Автор: Вейчук В. М. Укладач: Шпортько О. В.

# Лабораторна роботи № 9

**Тема.** Налаштування рівнів безпеки сучасних браузерів.

**Мета.** Формування вмінь і навиків налаштування рівнів безпеки сучасних браузерів – Chrome, IE, Mozilla Firefox, Opera та ін. для обмеження впливу людського фактору на інформаційну безпеку. Порівняння рівня безпеки сучасних браузерів.

## Теоретичні відомості

**Фішинг** — це технологія онлайнового шахрайства, яка використовується зловмисниками для отримання особистої інформації користувачів.

Існує кілька тактик виманювання інформації, зокрема повідомлення електронної пошти та веб-сайти, які використовують підроблені відомі та надійні бренди. Типовою фішинг-махінацією є використання оманливих повідомлень, які виглядають як повідомлення від відомих компаній або веб-сайтів, наприклад, банків, емітентів кредитних карток, благодійних організації або з сайтів організацій, що займаються електронною комерцією.

**Cookie** — це невелика порція текстової інформації, яку сервер передає браузеру. Коли користувач звертається до сервера (набирає його адресу в рядку браузера), сервер може зчитувати інформацію, що міститься в cookies, і на підставі її аналізу здійснювати які-небудь дії. Наприклад, у випадку авторизованого доступу до чого-небудь через веб, у cookies зберігаються логін і пароль протягом сесії, що дає можливість користувачу не вводити їх знову при запитах кожного документа, захищеного паролем.

**SSL** (Secure Sockets Layer - рівень захищених сокетів) - протокол рівня передачі даних, який пропонує захищений канал передачі даних між клієнтом і сервером з використанням аутентифікації, цифрових підписів і шифрування. Для шифрування/дешифрування трафіку використовується ключ (сертифікат), отриманий клієнтом від сервера.

В основі технології SSL лежать спеціально розроблені криптографічні алгоритми, що використовують поняття публічного і приватного ключів. Таким чином SSL-сертифікат - це комбінація спеціальним чином згенерованого приватного і публічного ключів, виписана на певне доменне ім'я, програму або IP-адресу. Публічний і приватний ключі є звичайними текстовими файлами, що містять табульований набір символів. Протокол SSL гарантує безпечне з'єднання між сервером і браузером користувача. При використанні каналу, захищеного SSL-сертифікатом, інформація передається в закодованому вигляді по протоколу HTTPS, і розшифрувати її можна тільки за допомогою спеціального ключа, який відомий тільки власнику сертифіката і довіреному Центру сертифікації, який видав даний SSL-сертифікат. Використання SSL дозволяє вирішити наступні завдання:

- забезпечення цілісність інформації (гарантія того, що дані не були змінені в процесі передачі);
- підтвердження дійсності сторін, що беруть участь в обміні інформацією (у діалозі);
- гарантування безпеки передачі даних (дані передаються по мережі в зашифрованому вигляді).

### Підготовчий етап заняття

1. Відкрийте браузер Coogle Chrome.
2. Відкрийте меню Chrome  на панелі інструментів браузера.
3. Виберіть у ньому пункт **Настройки.**
4. Самостійно встановіть українську мову інтерфейсу та при потребі перезавантажте браузер і знову ввійдіть на сторінку налаштувань.

### Налаштування параметрів безпеки Google Chrome

5. При наявності натисніть посилання **Показати розширені налаштування.**
6. Перегляньте список налаштувань, які можна змінювати в Google Chrome**.**

### Захист від фішингу та шкідливих програм

7. Переконайтеся, що у розділі **Конфіденційність** прапорець **Активувати захист від фішингу та шкідливих програм** встановлений по замовчуванню. Коли цей прапорець встановлений, Google Chrome показує попередження, якщо відкривається сайт, який підозрюється в фішингу або поширенні зловмисних програм.

### Налаштування та сертифікати SSL

8. У розділі **HTTPS/SSL** натисніть кнопку **Керування сертифікатами** та перегляньте різновиди та дані встановлених сертифікатів. Для чого вони використовуються?
9. Самостійно поверніться до сторінки налаштувань Google Chrome**.**

### Налаштування веб-вмісту сторінок

10. У розділі **Конфіденційність** натисніть кнопку **Налаштування вмісту**.

11. У вікні, що з’явиться (рис. 1) натисніть кнопку **Усі файли cookie та дані із сайтів…**, щоб відкрити діалогове вікно **Файли cookie та дані із сайтів** (рис. 2).

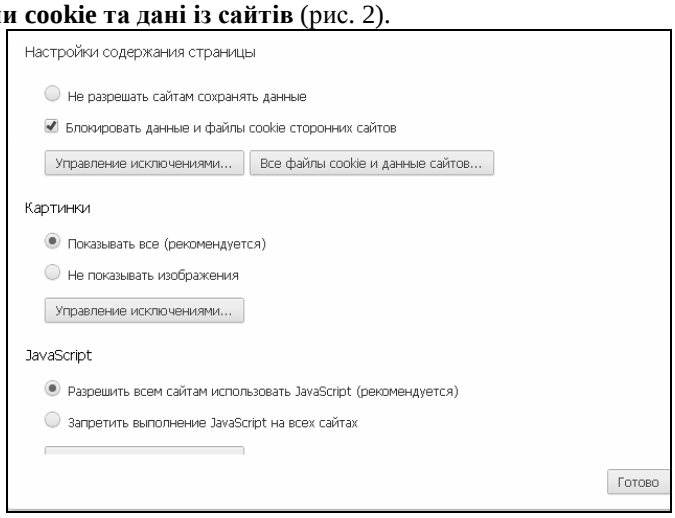


Рис. 1. Вікно налаштування вмісту сторінок Google Chrome

12. Самостійно видаліть файли cookie від сайтів, які не заслуговують на вашу довіру. Якщо необхідно швидко видалити всі файли cookie, то натисніть кнопку **Видалити все**.

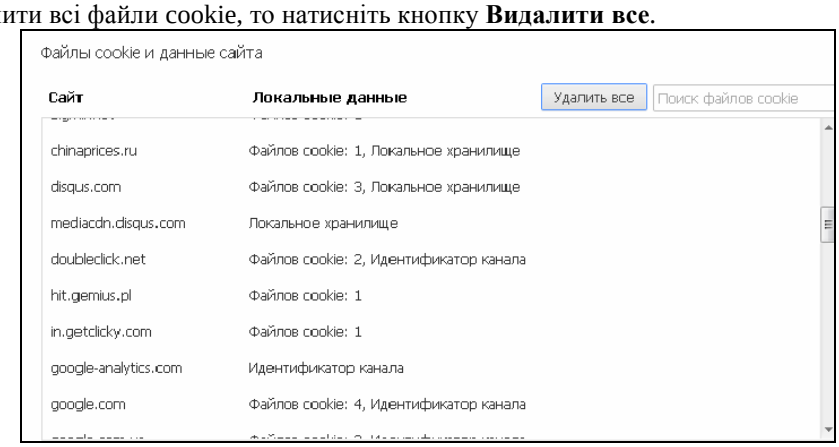


Рис.2.Діалогове вікно Файли cookie та дані із сайтів

13. Щоб браузер Google Chrome автоматично видаляв файли cookie при закритті усіх вікон, у діалоговому вікні **Налаштування вмісту** встановіть прапорець **Зберігати локальні дані лише до закриття веб-оглядача**. Якщо ж необхідно заблокувати всі файли cookie, виберіть **Не дозволяти сайтам зберігати дані**. При блокуванні файлу cookie в адресному рядку відображається  .
14. Для задання винятків з правил обробки cookie-файлів натисніть кнопку **Керувати винятками**. У вікні, яке відкриється, введіть ім'я домену, для якого потрібно встановити виняток (ваш улюблений сайт). Щоб створити виключення для всього домену, вставте перед його ім'ям [*.] (рис. 3). Для задання домену також можна вказати його IP-адресу, IPv6-адресу або URL.

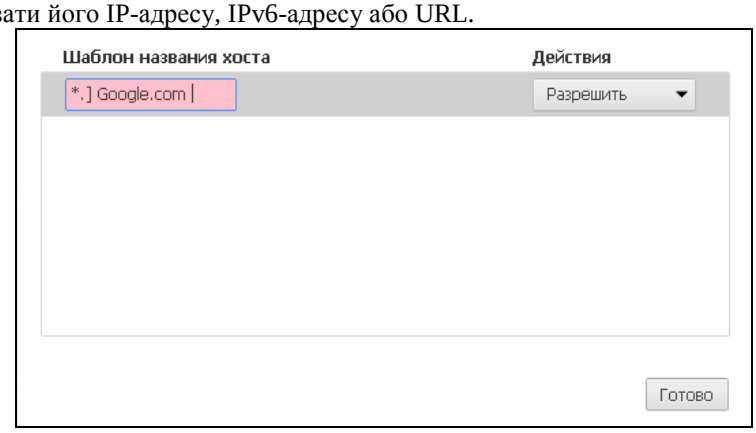


Рис. 3. Вікно формування винятків

15. За допомогою меню **Поведінка** дозвольте обраному сайту створювати файли cookie (при виборі ж параметра **Очищати під час виходу** файли cookie видалятимуться, як тільки ви закриєте браузер).
16. Самостійно дослідіть інші налаштування вмісту сторінки браузера Google Chrome.

17. Закрийте Google Chrome.

**Налаштування параметрів безпеки браузера Internet Explorer**

18. Завантажте браузер Internet Explorer (надалі – IE).
19. Для перевірки можливості блокування окремого вузла виконайте наступні дії:
    19.1. В головному меню оберіть підпункт **Сервіс – Властивості оглядача**;
    19.2. У вікні, що з'явиться, перейдіть на вкладку **Конфіденційність** (рис. 4) та натисніть кнопку **Вузли**;

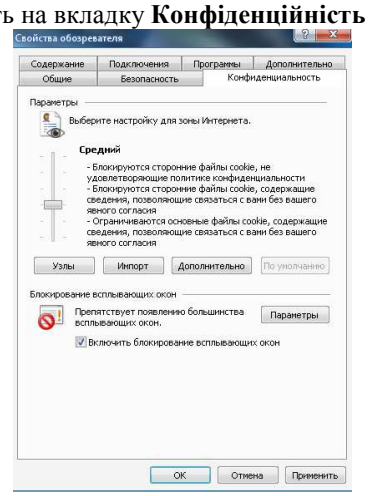


Рис. 4. Налаштування параметрів конфіденційності в IE

    19.3. У виведеному вікні в рядку для задання адреси введіть адресу сайту *www.ukr.net*, і натисніть кнопку **Блокувати**;
    19.4. Зайдіть на сайт *www.ukr.net* та спробуйте відкрити на ньому вашу поштову скриньку. Що при цьому відбувається?
    19.5. Самостійно видаліть вузол *www.ukr.net* зі списку заблокованих вузлів та спробуйте знову зайти на цьому вузлі у вашу поштову скриньку. Чи вдалося це зробити?

**В домашніх умовах:**

20. В IE самостійно перейдіть у вікно **Властивості оглядача** та активізуйте у ньому вкладку **Безпека**.
21. Відмітьте піктограму **Інтернет** і у групі **Рівень безпеки для цієї зони** натисніть кнопку **Інший** (рис. 5).

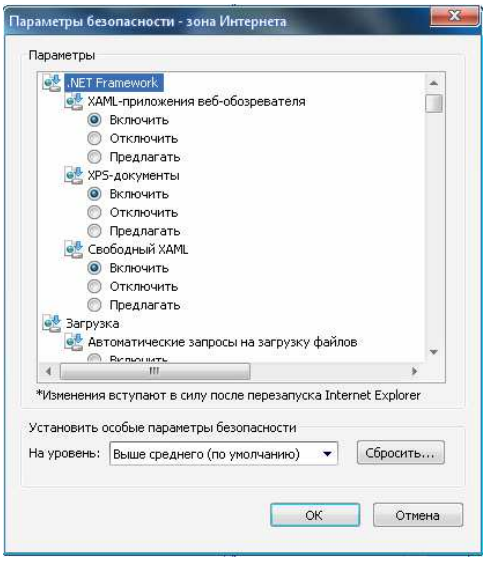


Рис. 5. Налаштування параметрів безпеки в IE

22. У розділі **Параметри** перегляньте налаштування параметрів безпеки, самостійно забезпечте завантаження файлів на основі вмісту, а не розширення та блокування спливаючих вікон і натисніть кнопку **ОК**.
23. Для підвищення загального рівня безпеки і захисту комп'ютера від будь-яких несанкціонованих завантажень, використайте можливість занесення небезпечних сайтів у зону **Обмежені вузли**. Для перевірки цієї можливості виконайте наступні дії:
    23.1. Самостійно поверніться у вікно **Властивості оглядача**;
    23.2. На вкладці **Безпека** відмітьте посилання **Обмежені вузли**;
    23.3. Натисніть кнопку **Вузли**, в рядку для задання адреси введіть *comp.ucoz.net* та натисніть кнопку **Додати** (рис. 6);

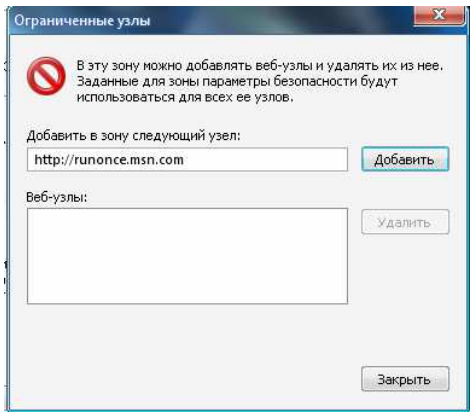


Рис. 6. Вікно формування списку заборонених вузлів

23.4. Почергово закрийте вікна **Обмежені вузли** та **Властивості оглядача** з збереженням внесених змін;
23.5. Спробуйте завантажити сторінку *comp.ucoz.net*. Що при цьому відбувається?
23.6. Самостійно видаліть вузол *comp.ucoz.net* зі списку обмежених вузлів та забезпечте відображення цієї сторінки у вікні оглядача.

## Завершальний етап заняття

24. Створіть електронний лист з відповідями на контрольні запитання у своїй поштовій скриньці на сайті *gmail.com*. Тему листа сформуйте за шаблоном *<група>_<номер лабораторної>_<прізвище ім'я>*, наприклад: *ЕК51_ЛР9_Величко Володимир*. Надішліть створений лист на адресу *LRZaxInf@gmail.com*

**Контрольні запитання.**

1. Які можливості налаштування безпеки має Google Chrome?
2. Як вимкнути потенційно вразливі компоненти браузера?
3. Що таке файли cookies? Навіщо їх видаляють?
4. Налаштування яких параметрів вмісту сторінки можливо у браузері Google Chrome?
5. Як в IE заблокувати окремі вузли? Навіщо це робити?
6. Як в IE віднести окремий вузол до переліку обмежених? Навіщо це робити?
7. Який з сучасних браузерів захищений найкраще на Вашу думку? Обґрунтуйте свою позицію