Модуль: Шкідливе програмне забезпечення

Практична вправа:
«Вбудована в ОС Windows 10 система захисту від вірусів і загроз»

Навчальна мета заняття: налаштувати і перевірити ефективність вбудованої в ОС Windows 10 системи захисту від вірусів і загроз.

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

Устаткування:
персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі Інтернет, веб-браузер Google Chrome, тестові файли.

Порядок проведення заняття

На панелі задач у полі пошуку ввести запит «захист», обрати «Захист від вірусів і загроз» – «Налаштування захисту від вірусів і загроз» – «Керування параметрами», увімкнути (або переконатися, що ввімкнено) «Захист у реальному часі», «Захист у хмарі», «Автоматичне надсилання зразків» (рис. 1).

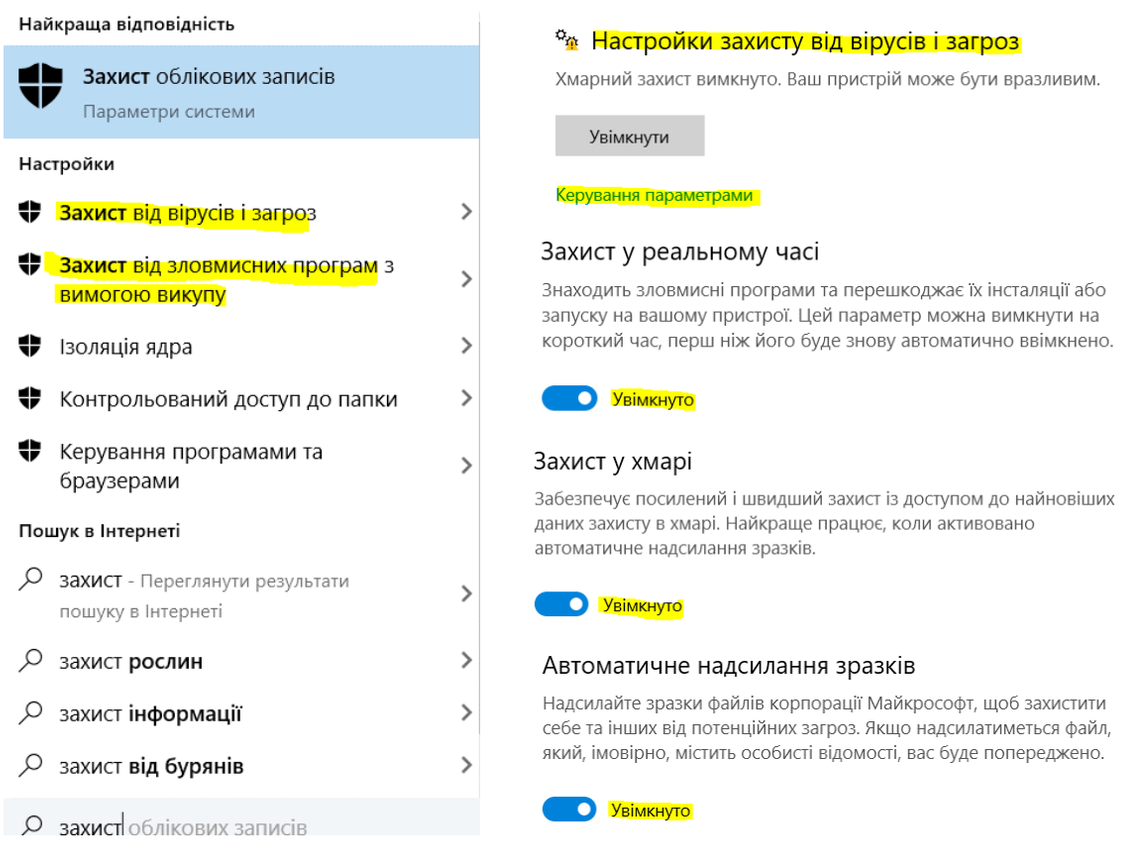

Рис. 1. Налаштування захисту від вірусів

Перейти із розділу «Налаштування захисту від вірусів і загроз» до розділу «Брандмауер і захист мережі» і переконатися, що брандмауер увімкнений (рис. 2). Якщо брандмауер вимкнений, то клацнути на відповідні посилання («Мережа домена», «Приватна мережа», «Загальнодоступна мережа») та ввімкнути брандмауер.

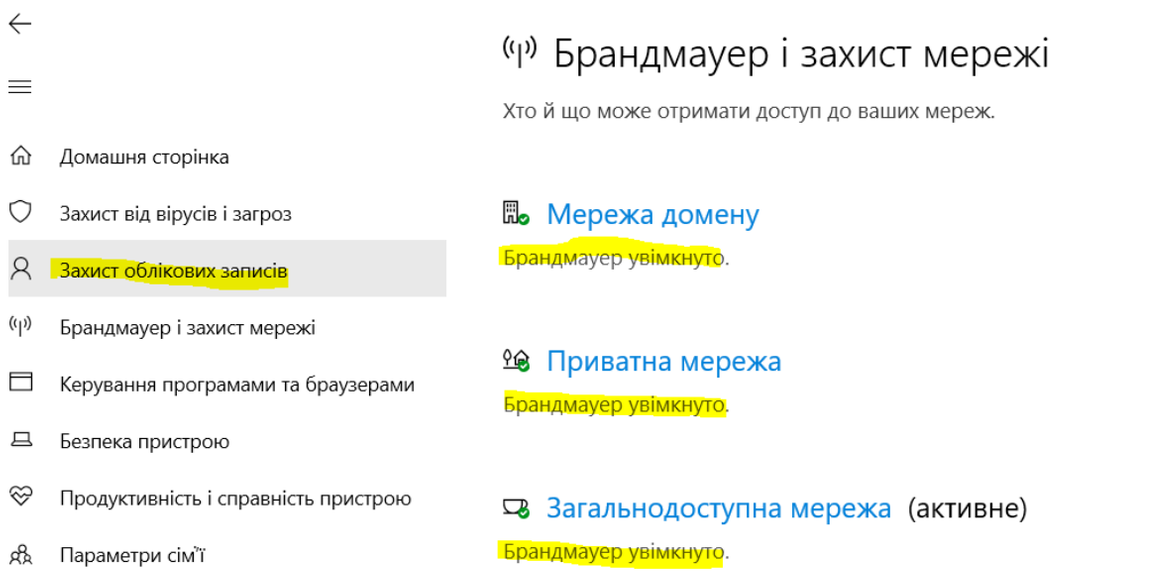

Рис. 2. Налаштування захисту мережі

Перейти із розділу «Налаштування захисту від вірусів і загроз» до розділу «Керування програмами та браузерами», де обрати (рис. 3):

- «Блокувати» («Попереджати») для параметру «Перевірити програми та файли»;
- «Блокувати» («Попереджати») для параметру «SmartScreen для Microsoft EDGE»;
- «Попереджати» для параметру «Фільтр SmartScreen для програм з Microsoft Store».

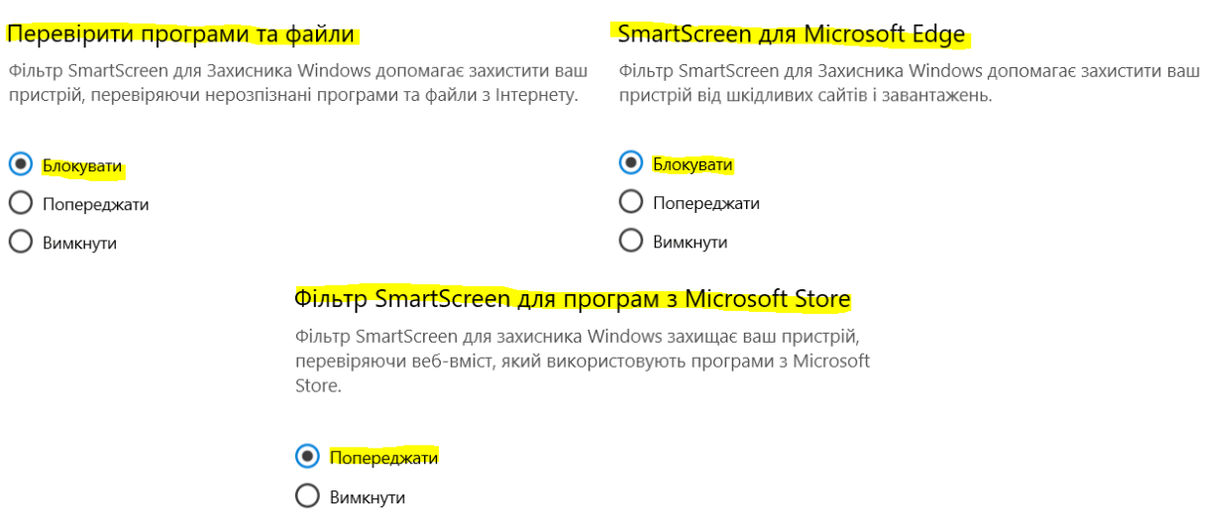

Рис. 3. Налаштування SmartScreen

У розділі «Керування програмами та браузерами» перейти до «Налаштування запобігання експлойтам» та переконатися, що для усіх налаштувань встановлено «Використовувати стандартне значення (Увімкнуто)» (рис. 4).

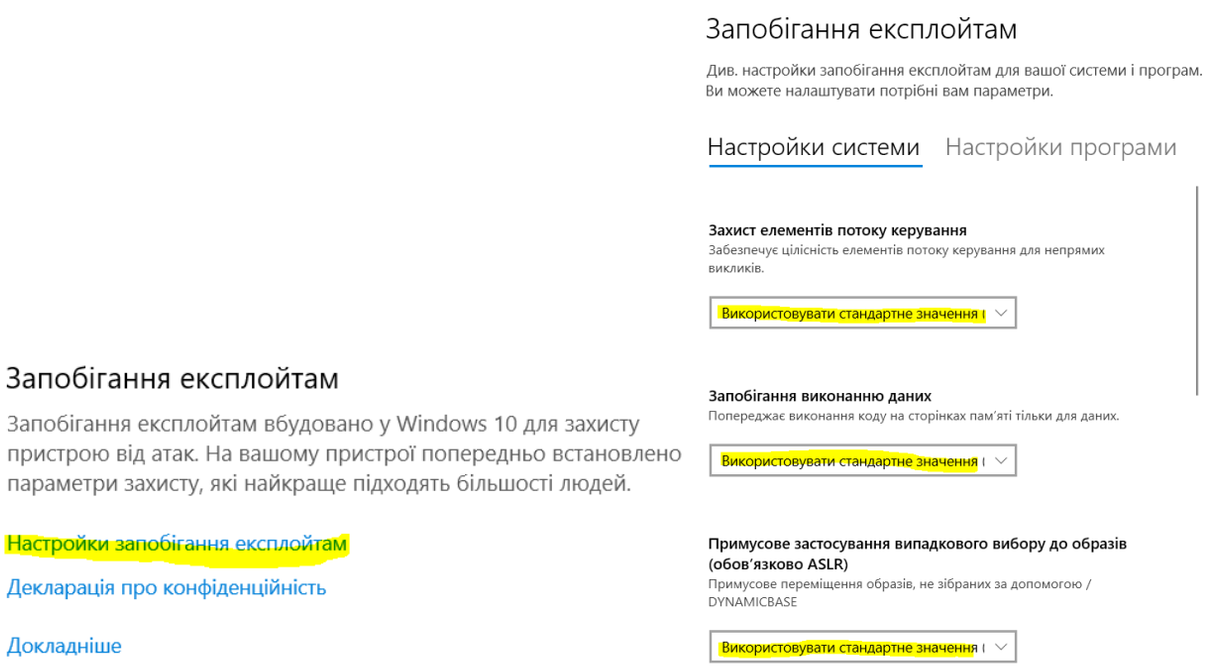

Рис. 4. Налаштування «Настройки запобігання експлойтам»

Після здійснення усіх дій вийти із меню налаштувань системи.

У налаштуваннях веб-браузера Google Chrome «Конфіденційність і безпека» – «Безпечний перегляд» обрати «Захист вимкнено (не рекомендовано)» (рис. 5) та спробувати завантажити будь-який доступний у мережі файл зі шкідливим кодом, наприклад, за посиланням is.gd/7Xad5B.

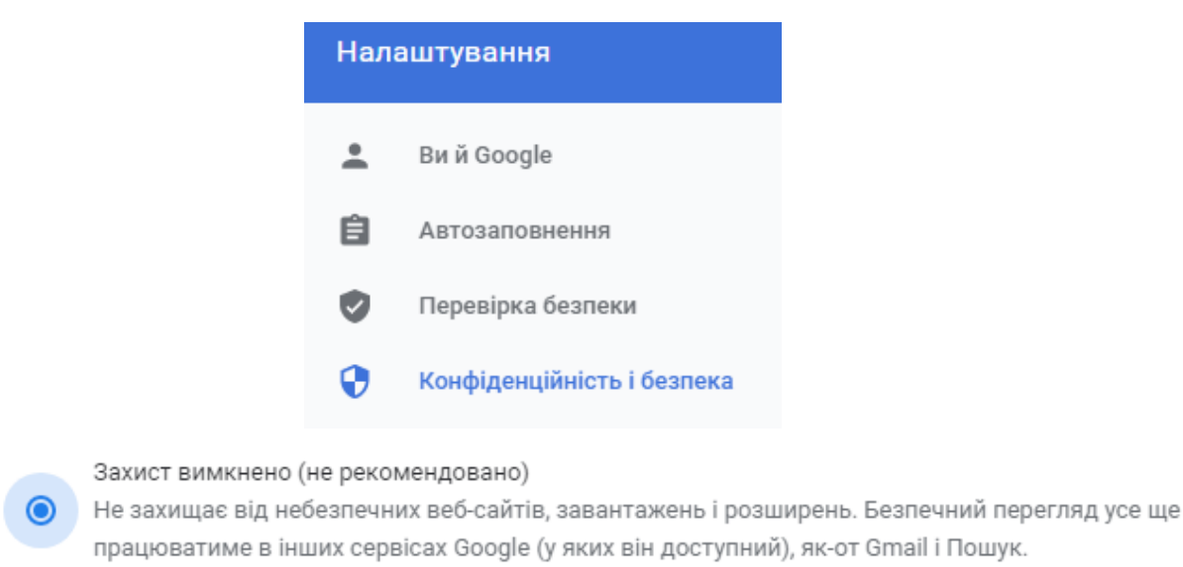

Рис. 5. Вимкнення захисту у веб-браузері Google Chrome

Після завантаження файлу зі шкідливим кодом переконатися, що системою захисту від вірусів було виявлено та заблоковано цей шкідливий файл (рис. 6).

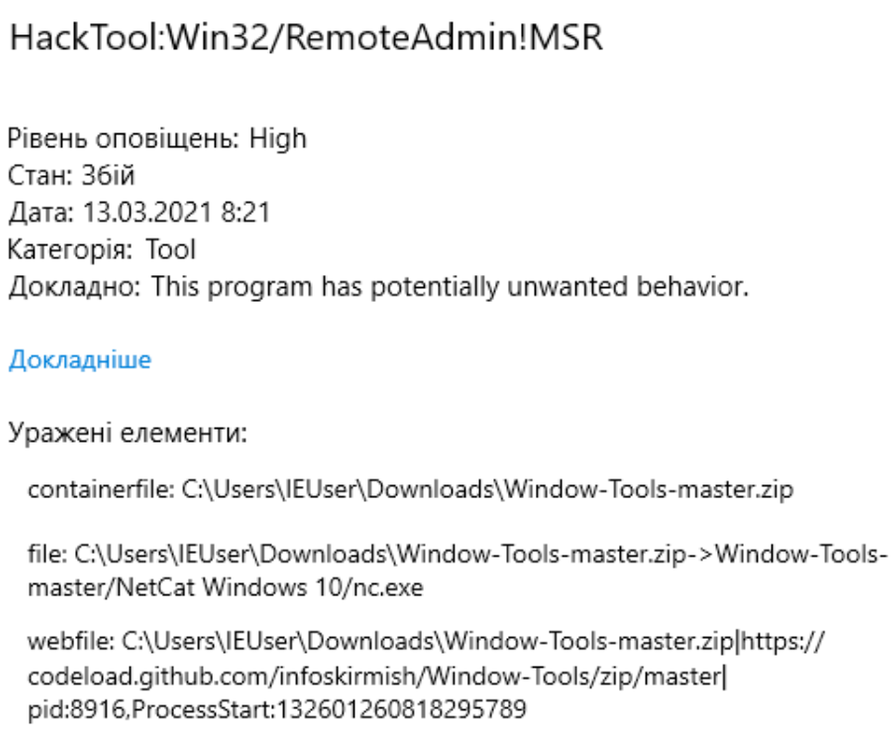

Рис. 6. Виявлення та блокування шкідливого файлу