

Модуль: Безпечне користування мережею Інтернет



Практична вправа:

«Безпечний перегляд веб-сторінок та способи організації безпечного з'єднання в мережі»



Навчальна мета заняття: здійснити налаштування браузера 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 веб-сторінок, 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).

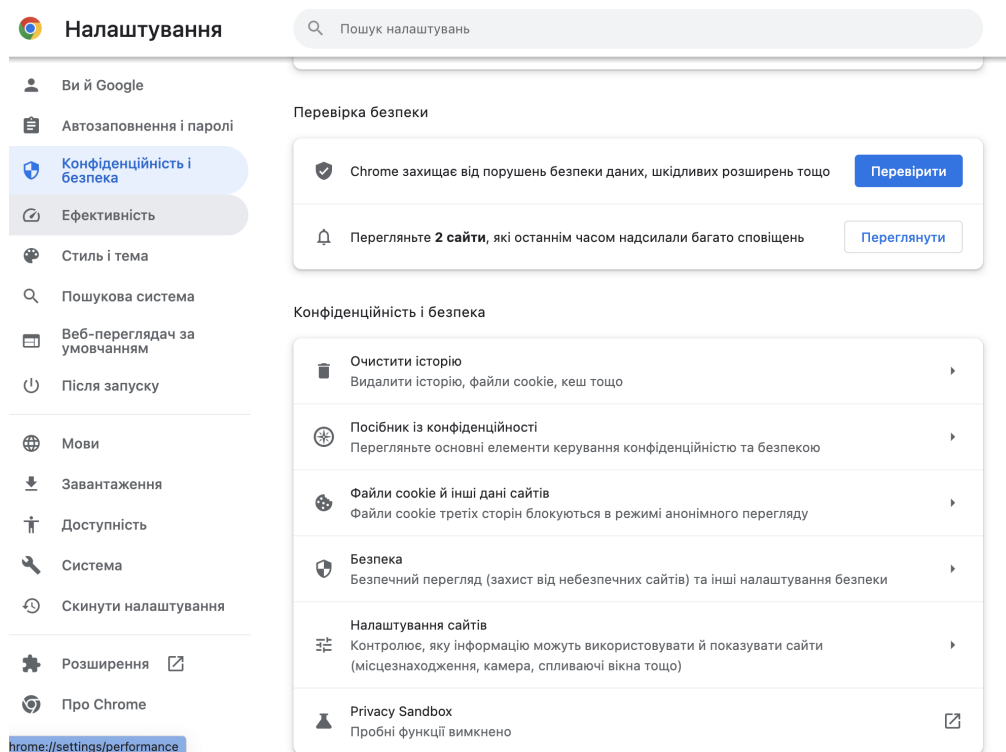


Рис. 1. Налаштування безпеки у браузері Chrome

Якщо налаштування безпеки не повною мірою влаштовують користувача, можна встановити додаткові плагіни. Як плагіни 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/>).

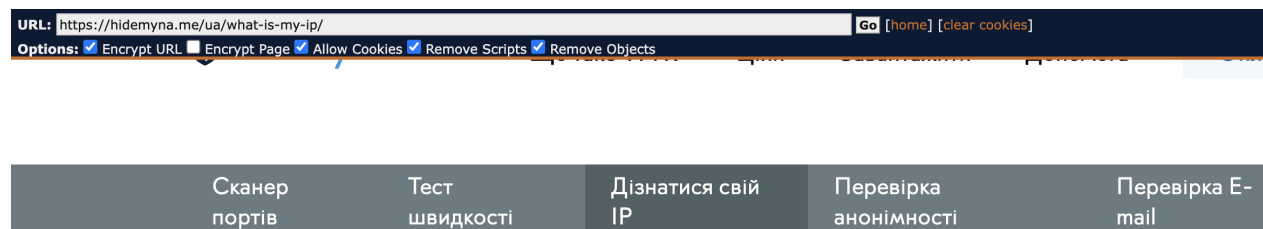
1. Налаштуйте параметри безпеки та конфіденційності браузера. Поясніть свій вибір налаштувань.

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, зокрема 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-веб-сервер. Ввести у відповідному вікні адресу hidemyna.me/ua/what-is-my-ip або 2ip.ua. Оцінити одержані результати (рис. 2).



Дізнатися свою IP-адресу

Знаючи вашу IP-адресу, зловмисники можуть отримати дуже багато інформації. Нижче лише її мала частина.

Ваш IP-адреса	Хост	149-210-148-6.colono.transip.net
149.210.148.6	Система	macOS
Змінити IP-адресу	Ваш браузер	Chrome 115.0
	Звідки ви	Netherlands

Рис. 2. Результат використання проксі-сервера

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. Як приклад 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](https://protonvpn.com/downloads)).

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

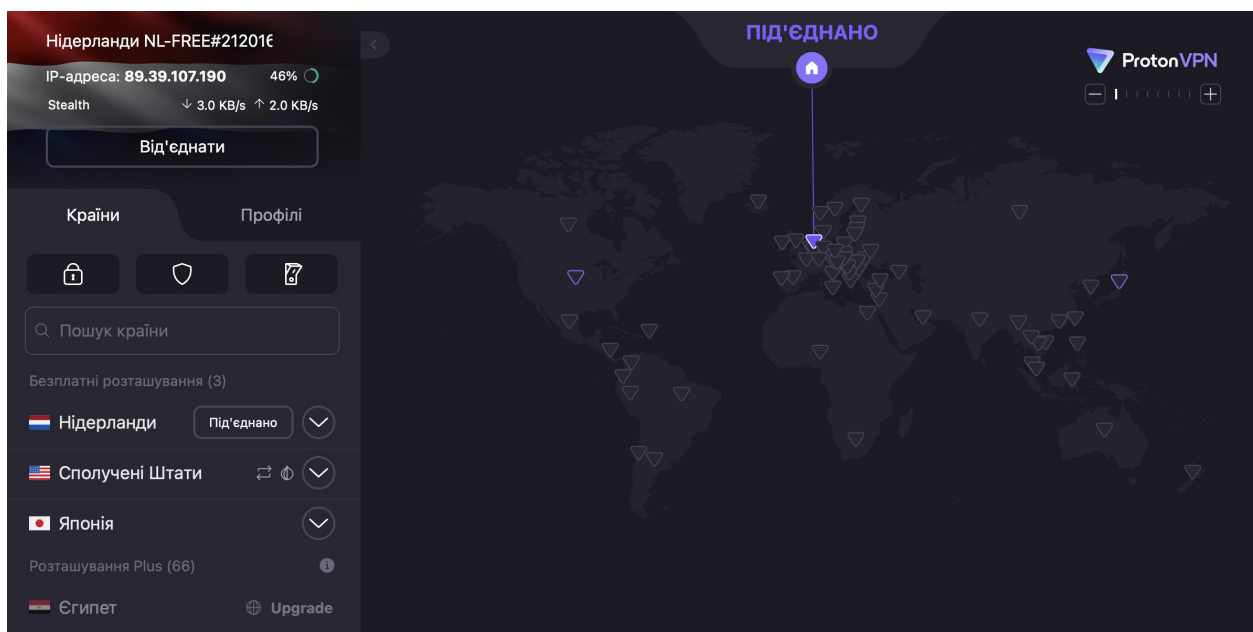


Рис. 3. Зовнішній вигляд клієнта Proton VPN

1. Відпрацювати підключення через одиничний та ланцюжок проксі-серверів.
2. Відпрацювати принаймні два способи налаштування VPN-з'єднання: 1) через налаштування параметрів мережевого 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.