МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

кафедра протидії кіберзлочинності, факультет № 4

МЕТОДИЧНІ МАТЕРІАЛИ
до лабораторних занять

з навчальної дисципліни **Основи кібербезпеки**

обов'язкових компонент освітньої програми першого рівня вищої освіти 125 Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 № 7

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 16.08.2023 № 8

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 № 7

Розглянуто на засіданні кафедри протидії кіберзлочинності (*протокол від 15.08.2023 № 19*

Розробник:
Завідувач кафедри протидії кіберзлочинності, к.ю.н., професор Манжай О.В.

Рецензенти:

Тулупов В.В., доцент кафедри кібербезпеки та DATA-технологій факультету № 6 Харківського національного університету внутрішніх справ к.т.н., доцент;

Павликівський В.І., перший проректор Харківського університету, д.ю.н., професор

1. Розподіл часу навчальної дисципліни за темами

(денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 1							
Тема № 1 **Загальні правила безпечної роботи з пристроями та програмами.**	**44**	**12**	**0**	**12**	**0**	**20**	**Екзамен**
Тема № 2 **Базові правила убезпечення роботи в комп'ютерній мережі**	**46**	**12**	**0**	**0**	**12**	**22**	
Всього за семестр № 1:	**90**	**24**	**0**	**12**	**12**	**42**	

(заочна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 1							
Тема № 1 **Загальні правила безпечної роботи з пристроями та програмами.**	**44**	**2**	**0**	**2**	**0**	**40**	**Екзамен**
Тема № 2 **Базові правила убезпечення роботи в комп'ютерній мережі**	**46**	**2**	**0**	**0**	**2**	**42**	
Всього за семестр № 1:	**90**	**4**	**0**	**2**	**2**	**82**	

2. Методичні вказівки до практичного навчання

Тема № 2 Базові правила убезпечення роботи в комп'ютерній мережі

Лабораторне заняття «Аналіз поштового повідомлення»

Навчальна мета заняття: отримати практичні навички аналізу поштового повідомлення.

Час проведення: 1 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено**.

Фішінгові повідомлення часто надходять користувачам за допомогою електронної пошти.

Змоделюємо ситуацію, яким чином це може відбуватися та як можна запобігти цьому негативному явищу.

Спершу слід зареєструвати тестову поштову скриньку, на яку будемо одержувати відповідні повідомлення. Після реєстрації електронної поштової скриньки слід надіслати на неї неправдиве повідомлення з підміною заголовка. Для цього можуть бути використані сервіси https://emkei.cz/, https://anonymousemail.me/ тощо. Приклад відповідним чином сформованого листа наведено на рис. 1.

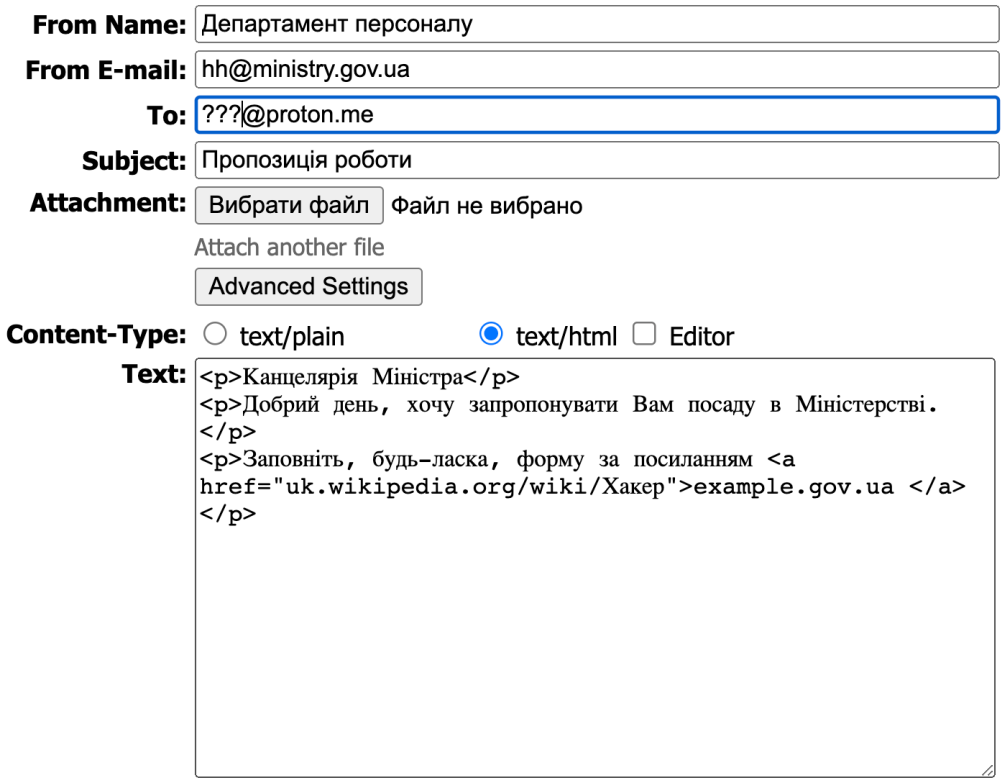


Рис. 1. Відправлення неправдивого повідомлення

У результаті на поштову скриньку надійде лист як на рис. 2.

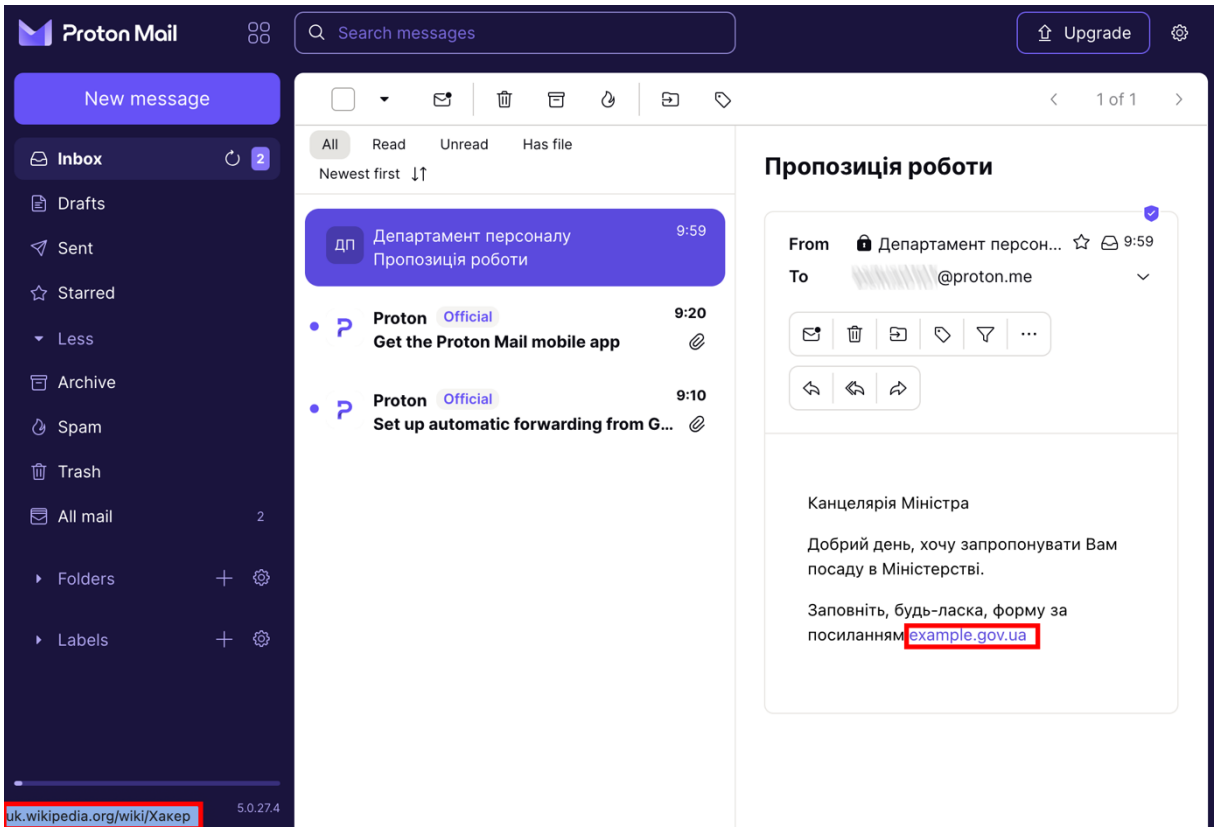


Рис. 2. Повідомлення, що надійшло

Для того, щоб виявити підробку в листі, потрібно дослідити його поштовий заголовок. Для цього слід після відкриття листа натиснути «Переглянути заголовок».

```
Return-Path: <hh@ministry.gov.ua>
X-Original-To: ???@proton.me
Delivered-To: ???@proton.me
Received: from emkei.cz (emkei.cz [89.187.129.22]) (using TLSv1.3 with cipher
 TLS_AES_256_GCM_SHA384 (256/256 bits)
  key-exchange X25519 server-signature RSA-PSS (4096 bits) server-digest
SHA256) (No
 client certificate requested) by mailin005.protonmail.ch (Postfix) with ESMTPS
id
 4RYPgY4Bbzz9vNPV for <???@proton.me>; Sun, 27 Aug 2023 06:59:21 +0000 (UTC)
Received: by emkei.cz (Postfix, from userid 33) id 2E8B35849E1; Sun, 27 Aug
2023 08:59:15
 +0200 (CEST)
Authentication-Results: mailin005.protonmail.ch; dmarc=none (p=none dis=none)
 header.from=ministry.gov.ua
Authentication-Results: mailin005.protonmail.ch; spf=none
smtp.mailfrom=ministry.gov.ua
Authentication-Results: mailin005.protonmail.ch; arc=none smtp.remote-
ip=89.187.129.22
Authentication-Results: mailin005.protonmail.ch; dkim=none
To: ???@proton.me
Subject: =?utf-8?B?0J/RgNC+0L/QvtC30LjRhtGW0Y8g0YDQvtCx0L7RgtC4?=
From: =?utf-8?B?ItCU0LXQv9Cw0YDRgtCw0LzQtdC90YIg0L/QtdGA0YHQvtC90LDQu9GDIiA8?=
 =?utf-8?B?aGhAbWluaXN0cnkuZ292LnVhPg==?=
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: hh@ministry.gov.ua
Reply-To: hh@ministry.gov.ua
Content-Type: text/html
Message-Id: <20230827065915.2E8B35849E1@emkei.cz>
Date: Sun, 27 Aug 2023 08:59:15 +0200
X-Rspamd-Server: cp3-mailin-005.plabs.ch
X-Rspamd-Queue-Id: 4RYPgY4Bbzz9vNPV
```

```
      X-Rspamd-Action: add header
      X-Spamd-Result: default: False [8.80 / 25.00]; MISSING_MIME_VERSION(2.00)[];
       MIME_HEADER_CTYPE_ONLY(2.00)[]; PHISHING(2.00)[example.gov.ua->wikipedia.org];
       HFILTER_FROMHOST_NORES_A_OR_MX(1.50)[ministry.gov.ua]; AUTH_NA(1.00)[];
       MIME_HTML_ONLY(0.20)[]; ONCE_RECEIVED(0.10)[]; FROM_EQ_ENVFROM(0.00)[];
       MIME_TRACE(0.00)[0:~]; RCVD_TLS_LAST(0.00)[]; RCVD_COUNT_ONE(0.00)[1];
       NEURAL_SPAM(0.00)[0.986]; ASN(0.00)[asn:35592, ipnet:89.187.129.0/24,
country:CZ];
       R_DKIM_NA(0.00)[]; DMARC_NA(0.00)[ministry.gov.ua]; RCPT_COUNT_ONE(0.00)[1];
       FROM_HAS_DN(0.00)[]; ARC_NA(0.00)[]; HAS_X_PRIO_THREE(0.00)[3];
R_SPF_NA(0.00)[no SPF
      record]; REPLYTO_ADDR_EQ_FROM(0.00)[]; TO_MATCH_ENVRCPT_ALL(0.00)[];
TO_DN_NONE(0.00)[];
       HAS_REPLYTO(0.00)[hh@ministry.gov.ua]
      X-Spam: Yes
      X-Pm-Spam: 0yezJI6cihyJeYR3pi42biOpJJvbmsCIeI1msjN3X3blJp7IjBlNIIoj2sUjLlITJ
       o4IjsjgLIBlSiQ0TiOx0wiOSPFJUR9FQEVkUUSUN9OSUwjoILJCfiVGZWdfd5maW6yIbeJyQE9kU
       jI7pBfInh3BcbIS6x4CMzM2cU0OT3zEMMkDy1kDOSNiw1haWf2VZbFmt6ISZmIzhFjdGv19aYNnl
       lZncFZy8IzMDxDgMMICs1JnIlbu91lYWijoIYxWslZWLXY1RVzcmiiwIbFWpj9FbXYlR9yZ2uV9e
       Y1WliojIVVEBRFQVsyIUI1mhfxWa2Y0FdvZWfnlccJHv6IiYCM44Y5MT9jlMf0XshNmIGdnVJ5b3
       ijoIVBVEFRVQyUsINyIniWQaOIi2hVGNjZ0QFhYjlTdMNMm3mJjMDN1QYiYTiSwfcE2iisnOXafN
       Bhc36SIbMwSivN2cmciUYsOjjnNIbJ3l6ICZiN14JyLCvXBZcQniisnOkTf95TREP0ZXU9lGN9kU
       jIbp4wNCiSwXQFkZfNVRTNiAsxOlsjALINnjlJ3biOwAQ5LjiTkOXwSiGB1U0XFh9fTETEFUUIy6
       w0yWjLdBJELCN0lSXF0EfB1UlTEh1BT0iU4SOslwdljLCLTJZfUEOk9TRIS6uAzWFMs0hUIkfUxT
       TVUTHF0USR6IAuWzsF0MI1kJfVUTFSNR9PTFZkxTIpjbx4CMSXiwRNSFNF9TS1UFP50X0XUhxfTU
       HEFVIpjb04CMSXiwlNTUIV9RRFUEfJVR1QZRVfUEM05TWIS6uAzWVMs0RWIlTF9RUFEDS9VRVQJR
       9NT1GU5SUIC6uAzWFM91fX0=
      X-Pm-Origin: external
      X-Pm-Transfer-Encryption: TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256
bits)
      X-Pm-Content-Encryption: on-delivery
      X-Pm-Spamscore: 6
      X-Pm-Spam-Action: inbox
      Mime-Version: 1.0
```

Базовий формат поштових повідомлень (листів, messages) і статей USENET (article) визначається RFC 822 і його «спадкоємцем» RFC 2822. Кожне повідомлення (лист, message, стаття, article) складається з конверта і вмісту. Конверт зберігає адресну інформацію, необхідну для відправлення і передачі повідомлення одержувачеві. Формат конверта визначається середовищем розповсюдження. Для його автоматичного створення може використовуватися інформація з вмісту повідомлення. Стандарт визначає тільки формат вмісту повідомлення і лише у момент передачі, тобто повідомлення можуть зберігатися абсолютно в іншому форматі. Повідомлення ділиться на рядки і складається з секції заголовків і тіла повідомлення (можливо, порожнього).

Заголовок електронного поштового листа можна дослідити або вручну, або за допомогою програм чи сервісів (рис. 3.)

IP Address	93.99.104.210
Country	Czech Republic
Region	-
City	-
ISP	Liberty Global
Organization	Liberty Global
Latitude	50.0848
Longitude	14.4112

Рис. 3. Результат аналізу заголовка поштового листа за допомогою сервісу iplocation.net

Виходячи з даних, наведених в теоретичних відомостях:

1. Зареєструвати поштову скриньку та надіслати тестове повідомлення.
2. Проаналізувати заголовок та тіло листа зі своєї електронної поштової скриньки. Визначити адресу відправника та маршрут руху листа за допомогою сервісів: https://www.iplocation.net/trace-email, https://mha.azurewebsites.net/, https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=73671c03-950e-4f79-88ee-f78a785b2eef, https://www.ip2location.com/free/email-tracer, https://www.whatismyip.com/email-header-analyzer/.

*Приклад. «**Розшифровка типового заголовка листа»***

Return-path: *******@ukr.net*** *– зворотна адреса, вказана відправником;*

Received: from [212.9.224.21] (port=25 helo=mail-out.iptelecom.net.ua) *– лист отримано від хосту mail-out.iptelecom.net.ua з IP-адресою 212.9.224.21;*

by mx5.mail.ru *– ім'я комп'ютера, який приймав повідомлення;*

with esmtp id 1COlNS-000F0L-00 *– комп'ютер, що прийняв повідомлення, надав йому ідентифікаційний номер 1COlNS-000F0L-00;*

Tue, 18 Nov 2008 02:14:18 +0300 *– передавання листа здійснювалося у вівторок, 18 листопада 2008 року о 02:14:18 за часом третього часового поясу, який випереджає Гринвічський часовий пояс на 3 години, звідси «+0300»;*

Received-SPF: none (mx5.mail.ru: 212.9.224.21 is neither permitted nor denied by domain of ukr.net) client-ip=212.9.224.21 *– отримана відповідь на SPF-запит. Технологія SPF (Sender Policy Framework) є одним зі способів ідентифікації відправника електронного листа та надає додаткову можливість фільтрування потоку пошти на наявність у ньому повідомлень зі спамом. За допомогою SPF пошта поділяється на «дозволену» й «заборонену» відносно домену одержувача чи відправника. В цьому випадку, поштовий сервер-одержувач mx5.mail.ru здійснив SPF-запит до домену ukr.net, де було отримано відповідь про фактичну відсутність SPF-захисту (дослівно: mx5.mail.ru здійснив SPF-запит до домену ukr.net про наявність у списках IP-адреси 212.9.224.21, на що було отримано відповідь про те, що цю адресу не внесено ані в дозволені, ані в заборонені списки SPF домену ukr.net);*

envelope-from=*@ukr.net*** *– заголовок, який додається до листа деякими поштовими програмами під час доставки кінцевому одержувачу;*

helo=mail-out.iptelecom.net.ua;

Received: from h136.246.159.dialup.iptcom.net ([213.159.246.136]:64011 "HELO copm1" ident: "NO-IDENT-SERVICE[2]" whoson: "s-m-i-t");

by pechkin.iptelecom.net.ua with SMTP id S358789AbUKAXOS (ORCPT <rfc822;igoset@mail.ru> + 3 others);

Tue, 18 Nov 2008 01:14:18 +0200 *– час, коли одержано лист;*

Message-ID: <021501c4c068$4d89ba20$0200a8c0@copm1> *– процес одержання листа первинним провайдером для подальшого пересилання з ПК, підключеного за допомогою модемного з'єднання (h136.246.159.dialup.iptcom.net). Розшифрування є аналогічним вищевикладеному;*

From: *@ukr.net*** *– напис на «конверті», від кого лист;*

To: <**@mail.ru>, <**@ukrpost.net>, <@mail.ru>, <**@ukr.net>, <**@yahoo.co.uk>, <**@ok.ru>, <**@yandex.ru>, <****@mail.ru>, <*****@mail.ru>, <**@bk.ru>, *@ukr.net*** *– адреси доставки листа;*

Subject: =?koi8-r?B?8NLFxMzP1sXOycU=?= *– тема листа (у разі заміни кодування тема матиме вигляд напису «Предложение»);*

Date: Tue, 18 Nov 2008 00:52:14 +0200 *– дата та час створення листа (вівторок 2 листопада 2008 р., о 00:52:14 на комп'ютері зі встановленим 2-м часовим поясом);*

MIME-Version: 1.0 *– версія стандарту, відповідно до якого створено цей лист;*

Content-Type: multipart/alternative *– формат змісту листа. Визначається тип інформації в листі та спосіб її відображення. Зокрема, встановлюється кодування листа, якщо використовується який-небудь національний набір символів;*

boundary="----= NextPart_000_0015_01C4C076.3170DA90" *– стандартизація розбивання великих листів на декілька частин. У полі «Content-Type» після значення «multipart/<subtype>» зазначається рядок – унікальний обмежувач фрагментів "boundary=<boundary string>". А потім перед кожним фрагментом пишеться цей рядок з двома мінусами попереду, а в кінці фрагментації – ще один рядок, який завершується такими ж двома мінусами.*

X-Priority: 3 *– пріоритет листа, позначений цифрами.*

X-MSMail-Priority *– нестандартне поле Microsoft – пріоритет листа. Буває «звичайним», «невідкладним» та «не невідкладним». Зазвичай використовуються слова: «Normal», «Urgent», «Non-urgent». Може впливати на швидкість обробки та передачі листа різними проміжними поштовими системами;*

X-Mailer: Microsoft Outlook Express 5.50.4927.1200 *– інформація про поштову програму, яка використовувалася для створення листа;*

X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4927.1200 *– інформація про фірму виробника програмного забезпечення;*

X-Spam: Not detected *– лист не визначено як спам.*

Лабораторне заняття «Захист від фішінгових атак»

Навчальна мета заняття: ознайомлення з принципами фішингових атак та протидії ним.

Час проведення: 1 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено**.

Фішінг (англ. *fishing* – рибна ловля) – одержання доступу до конфіденційних даних користувачів, яке досягається шляхом проведення масових розсилань електронних листів від імені популярних брендів, наприклад, від імені соціальних мереж (Facebook, Twitter, Instagram), банків (Приватбанк, Ощадбанк), інших сервісів (Google.com). У листі часто міститься пряме посилання на сайт, який зовні складно відрізнити від справжнього. Опинившись на такому сайті, користувач може повідомити інформацію, що дозволяє одержати доступ до облікових записів тощо.

Фейк (Fake) – точна копія головної сторінки (або будь якої іншої сторінки) оригінального сайту, яка використовується для фішінгу з метою отримання конфіденційних даних користувачів.

Для демонстрації техніки фішінгу можуть бути використані декілька способів. Скористаємося одним з них.

1. Створити фейкову сторінку.

Для створення фейку сайту можна скористатися такою технікою:

- завантажити оригінальну сторінку сайту з формою авторизації;
- відкрити вихідний код оригінальної сторінки (наприклад, з використанням правої кнопки миші);
- скопіювати вихідний код сторінки в текстовий файл та назвати його index.html.

2. Для розміщення сторінки в мережі слід завантажити утиліту ngrok. Для роботи з утилітою ngrok слід зареєструватися та отримати токен відповідно до інструкції (https://dashboard.ngrok.com/get-started/setup).

Запустити її з командного рядка:

ngrok http 80

Завантажити набір Uniform Server для створення та управління сайтами та привести його у готовність.

Створити в папці UniServerZ\www каталог з назвою сайту скопійованої сторінки.

Розмістити в папці www/назва_сайту скрипти сайту.

Запустити UniController (рис. 1).

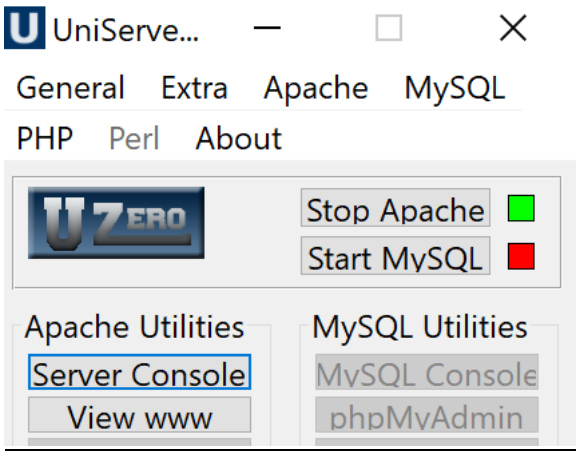


Рис. 1. Запуск Uniform Server

Перевірити роботу сайту.

Одним з додаткових інструментів фішингу може бути телефонування жертві з підміненого номера (Caller ID Spoofing), приклад налаштування та результат якого зображено на рис. 2.

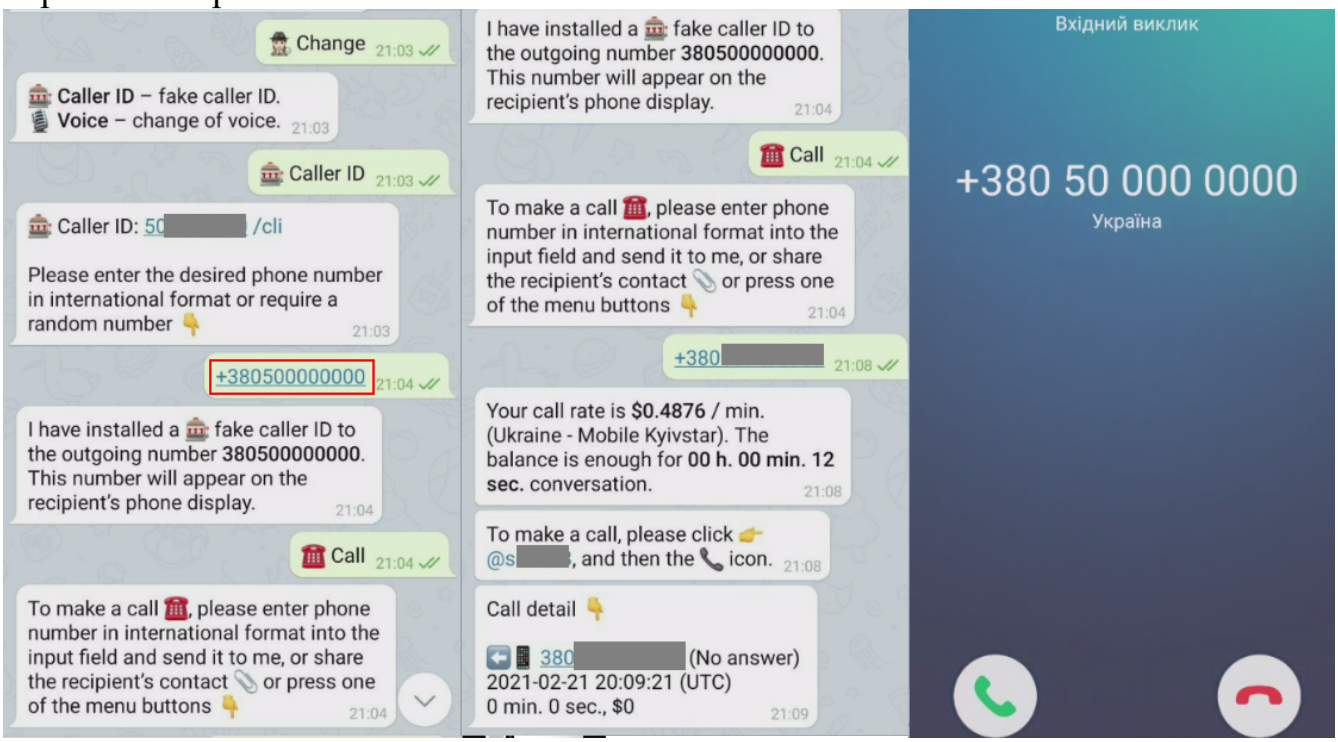


Рис. 2. Caller ID Spoofing

Для того, щоб захиститись від атак подібного виду, потрібно уважно перевіряти повідомлення, які надходять, та користуватись антифішінговими інструментами. Відповідні інструменти нерідко вбудовано у браузери.

Лабораторне заняття «Безпечний перегляд вебсторінок та способи організації безпечного з'єднання в мережі»

Навчальна мета заняття: здійснити налаштування браузеру та встановлення додаткових плагінів для безпечного серфінгу в мережі; відпрацювати різні технології забезпечення з'єднання в мережі.

Час проведення __1 год__. Місце проведення: комп'ютерний клас_____.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет.

Перелік VPN-сервісів та проксі-серверів:
free-proxy.cz
vpnbook.com
protonvpn.com

Перегляд вебсторінок, як правило, здійснюється за допомогою програм-браузерів, найпоширенішими серед яких є Chrome та Firefox. В усіх сучасних браузерах присутнє меню налаштувань, за допомогою якого можна здійснити налаштування безпеки та конфіденційності (рис. 1).

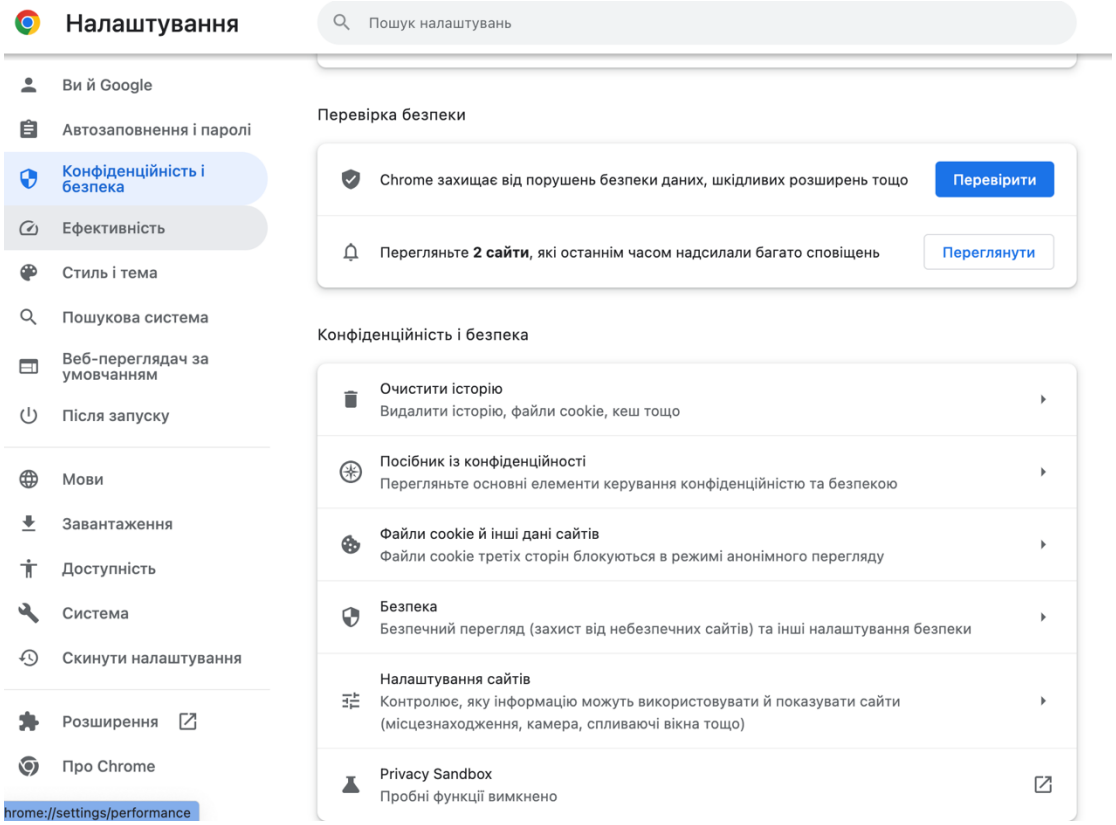


Рис. 1. Зліва направо налаштування безпеки у браузерах Firefox та Chrome

Якщо налаштування безпеки не повною мірою влаштовують користувача можна встановити додаткові плагіни. У якості плагінів за напрямом безпеки можна навести:
- AdBlock для блокування спливаючих вікон (https://adblockplus.org/ru/download);
- RequestPolicy для блокування міжсайтових запитів (https://www.requestpolicy.com/);
- Click&Clean для видалення тимчасових файлів у браузері (https://www.hotcleaner.com/).

1. Налаштуйте параметри безпеки та конфіденційності браузера. Поясніть свій вибір налаштувань.

2. Встановіть додаткові плагіни, описані в матеріалах до заняття. Опишіть порядок їх використання.

Для налагодження безпечного з'єднання з віддаленими ресурсами може бути застосовано проміжні убезпечуючі механізми, як-от: проміжні проксі- або VPN-сервери. Для демонстрації роботи таких серверів можна здійснити таке.

Проксі-сервери

Відкрити сторінку http://free-proxy.cz/en/web-proxylist/, після чого обрати будь-який проксі-вебсервер. Ввести у відповідному вікні адресу hidemyna.me/ua/what-is-my-ip або 2ip.ua. Оцінити одержані результати (рис. 2).

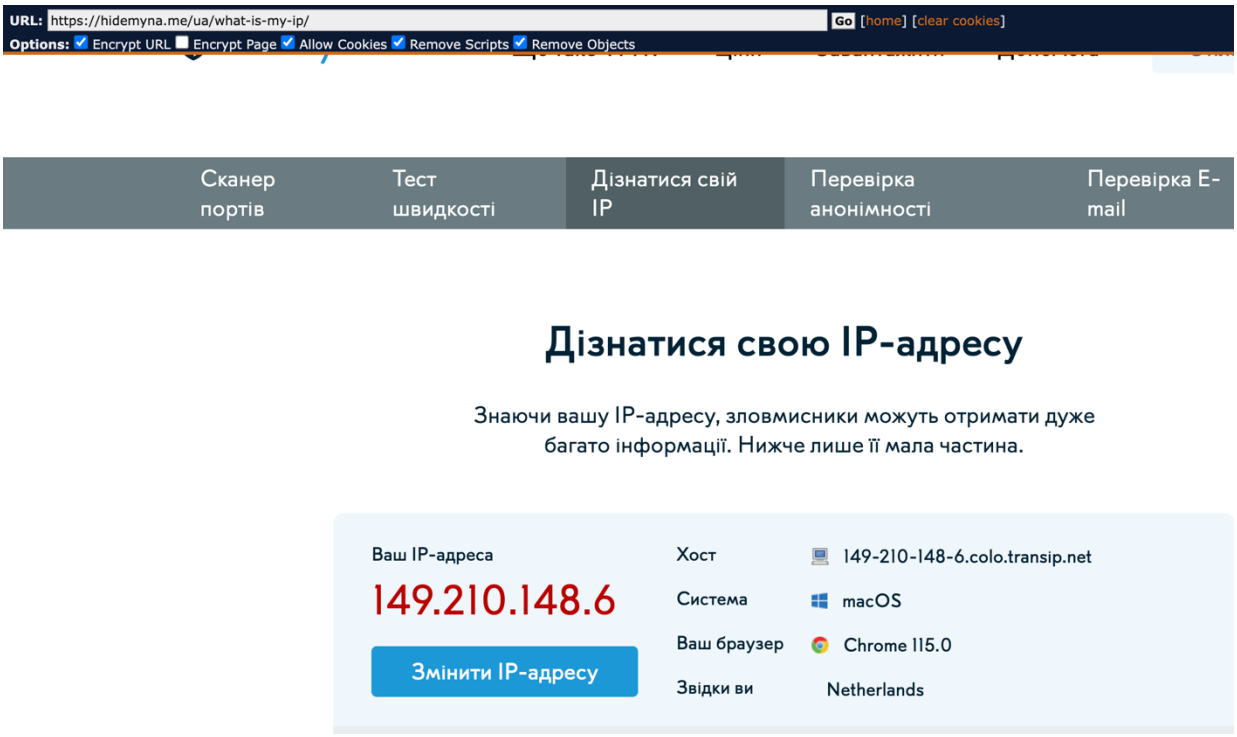


Рис. 2. Результат використання проксі-серверу

VPN-сервери

На відміну від проксі-серверів, які працюють за окремими портами, VPN-сервери надають можливість організації повноцінного захищеного з'єднання між користувачем та відповідними ресурсами. Для користування VPN-сервером потрібно знати його налаштування та відповідні автентифікаційні дані.

Як правило, налаштувати відповідне підключення можна без необхідності встановлення додаткового програмного забезпечення. Для цього, наприклад, у системі Windows 10 слід відкрити «Центр управління мережами та спільним доступом» та створити нове з'єднання.

Далі слід вказати адресу VPN-сервера та перейти у розділ «Зміна параметрів адаптера» та двічі натиснути на новоутвореному з'єднанні. Після цього слід ввести відповідне ім'я користувача і пароль та дочекатися з'єднання.

Більш універсальний спосіб налаштування VPN-з'єднання полягає у використанні спеціальних програм для організації такої діяльності. З цією метою може бути використано, наприклад, безкоштовний застосунок OpenVPN, який можна завантажити за адресою: https://openvpn.net/community-downloads/.

Після встановлення програми відповідні файли налаштування з'єднання записуються у папку Config програми OpenVPN. Запустивши програму слід обрати відповідну конфігурацію та під'єднатися до VPN-сервера.

Альтернативним способом налаштування VPN є застосування окремих програмних клієнтів від надавачів послуг VPN. У якості прикладу наведемо порядок підключення Proton VPN (protonvpn.com). З метою використання відповідного застосунку слід завести обліковий запис на

сайті protonvpn.com та завантажити застосунок для відповідної операційної системи (account.protonvpn.com/downloads).

У подальшому потрібно авторизуватисця у завантаженому застосунку та просто обрати потрібний спосіб підключення (рис. 3).

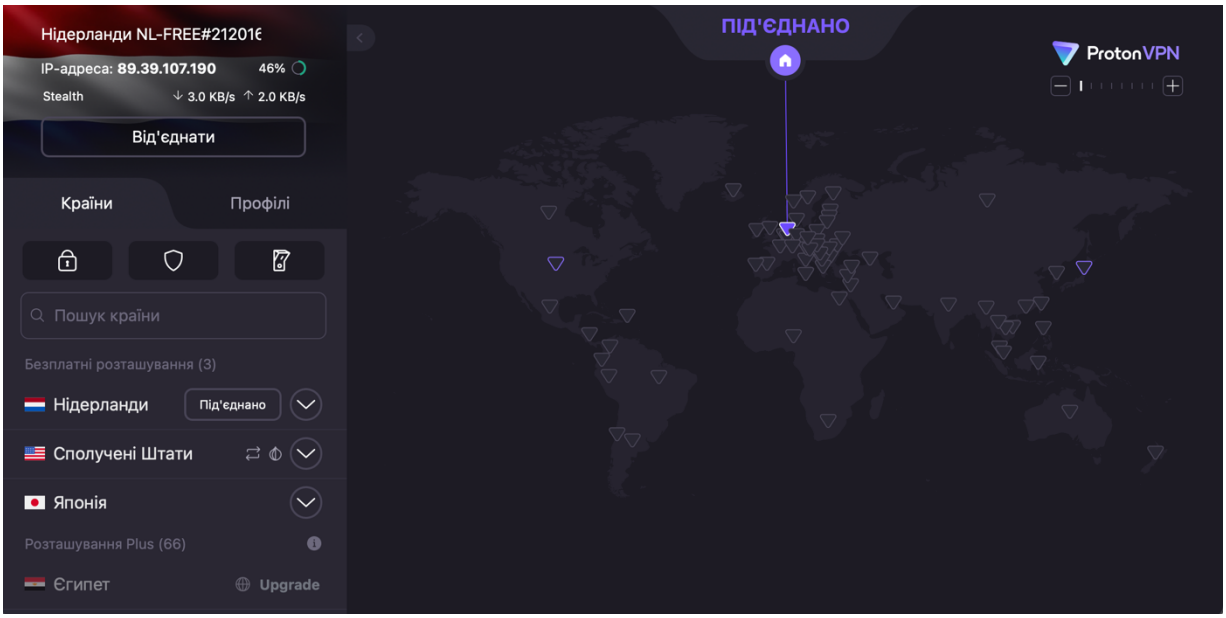


Рис. 3. Зовнішній вигляд клієнту Proton VPN

1. Відпрацювати підключення через одиничний та ланцюжок проксі-серверів.
2. Відпрацювати принаймні два способи налаштування VPN-з'єднання: 1) через налаштування параметрів мережного підключення операційної системи та 2) за допомогою VPN Client).
3. Переконатися у зміні параметрів виходу в мережу (наприклад, скориставшись сайтом 2ip.ua).
4. Встановити Firewall та антивірус ZoneAlarm.

Лабораторне заняття «Накладання електронного підпису»

Навчальна мета заняття: відпрацювати різні технології забезпечення з'єднання в мережі.

Час проведення: 1 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено**.

Реквізитом електронного документа є ***електронний підпис*** – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються та використовуються ним як підпис. Електронний підпис накладається за допомогою *особистого ключа* та перевіряється за допомогою *відкритого ключа*.

Отже, ***особистий ключ*** – це параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів, а ***відкритий ключ*** – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів.

Загальна схема накладання електронного підпису наведена на рис. 1, а його перевірки – на рис. 2.

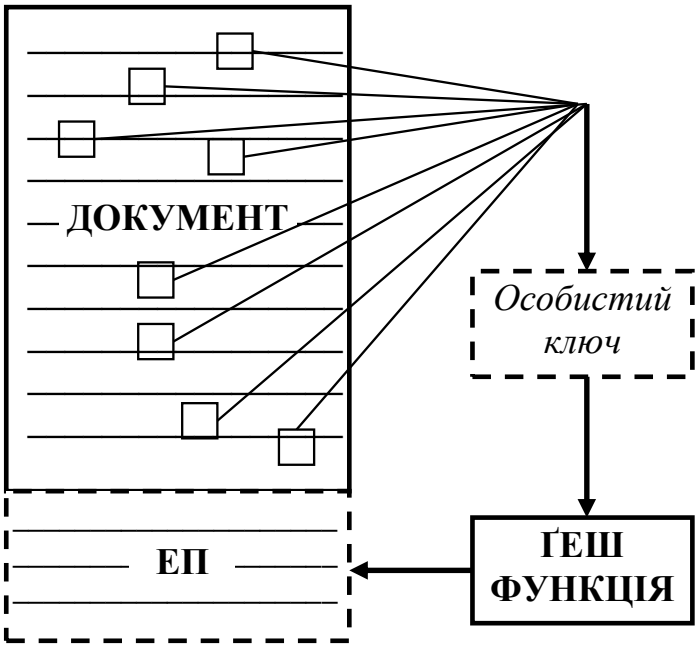


Рис. 1. Приблизна модель накладання електронного підпису

Рис. 2. Приблизна модель перевірки електронного підпису

Накладання електронного підпису не забезпечує конфіденційності документа, тобто його зміст **не шифрується**, але при цьому можна впевнитись у *цілісності* документа й *ідентифікувати його підписувача*.

Одним із швидких способів організації роботи з електронним підписом можна описати таким чином:

1. Одержати ключі електроннного підпису через електронний кабінет у банку. Наприклад, авторизуватись в системі Приват24 та в меню Усі послуги → Бізнес → Електронний цифровий підпис → Завантажити сертифікат згенерувати відповідні файли, потрібні для безпечного електронного документообігу. При виконанні цього завдання може знадобитися встановлення додаткових плагінів для браузера Google Chrome.

2. З використанням ресурсу sign.diia.gov.ua накласти електронний підпис на довільний файл. За допомого сервісу sign.diia.gov.ua/verify перевірити цілісність документу. Змінити підписаний файл. Провести повторну перевірку.

3. З використанням електронного підпису авторизуватись на порталі електронних послуг пенсійного фонду (portal.pfu.gov.ua). Перевірити відомості про свої відрахування.

4. З використанням електронного підпису авторизуватись в електронному кабінеті на потралі Державної фіскальної служби України (cabinet.sfs.gov.ua). Перевірити відомості про свої доходи.

Лабораторне заняття «Двофакторна автентифікація поштового облікового запису. Менеджер паролів»

Навчальна мета заняття: відпрацювати навички налаштування двофакторної автентифікації для різних облікових записів та використанння менеджеру паролів.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», смартфони або телефони у слухачів.

Порядок проведення заняття

Створити безкоштовні особисті поштові облікові записи в доменах gmail.com та protonmail.com.

Налаштувати двофакторну автентифікацію через Google Authenticator для облікових записів gmail.com та protonmail.com.

Встановити і налаштувати менеджер паролів KeePass.

Для облікового запису gmail.com

Перейти у розділ «Ваш обліковий запис» – «Безпека» – «Як ви входите в обліковий запис Google». Обрати «Двохетапна перевірка» – «Розпочати» (рис. 1).

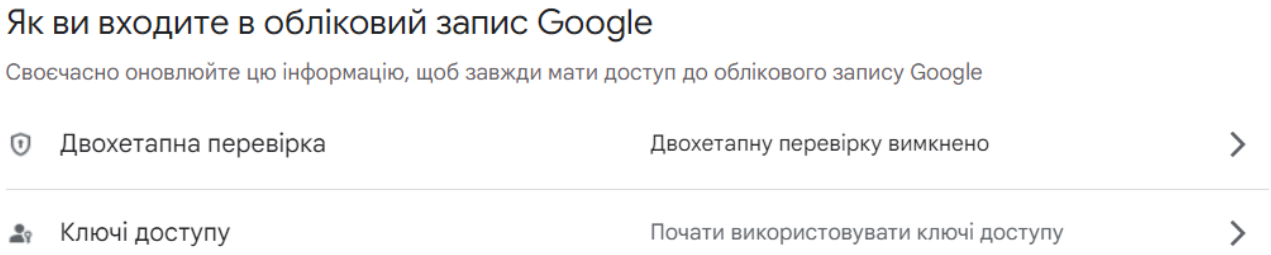
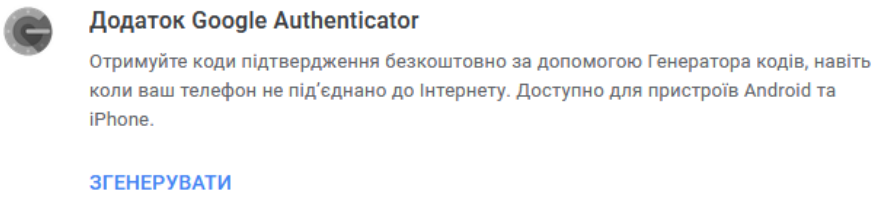


Рис. 1. Розділ налаштувань двохетапної перевірки

Обрати автентифікацію через коротке текстове повідомлення і зареєструвати особистий телефон через отримання коду в sms і вводу його у відповідному полі налаштувань.

Знову увійти в «Безпека» – «Вхід в обліковий запис Google» – «Двоетапна перевірка» – «Розпочати» та додати інші варіанти другого етапу перевірки, щоб підтверджувати свою особу, а саме «Додаток Google Authenticator». Завантажити за наданим посиланням у смартфон додаток «Генератор кодів Google» (рис. 2) та дотримуйтесь інструкцій щодо його налаштування.



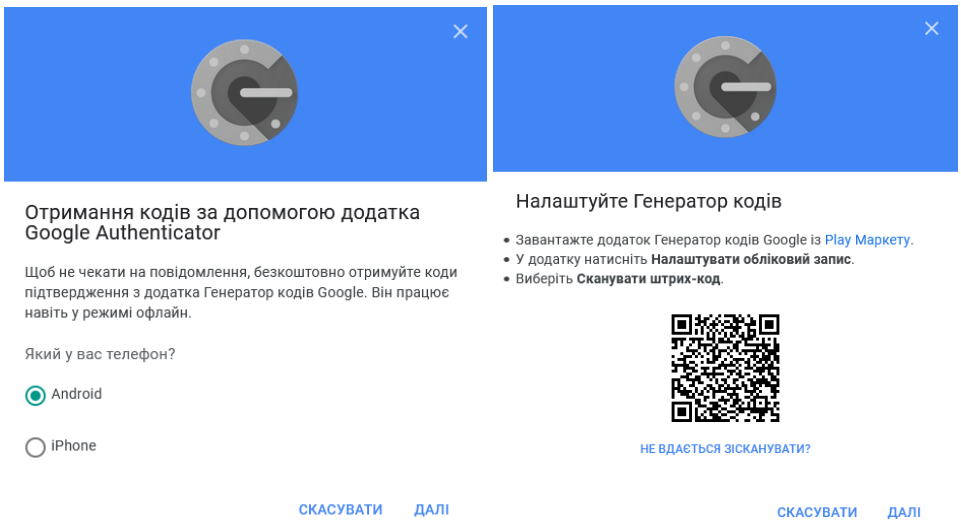


Рис. 2. Інструкції майстру налаштувань Google Authenticator

Після закінчення налаштувань вийти із облікового запису та пройти вже двоетапну автентифікацію.

Для облікового запису protonmail.com

У поштовому обліковому записі protonmail перейти у розділ «Налаштування» – «Обліковий запис і пароль» – «Увімкнути двоетапну перевірку» (рис. 3).

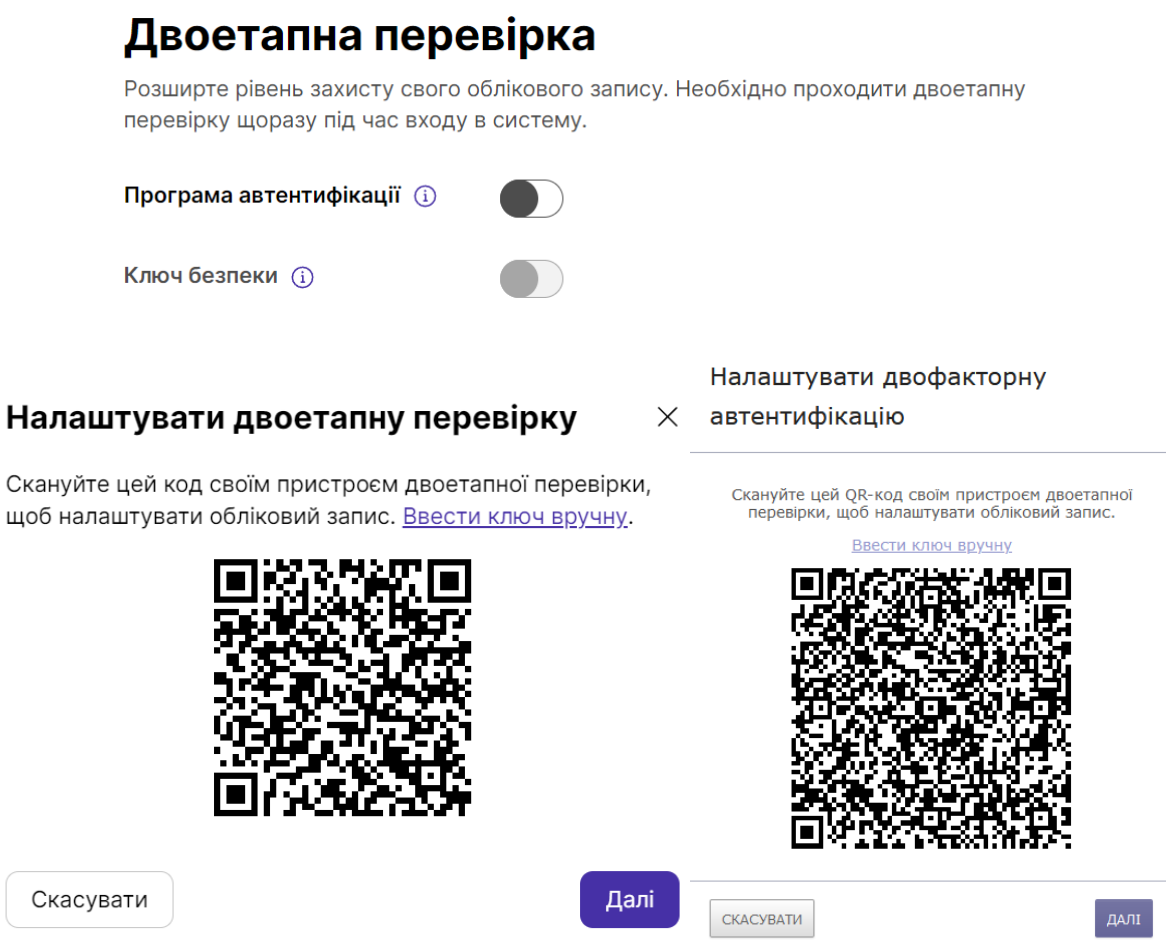


Рис. 3. Інструкції майстра налаштувань двофакторної автентифікації

Скористатися вже встановленим у смартфоні застосунком Google Authenticator (встановлюється з Google Play або App Store) і налаштувати двоетапну автентифікацію. Вийти із облікового запису та пройти вже двоетапну автентифікацію.

Для облікового запису gmail.com

Перейти у розділ «Ваш обліковий запис» – «Безпека» – «Як ви входите в обліковий запис Google». Вибрати «Ключі доступу» – «Почати використовувати ключі доступу» - «Створити ключі доступу» (рис. 4), де буде зазначений мобільний пристрій Android, на якому вже автоматично створені ключі і активний відповідний обліковий запис Google.

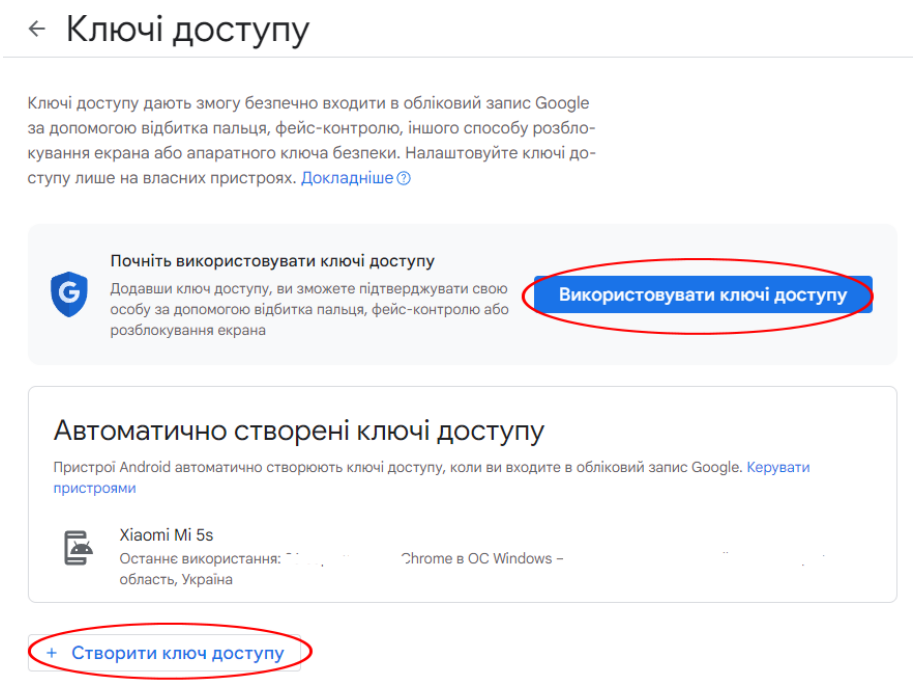


Рис. 4. Початкове вікно налаштування використання ключів доступу

Клікнути на опцію «Використовувати ключі доступу» для використання зазначеного пристрою (рис. 5) як засобу автентифікації через його розблокування і без введення паролю.

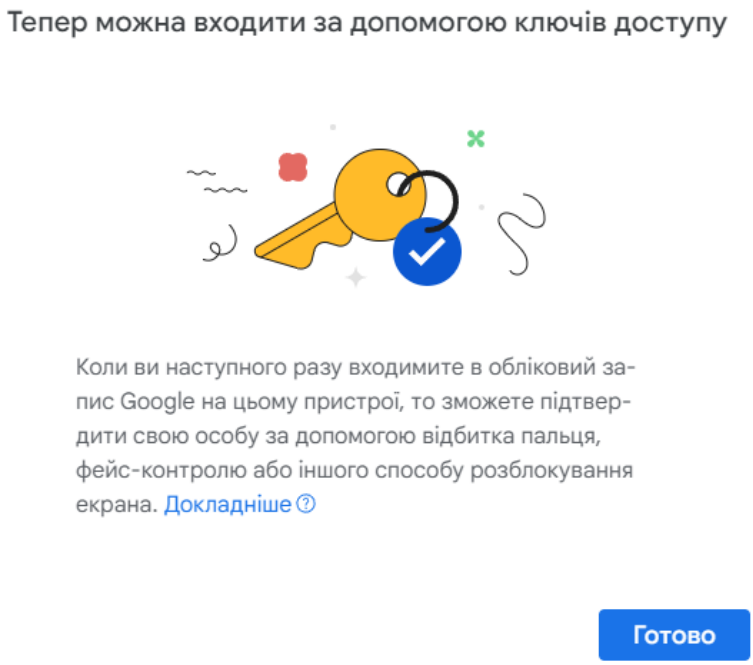


Рис. 5. Активація налаштування «Ключі доступу»

Якщо обрати опцію «Створити ключі доступу» (рис. 4), то можна ключі створити на іншому пристрої, обравши «Скористатись іншим пристроєм» - «Вибрати інший телефон або планшет» (рис. 6)

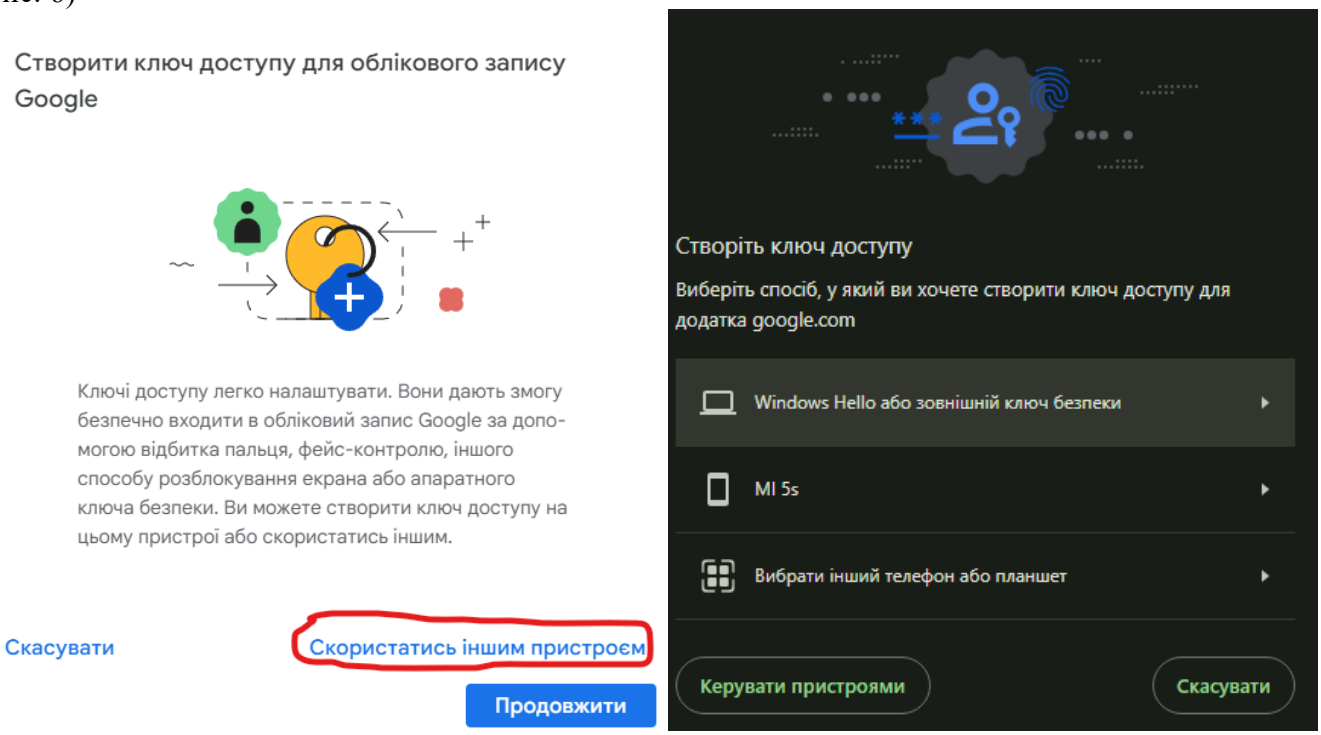


Рис. 6. Налаштування іншого пристрою для доступу в обліковий запис Google

Далі Chrome запропонує QR-код для зв’язування пристрою з комп’ютером, сканування якого ініціює створення на ньому відповідних ключів (рис. 7).

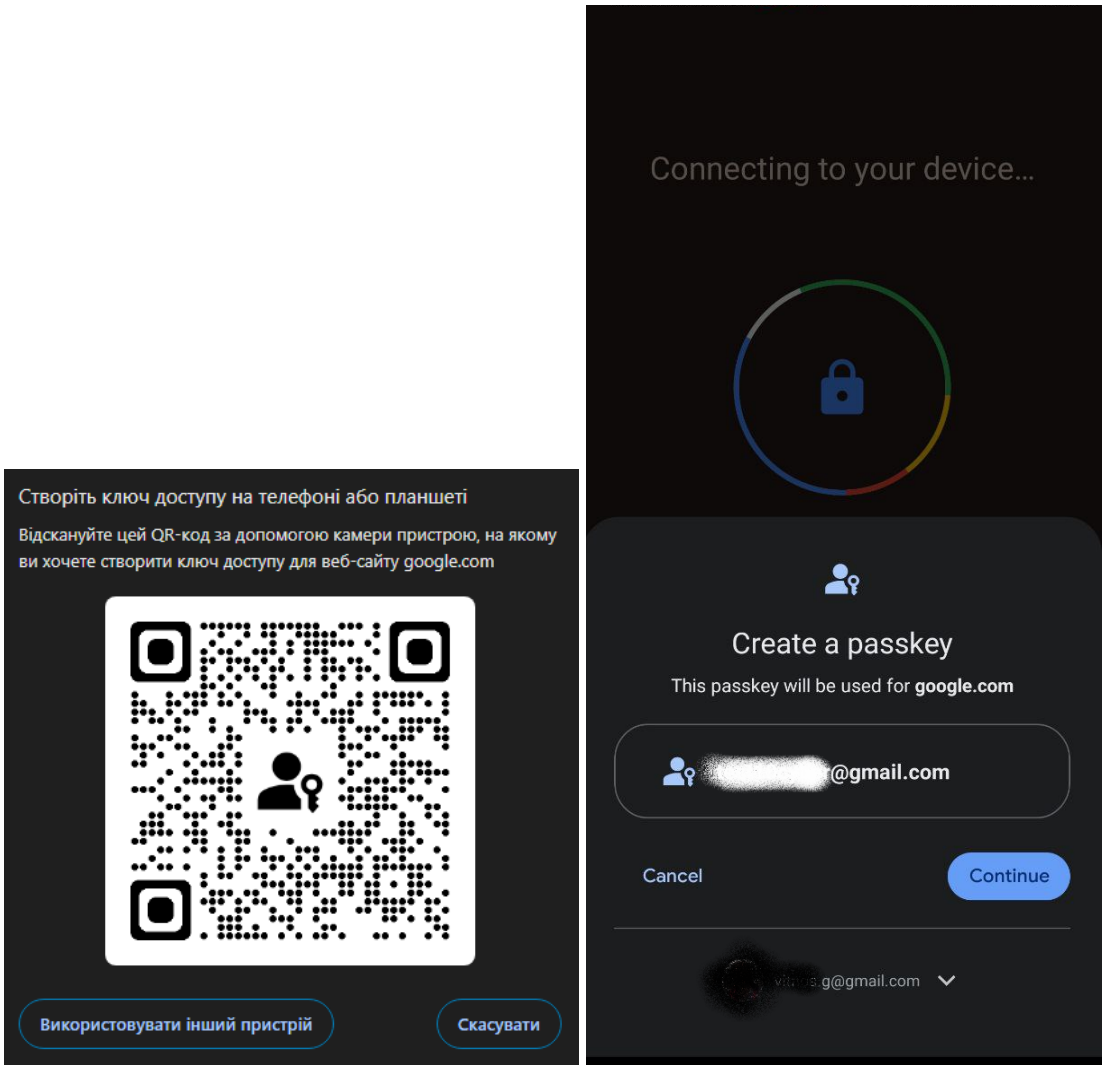


Рис. 7. Створення ключів доступу на мобільному пристрої через QR-код

Для перевірки автентифікації за ключами доступу вийти з облікового запису Google та спробувати знову ввійти, обравши «Спробувати інший спосіб» - «Використати ключ доступу» (рис. 8).

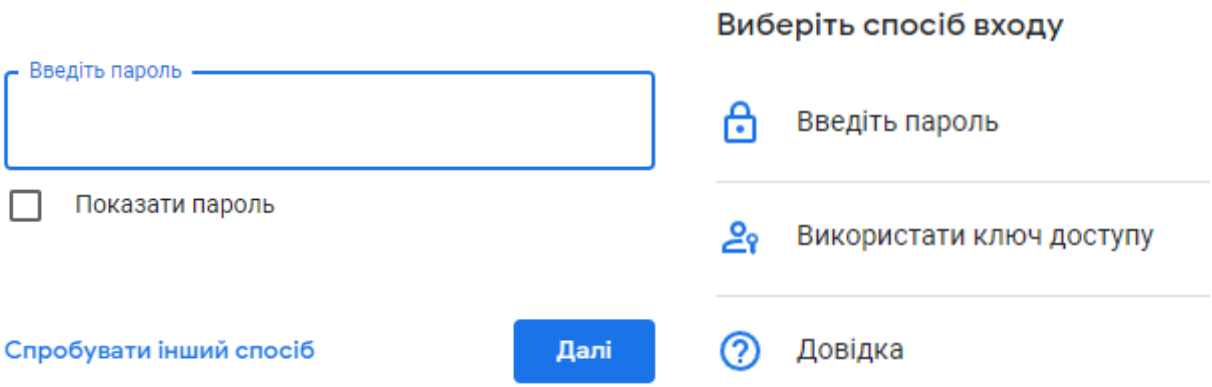


Рис. 8. Вибір автентифікації через ключ доступу

Завершити автентифікацію з використанням свого смартфону, в якому з’явиться запит відсканувати відбиток пальця, пройти фейс-контроль або розблокувати екран (рис. 9)

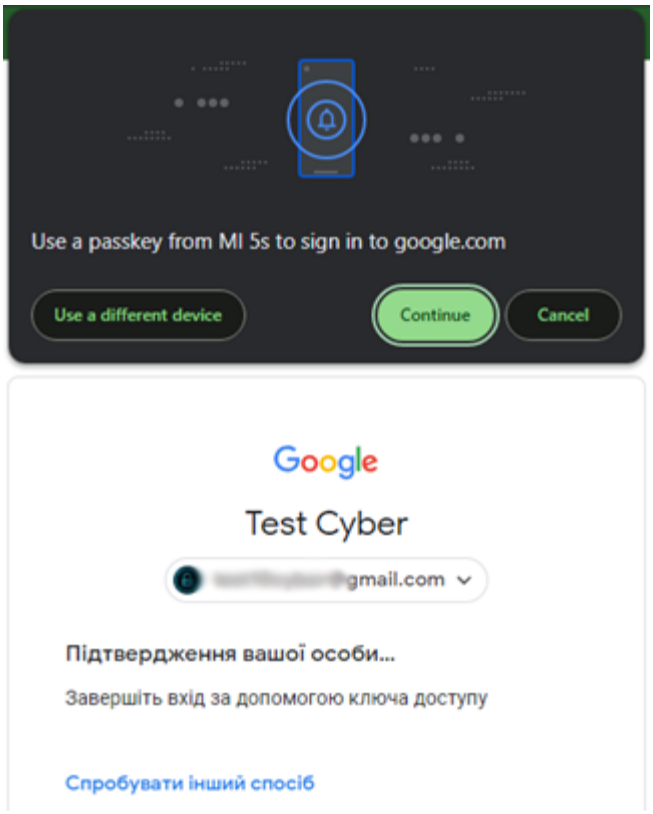


Рис. 9. Запит на продовження автентифікації через ключі доступу на смартфоні

Важливо. Коли створюється ключ доступу, то обирається можливість входу без пароля за допомогою ключа доступу, тому це можна робити лише на особистих пристроях. Навіть якщо вийти зі свого облікового запису Google, створивши ключ доступу на пристрої, то кожен, хто може розблокувати пристрій, зможе знову ввійти у ваш обліковий запис Google за допомогою ключа доступу.

Парольний менеджер KeePass.

Завантажити (https://keepass.info/index.html), встановити та запустити парольний менеджер KeePass Password Safe (рис. 10).

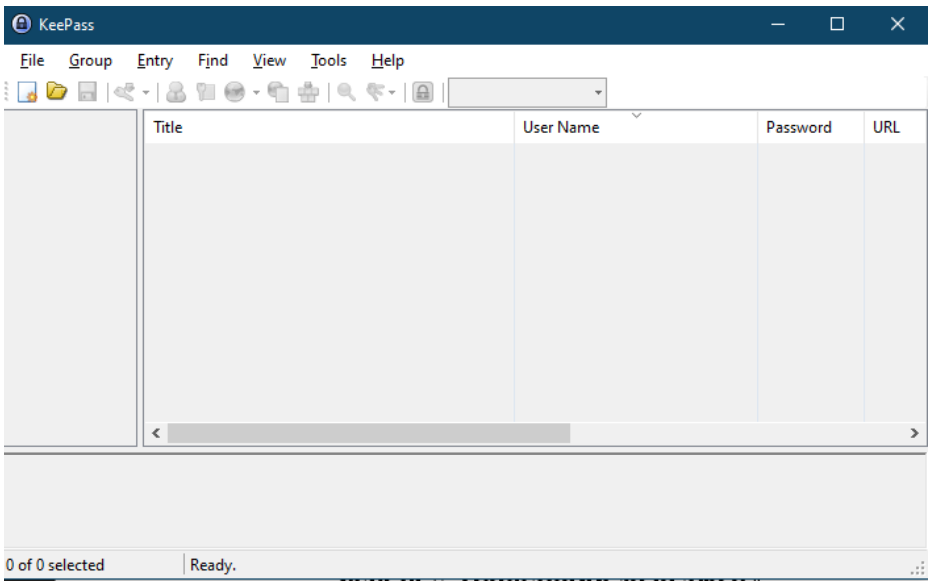


Рис. 10. Головне вікно KeePass

Комбінацією клавіш (Ctrl+N) створити та вказати місце зберігання файлу нової бази паролів (рис. 11).

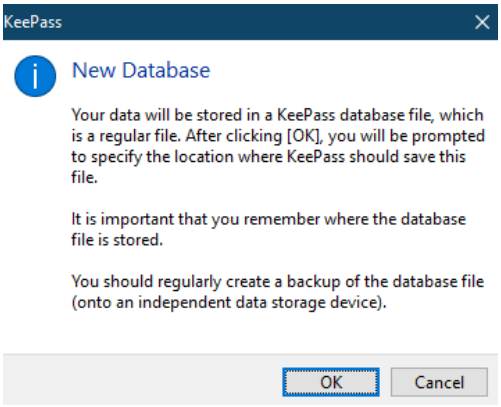


Рис. 11. Повідомлення щодо створення нової бази паролів

Придумати та запам’ятати майстер-пароль (парольну фразу) довжиною не менше 10-ти символів із використанням маленьких та великих літер, цифр та спеціальних символів. Ввести майстер-пароль (парольну фразу) та вибрати ім’я для бази паролів (рис. 12). Додатково можна роздрукувати основні дані щодо місця зберігання основної бази паролів, її резервної копії та підказки щодо майстер-пароля (рис. 13).

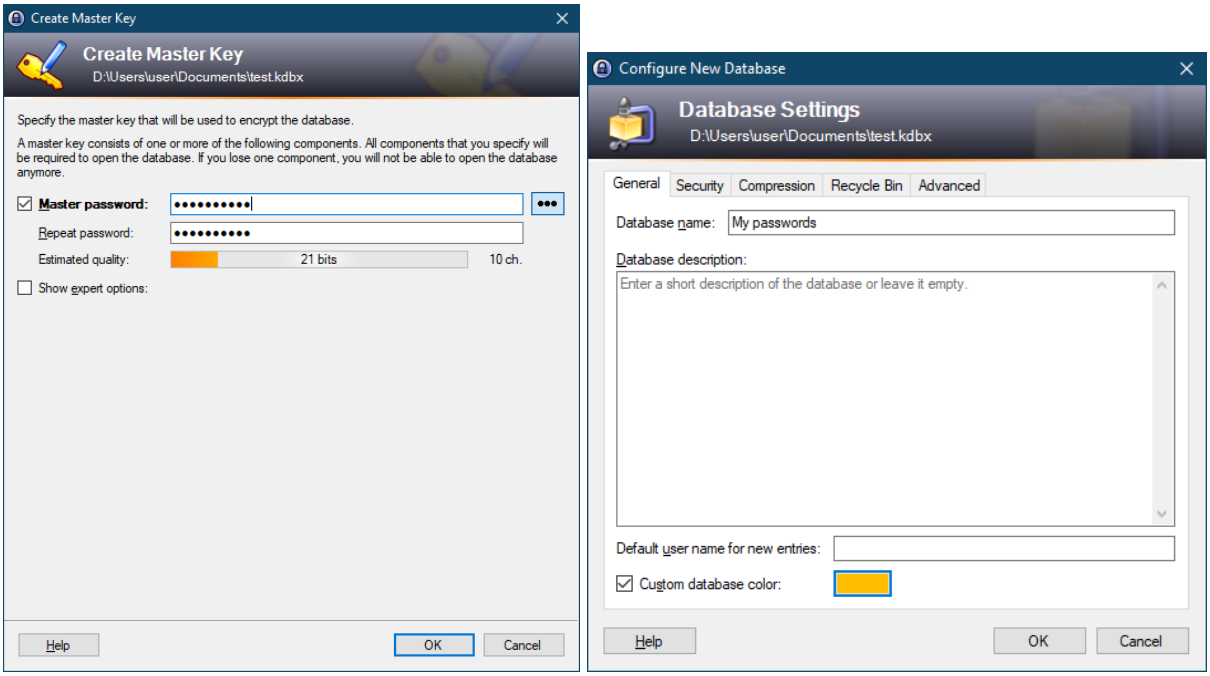


Рис. 12. Створення майстер-паролю та налаштування бази

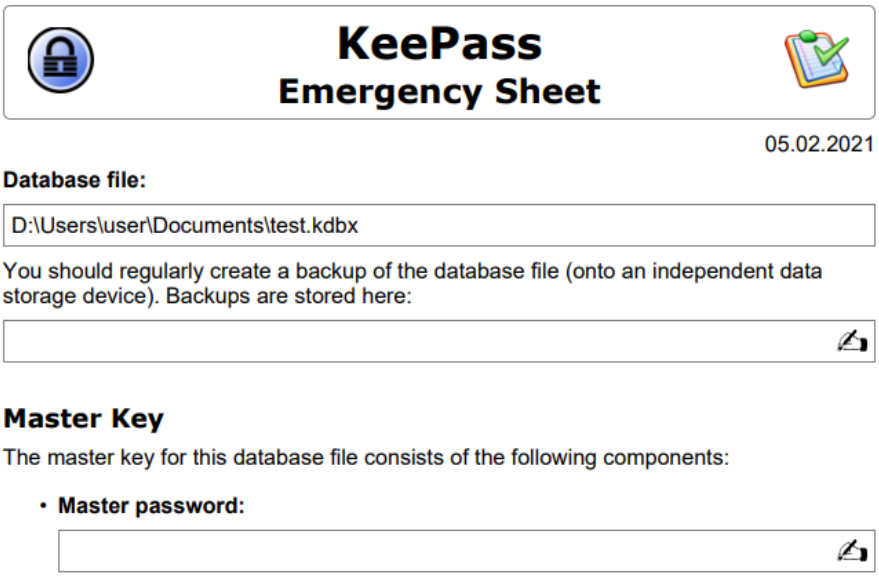


Рис. 13. Пам'ятка щодо місця зберігання основної бази паролів, її резервної копії та підказки щодо майстер-пароля

В основному вікні KeePass зліва обрати теку «eMail», створити новий запис (комбінація клавіш Ctrl+I), заповнити поля для свого поштового облікового запису, перейти у налаштування Генератора паролів і обрати довжину пароля та абетку символів, з яких буде генеруватися пароль (рис. 14). Завершити редагування, зберегти зміни (комбінація клавіш Ctrl+S) і переглянути створений запис (рис. 15).

Зверніть увагу, що деякі вебсервіси забороняють наявність в паролі спеціальних символів. У такому випадку, або після генерації паролю вручну видалити спеціальні символи або виключити їх із абетки налаштувань Генератора паролів.

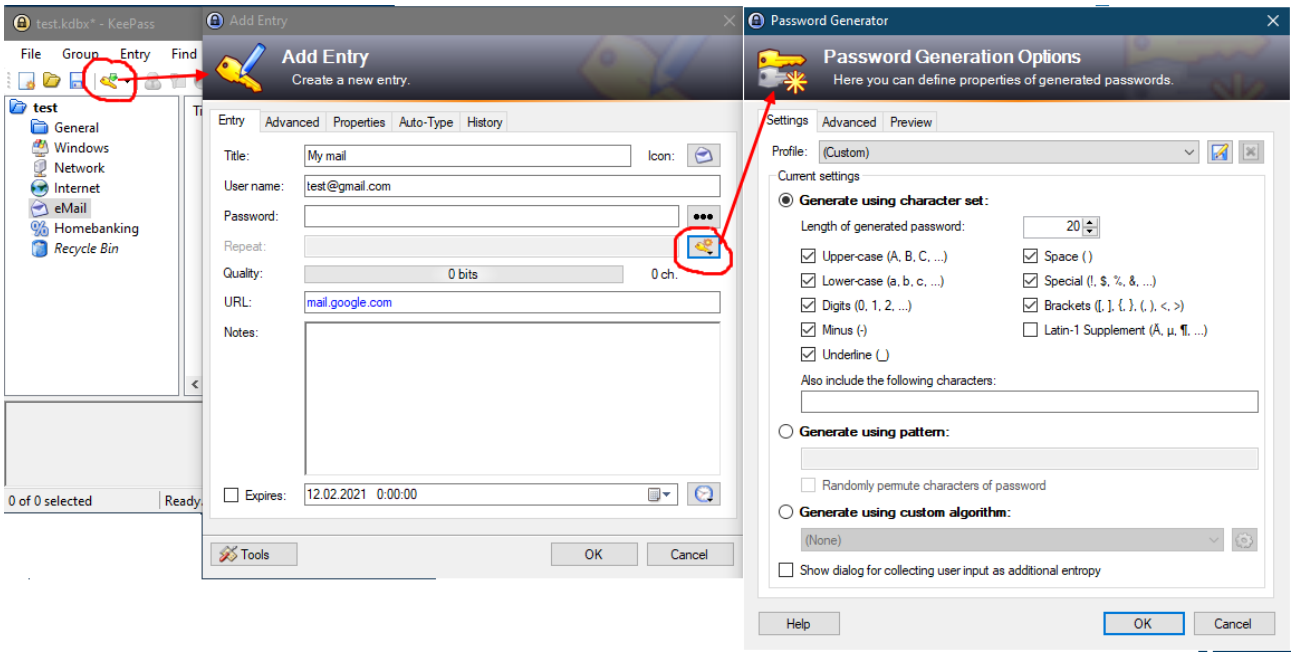


Рис. 14. Створення і налаштування параметрів нового запису у базі паролів

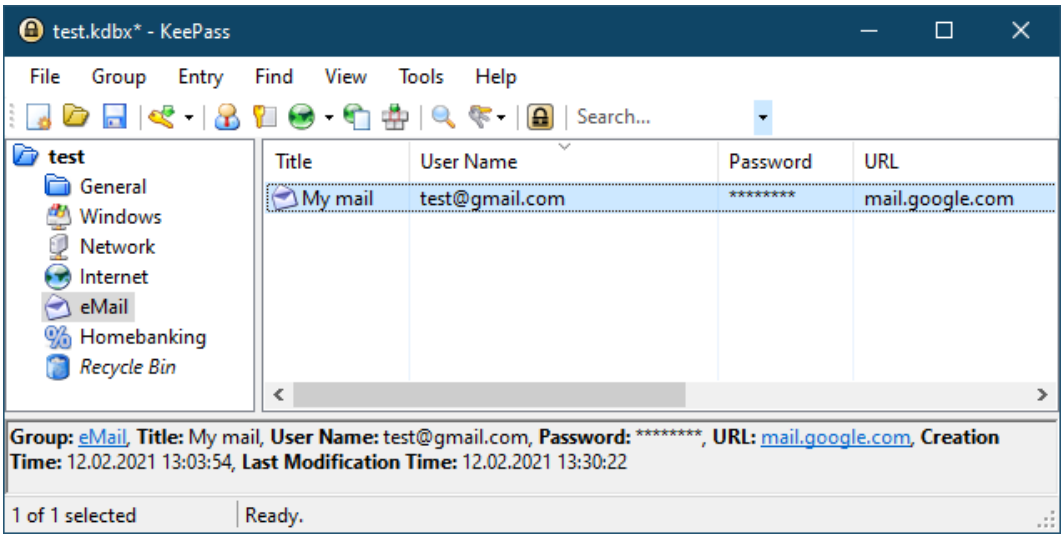


Рис. 15. Створений запис у базі паролів

Пройти автентифікацію в поштовому сервісі, використовуючи менеджер паролів. Для цього в KeePass обирається відповідний запис та почергово копіюється у буфер логін (комбінація клавіш Ctrl+B) та пароль (комбінація клавіш Ctrl+C), які почергово вставляються у відповідні поля форми автентифікації поштового сервісу.

Лабораторне заняття «Електронний підпис та шифрування повідомлень»

Навчальна мета заняття: отримати навички підписувати та зашифровувати повідомлення.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome».

Порядок проведення заняття

Виконати такі дії:

- встановити на свій флеш-накопичувач утиліту **gpg4usb**;
- згенерувати пару своїх ключів;
- експортувати свій публічний ключ в окремий файл *_pub.asc;
- обмінятися своїм публічним ключем з іншими;
- імпортувати у програму публічні ключі інших;
- створити повідомлення для співрозмовника, підписати повідомлення та зашифрувати його з використанням публічного ключа адресата;
- отримати підписане та зашифроване повідомлення, розшифрувати повідомлення та перевірити електронний підпис.

За посиланням https://www.gpg4usb.org/download.html вибрати та завантажити на особистий флеш-накопичувач архів утиліти gpg4usb. Розпакувати архів, запустити утиліту start_windows.exe та обрати зручну мову інтерфейсу (рис. 1).

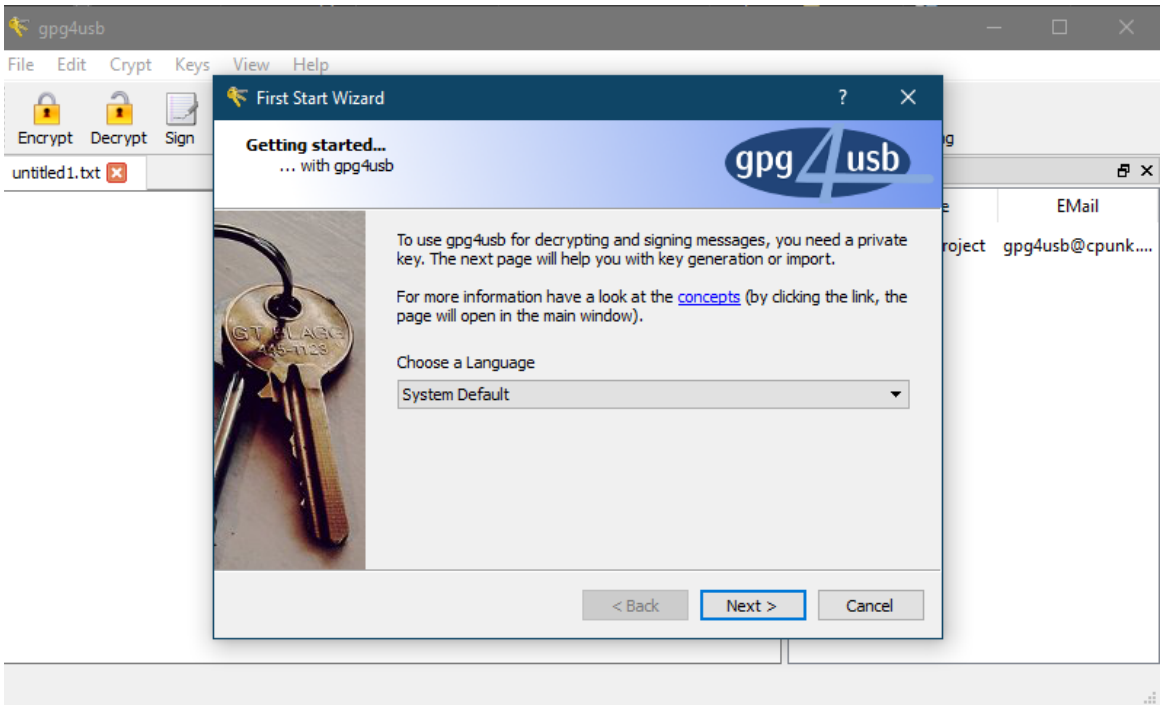


Рис. 1. Налаштування мови інтерфейсу gpg4usb

Далі клікнути на посилання «Створити нову ключову пару», обрати «Створити новий Ключ» та заповнити відповідні поля персональними даними (пароль згенерувати та зберегти у менеджері паролів). Завершити налаштування у майстрі першого запуску (рис. 2).

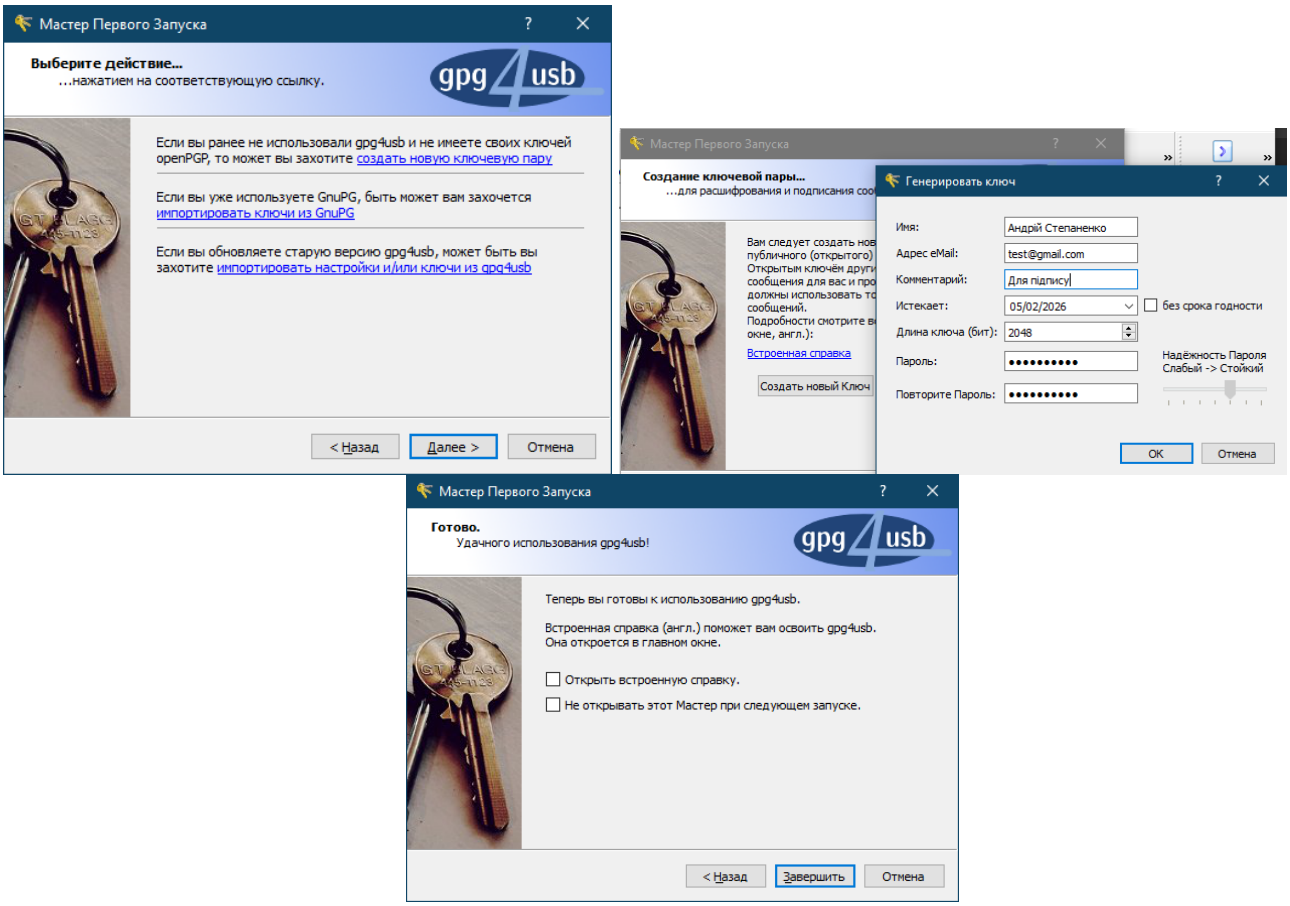


Рис. 2. Генерування ключів у майстрі першого запуску

Запустити «Менеджер ключів», обрати обліковий запис своїх ключів, вибрати «Експорт обраних ключів у файл» та зберегти свій публічний ключ (наприклад, Андрій Степаненко test@gmail.com(202AA4030C558985)_pub.asc) на флеш-накопичувач (рис. 3).

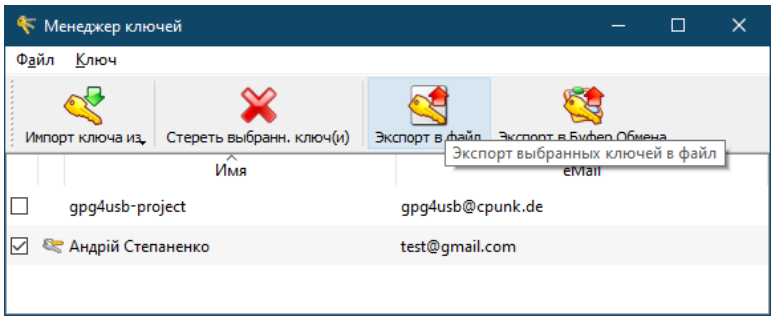
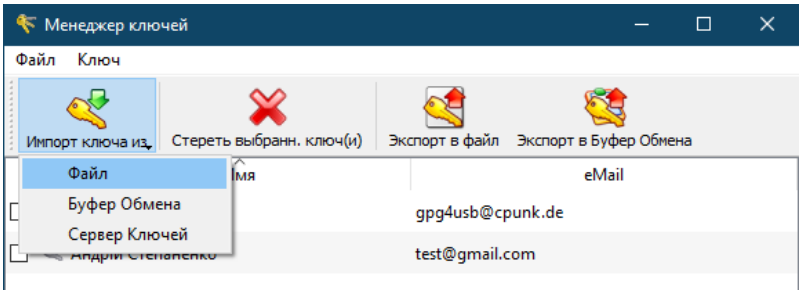


Рис. 3. Експорт публічного ключа

Слухачам обмінятися між собою своїми публічними ключами (Андрій Степаненко test@gmail.com(202AA4030C558985)_pub.asc) – це можна зробити пересиланням поштою або локальним копіюванням на свої носії.

У менеджері ключів здійснити імпорт у програму файлів публічних ключів, отриманих від інших слухачів (рис. 4).



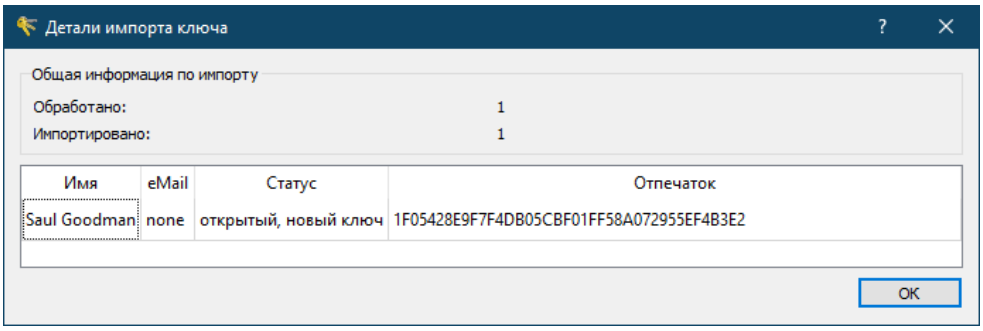


Рис. 4. Імпорт публічних ключів співрозмовників

Створити довільне повідомлення для співрозмовника, вказати дату, час та зазначити свій ключ у правому віконці програми. Обрати «Підписати» повідомлення, ввести пароль для свого приватного ключа та отримати підпис (рис. 5).

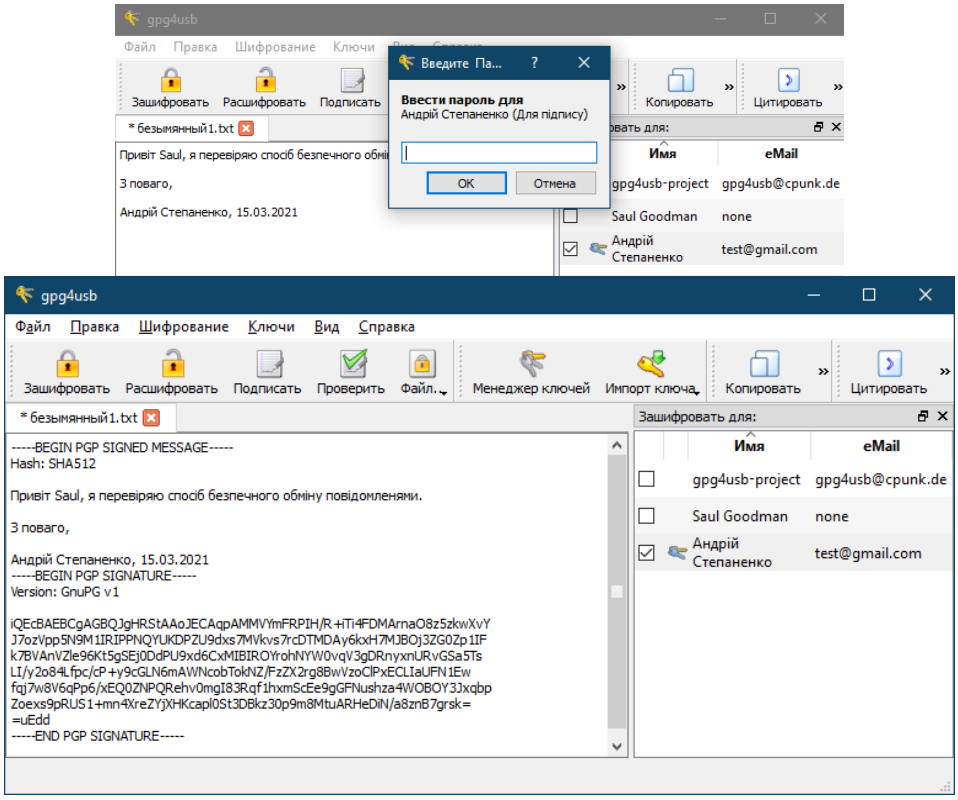


Рис. 5. Підпис повідомлення

Зняти позначку зі свого ключа та поставити на ключі співрозмовника у правому віконці програми, обрати «Зашифрувати» (рис. 6). Отримане зашифроване повідомлення відіслати своєму співрозмовнику.

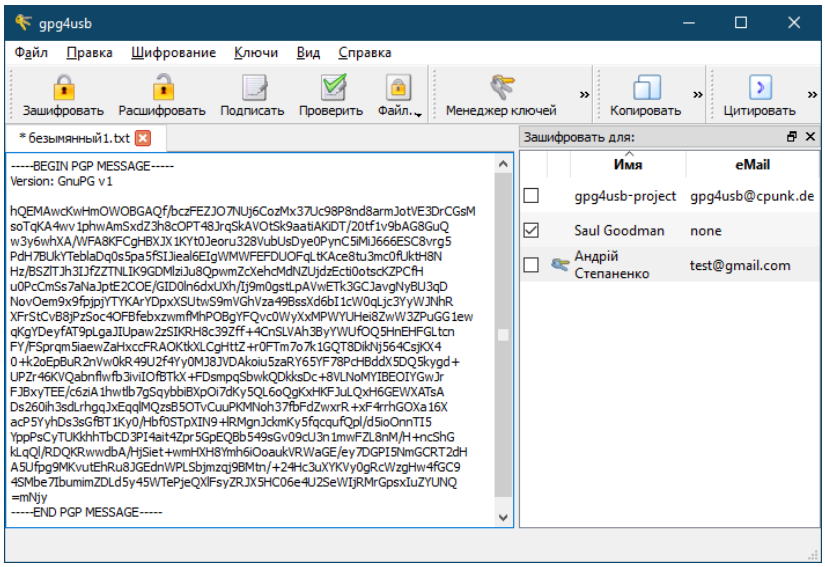


Рис. 6. Шифрування повідомлення

Співрозмовник, отримавши зашифроване повідомлення або копіює його зміст у буфер пам'яті та вставляє у порожнє поле текстового файлу gpg4usb, або відкриває його як текстовий файл в gpg4usb. Після чого у правому полі програми позначає рядок із зазначенням своїх ключів, обирає «Розшифрувати», вводить пароль до свого приватного ключа та отримує розшифроване повідомлення (рис. 7).

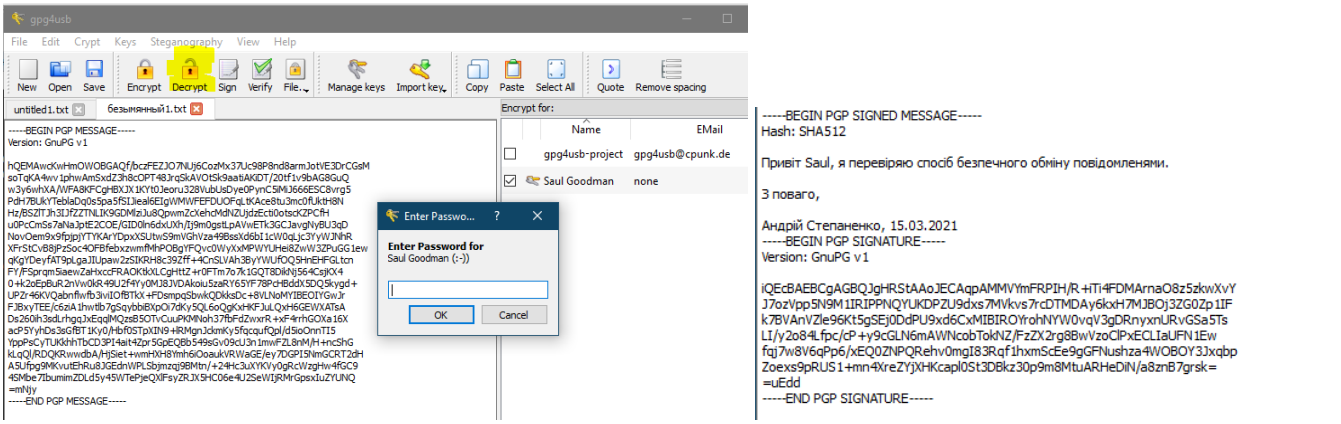


Рис. 7. Розшифрування повідомлення

У правому полі програми співрозмовник позначає рядок із зазначенням ключа відправника, обирає «Перевірити» та «Деталі» підпису (рис. 8). Виправити або додати у повідомленні одну літеру та повторити перевірку підпису у зміненому повідомлені (рис. 9).

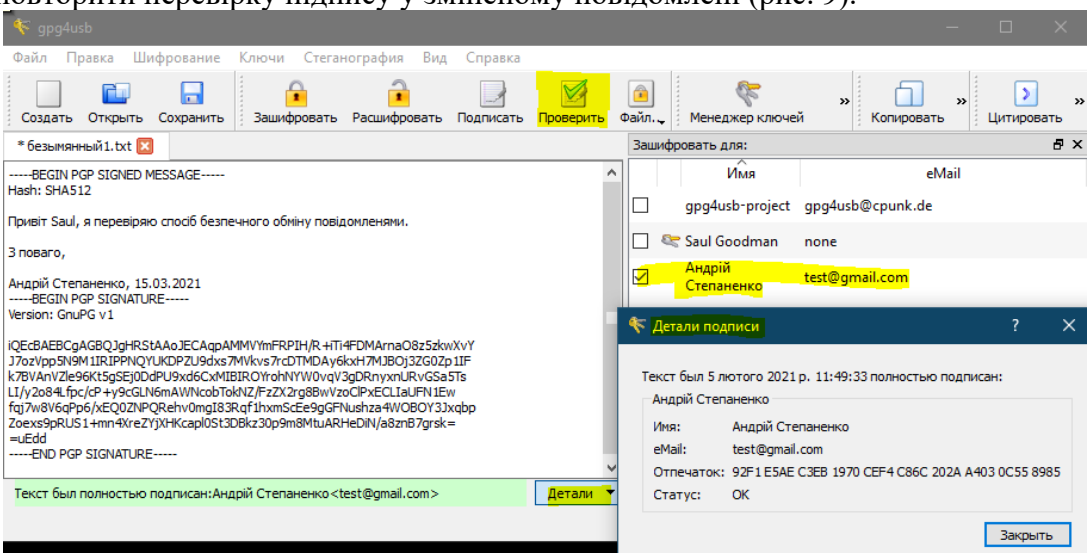


Рис. 8. Успішна перевірка підпису відправника повідомлення

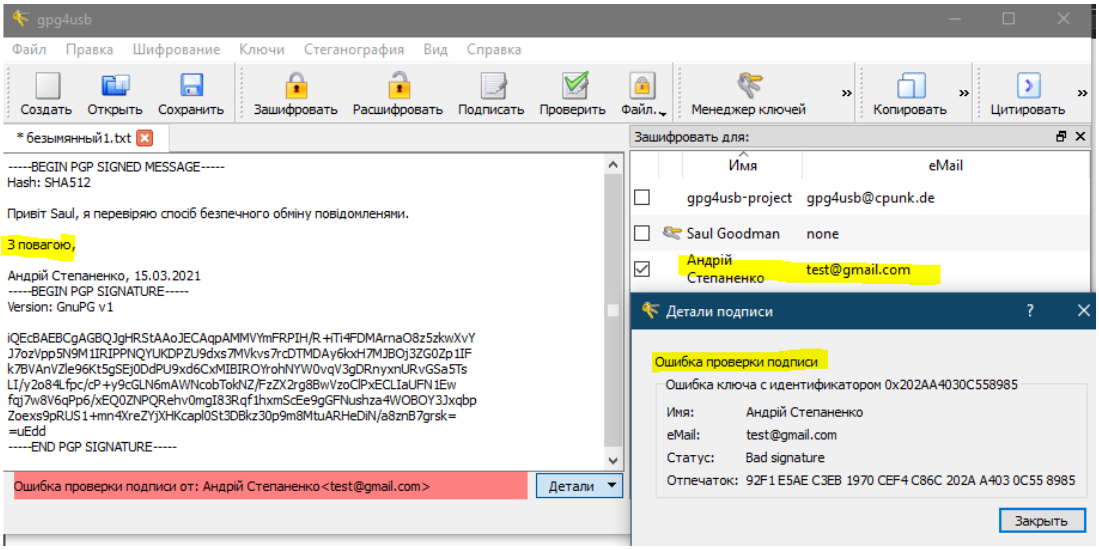


Рис. 9. Невдала перевірка підпису відправника повідомлення

Установити і налаштувати в обліковому записі Google розширення електронного підпису та шифрування. В обліковому записі ProtonMail здійснити налаштування інтегрованого сервісу електронного підпису та шифрування листів, які спрямовуються на зовнішні поштові домени. Після налаштувань переслати підписані та зашифровані листи між поштовими доменами protonmail.com та gmail.com. Переконатися у забезпеченні конфіденційності та цілісності такого листування.

Додати в Google Chrome розширення FlowCrypt: Encrypt Gmail with PGP (https://chrome.google.com/webstore/detail/flowcrypt-encrypt-gmail-w/bnjglocicdkmhmoohhfkfkbbkejdhdgc?hl=ua), клацнути на розширення та надати дозвіл FlowCrypt отримувати доступ до облікового запису Google (рис. 10).

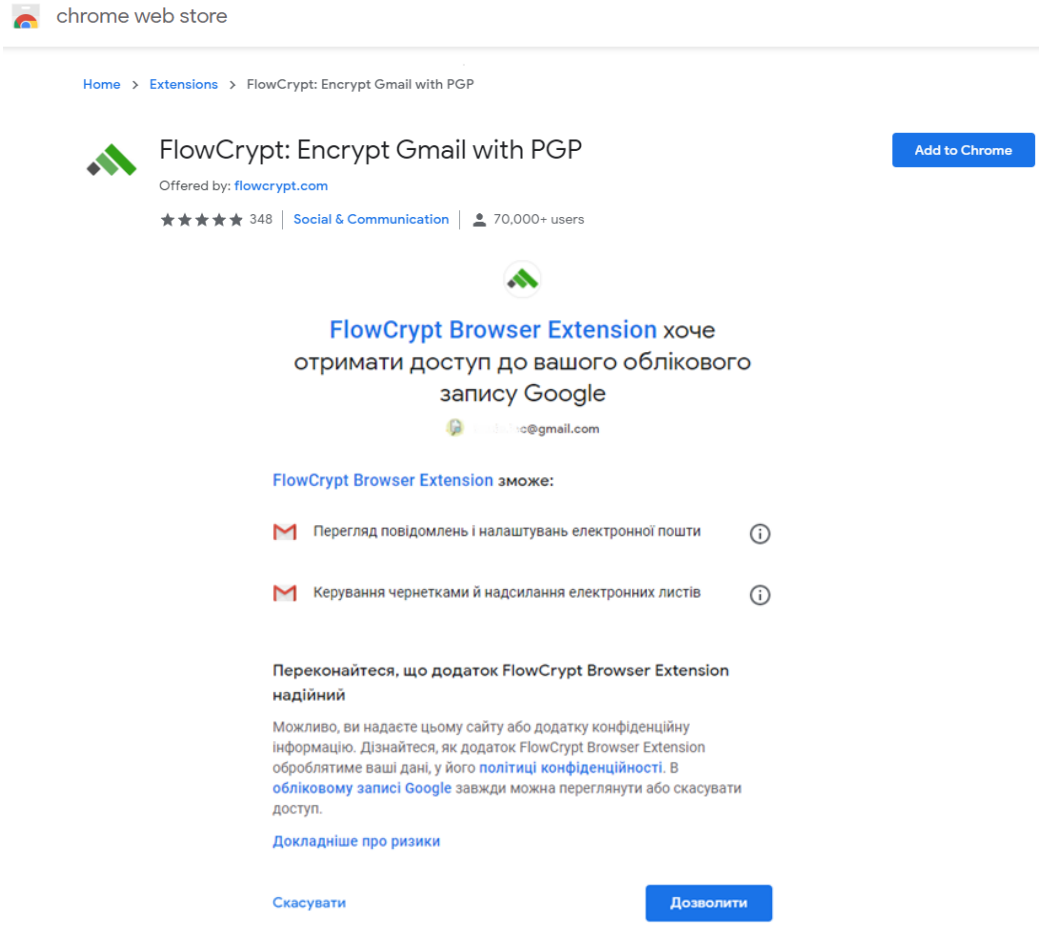


Рис. 10. Встановлення та надання дозволу FlowCrypt

У FlowCrypt згенерувати і зберегти ключі: обрати New encryption key, Encryption key type – RSA 2048bit – Create and save (рис. 11).

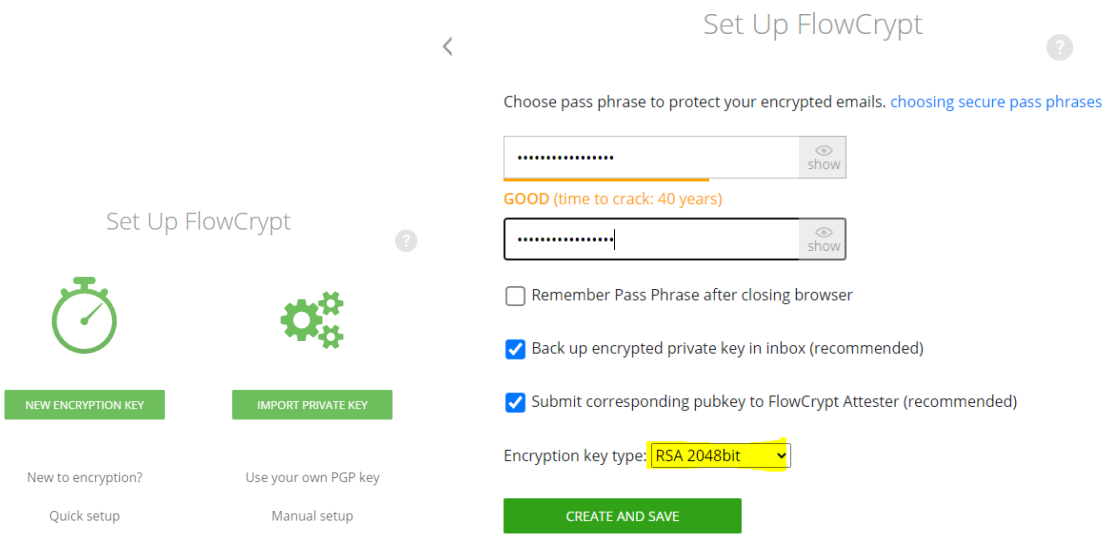


Рис. 11. Створення і збереження ключів для облікового запису

Після налаштувань розширення в поштовому клієнті з'явиться кнопка Secure Compose (рис. 12).

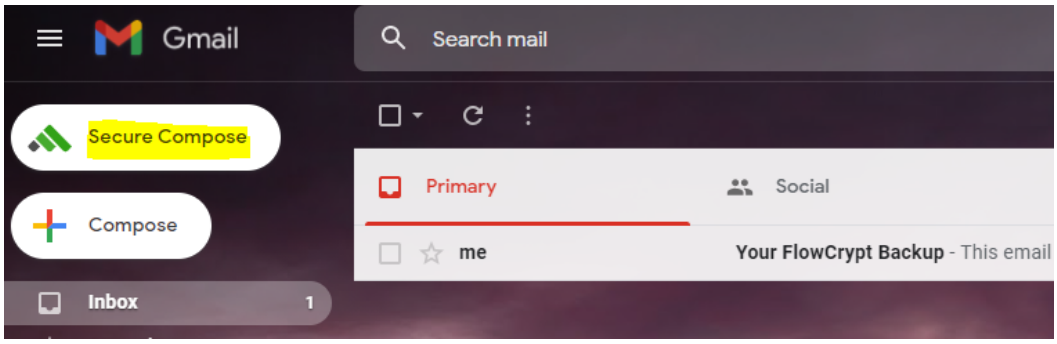


Рис. 12. Кнопка FlowCrypt Secure Compose

Авторизуватися у своєму обліковому записі ProtonMail. Перейти у «Налаштування» – «Безпека» і ввімкнути «External PGP Settings (optional)», Address Verification (optional) (рис. 22).

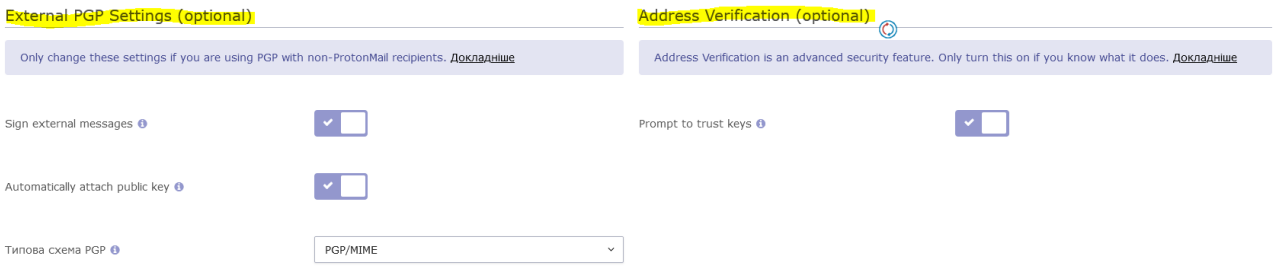


Рис. 13. Включення опцій підпису та шифрування

Відправити на адресу @gmail.com лист, до якого буде автоматично додано публічний ключ облікового запису @protonmail.com.

У @gmail.com після відкриття листа від @protonmail.com здійснити імпорт відкритого ключа @protonmail.com, та відповісти з підписом і шифруванням, натиснувши Secure Reply (рис. 23).

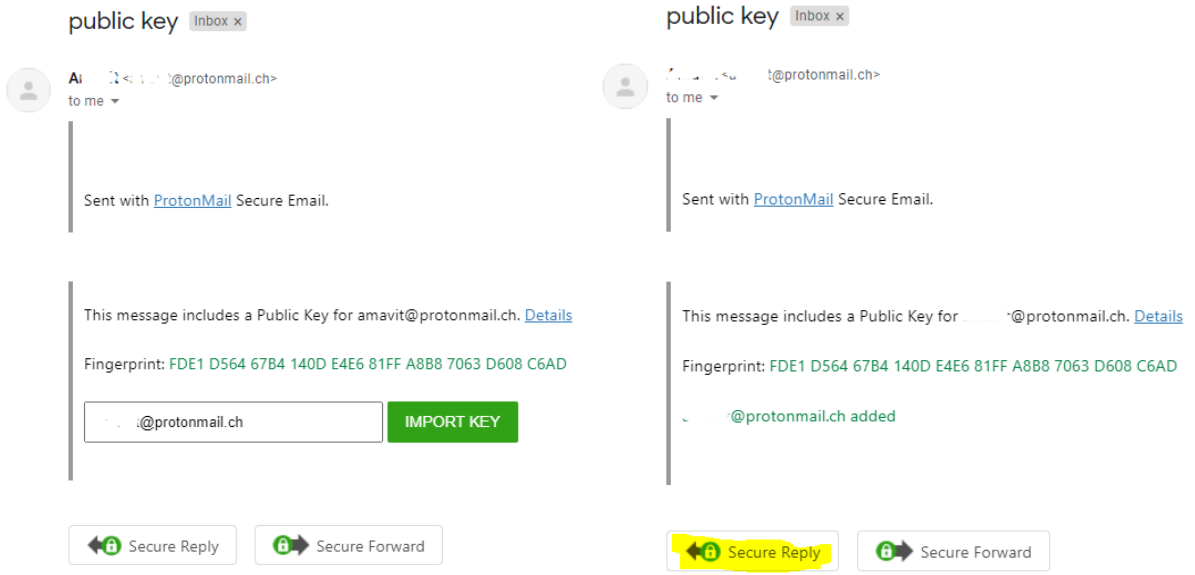


Рис. 14. Отримання публічного ключа та відповідь з підписом та шифруванням

У @protonmail.com буде автоматично розшифровано листа і перевірено підпис, але зазначено, що перевірка підпису була зроблена публічним ключом, який ще не є довіреним. Натиснути «ДОВІРЕНИЙ КЛЮЧ» (рис. 15).

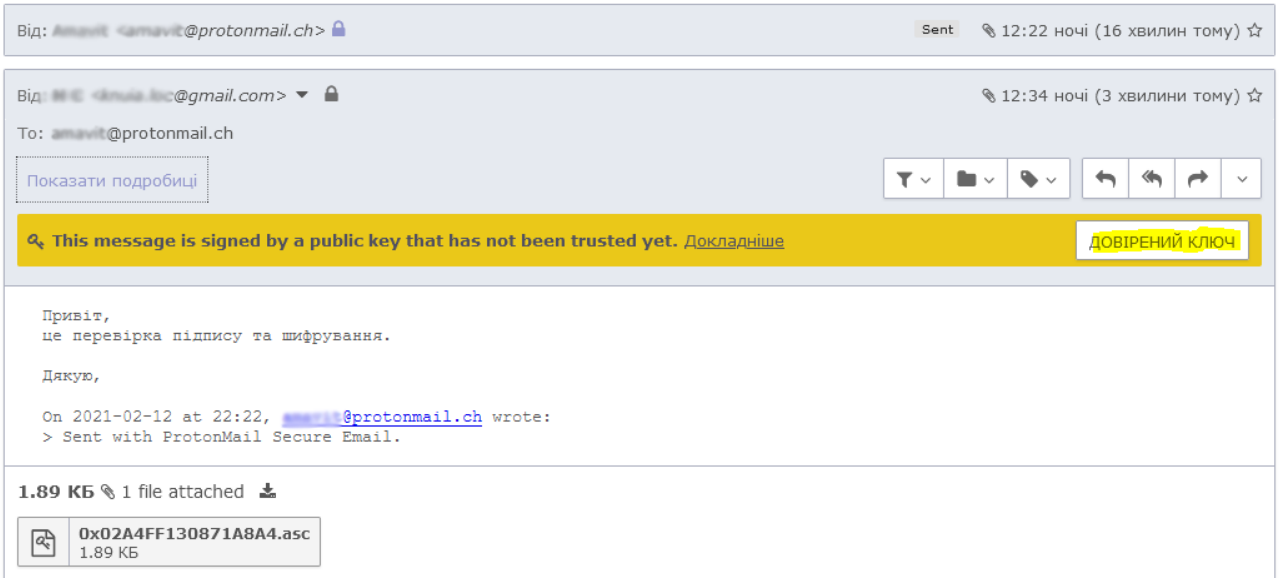


Рис. 15. Розшифрований і перевірений на правдивість підпису лист з пропозицією позначити публічний ключ як довірений

Далі всі листи між обліковими записами @gmail.com і @protonmail.com будуть автоматично підписуватися і шифруватися перед відправкою, а під час отримання перевірятись та розшифровуватись.

Лабораторне заняття «Двофакторна автентифікація облікового запису Facebook. Метадані фотозображень»

Навчальна мета заняття: навчитись налаштовувати двофакторну автентифікацію облікового запису Facebook та контролювати метадані фотозображень.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», особисті смартфони або телефони у слухачів, дата-кабелі підключення смартфона до комп'ютера, підготовлені файли фотозображень з метаданими.

Порядок проведення заняття

Двофакторна автентифікація облікового запису Facebook.

Створити, якщо немає, обліковий запис у соціальній мережі «Facebook». Встановити для Facebook-облікового запису двофакторну автентифікацію через Google Authenticator.

В обліковому записі перейти в «Налаштування та конфіденційність» – «Налаштування» – «Пароль і безпека» (рис. 1) – «Двоетапна перевірка» – «Використання двоетапної перевірки» – «Використовувати додаток для автентифікації» (рис. 2).

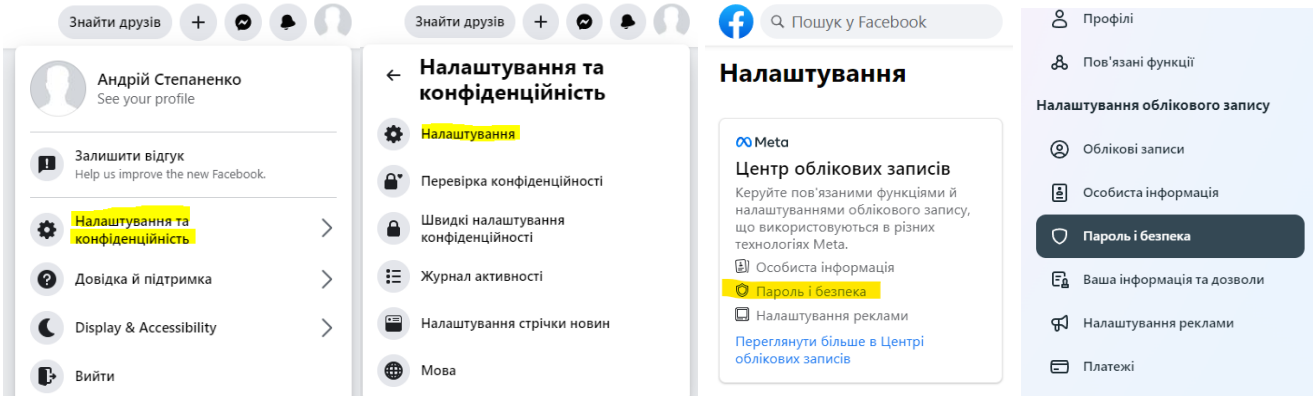


Рис. 1. Шлях до налаштувань «Пароль і безпека»

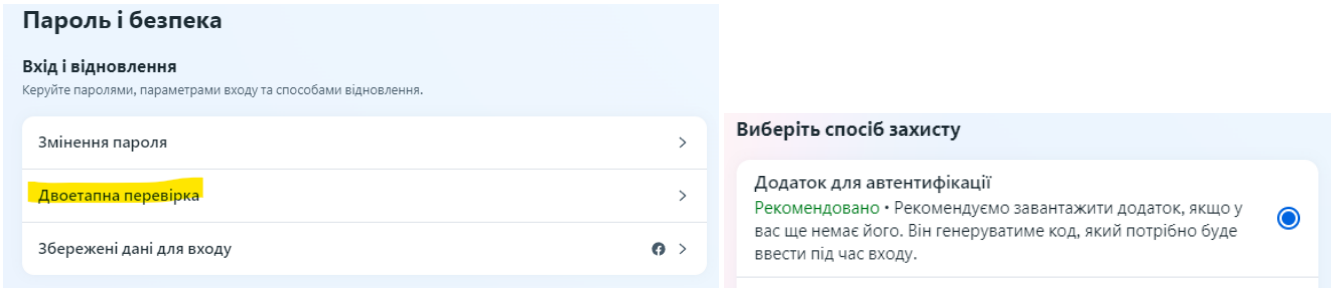


Рис. 2. Шлях до налаштування додатка автентифікації

Переконатися, що у власному смартфоні встановлений Google Authenticator (встановлюється з Google Play або App Store), увійти до «Використовувати додаток для автентифікації», зчитати додатком смартфону Google Authenticator QR-код та ввести код підтвердження (рис. 3).

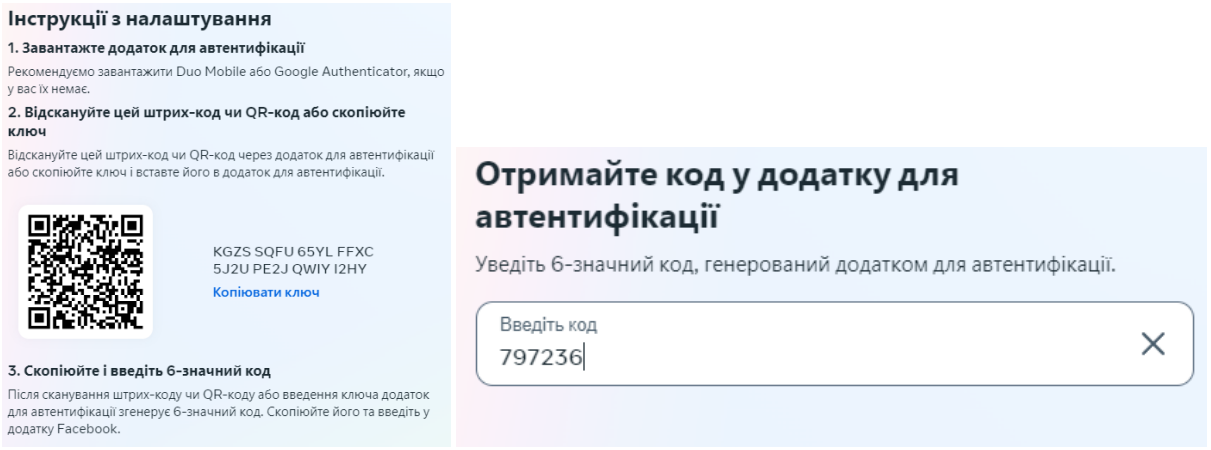


Рис. 3. Налаштування двоетапної перевірки

Після налаштування двоетапної перевірки повернутися у розділ «Використання двоетапної перевірки» - «Захисні ключі» - «Зареєструвати захисний ключ» (рис. 4) – Security key setup (Встановлення ключа безпеки) - Insert your security key into the USB port (Вставити ваш ключ безпеки в USB порт) – Скасувати (Cancel) (рис. 5). Далі обрати свій пристрій з ключами безпеки, який використовувався для автентифікації в аккаунті Google і додатково ввести свій пароль (рис. 6).

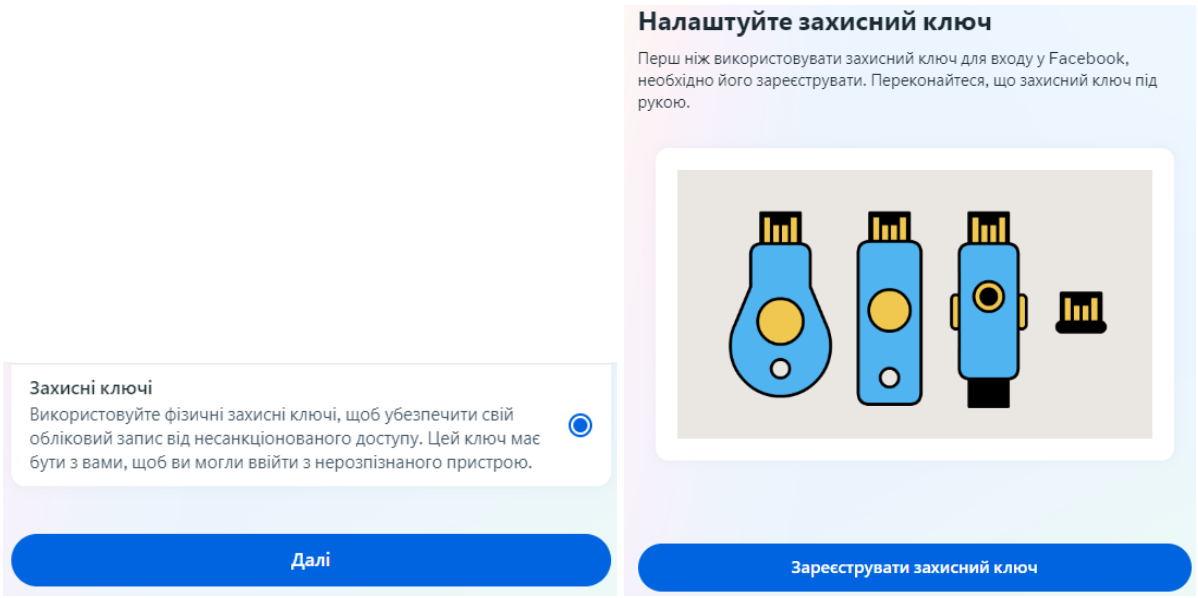


Рис. 4. Налаштування автентифікації через захисні ключі

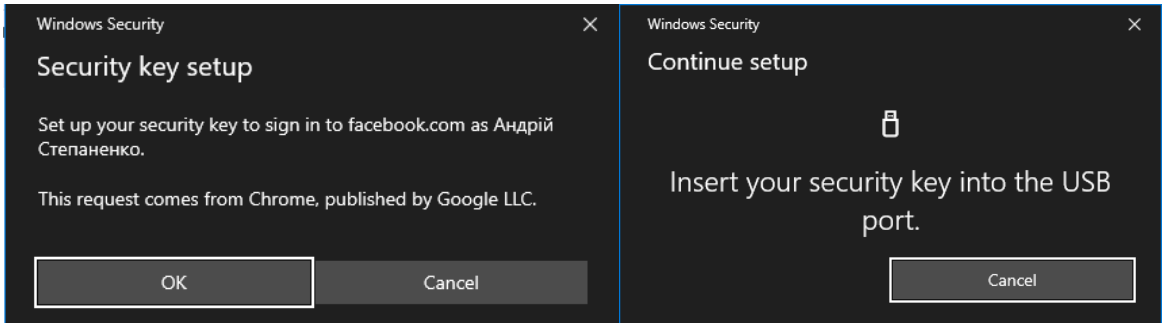


Рис. 5. Продовження налаштування автентифікації через захисні ключі

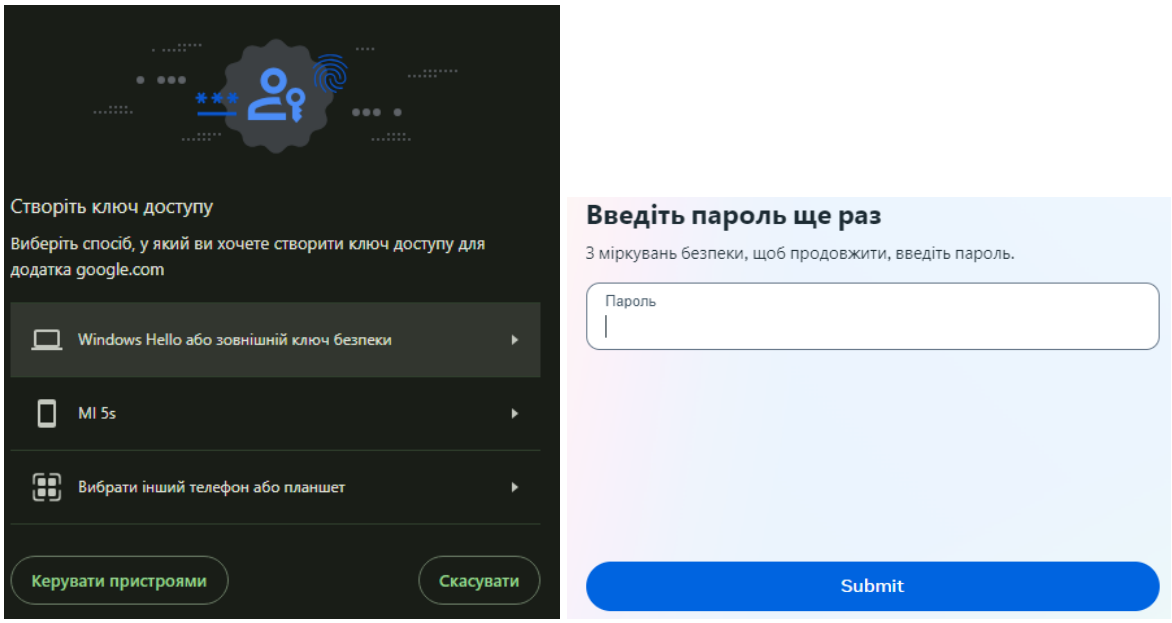


Рис. 6. Вибір свого пристрою з ключами безпеки

Повернутись у розділ «Пароль і безпека» і переглянути проблеми з безпекою, виконавши перевірку додатків, пристроїв і надісланих електронних листів (рис. 7).

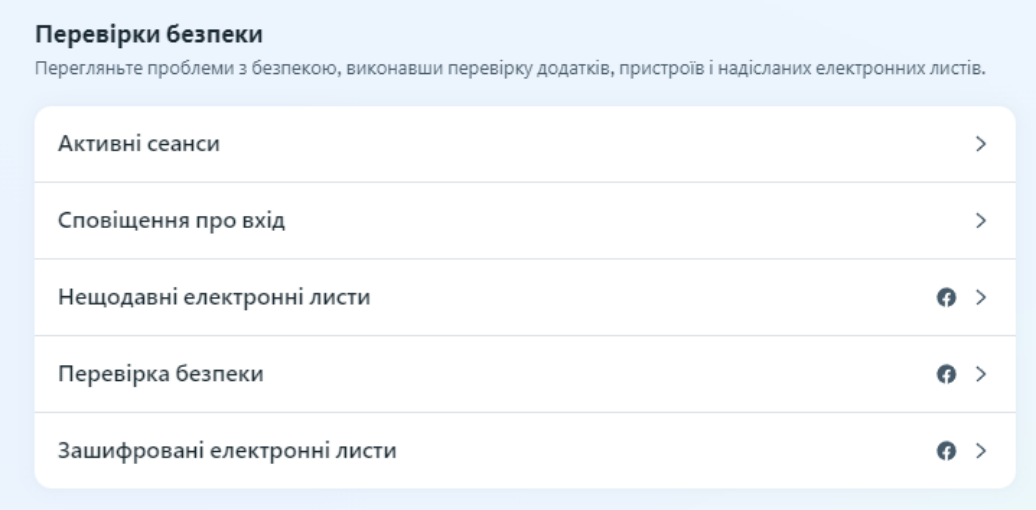


Рис. 7. Перевірка безпеки облікового запису

Після закінчення налаштувань вийти із облікового запису та увійти з використанням двоетапної автентифікації та пристрою з ключами.

Метадані фотозображень.

В особистому смартфоні включити GPS, підійти до вікна у приміщенні й дочекатися встановлення координат свого місцезнаходження, перевіривши цей факт запуском додатку «Карти», де відобразиться точне місцезнаходження смартфона.

Зробити декілька фотознімків фотокамерою смартфона, підключити смартфон до комп’ютера та завантажити фотозображення на комп’ютер. Або скопіювати на комп’ютер підготовлені файли фотозображень з метаданими.

Перевірити наявність метаданих у файлах фотозображень та видалити їх.

Завантажити, встановити і запустити утиліту перегляду та редагування метаданих «AnalogExif» (https://sourceforge.net/projects/analogexif). Відкрити у AnalogExif фотозображення, переглянути метадані, двічі клацнути на поле Location та скопіювати у буфер координати (рис. 8).

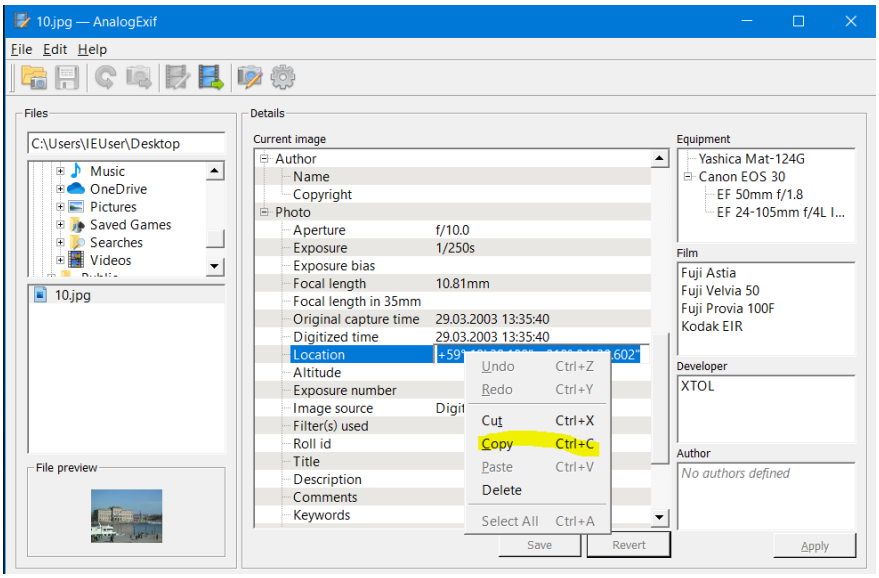


Рис. 8. Перегляд метаданих фотозображення

Відкрити веббраузер «Google Chrome», вставити координати в адресний рядок і здійснити пошук місця фотозйомки (рис. 9).

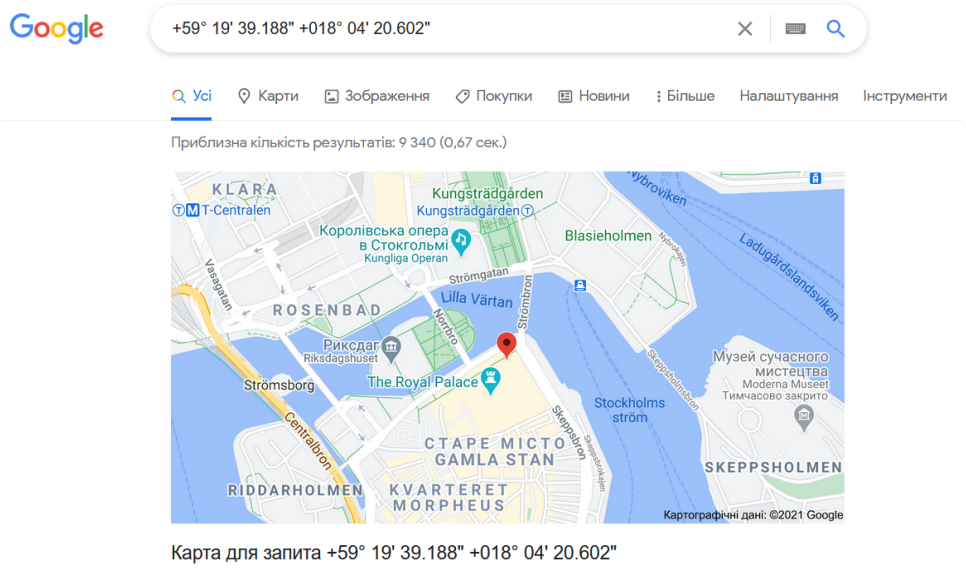


Рис. 9. Пошук місця фотозйомки за координатами з метаданих фотозображення

У Провіднику файлів через контекстне меню (клацнути правою кнопкою миші) подивитися «Властивості файлу фотозображення», перейти у вкладку «Докладно» та клацнути на «Видалити властивості та особисті відомості» – «Вибрати всі» – «ОК» (рис. 10).

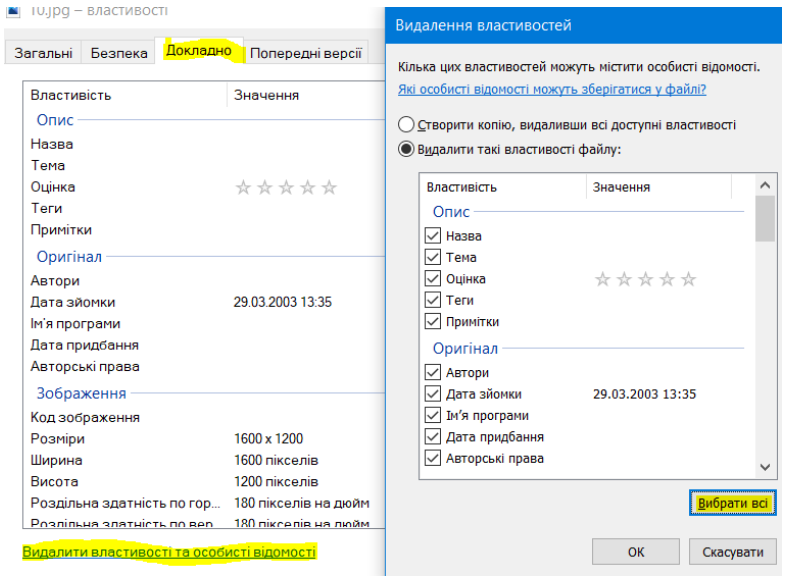


Рис. 10. Видалення метаданих фотозображень

Знову відкрити у AnalogExif фотозображення та переконатися, що метадані відсутні та можна їх безпечно завантажувати у соціальні мережі.

Лабораторне заняття «Виявлення провісників та індикаторів інциденту інформаційної безпеки»

Навчальна мета заняття: навчитись виявляти провісники та індикатори інцидентів інформаційної безпеки.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome».

Порядок проведення заняття

Задача 1.

1. Налаштувати ведення та забезпечення доступу до журналу подій Windows Defender Firewall.
2. Встановити Nmap Security Scanner та здійснити сканування системи, яке розглядається як підготовка до атаки.
3. Виявити провісники атаки та заповнити звіт щодо події інформаційної безпеки.

Виконання.

Через рядок пошуку відкрити Windows Defender Firewall with Advanced Security (пошуковим виразом може бути "Засоби адміністрування") (рис. 1).

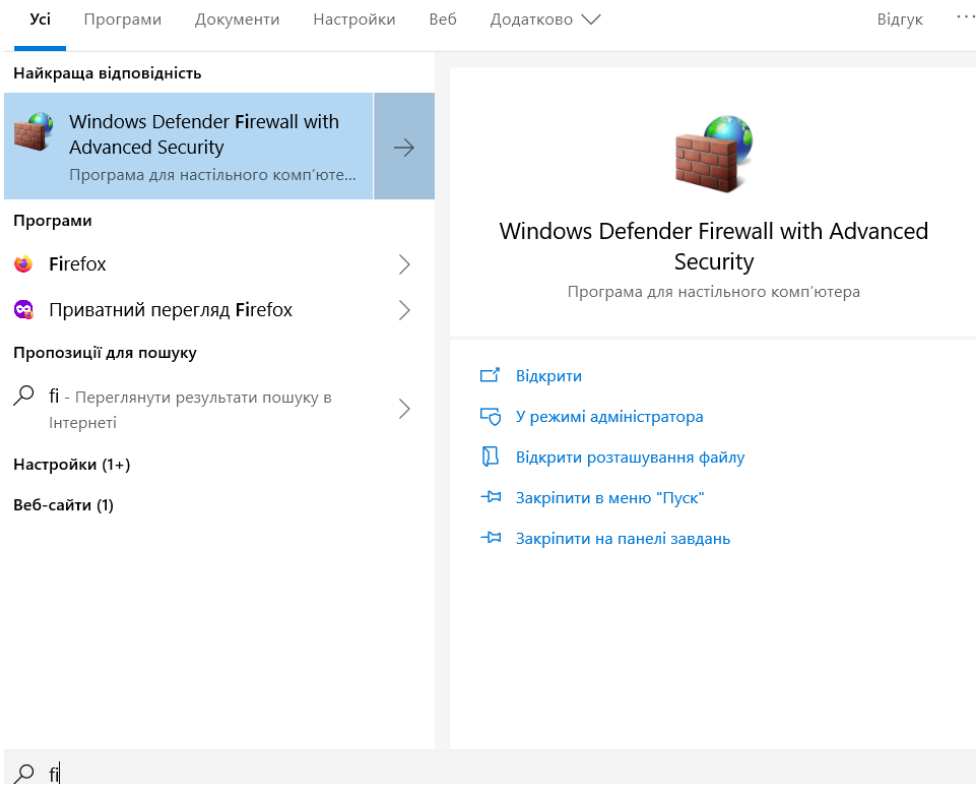


Рис. 1. Відкриття Windows Defender Firewall with Advanced Security

У Windows Defender Firewall with Advanced Security (рис. 2):

- відкрити налаштування Windows Defender Firewall Properties;
- пересвідчитись, що Firewall активований (Firewall state: on);
- для кожної вкладки Domaine Profile, Private Profile, Public Profile через опцію Logging – Customize включити записування у журнал подій про блокування мережевих пакетів (Log dropped packets: Yes) та успішне встановлення мережевого з'єднання (Log successful connections: Yes).

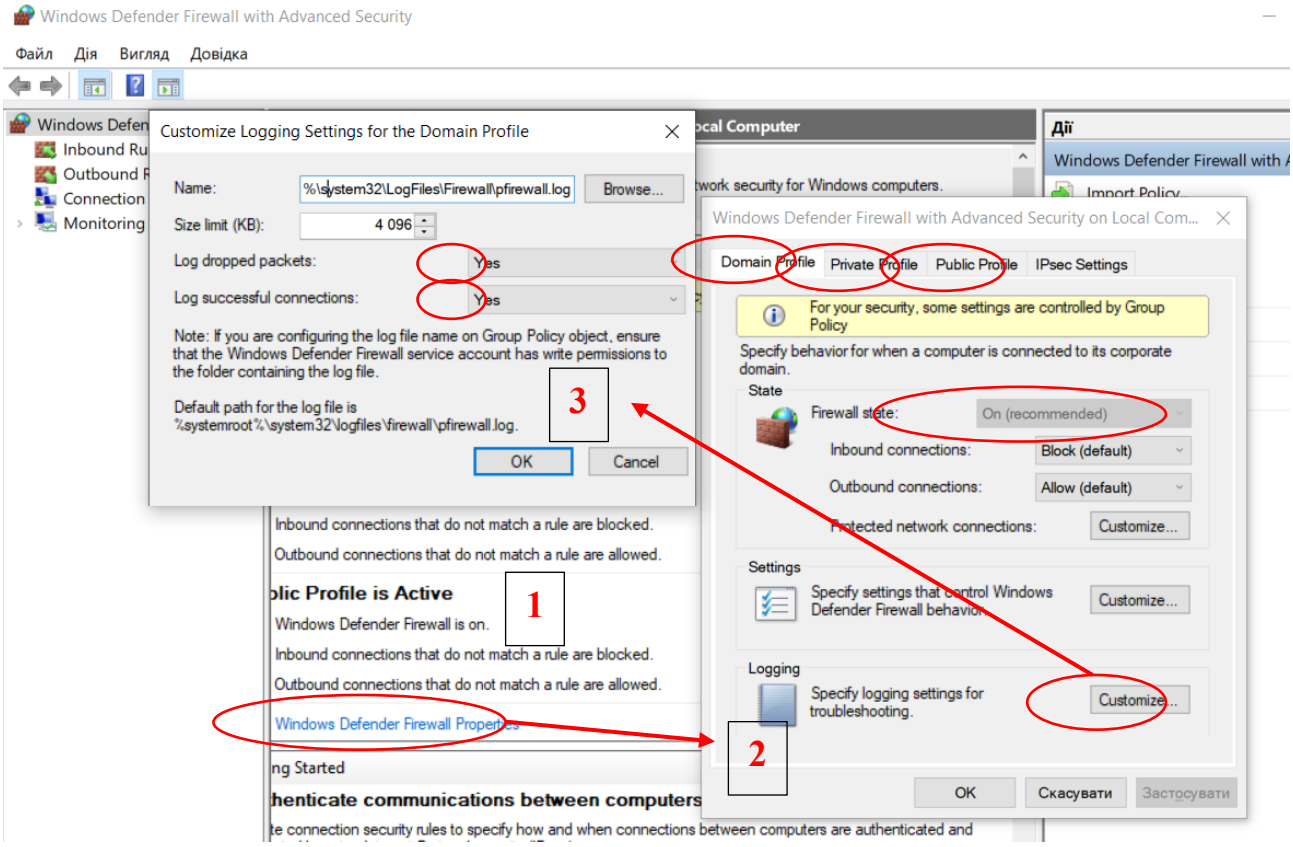


Рис. 2. Налаштування журналу подій Windows Defender Firewall

У каталозі C:\Windows\System32\LogFiles\Firewall знайти файл pfirewall.log (рис.3).

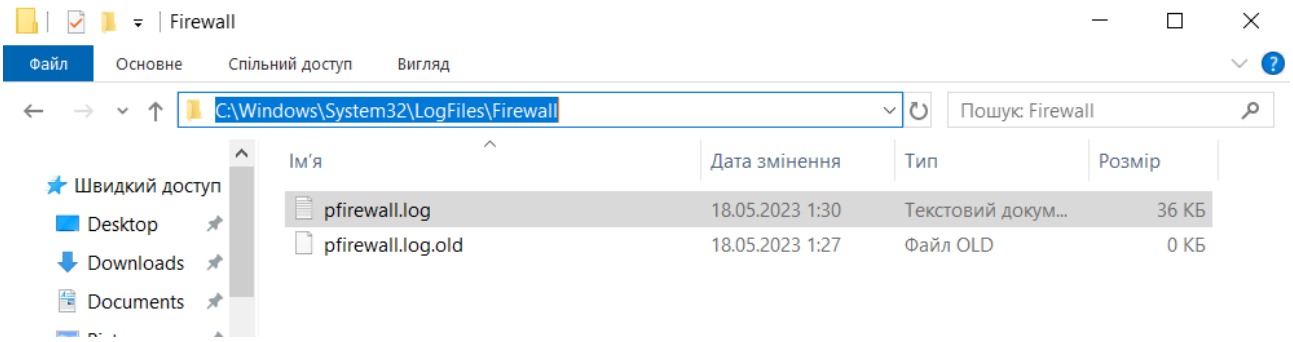


Рис. 3. Локація журналу подій pfirewall.log

Через властивості файлу pfirewall.log перейти по вкладкам Безпека – Додатково – Дозволи – Продовжити (рис. 4), а потім – Увімкнути успадкування (рис. 5).

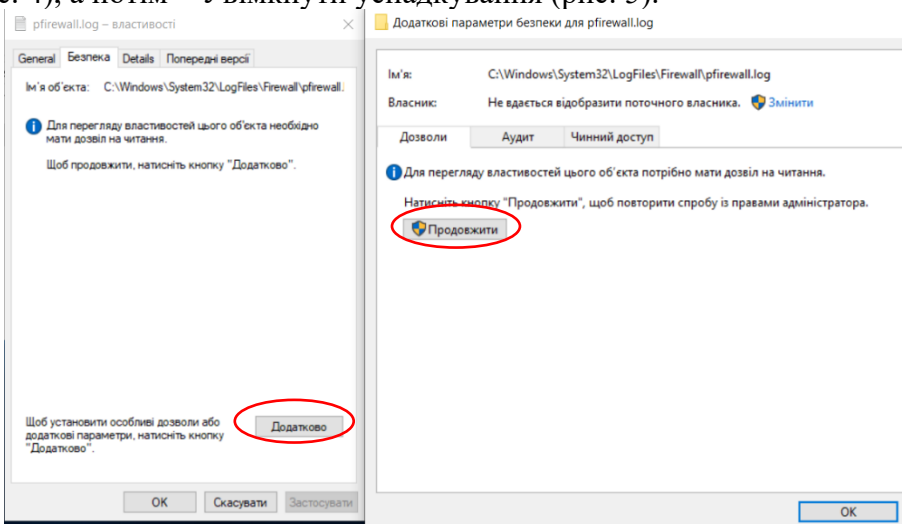


Рис. 4. Налаштування параметрів доступу до файлу pfirewall.log

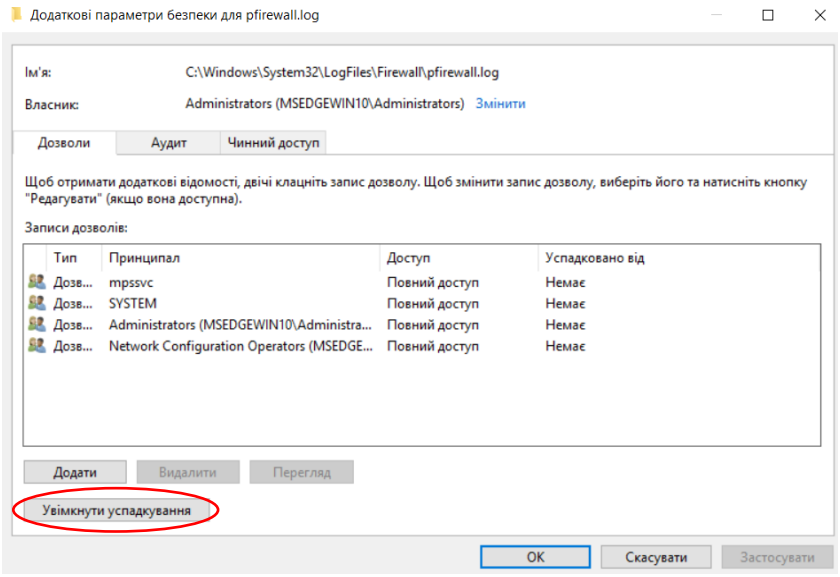


Рис. 5. Увімкнення успадкування прав доступу для файлу pfirewall.log

Переконатися, що файл журналу pfirewall.log доступний для читання, відкривши його текстовим редактором (рис. 6).

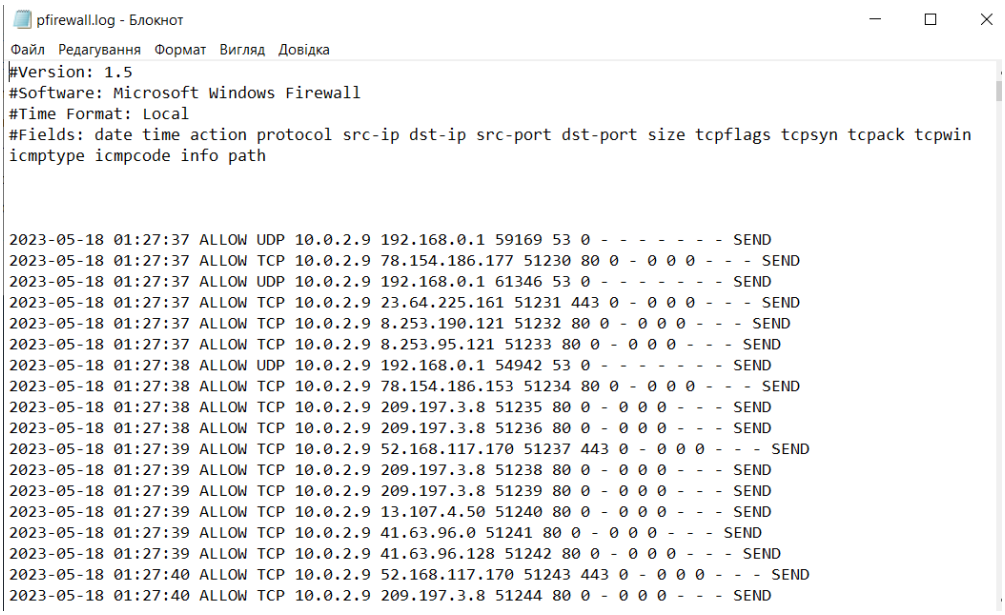


Рис. 6. Зміст журналу аудиту Microsoft Windows Firewall

У журналі аудиту Microsoft Windows Firewall (рис. 6) зазначені: дата і час, дозвіл на встановлення з'єднання (ALLOW), протокол з'єднання (UDP, TCP), IP адреси з'єднання (src-ip, dst-ip), порти з'єднання (src-port, dst-port), інше.

Завантажити та встановити Nmap Security Scanner в ОС Windows (https://nmap.org/download#windows) (рис. 7).

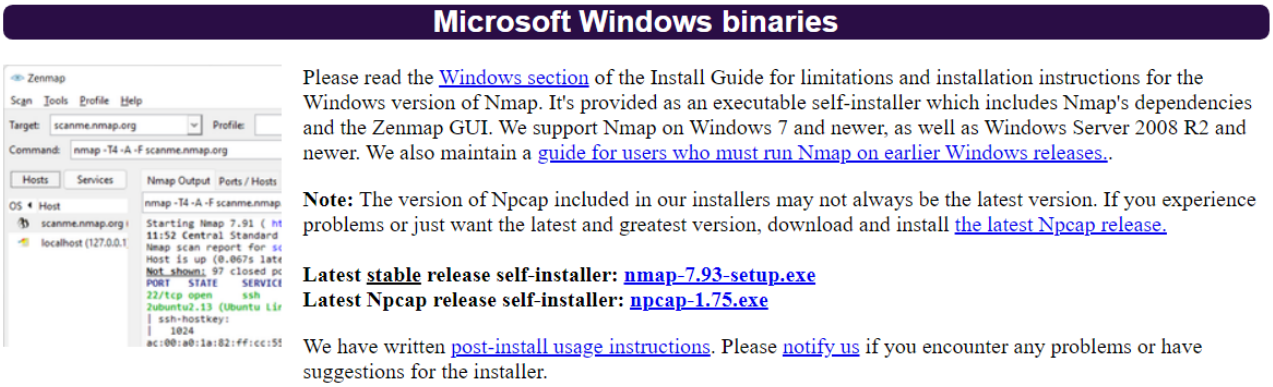


Рис. 7. Сторінка завантаження Nmap Security Scanner для ОС Windows

Відкрити сканер через ярлик «Nmap - Zenmap GUI», у полі Target вписати loopback IP адрес своєї системи: 127.0.0.1 та у режимі Quick scan plus запустити сканування (рис. 8). Сканування є підготовчим етапом перед атакою на систему, при якому здійснюється послідовний перебір портів підключення до цільової системи.

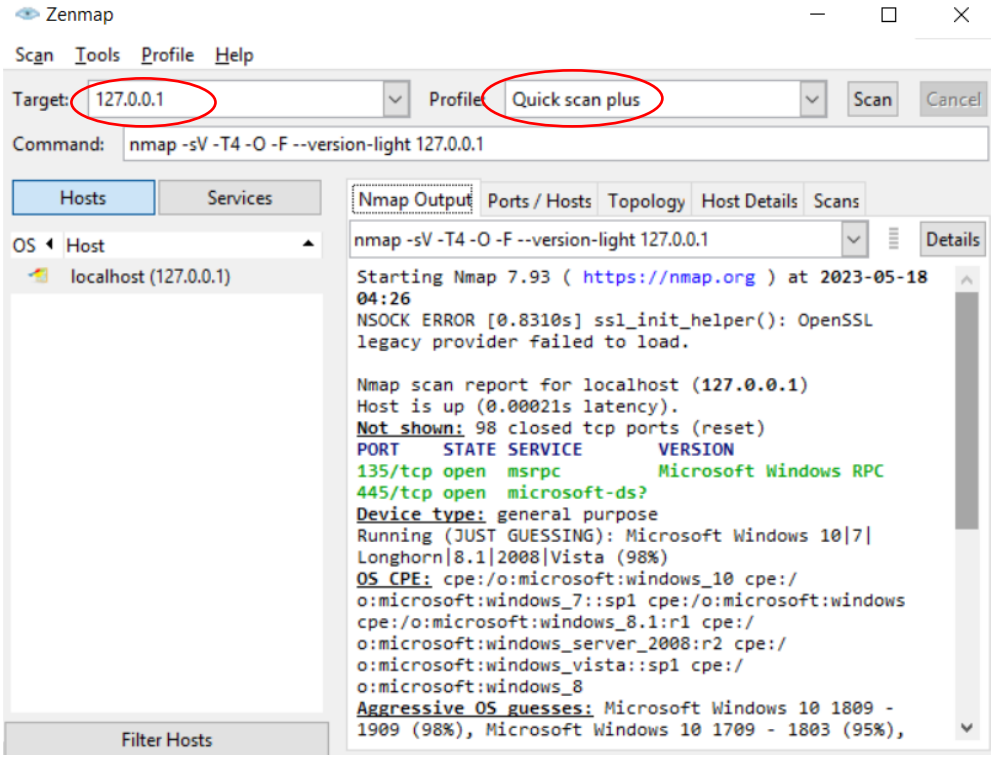
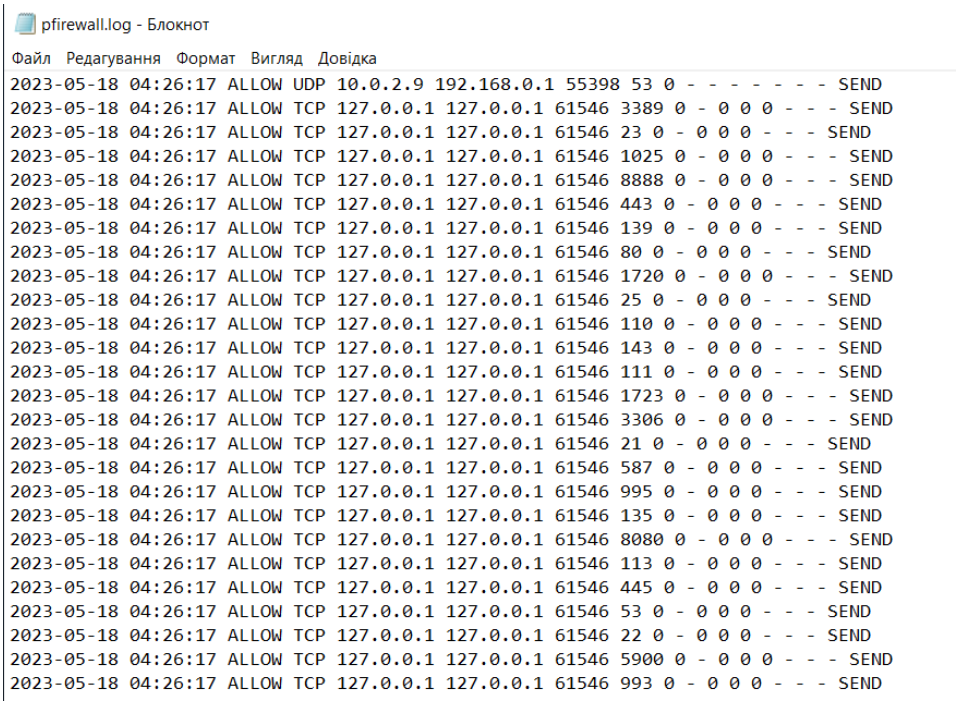


Рис. 8. Запуск сканування своєї системи

Відкрити файл журналу аудиту pfirewall.log та знайти записи, які свідчать про сканування портів системи і є провісниками майбутньої атаки на систему (рис. 9). Основною ознакою сканування є наявність великою кількості одночасних підключень з одного IP адреса до різних портів системи.


pfirewall.log - Блокнот

Файл Редагування Формат Вигляд Довідка

```
2023-05-18 04:26:17 ALLOW UDP 10.0.2.9 192.168.0.1 55398 53 0 - - - - - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 3389 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 23 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 1025 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 8888 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 443 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 139 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 80 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 1720 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 25 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 110 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 143 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 111 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 1723 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 3306 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 21 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 587 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 995 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 135 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 8080 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 113 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 445 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 53 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 22 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 5900 0 - 0 0 0 - - - SEND
2023-05-18 04:26:17 ALLOW TCP 127.0.0.1 127.0.0.1 61546 993 0 - 0 0 0 - - - SEND
```

Рис. 9. Записи журналу аудиту pfirewall.log, які свідчать про сканування портів системи

Заповнити шаблон звіту про подію інформаційної безпеки (табл.1).

Таблиця 1. Шаблон звіту про події інформаційної безпеки

ЗВІТ ПРО ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ			
1. Дата події		3. Ідентифікаційні номери відповідної події та/або інциденту (якщо застосовне)	
2. Номер події (надається фахівцем ISIRT)			
4. РЕКВІЗИТИ ОСОБИ, ЩО ЗВІТУЄ			
4.1 Ім'я та прізвище		4.2 Адреса	
4.3 Організація		4.4 Відділ	
4.5 Телефон		4.6 E-male	
5. ОПИС ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ			
5.1 Опис події: • Що сталося. • Яким чином сталося. • Чому так сталося. • Які компоненти/активи піддались впливу. • Оцінка впливу на діяльність організації. • Будь-які виявлені вразливості			
6. ДЕТАЛІ ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ			
6.1 Дата та час події			
6.2 Дата та час виявлення події			
6.3 Дата та час повідомлення про подію			
6.4 Чи відповідь на цю подію усунула небезпеку?		ТАК ☐ НІ ☐ (позначте відповідне)	
6.5 Якщо так. вкажіть, скільки часу тривала подія (у днях/годинах/хвилинах)			

Задача 2.

1. Налаштувати аудит входу користувача в систему.
2. Ввести декілька раз неправильний пароль при вході до ОС Windows.

3. Виявити індикатори інциденту інформаційної безпеки та заповнити звіт щодо події інформаційної безпеки.

Виконання.

Через рядок пошуку відкрити Налаштування групової політики (Edit group policy) (рис. 10).

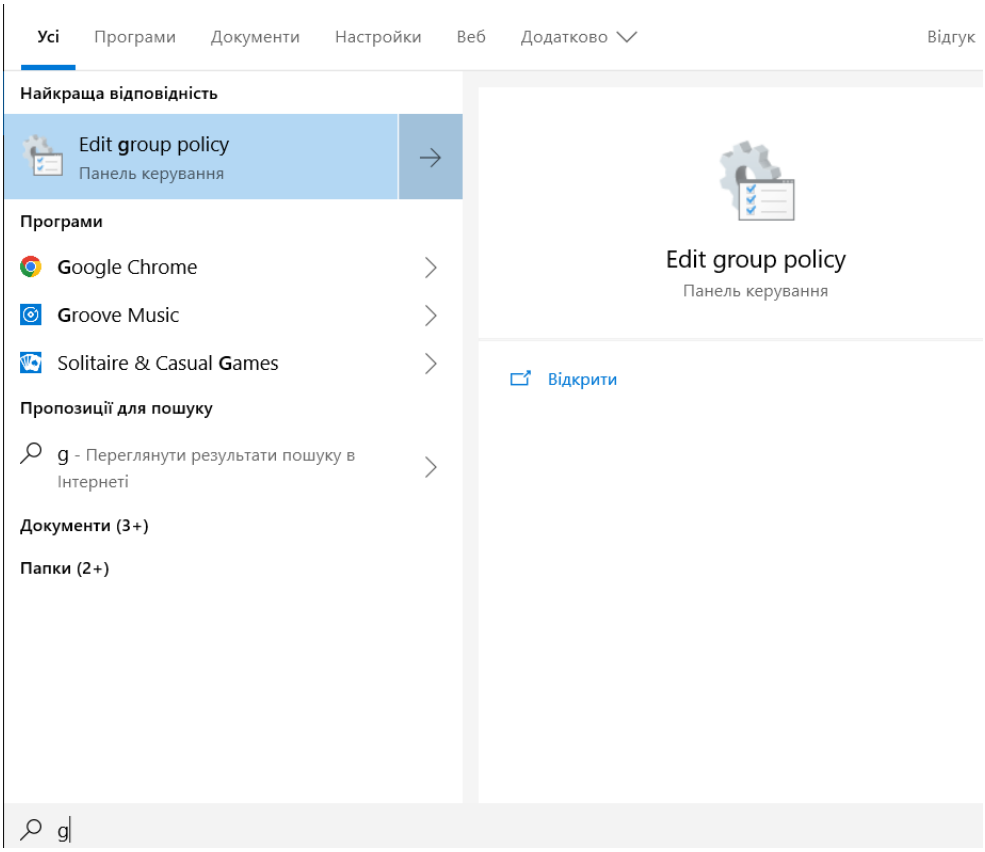


Рис. 10. Відкриття Налаштування групової політики (Edit group policy)

У розділі Конфігурація комп'ютера – Налаштування Windows – Security Settings – Advanced Audit Policy Configuration – 'System Audit Policies - Local Group Policy Object' - Account Logon кликнути на параметр Audit Credential Validation та налаштувати аудит вдалих та невдалих перевірок автентифікаційних даних користувача при вході у систему (рис. 11).

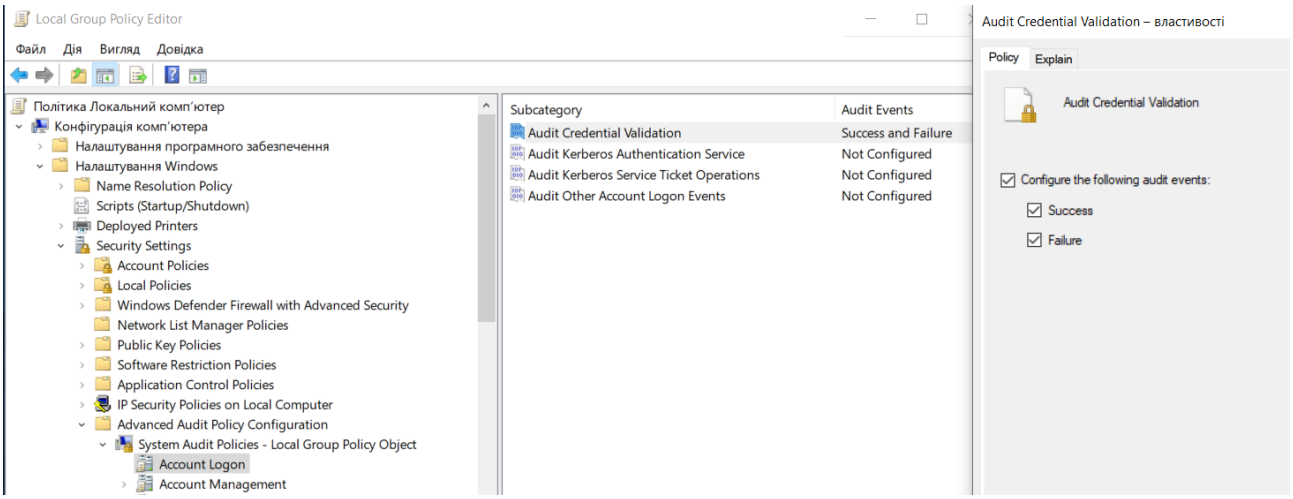


Рис. 11. Налаштування аудиту вдалих та невдалих перевірок автентифікаційних даних користувача при вході у систему

Після декількох спроб введення неправильного паролю (рис.12) через рядок пошуку відкрити Переглядач подій (Event Viewer) – Windows Log – Security та знайти невдалі спроби вводу паролю (рис. 13).

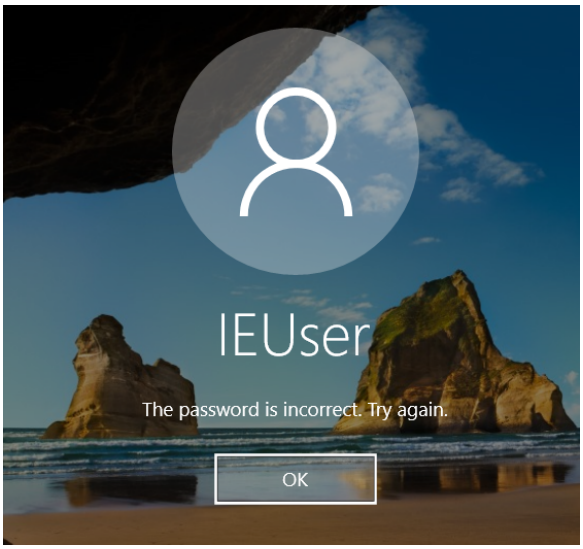


Рис. 12. Результат введення неправильного паролю

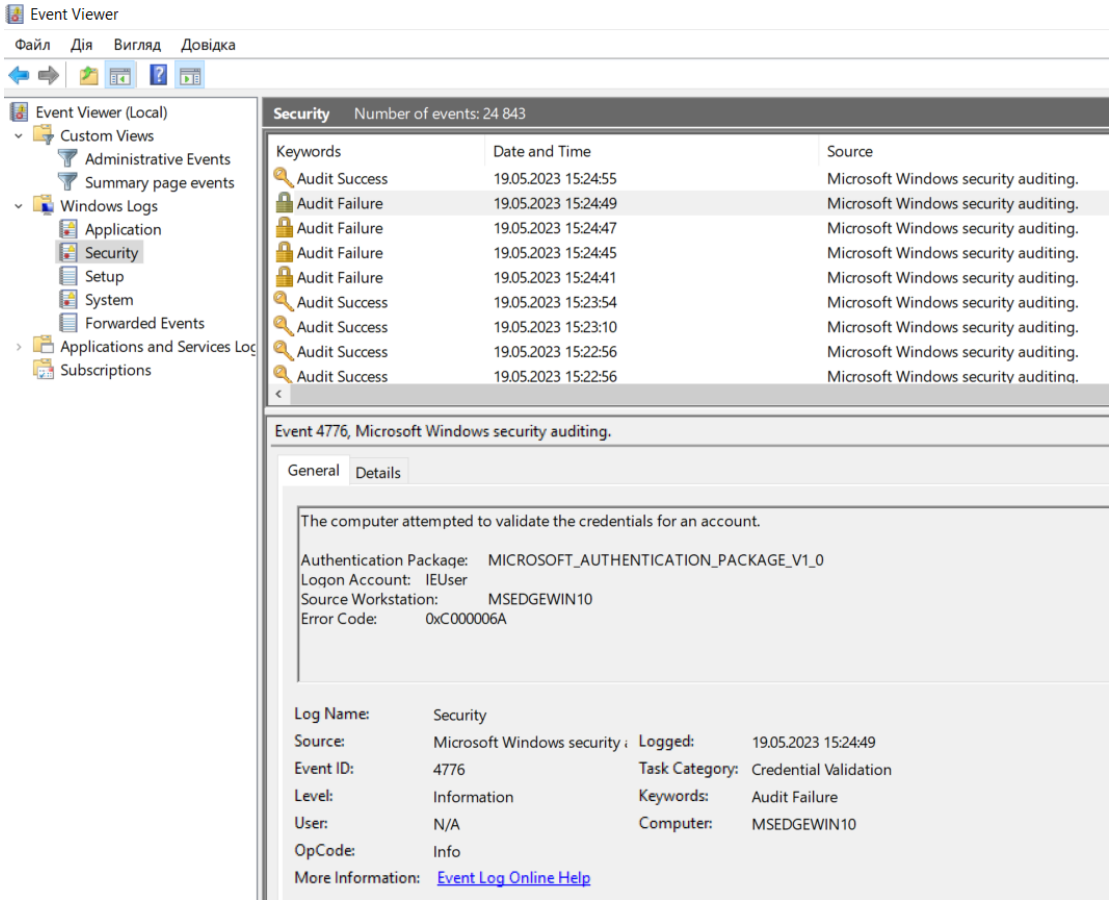


Рис. 13. Записи журналу подій про невдалі спроби входу у систему

Заповнити шаблон звіту про подію інформаційної безпеки (табл.1).

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Oles N. How to Catch a Phish: A Practical Guide to Detecting Phishing Emails. Apress Berkeley, CA, 2023. 147 p. DOI: https://doi.org/10.1007/978-1-4842-9361-4.
2. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: наук.-практ. посіб. Київ: К.І.С., 2021. 160 с. URL: https://rm.coe.int/handbook-pers-data-protect-2021-web/1680a37a69.
3. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки: монографія. Житомир : ЖНАЕУ, 2016. 636 с.
4. Манжай О. В., Манжай І. А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків : Промарт, 2020. 162 с. з іл. URL: https://univd.edu.ua/science-issue/issue/4315
5. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О. В. Манжай, В. В. Носов. К. : ВАІТЕ, 2021. 106 с.
6. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М.Барановський, В.В.Гузій , Д.І. Майорников, О.В. Манжай, В.В. Носов. Київ: ВАІТЕ, 2021. 262 с.

Допоміжна

7. Манжай О. В., Манжай І.А. Що таке кібергігієна? // Протидія кіберзлочинності та торгівлі людьми (18 травня. 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 65-67.
8. Носов В.В., Манжай О.В. Зміст та методологія практичного навчання з питань кібергігієни // Протидія кіберзлочинності та торгівлі людьми (18 травня. 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 72-73.
9. Maennel K., Mäses S., Maennel O. Cyber Hygiene: The Big Picture. In: Gruschka N. (eds) Secure IT Systems. NordSec 2018. *Lecture Notes in Computer Science*. 2020. Vol. 11252. Springer, Cham. (DOI: 10.1007/978-3-030-03638-6_18).
10. Pfleeger S. L., Sasse M. A., Furnham A. From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management*. 2014. Vol. 11. Iss. 4. pp. 489-510. (DOI: 10.1515/jhsem-2014-0035).
11. Review of cyber hygiene practices (December 2016). European Union Agency For Network and Information Security (ENISA). https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport, p. 4.
12. Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J. Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*. 2020. Vol. 128 (DOI: 10.1016/j.dss.2019.113160).
13. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
14. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
15. Про створення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11 березня 2021 року, введено в дію Указом Президента України від 19 березня 2021 року № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text.
16. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 10.05.2023).
17. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 10.05.2023).
18. Про захист персональних даних: закон України від 01.06.2010; [із змінами і доповненнями]. *Офіційний вісник України*. 2010. № 49 (09.07.2010), стор. 199, стаття 1604.

19. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України № 373 від 29.03.06; [із змінами і доповненнями]. *Офіційний вісник України*. 2006. № 13 (12.04.2006), стор. 164, стаття 878.

20. Про доступ до публічної інформації: закон України від 13.01.2011; [із змінами і доповненнями]. *Офіційний вісник України*. 2011. № 10 (18.02.2011), стор. 29, стаття 446.

21. Про затвердження документів у сфері захисту персональних даних: наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. *Баланс*. 2014, № 19, С. 5. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n11.

22. Про інформацію: закон України від 02.10.1992 р.; [із змінами і доповненнями]. *Відомості Верховної Ради України*. 1992. № 48 (01.12.1992). ст. 650.

23. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). *Офіційний вісник Європейського Союзу*. 04.05.2016. L 119. С. 1. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

24. Про захист інформації в інформаційно-комунікаційних системах. Закон України: від 05.07.1994, № 1170-VII. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

25. Про електронні комунікації: Закон України від 16.12.2020 : [із змінами і доповненнями]. *Офіційний вісник України*. 2021. № 6 (21.01.2021). Ст. 306.

Інформаційні ресурси в Інтернеті

26. Освітній серіал «Основи кібергігієни». URL: https://osvita.diia.gov.ua/courses/cyber-hygiene.

27. Ви вмієте розпізнавати фішинг? URL: https://phishingquiz.withgoogle.com/?hl=uk.