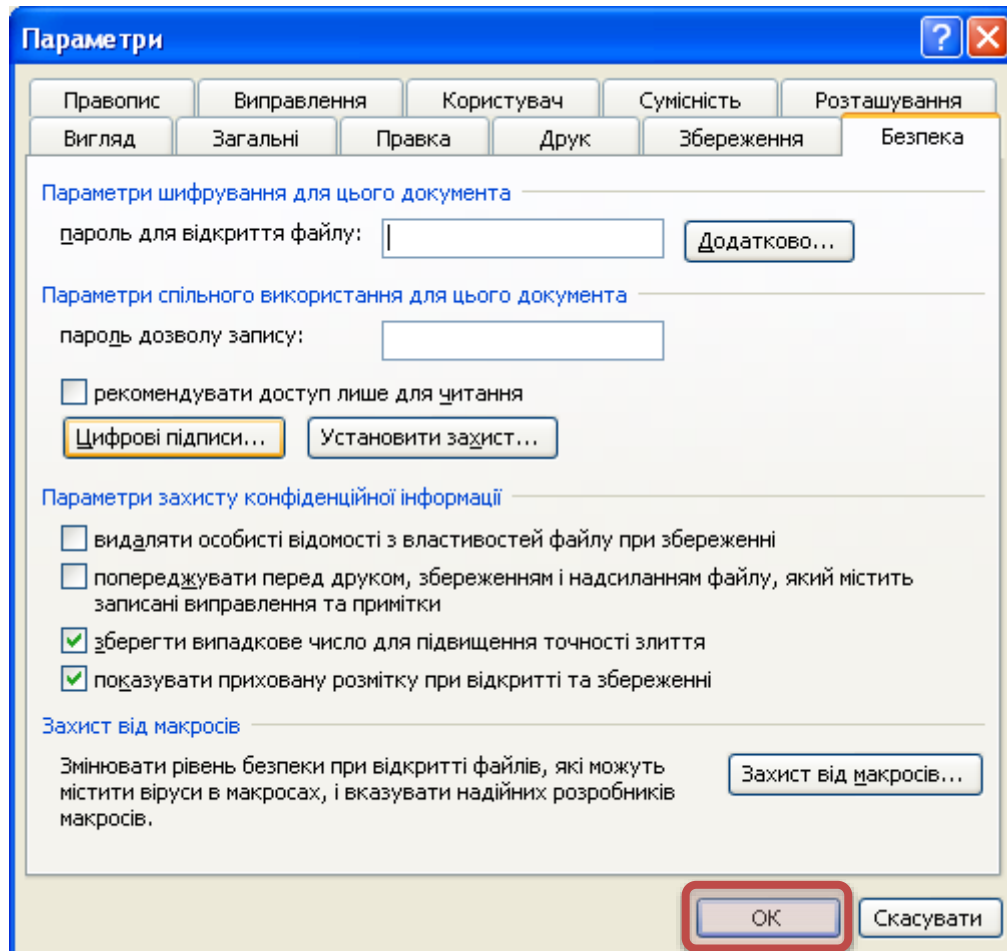


Рис. 88 Діалогове вікно "Параметри"

9. Дійсний електронний цифровий підпис буде відображено на інформаційній панелі підписаного документа MS Word (Рис. 89). Для того, щоб перевірити справжність сертифікату зробіть на ньому подвійний клік.

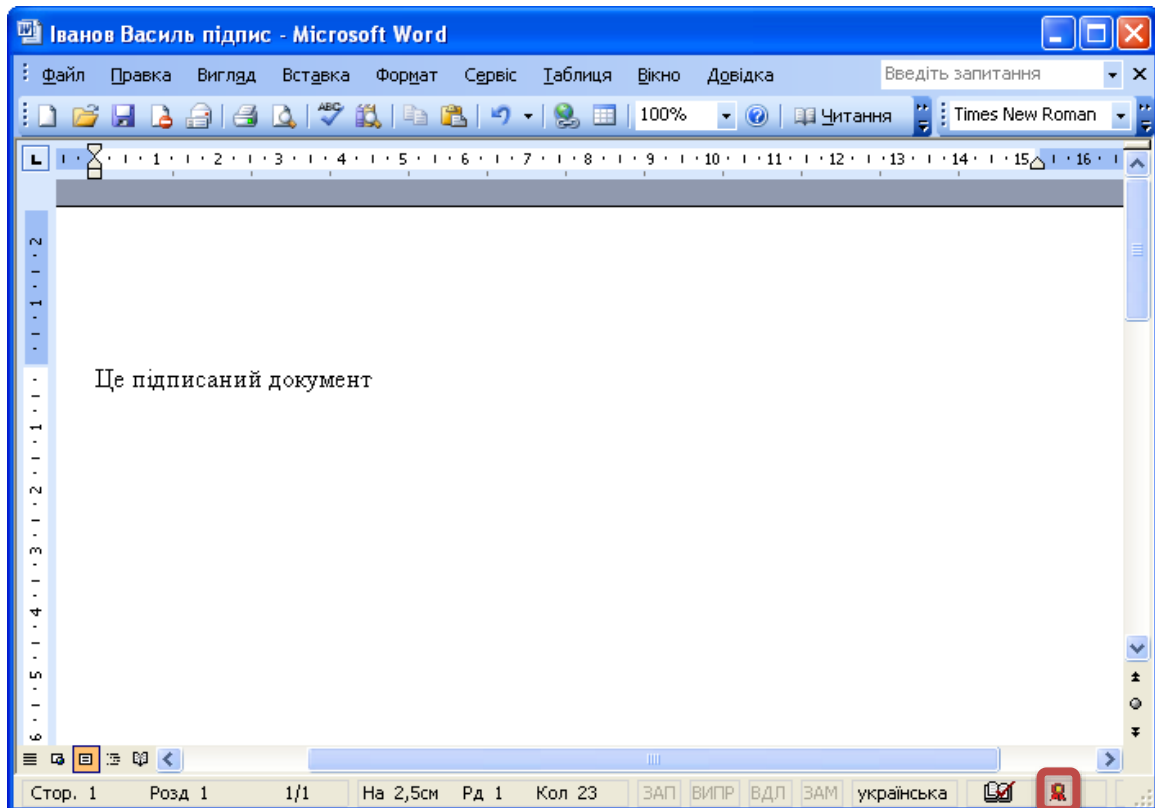


Рис. 89 Значок відображення цифрового підпису

10. Для перегляду сертифікату у діалоговому вікні «**Цифровий підпис**» виберіть сертифікат, який потрібно перевірити та натисніть кнопку «**Перегляд сертифікати...**» (Рис. 90).

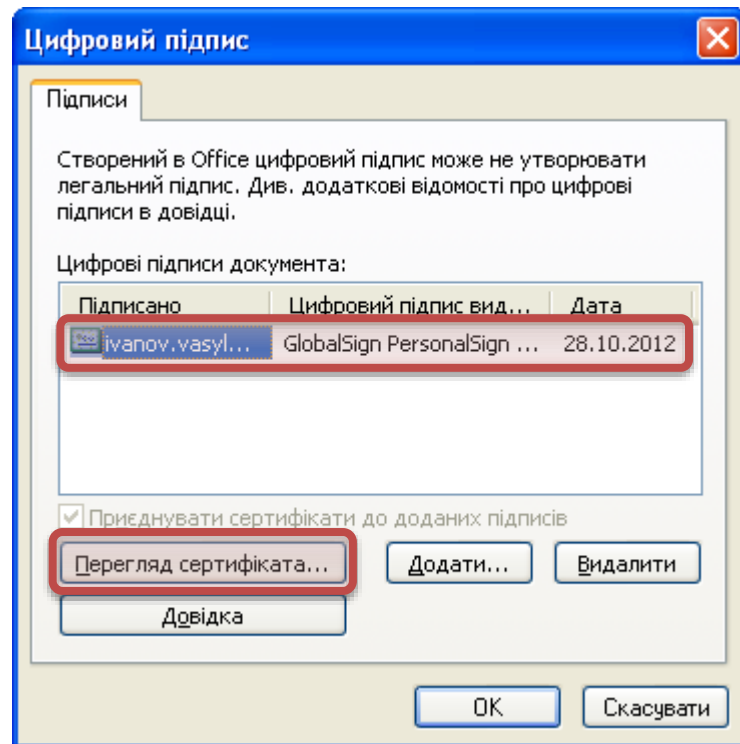


Рис. 90 Перегляд сертифікату

11. У вкладці «**General**» діалогового вікна «**Certificate**» можна проглянути загальну інформацію про сертифікат, а перейшовши у вкладку «**Certification Path**» – переглянути повний шлях сертифікації та справжність сертифікатів (Рис. 91).



Рис. 91 Загальна інформація про сертифікат

12. Після перевірки справжності сертифікату натисніть кнопку «**OK**» (Рис. 92).

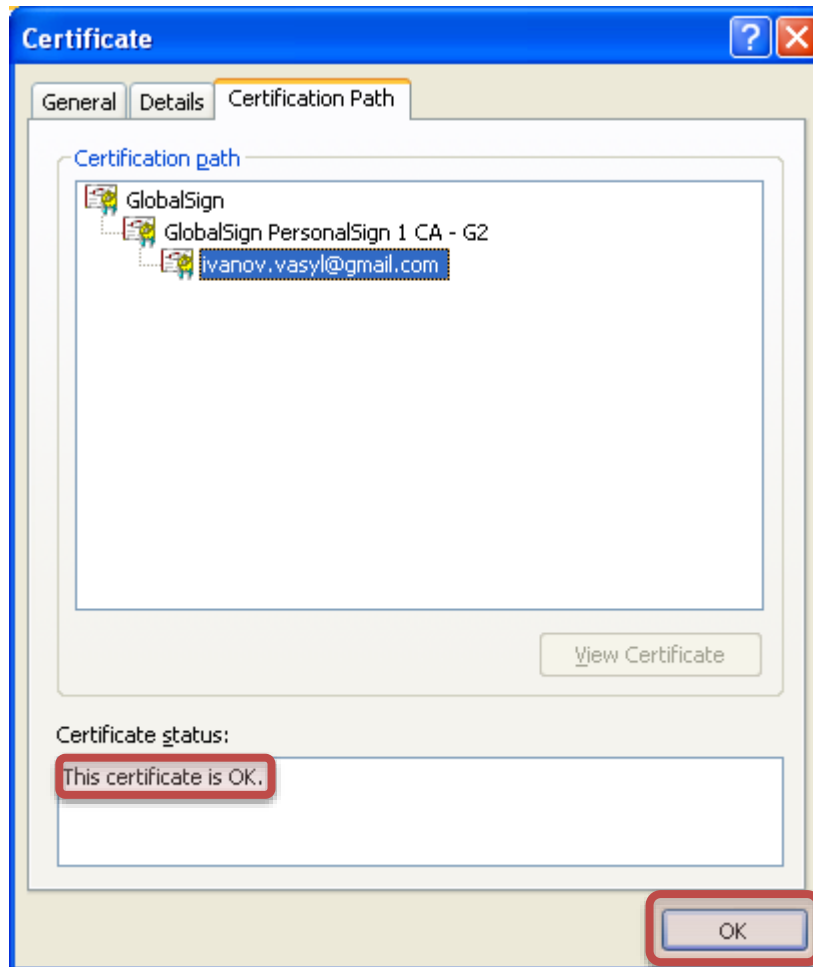


Рис. 92 Вкладка "Шлях сертифікації"

Використання сертифікату від Globalsign для надсилання підписаних, зашифрованих, підписаних/зашифрованих листів з допомогою The Bat

Підписування листів сертифікатом від Globalsign

Для підписання листа у The Bat з використанням сертифікату від Globalsign слід виконати низку ілюстрованих кроків¹:

1. Скористайтесь кнопкою на кнопочній панелі інструментів для надсилання листа, або ж меню Лист/Створити (Рис. 93).

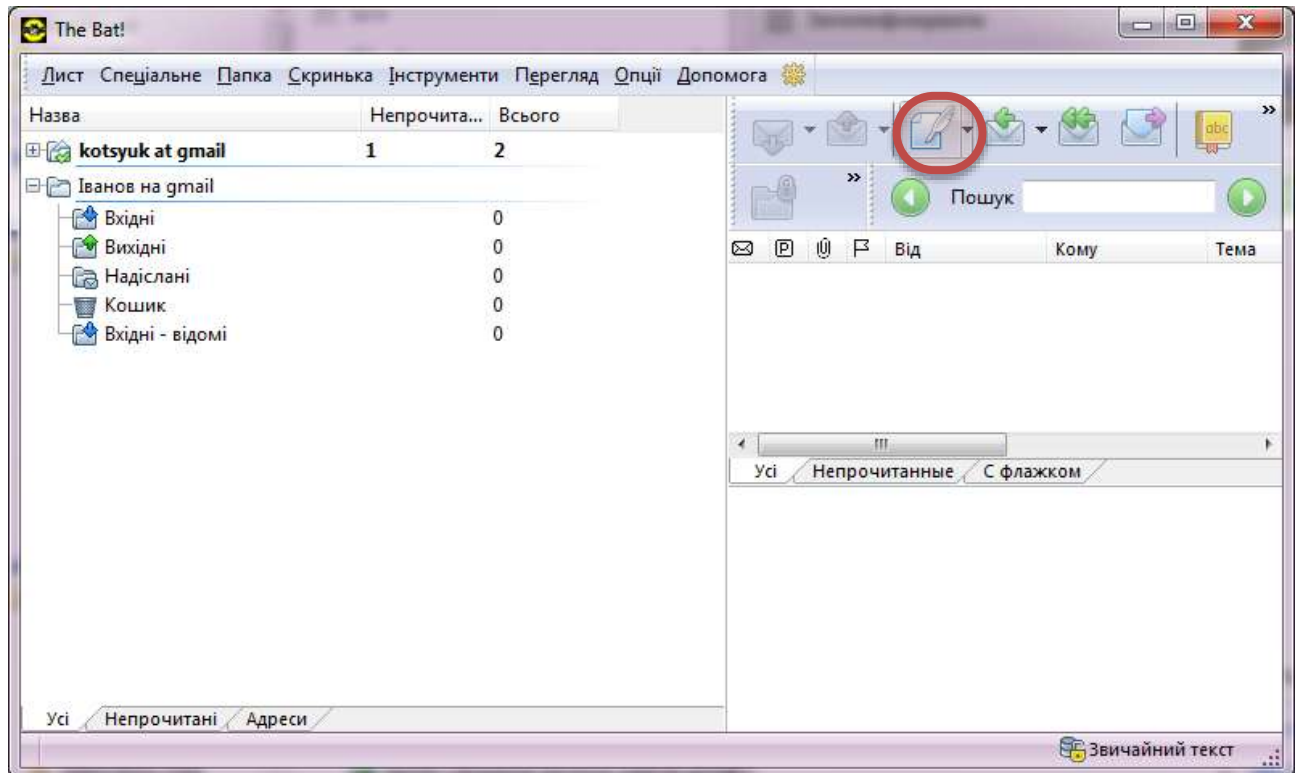


Рис. 93 Кнопка надсилання листа

¹ Для реалізації накладання підпису потрібно [імпортувати у The Bat сертифікат з особистим ключем від Globalsign](#)

- Для того, щоб накласти електронний цифровий підпис слід в меню «Конфіденційність» активувати можливість «Дозволити S/MIME» та «Підписати по закінченню» (Рис. 94).

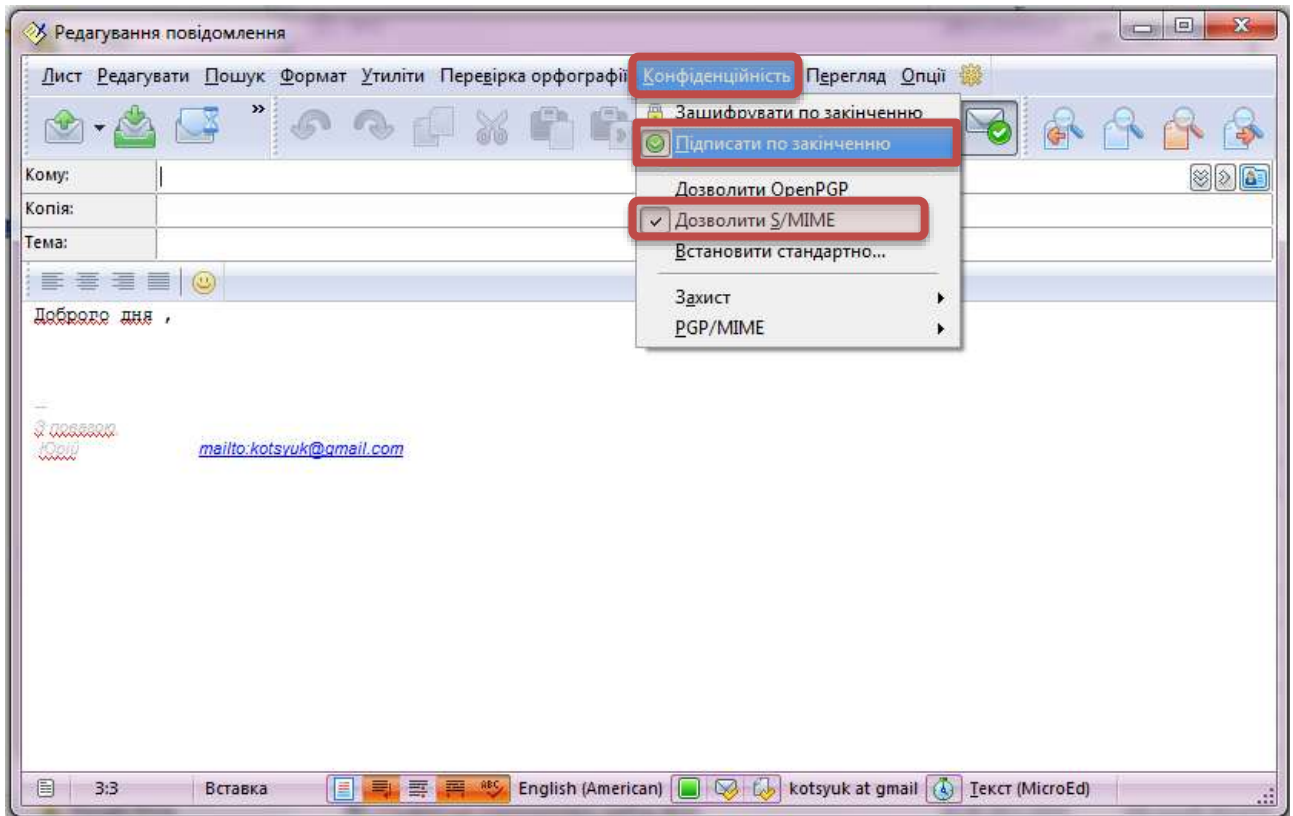


Рис. 94 Накладання підпису

3. Вкажіть одержувача¹ повідомлення, тему, як вказано на рисунку та, власне, тіло повідомлення (Рис. 95).
 - a. Ще раз перевірте чи накладатиметься у Вас підпис.
 - b. Після перевірки натисніть кнопку «Розмістити повідомлення у вихідних», це дасть можливість ще раз перевірити підпис перед відправкою.

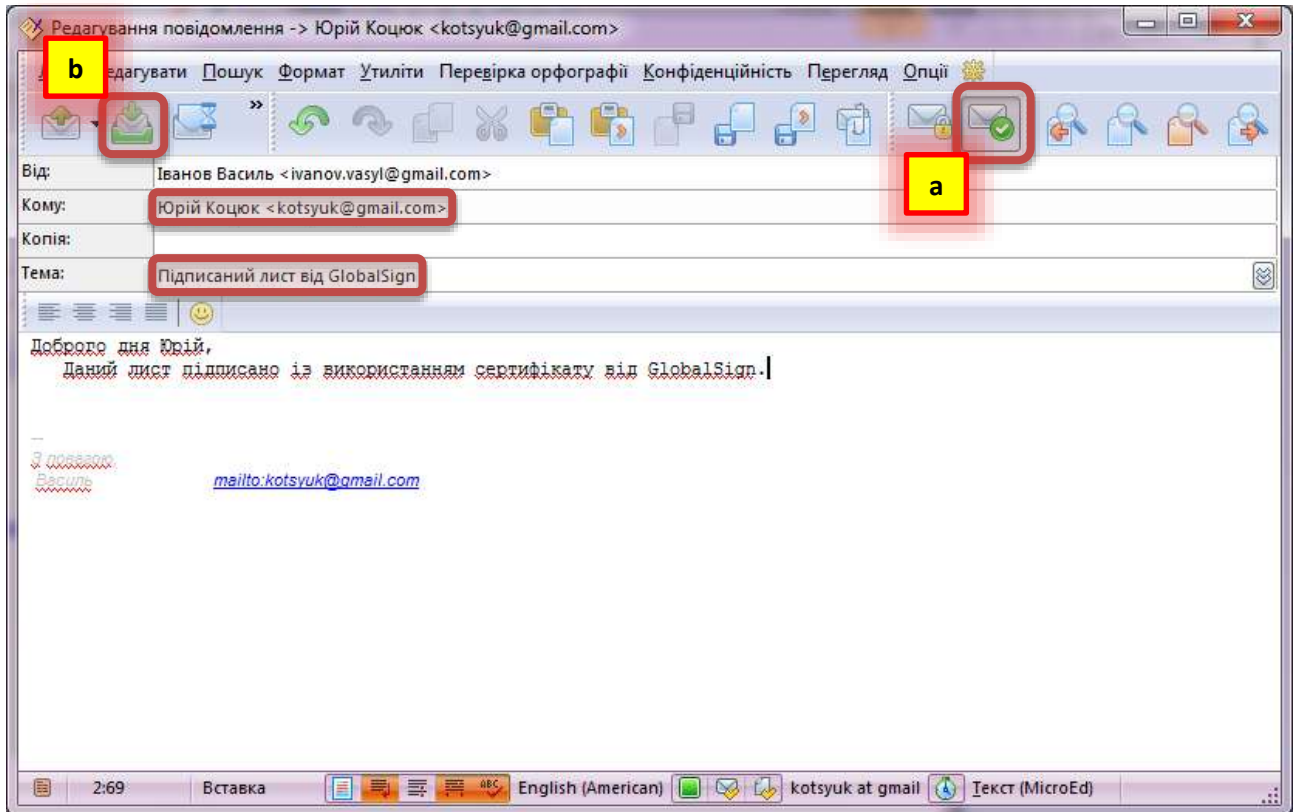


Рис. 95 Вказання одержувача

¹ В якості одержувача виберіть односторонника/партнера, який також надішле Вам підписаний лист. Рекомендується вибрати більше ніж одного партнера. Якщо партнера вибрати не вдається слід звернутися за допомогою до старости групи.

4. Серед існуючих ключів виберіть ключ від Globalsign¹ (Рис. 96) та натисніть кнопку «Так».

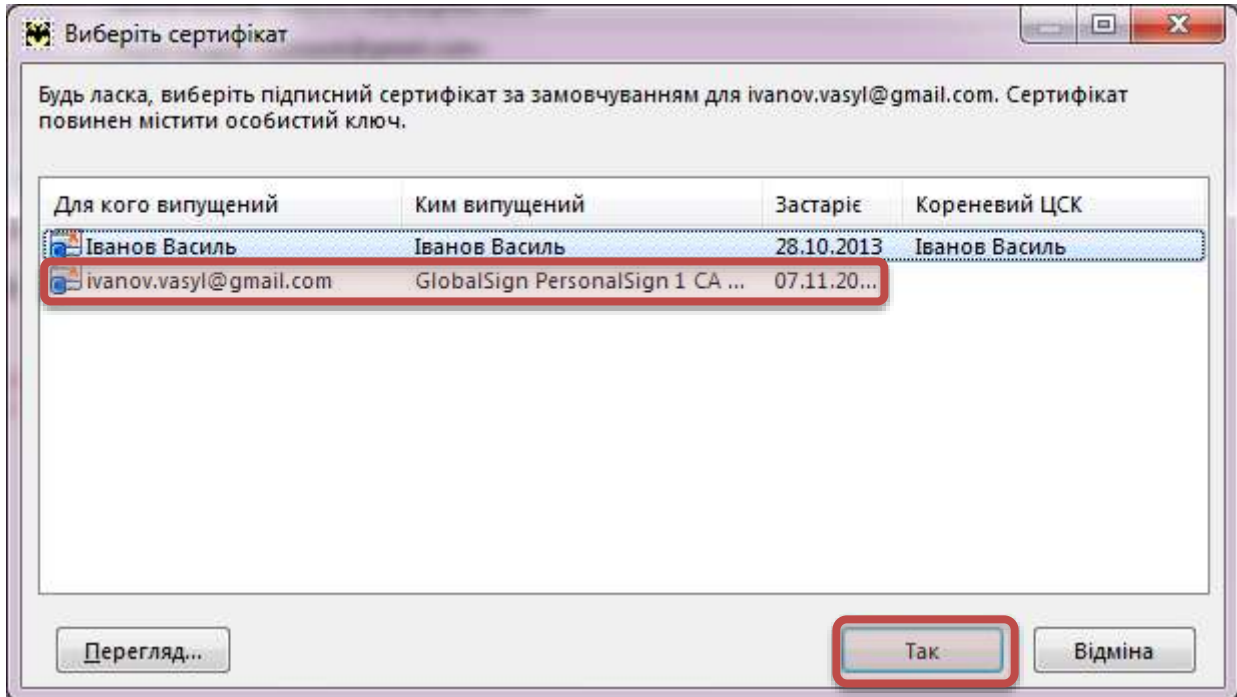


Рис. 96 Вибір сертифікату для підпису

5. Введіть пароль доступу до приватного ключа від Globalsign, та натисніть кнопку «Так» (Рис. 97)

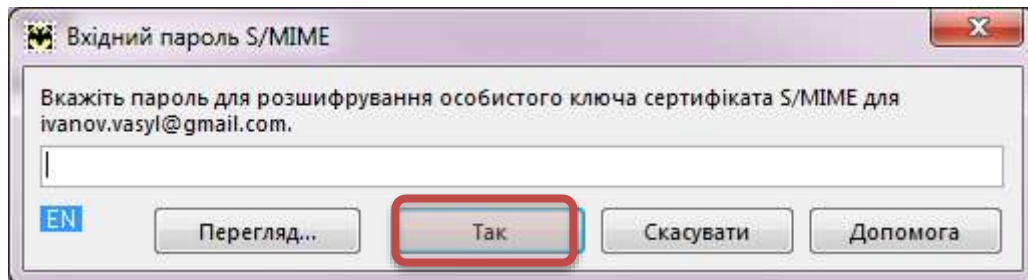


Рис. 97 Пароль приватного ключа від Globalsign

¹ Якщо у Вас більше одного сертифікату, то перед цією операцією слід виконати операцію [скидання підписів](#).

6. У папці «Вихідні» з'явиться готовий до відправки лист (Рис. 98).
 - a. Перейдіть у папку «Вихідні».
 - b. Виберіть підписаний лист.
 - c. Натисніть кнопку «Переглянути ДІЙСНІ підписи», щоб переконатися, що саме Ваш підпис накладено¹.

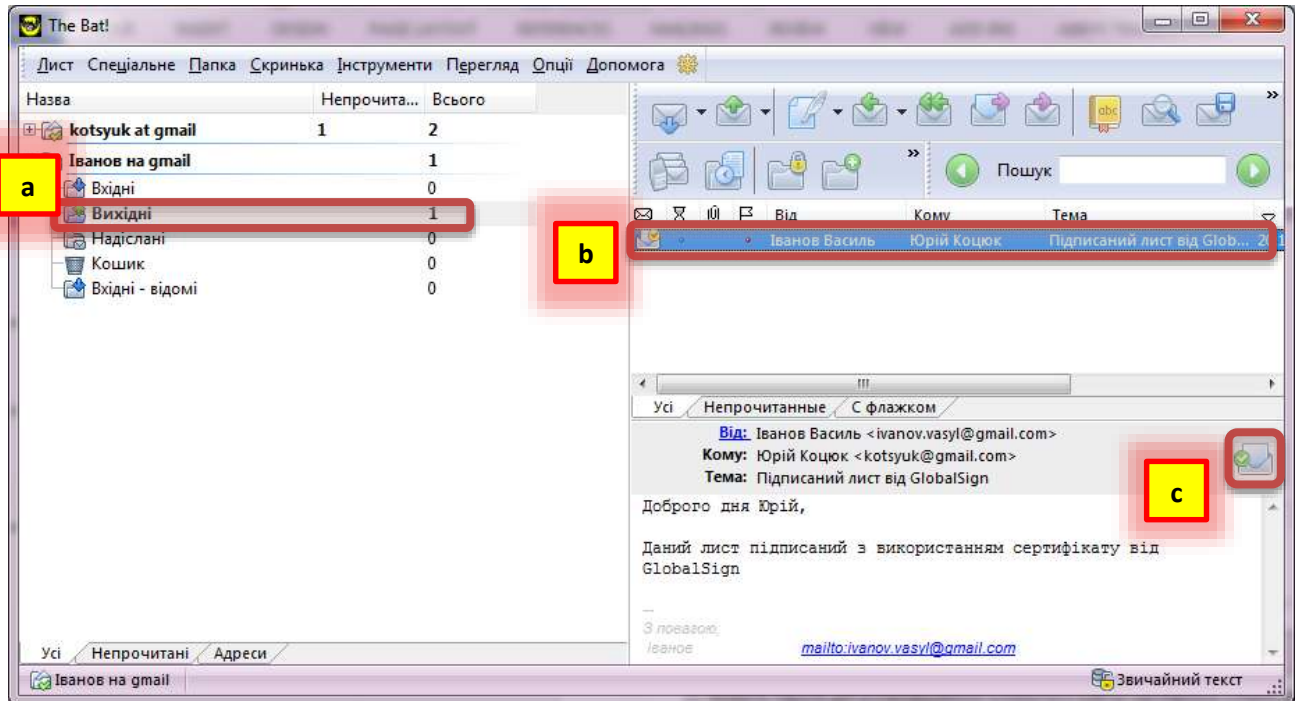


Рис. 98 Перевірка наявності підпису

¹ Якщо кнопки підпису немає, значить з якоїсь причини Вам не вдалося накласти підпис. Спробуйте повторити все з початку.

7. Переконайтеся, що використовується потрібний підпис та натисніть кнопку «Так» (Рис. 99).

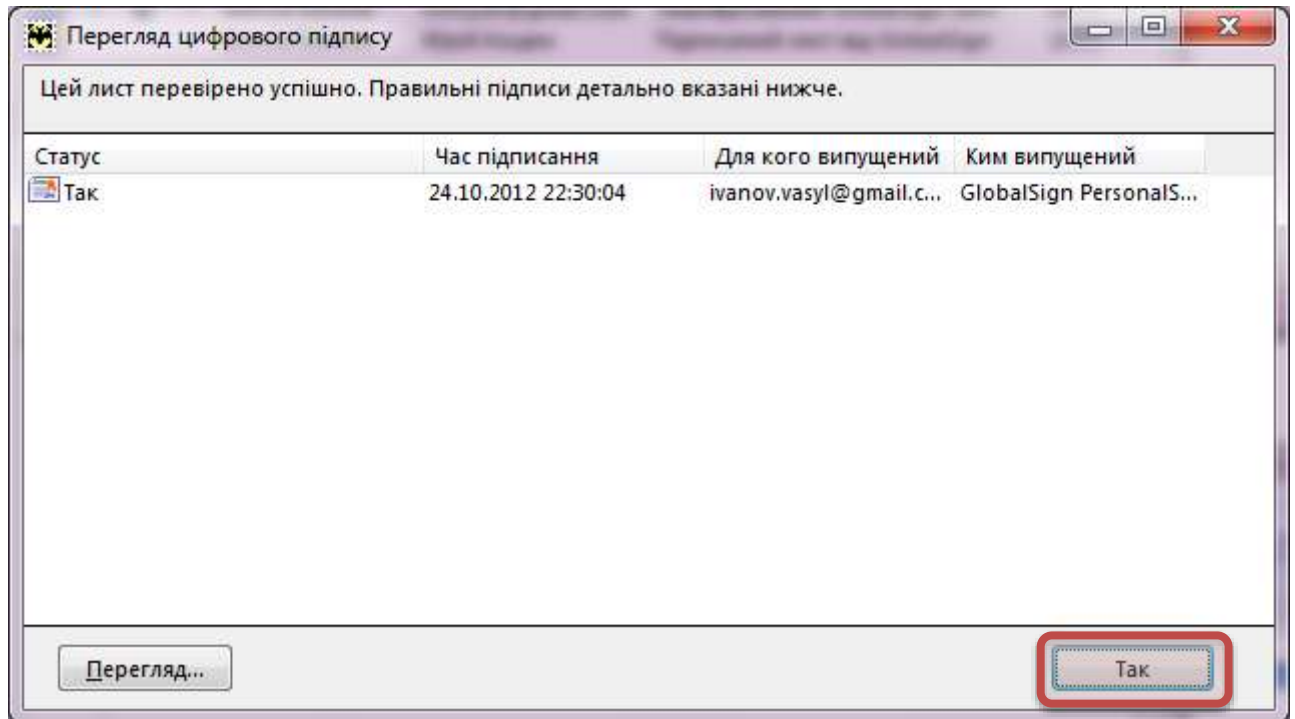


Рис. 99 Перегляд цифрового підпису

Шифрування листів із використанням сертифікату від Globalsign

Для здійснення шифрування листів із використанням сертифікату від Globalsign необхідно перш за все здійснити імпорт відповідного відкритого ключа в адресну книгу The Bat. Це можна здійснити кількома шляхами:

1. Безпосередній імпорт з використанням файлу експорту відкритого ключа.
2. Використання підписаного з використанням Globalsign однокорпусника¹ листа для здійснення операції імпорту в адресну книгу.

Так як перший спосіб використовувався в одному з попередніх завдань у даному прикладі буде продемонстрований другий спосіб, коли респонденти не можуть обмінятися ключами особисто.

¹ В якості одержувача виберіть однокорпусника/партнера, який також надішле Вам підписаний лист. Рекомендується вибрати більше ніж одного партнера. Якщо партнера вибрати не вдається слід звернутися за допомогою до старости групи.

Імпорт ключа в адресну книгу

1. Ініціюйте перевірку пошти на своїй поштовій скриньці (Рис. 100).

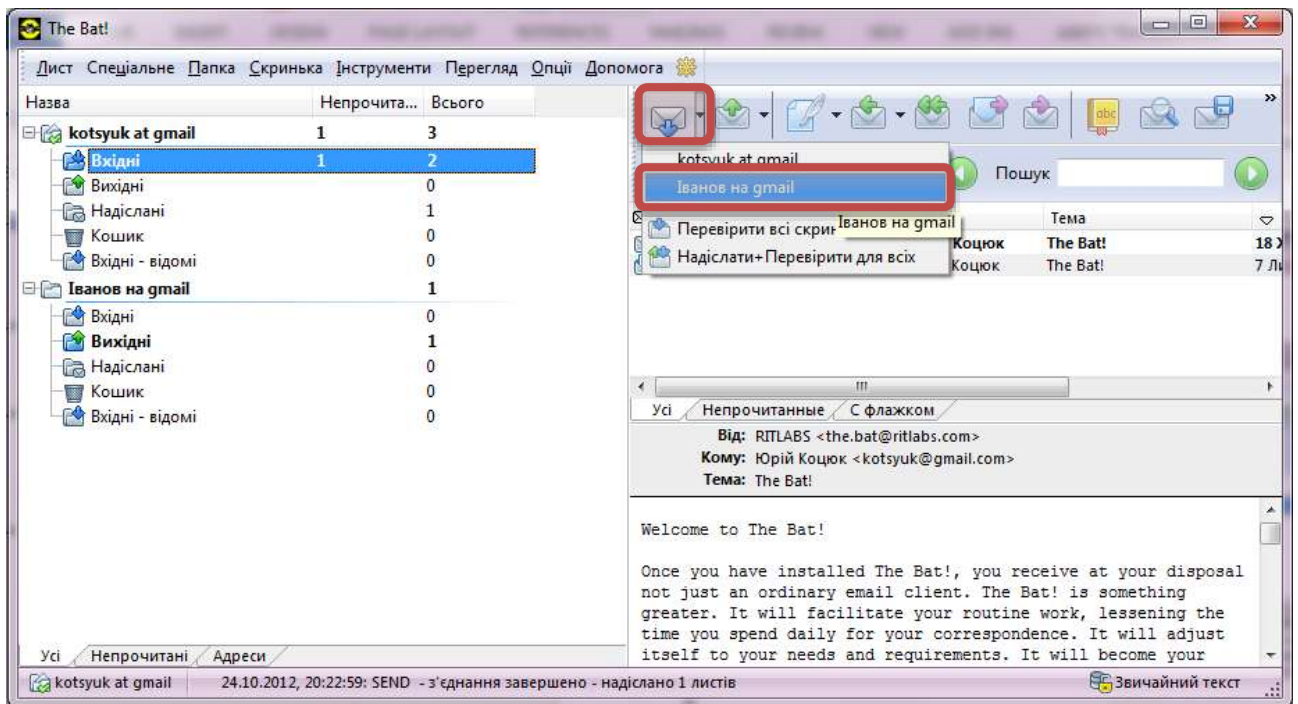


Рис. 100 Перевірка пошти

2. Введіть пароль доступу до своєї поштової скриньки та натисніть «Так» (Рис. 101).

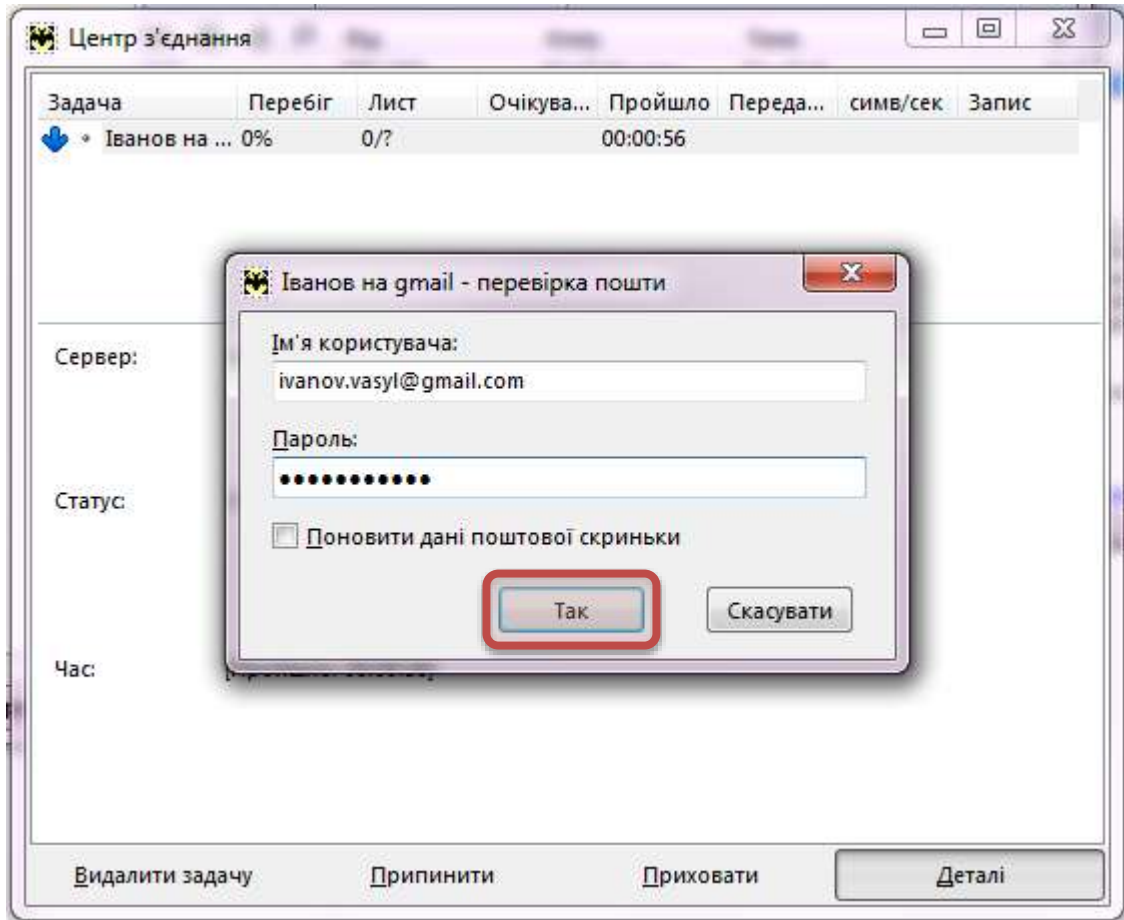


Рис. 101 Ввід пароля до поштової скриньки

3. Вкажіть потрібний лист в обробнику листів та натисніть кнопку «Обробити пошту» (Рис. 102).

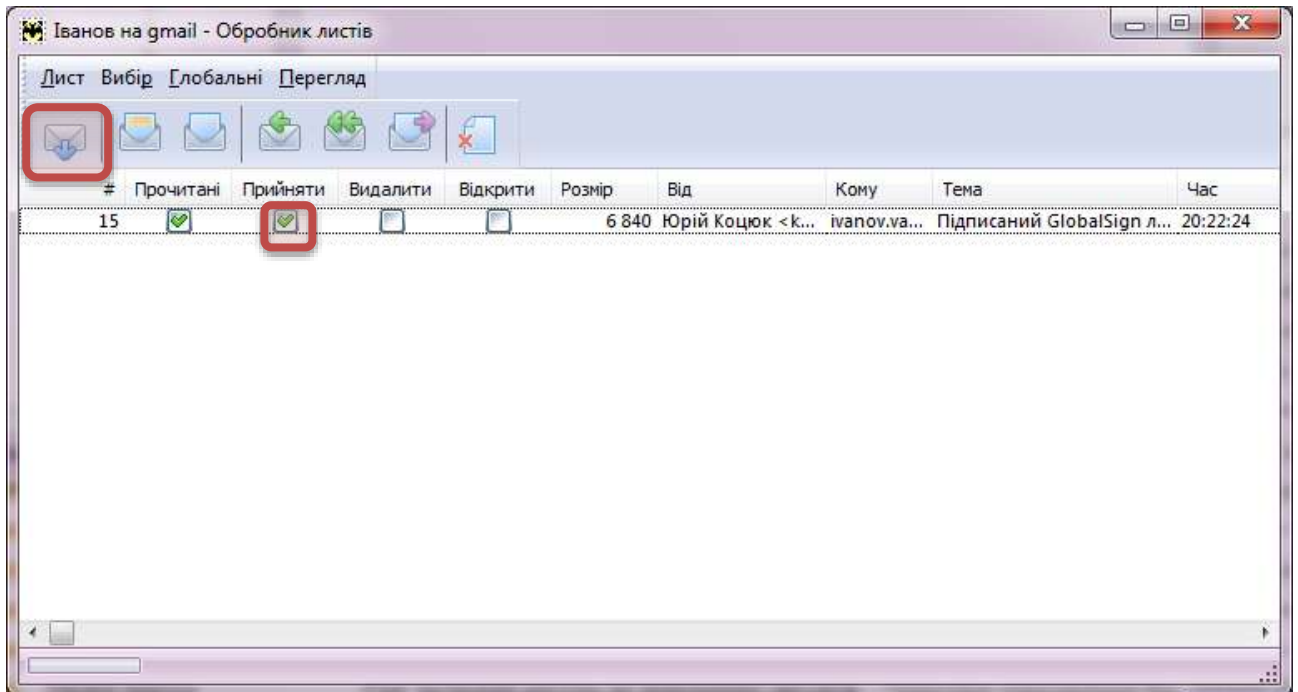


Рис. 102 Обробник листів

4. Відкривши у папці «Вхідні» отриманий лист, скористайтесь відповідною кнопкою, щоб перевірити підпис (Рис. 103).

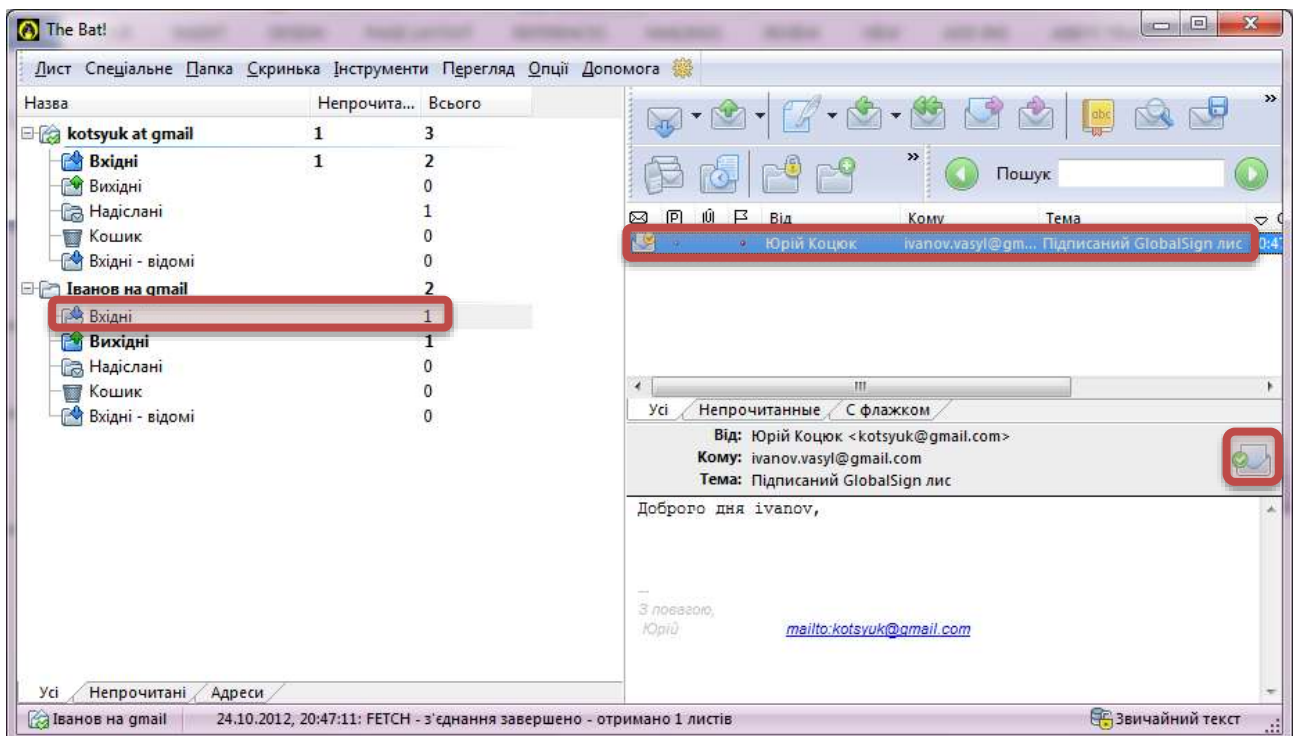


Рис. 103 Відкриття підписаного листа

- Зробіть подвійний клік на підписі для того, щоб перевірити його та додати до адресної книги (Рис. 104).

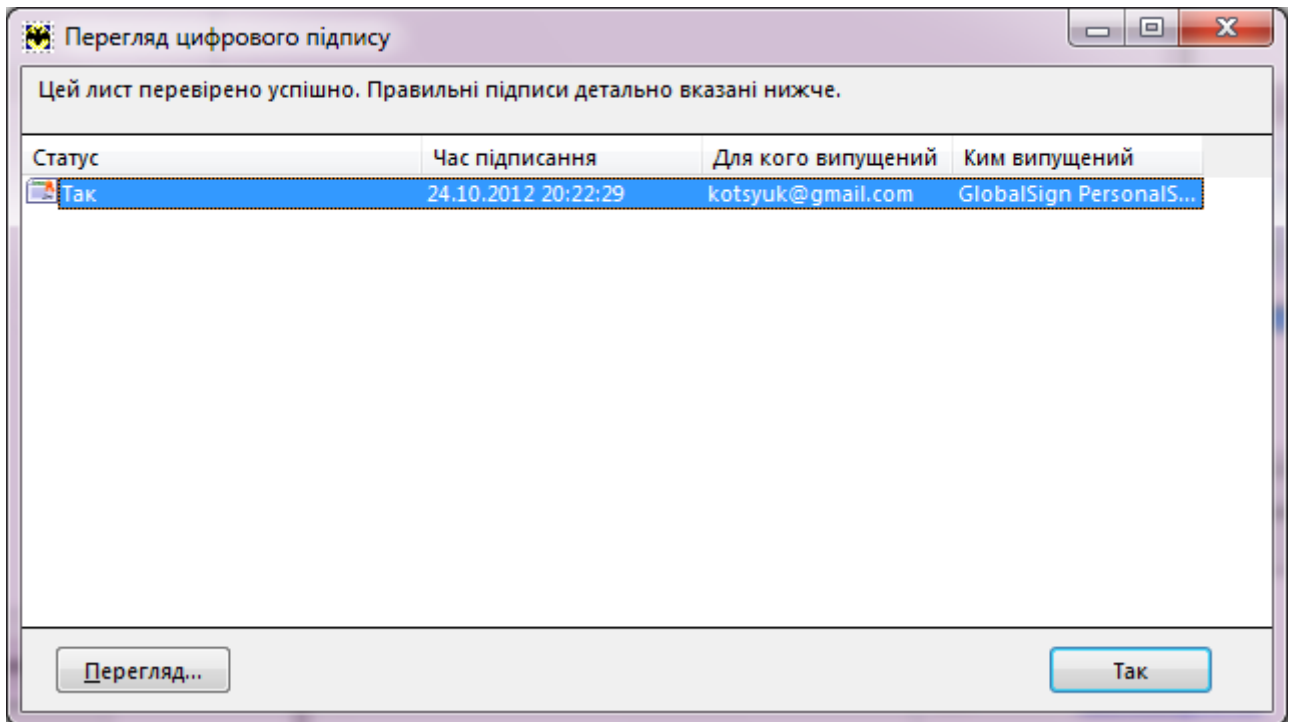


Рис. 104 Перегляд цифрового сертифікату

6. Додайте сертифікат до адресної книги та натисніть кнопку «Так» (Рис. 105). Якщо ж сертифікат не дійсний, слід перейти у вкладку «Шлях» та додати ланцюжок сертифікатів до довірчих.

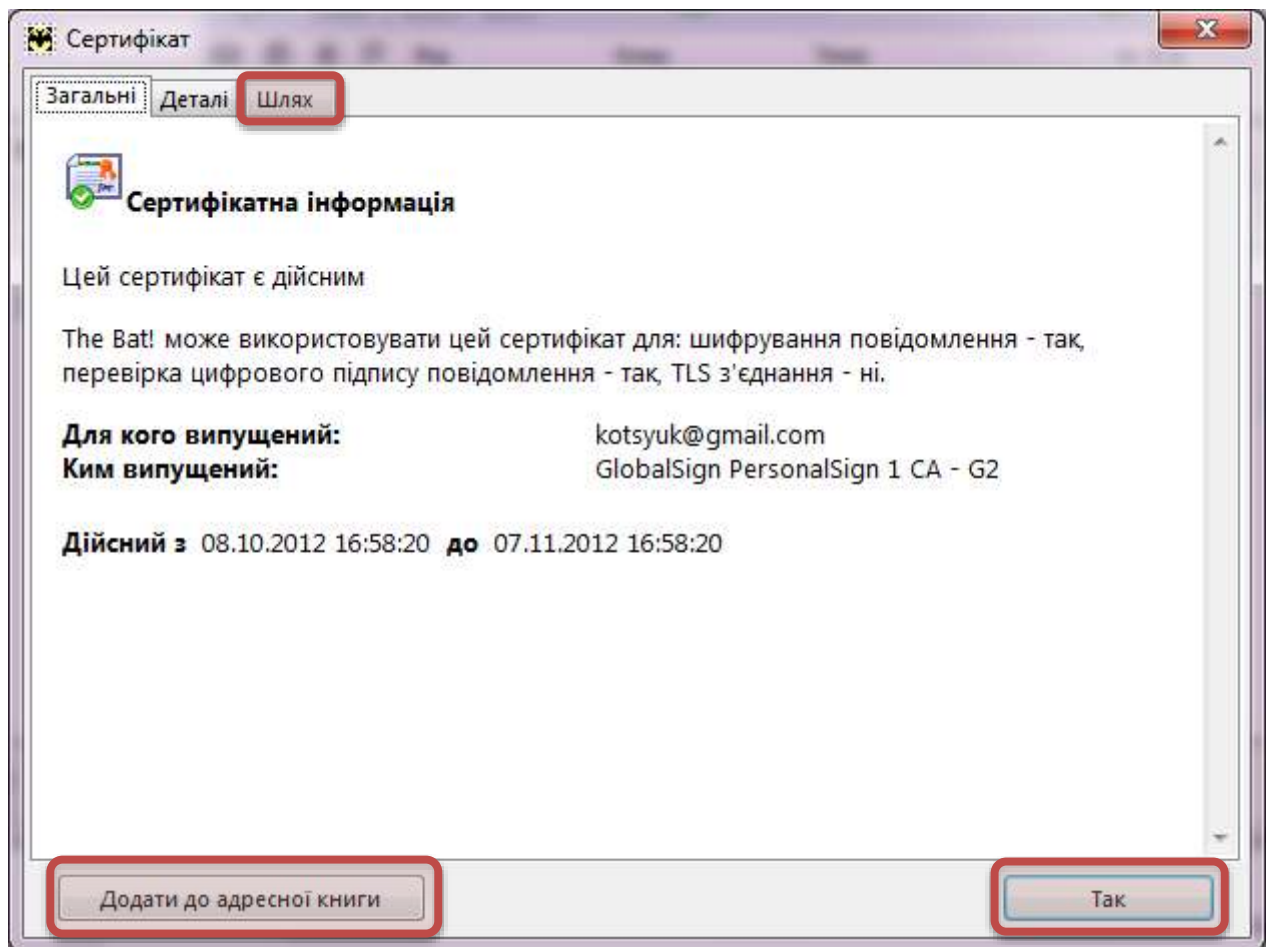


Рис. 105 Сертифікатна інформація

7. Щоб додати ланцюжок сертифікатів до довірчих, виберіть сертифікат кореневого центру сертифікації та натисніть кнопку «Додати до довірчих (Trusted)» (Рис. 106), після цього натисніть кнопку «Так».

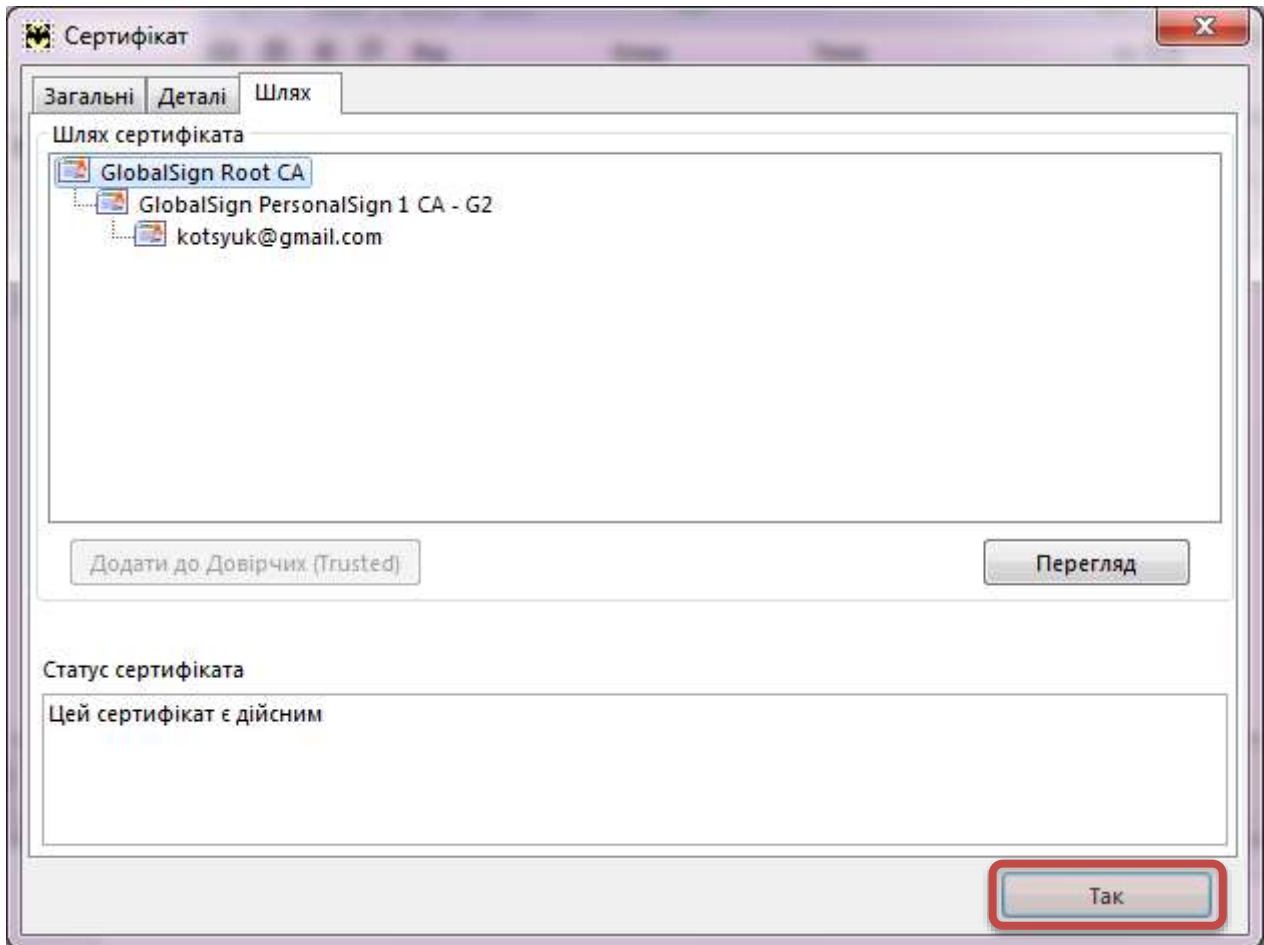


Рис. 106 Шлях сертифікації

8. Закінчіть перегляд сертифікату, натиснувши «Так» (Рис. 107).

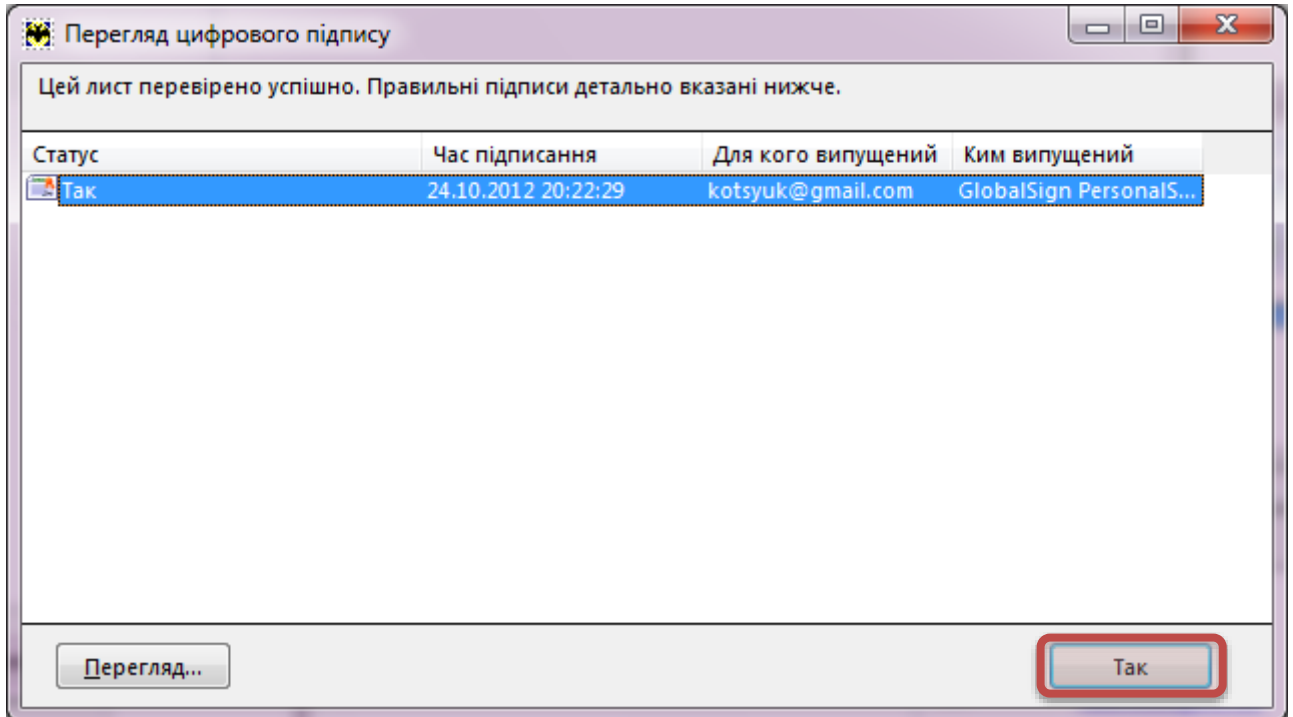


Рис. 107 Перегляд цифрового сертифікату

Надсилання зашифрованого листа

1. Викличте форму для надсилання листа натиснувши потрібну кнопку (Рис. 108).

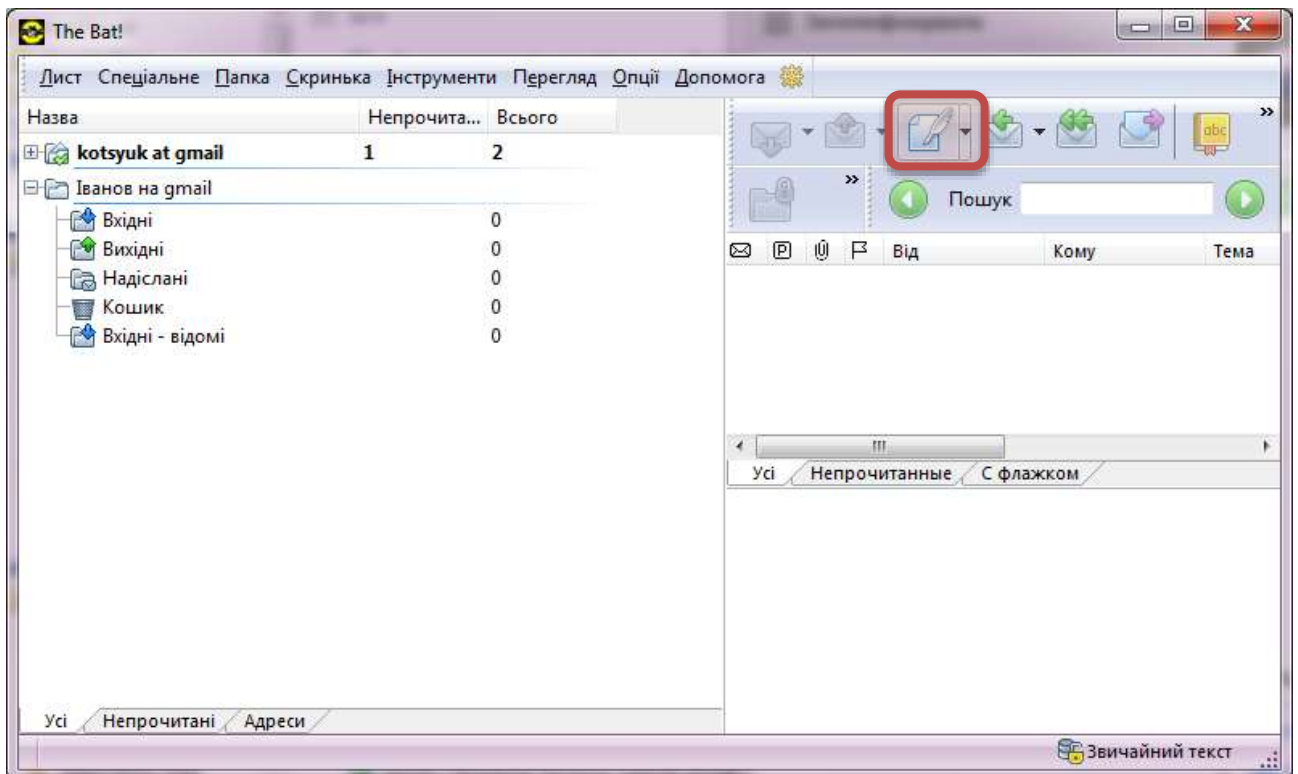


Рис. 108 Кнопка надсилання листа

2. Вкажіть адресу одержувача, тему повідомлення, та власне напишіть тіло повідомлення. Скористайтеся меню «Конфіденційність», для того щоб перевірити чи стоїть прапорець «Дозволити S/MIME», та активуйте можливість «Зашифрувати по закінченню» як вказано на рисунку нижче (Рис. 109).

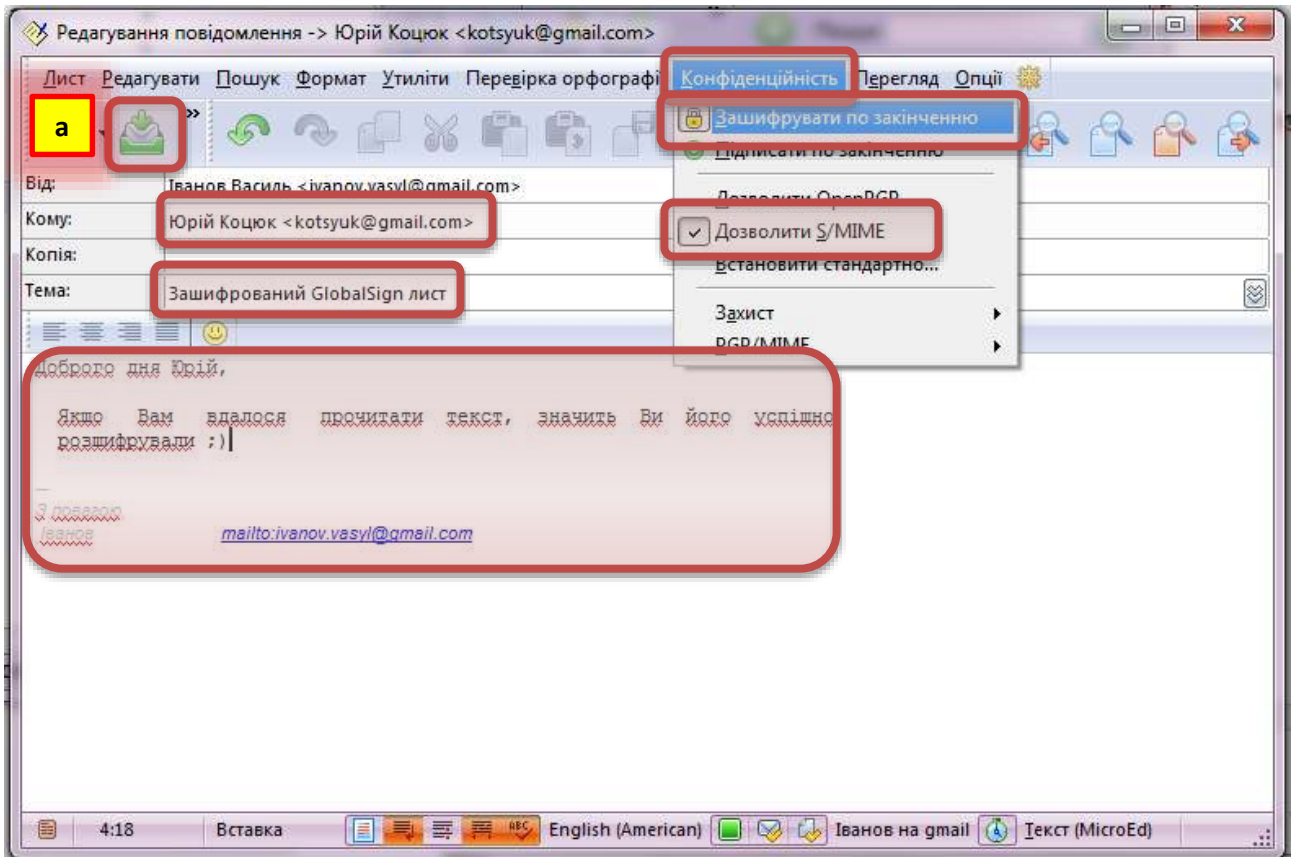


Рис. 109 Підготовка до відправки зашифрованого листа

3. Після виконаних у пункті 2 дій натисніть кнопку «**Підготувати до відправки**» (Рис. 109, а). У Вас з'явиться можливість вказати який із сертифікатів отримувача буде використано для зашифрування. Виберіть сертифікат від Globalsign та натисніть кнопку «Так» (Рис. 110).

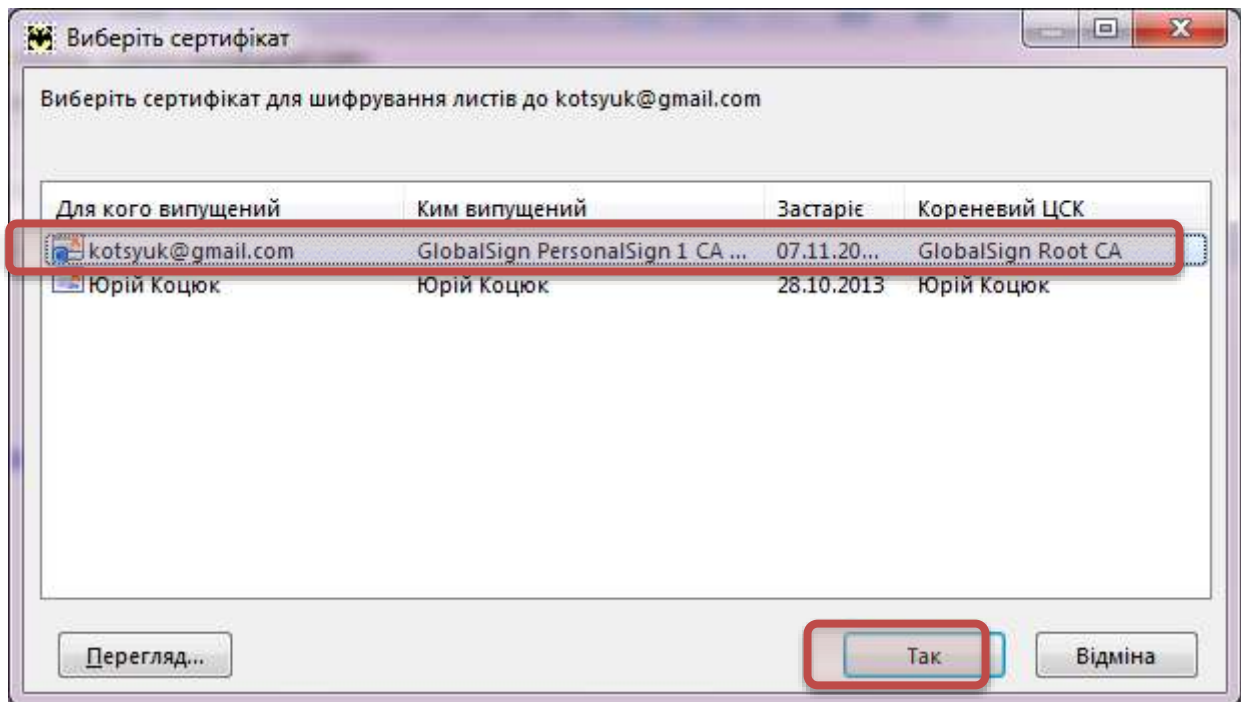


Рис. 110 Вибір сертифікату для шифрування листів

4. В результаті успішної операції шифрування у папці «Вихідні» з'явиться ще один лист. Якщо його вибрати, як показано на рисунку нижче (Рис. 111), то можна перевірити чи правильно його зашифровано, натиснувши на кнопку «Розшифрувати повідомлення S/MIME» (Рис. 111, а).

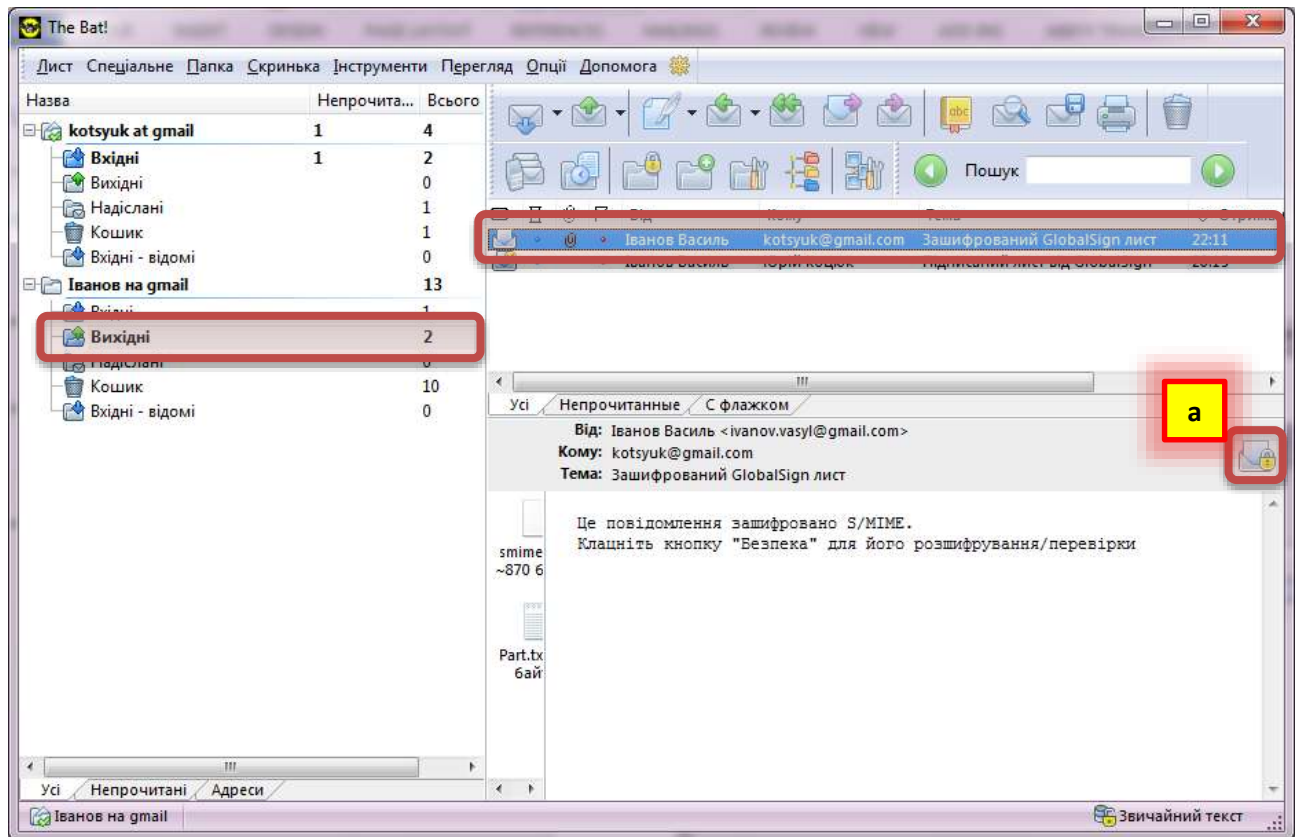


Рис. 111 Перегляд зашифрованого листа

5. В результаті перевірки система повідомить, що Ви не маєте права розшифрувати даний лист, натомість таке право має лише власник вказаного таємного ключа від Globalsign, тобто одержувач Вашого листа (Рис. 112). Тому просто натисніть кнопку «Відміна».

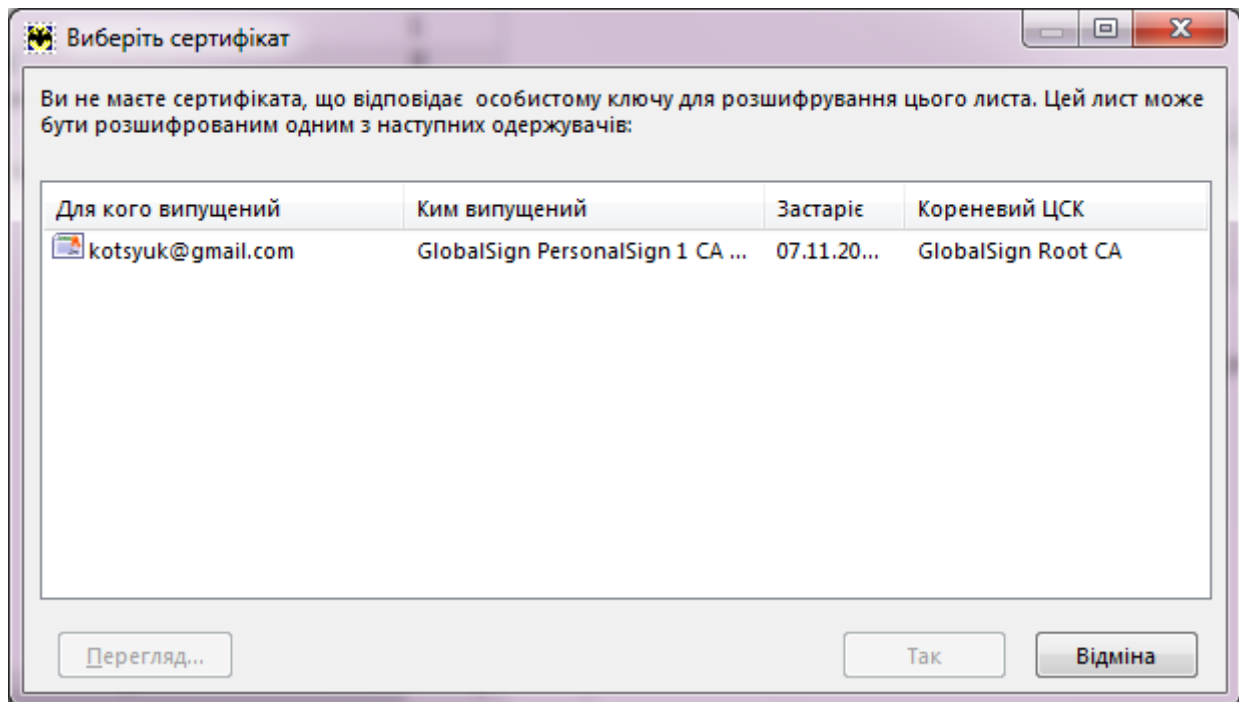


Рис. 112 Невдала спроба розшифрувати лист без таємного ключа

Шифрування та накладання підпису із використанням сертифікату від Globalsign

Однчасне підписування та шифрування листа передбачає наявність усіх умов необхідних як для підписування так і для шифрування (див. [Підписування листів сертифікатом від Globalsign](#) та [Шифрування листів із використанням сертифікату від Globalsign](#)). Якщо ж усі умови виконуються то підписання та шифрування листа можна здійснити виконавши низку вказаних нижче ілюстрованих кроків.

1. Скористайтеся кнопкою «**Нове повідомлення**» для відкриття форми написання листа (Рис. 113).

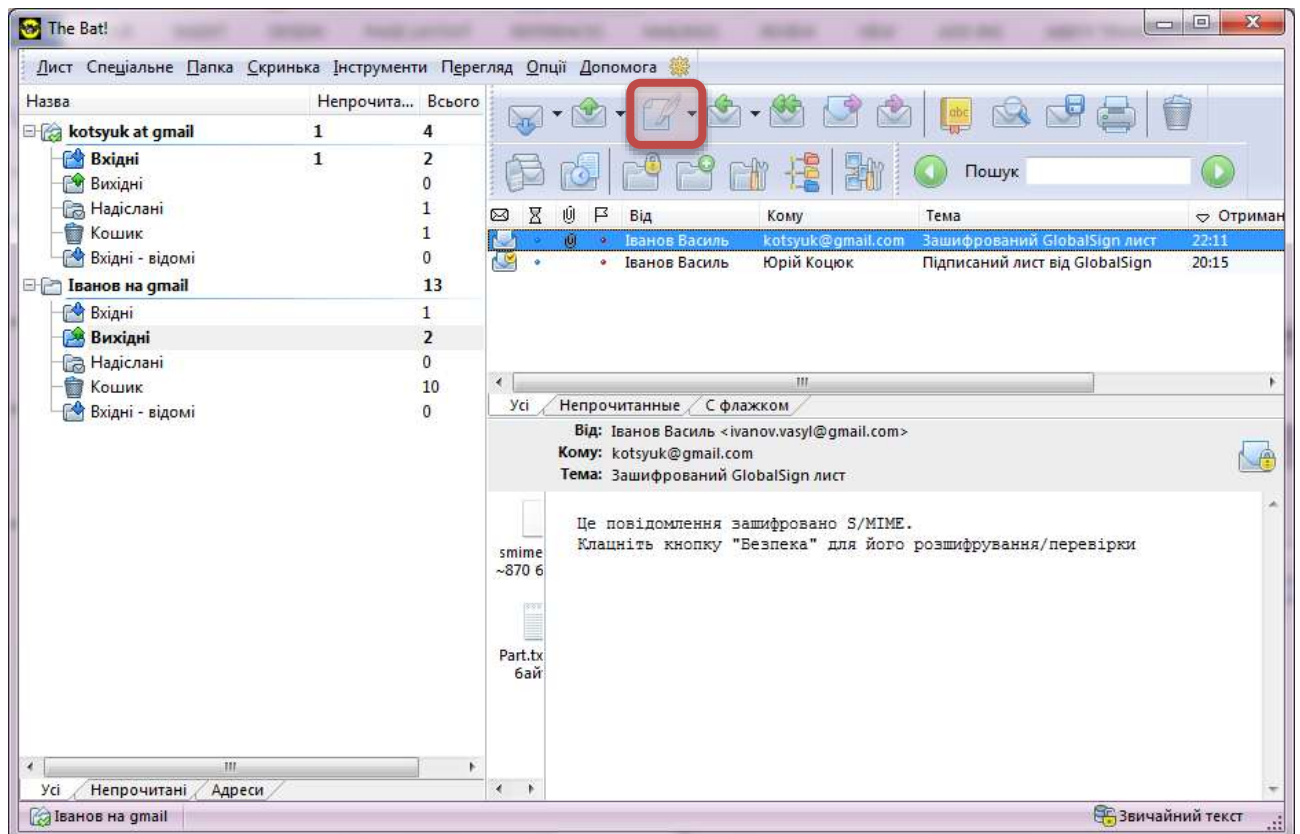


Рис. 113 Кнопка "Нове повідомлення"

2. Вкажіть адресу одержувача, тему повідомлення, та власне напишіть тіло повідомлення. Скористайтеся меню **«Конфіденційність»**, для того щоб перевірити чи стоїть прапорець **«Дозволити S/MIME»**, та активуйте можливість **«Зашифрувати по закінченню»** та **«Підписати по закінченню»** як вказано на рисунку нижче (Рис. 114).

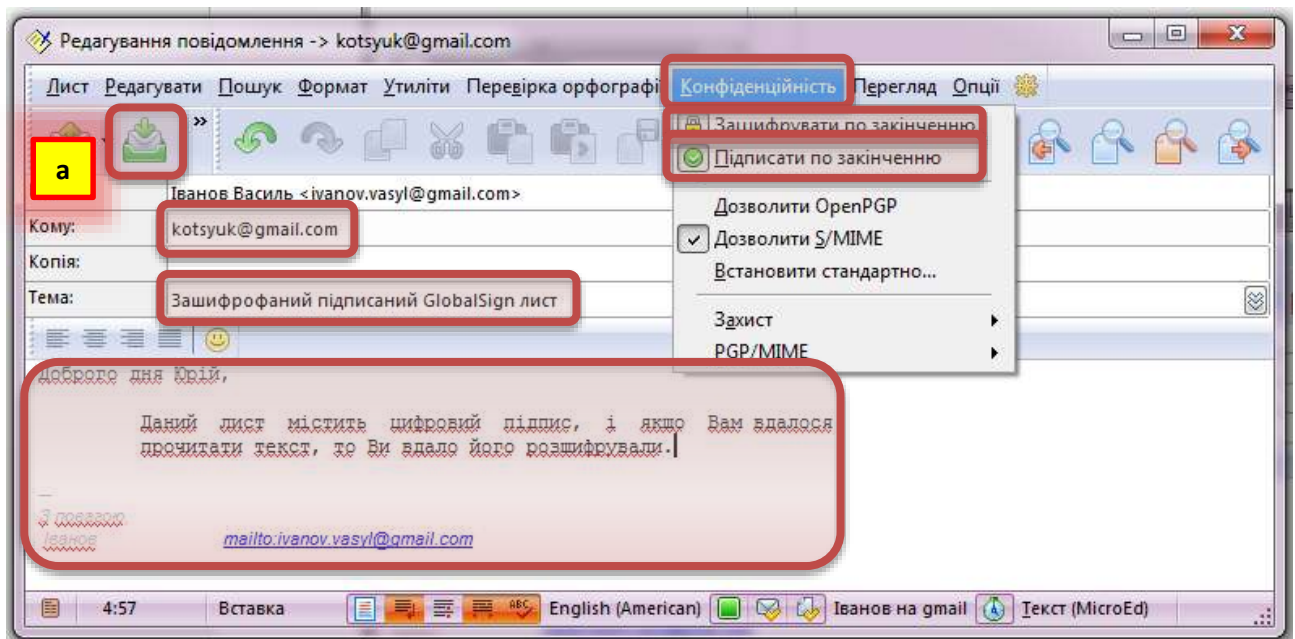


Рис. 114 Підготовка до відправки підписаного та зашифрованого листа

3. Після виконаних у пункті 2 дій натисніть кнопку **«Підготувати до відправки»** (Рис. 114, а). У наступному діалоговому вікні Вам буде надано можливість вибрати один з Ваших сертифікатів для підпису. Серед існуючих ключів виберіть ключ від Globalsign¹ (Рис. 115) та натисніть кнопку **«Так»**.

¹ Якщо у Вас більше одного сертифікату, то перед цією операцією слід виконати операцію [скидання підписів](#).

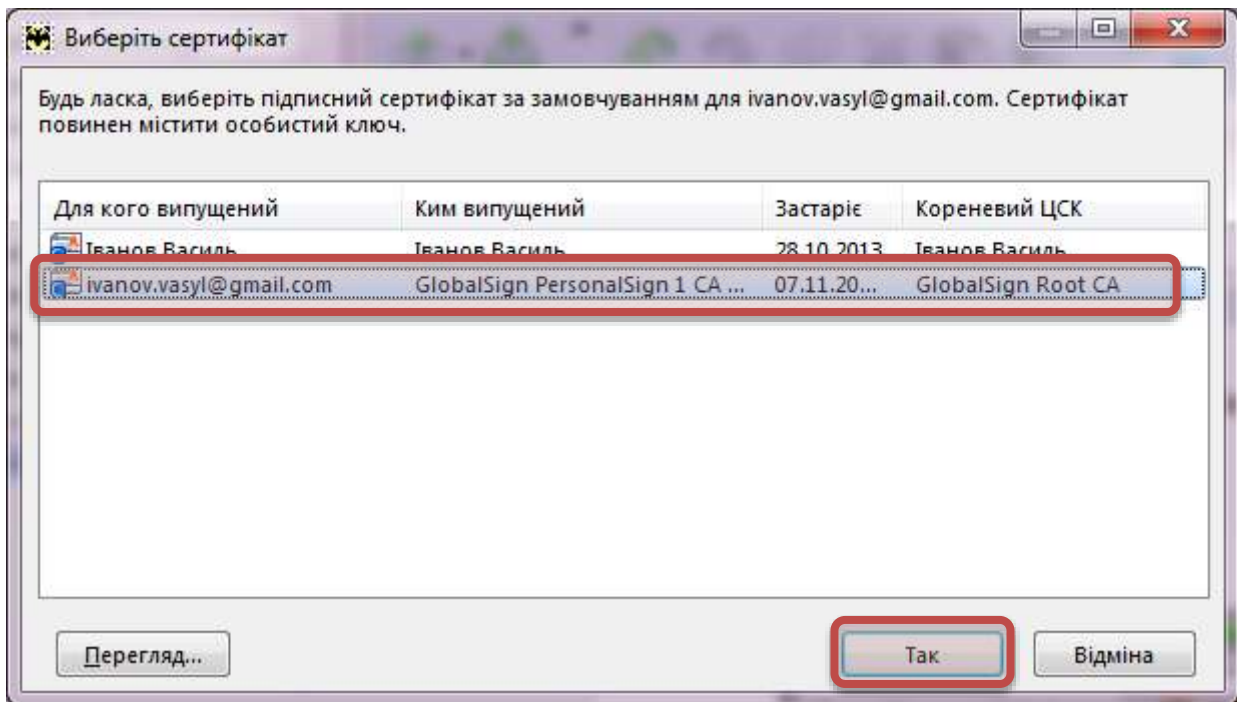


Рис. 115 Вибір сертифікату для підпису

4. Введіть пароль доступу до приватного ключа від Globalsign, та натисніть кнопку «Так» (Рис. 116)

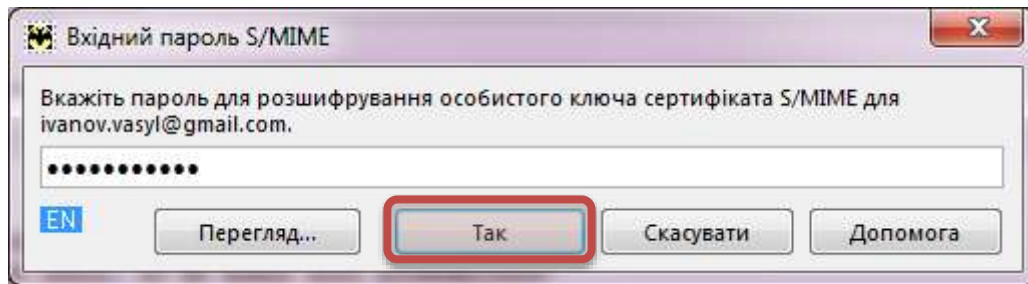


Рис. 116 Пароль для розшифрування особистого ключа

5. У наступному діалоговому вікні у Вас з'явиться можливість вказати який із сертифікатів отримувача буде використано для зашифрування. Виберіть сертифікат від Globalsign та натисніть кнопку «Так» (Рис. 117).

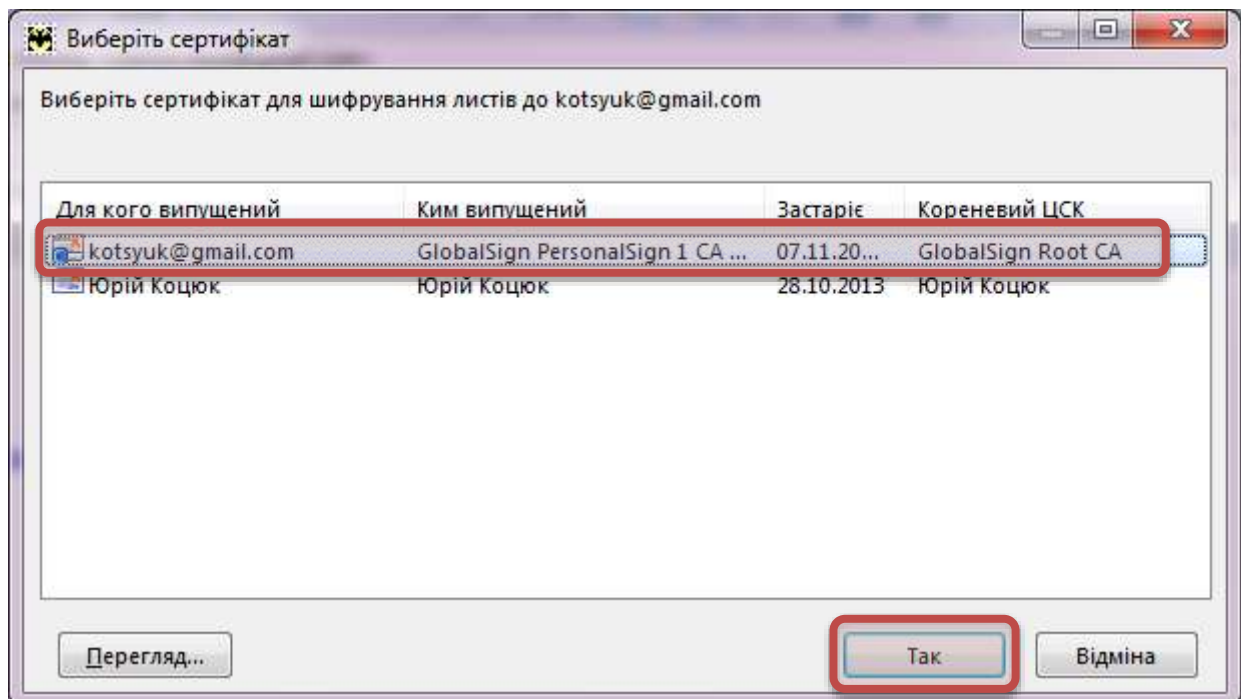


Рис. 117 Вибір сертифікату для шифрування листа

6. В результаті успішної операції шифрування у папці «**Вихідні**» з'явиться ще один лист. Якщо його вибрати, як показано на рисунку нижче (Рис. 118), то можна перевірити чи правильно його зашифровано та підписано, натиснувши на кнопку «**Безпека повідомлення**» (Рис. 118, а).

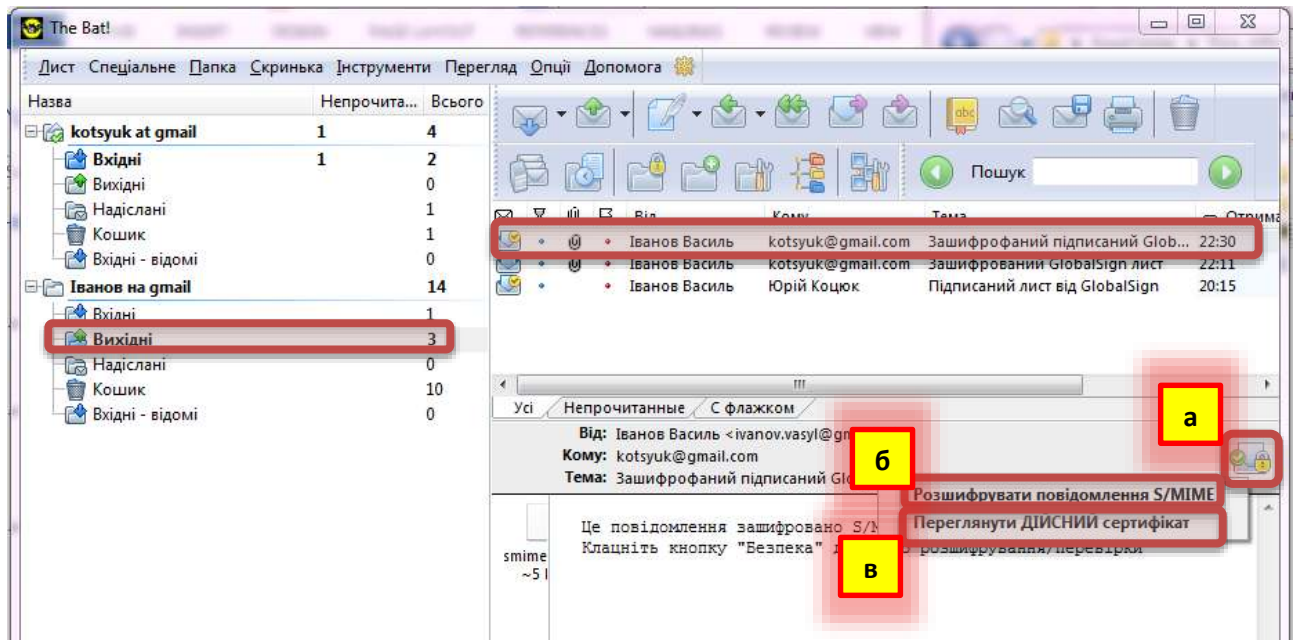


Рис. 118 Перевірка підписаного та зашифрованого листа

7. Для перевірки яким сертифікатом було зашифровано лист виберіть можливість «**Розшифрувати повідомлення S/MIME**» (Рис. 118, б). В результаті перевірки система повідомить, що Ви не маєте права розшифрувати даний лист, натомість таке право має лише власник вказаного таємного ключа від Globalsign, тобто одержувач Вашого листа (Рис. 119). Тому просто натисніть кнопку «**Відміна**».

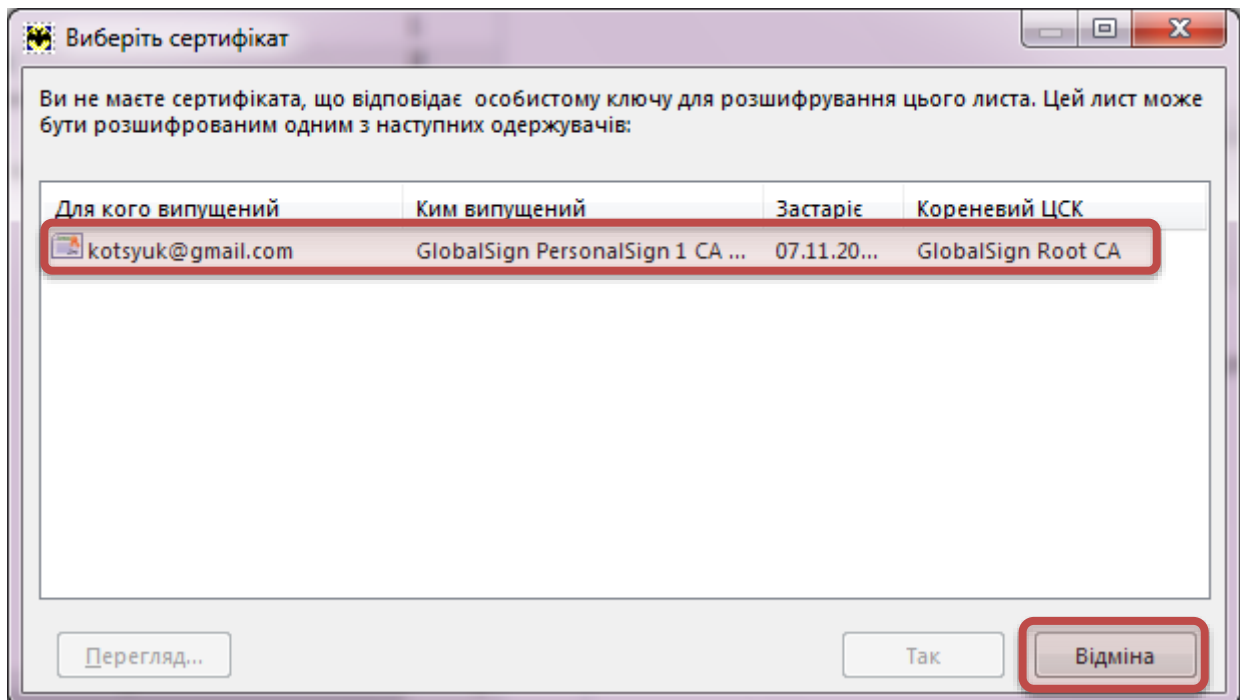


Рис. 119 Невдала спроба розшифрувати лист без таємного ключа

8. Для перевірки електронного цифрового підпису натисніть на кнопку «**Безпека повідомлення**» (Рис. 118, а) та виберіть можливість «**Переглянути ДІЙСНІ підписи**» щоб переконатися, що саме Ваш підпис накладено¹. (Рис. 118, в). Після перевірки натисніть кнопку «**Так**» (Рис. 120).

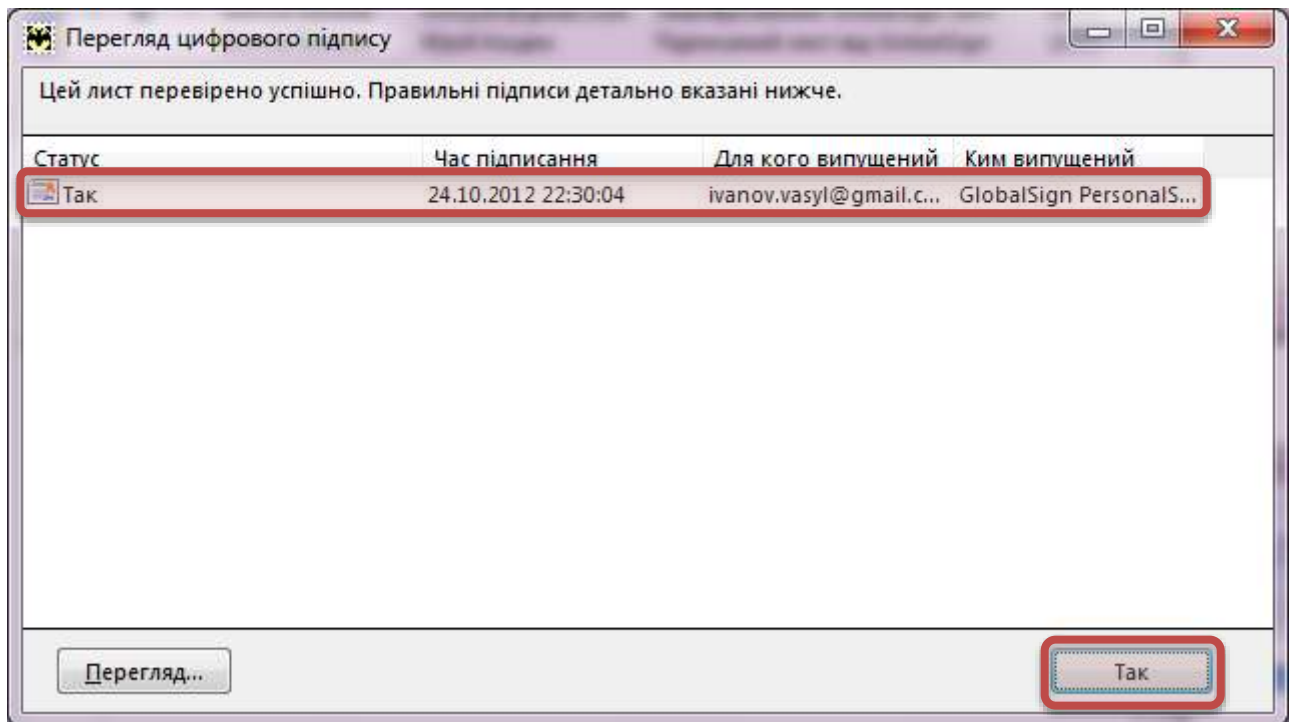


Рис. 120 Перегляд цифрового підпису

¹ Якщо кнопки підпису немає, або використано не той що слід підпис, значить з якоїсь причини Вам не вдалося накласти потрібний підпис. Спробуйте повторити все з початку.

Надсилання підготованих до відправки листів

1. Скористайтеся кнопкою для надсилання пошти, щоб надіслати свою пошту (Рис. 121).

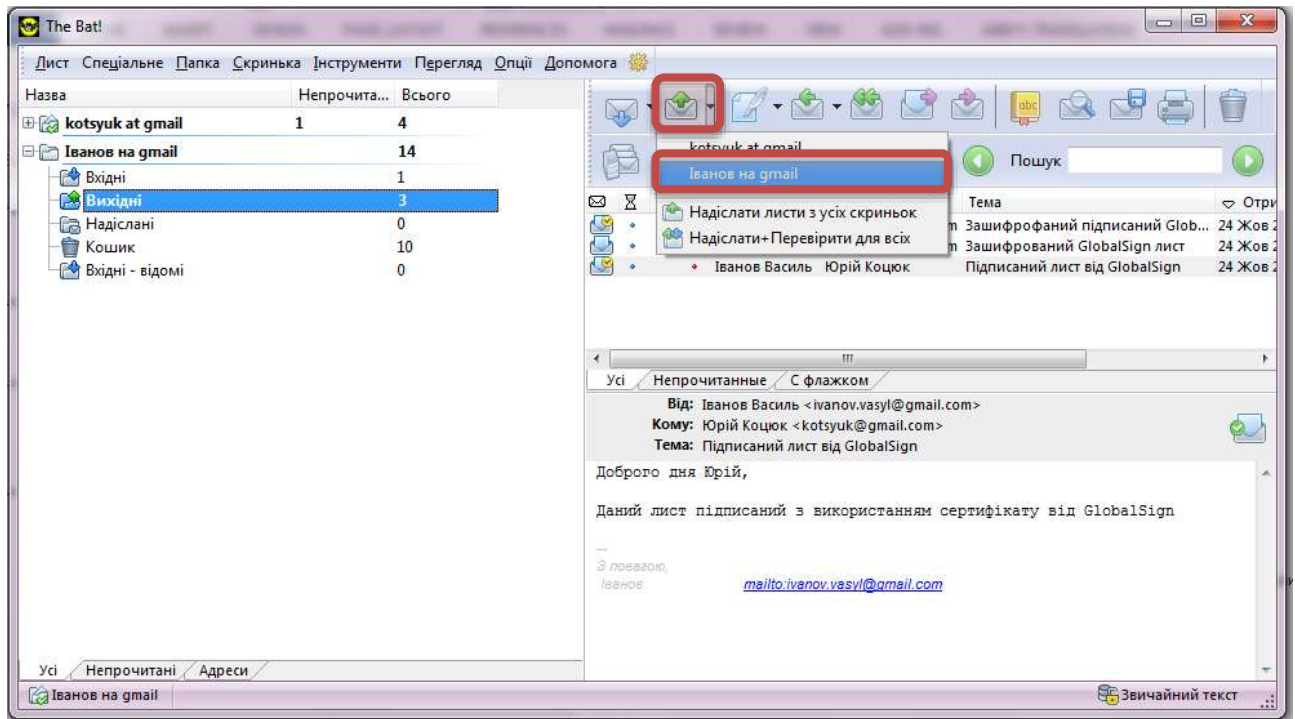


Рис. 121 Відправка пошти

2. Введіть пароль доступу до Вашої поштової скриньки та натисніть кнопку «Так» (Рис. 122).

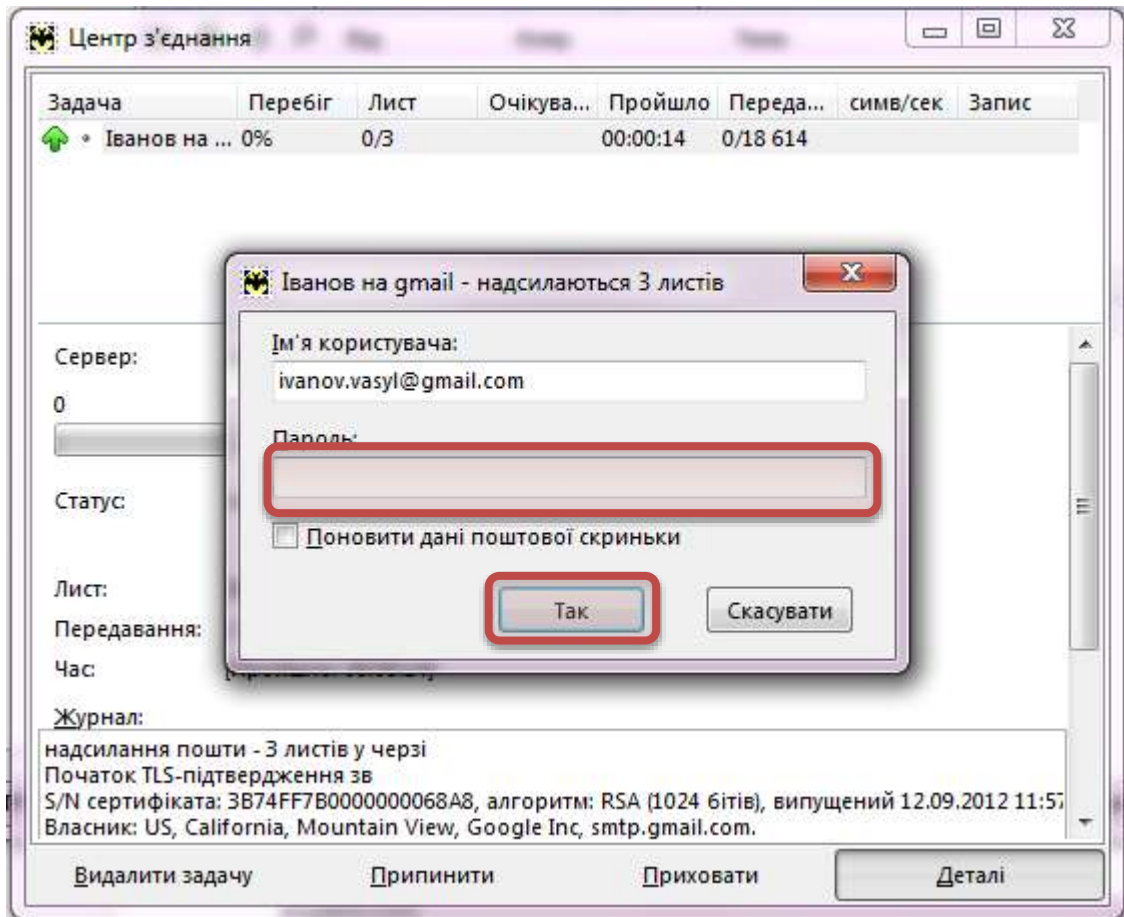


Рис. 122 Ввід пароля доступу до поштової скриньки

3. Якщо листи вдалося відправити вони зникнуть з папки «Вихідні» та з'являться у папці «Надіслані» (Рис. 123).

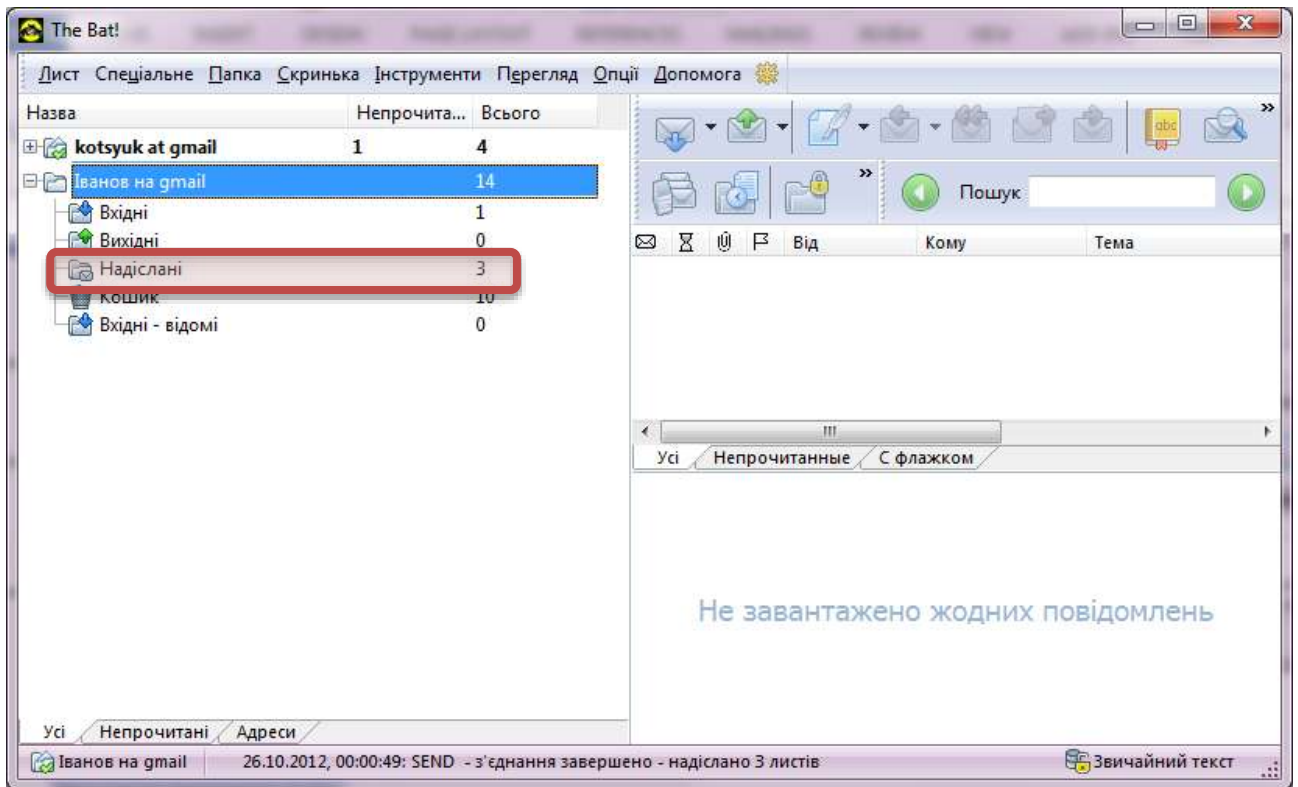


Рис. 123 Папка "Надіслані"