## 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).

Найкраща відповідність		<sup>о</sup> ». Настройки захисту від вірусів і загроз
<b>Захист</b> облікових записів Параметри системи		Хмарний захист вимкнуто. Ваш пристрій може бути вразливим.
Настройки		Увімкнути
Захист від вірусів і загроз	>	Керування параметрами
<ul> <li>Захист від зловмисних програм з вимогою викупу</li> <li>Ізоляція ядра</li> </ul>	>	Захист у реальному часі Знаходить зловмисні програми та перешкоджає їх інсталяції або запуску на вашому пристрої. Цей параметр можна вимкнути на короткий час, перш ніж його буде знову автоматично ввімкнено.
🗣 Контрольований доступ до папки	>	Увімкнуто
Керування програмами та браузерами	>	Захист у хмарі Забезпечує посилений і швилший захист із доступом до найновіших
Пошук в Інтернеті		даних захисту в хмарі. Найкраще працює, коли активовано автоматичне налсилання зразків
захист - Переглянути результати пошуку в Інтернеті	>	Увімкнуто
$\mathcal P$ захист <b>рослин</b>	>	Автоматичне надсилання зразків
Э захист інформації	>	Надсилайте зразки файлів корпорації Майкрософт, щоб захистити себе та інших від потенційних загроз. Якщо надсилатиметься файл, який, імовірно, містить особисті відомості, вас буде попереджено.
🔎 захист <b>від бурянів</b>	>	
Я захист облікових записів		Увімкнуто

## 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.

$\leftarrow$		(Ч) Брандмауер і захист мережі хто й що може отримати доступ до ваших мереж.
仚	Домашня сторінка	
$\bigcirc$	Захист від вірусів і загроз	🖫 Мережа домену
8	Захист облікових записів	Брандмауер увімкнуто.
(y)	Брандмауер і захист мережі	
	Керування програмами та браузерами	‱ Приватна мережа Брандмауер увімкнуто.
旦	Безпека пристрою	
$\otimes$	Продуктивність і справність пристрою	🕞 Загальнодоступна мережа (активне)
ጽ	Параметри сім'ї	Брандмауер увімкнуто.

### 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».

Перевірити програми та файли	SmartScreen для Microsoft Edge			
Фільтр SmartScreen для Захисника Windows допомагає захистити ваш пристрій, перевіряючи нерозпізнані програми та файли з Інтернету.	Фільтр SmartScreen для Захисника Windows допомагає захистити ваш пристрій від шкідливих сайтів і завантажень.			
Блокувати	• Блокувати			
О Попереджати	О Попереджати			
О Вимкнути	О Вимкнути			
Фільтр SmartScreen для пр	ограм з Microsoft Store			
Фільтр SmartScreen для захисника перевіряючи веб-вміст, який викор Store.	Фільтр SmartScreen для захисника Windows захищає ваш пристрій, перевіряючи веб-вміст, який використовують програми з Microsoft Store.			

Рис. 3. Налаштування SmartScreen

О Вимкнути

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

## Запобігання експлойтам

	Див. настройки запобігання експлойтам для вашої системи і програм Ви можете налаштувати потрібні вам параметри.
	Настройки системи Настройки програми
	Захист елементів потоку керування Забезпечує цілісність елементів потоку керування для непрямих викликів.
Запобігання експлойтам Запобігання експлойтам вбудовано у Windows 10 для захисту пристрою від атак. На вашому пристрої попередньо встановлено	Запобігання виконанню даних Попереджає виконання коду на сторінках пам'яті тільки для даних. Використовувати стандартне значення ( )
параметри захисту, які наикраще підходять опьшості людеи. Настройки запобігання експлойтам Декларація про конфіденційність	Примусове застосування випадкового вибору до образів (обов'язково ASLR) Примусове переміщення образів, не зібраних за допомогою / DYNAMICBASE
Докладніше	Використовувати стандартне значення Г 🗸

## 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.



Захист вимкнено (не рекомендовано)

Не захищає від небезпечних веб-сайтів, завантажень і розширень. Безпечний перегляд усе ще працюватиме в інших сервісах Google (у яких він доступний), як-от Gmail і Пошук.

## 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).

# HackTool:Win32/RemoteAdmin!MSR

Рівень оповіщень: High Стан: Збій Дата: 13.03.2021 8:21 Категорія: Tool Докладно: This program has potentially unwanted behavior.

#### Докладніше

Уражені елементи:

containerfile: C:\Users\IEUser\Downloads\Window-Tools-master.zip

file: C:\Users\IEUser\Downloads\Window-Tools-master.zip->Window-Toolsmaster/NetCat Windows 10/nc.exe

webfile: C:\Users\IEUser\Downloads\Window-Tools-master.zip|https:// codeload.github.com/infoskirmish/Window-Tools/zip/master| pid:8916,ProcessStart:132601260818295789

## Рис. 6. Виявлення та блокування шкідливого файлу