МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

кафедра протидії кіберзлочинності, факультет № 4

МЕТОДИЧНІ МАТЕРІАЛИ

до практичних 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 № 1 Загальні правила безпечної роботи з пристроями та програмами

Практичне заняття «Налаштування захисних механізмів у мобільному пристрої»

Навчальна мета заняття: відповідно до конкретних умов навчитися налаштовувати параметри мобільного пристрою та встановлених на ньому програм для безпечного використання.

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», програма виведення зображення з мобільного пристрою на екран монітора персонального комп'ютера, Telegram, Viber, WhatsApp

Порядок проведення заняття

Налаштування безпеки мобільного пристрою слід організовувати за двома головними напрямами:

1) налаштування операційної системи мобільного пристрою;
2) налаштування прикладних програм.

Що стосується першого напряму, то, передусім, для безпечного користування смартфоном слід встановити надійний механізм його розблокування. Для цього потрібно зайти у налаштування системи та встановити пароль, який буде достатньо довгим та складатиметься з літер, цифр та спеціальних символів (рис. 1).

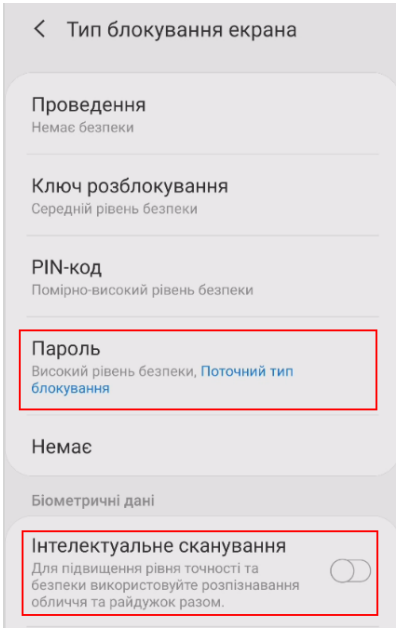


Рис. 1. Налаштування паролю для розблокування пристрою

Для виконання розглянутого завдання на iPhone: «Налаштування» → «Touch ID і код-пароль» → «Запит паролю: одразу» → «Змінити пароль» → «Довільний код (літери + цифри).

У випадку, якщо дозволяють функції пристрою, можна також налаштувати біометричну ідентифікацію.

Крім наведеного, слід переглянути інші налаштування безпеки та встановити їх таким чином, щоб вони відповідали потрібному рівню захисту (рис. 2).

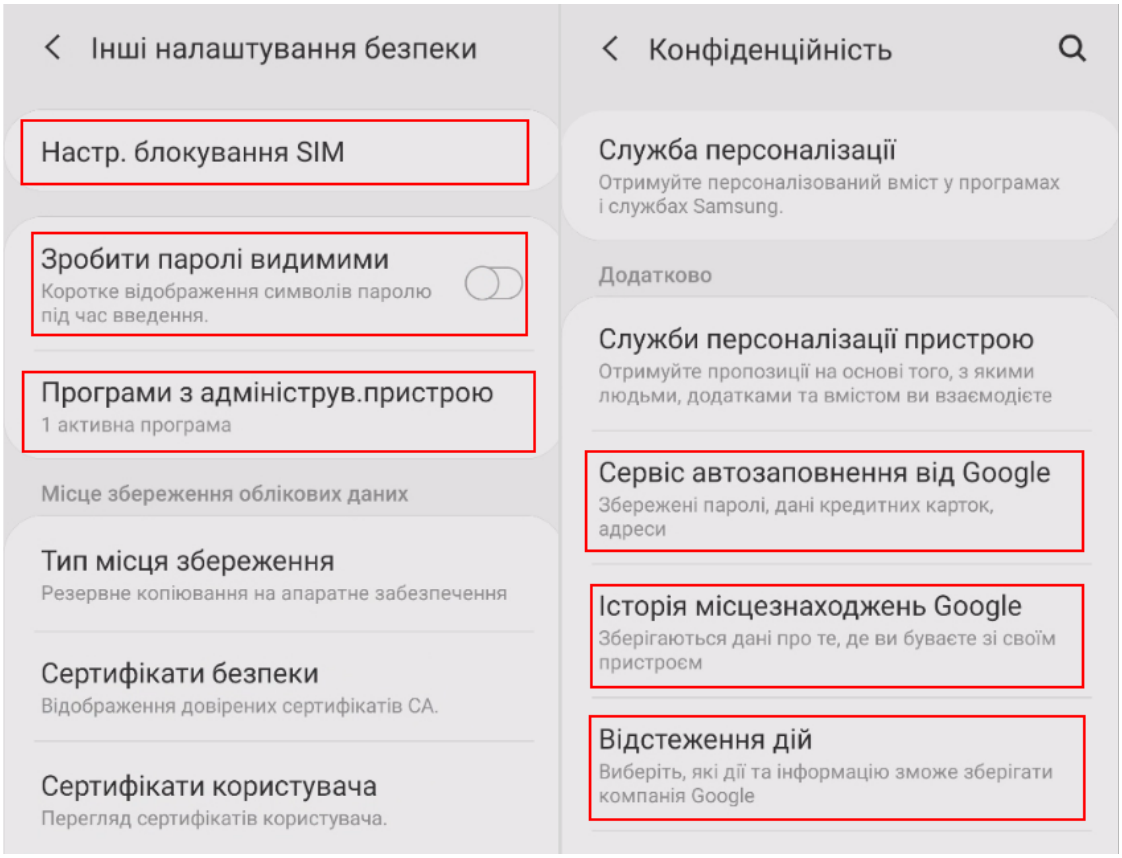


Рис. 2. Налаштування параметрів безпеки та конфіденційності

Після проведення загальних налаштувань операційної системи слід убезпечити себе від витоку інформації із заблокованого пристрою. Для цього, перш за все, потрібно вимкнути повідомлення на заблокованому екрані (рис. 3). Також відповідні налаштування можуть бути встановлені окремо для кожного застосунку («Налаштування» → «Програми»). Виконання описаних дій дозволить стороннім особам бачити приватні повідомлення.

Для виконання розглянутого завдання на iPhone: «Налаштування» → «Пароль» → «Доступ з блокуванням екрану»; «Налаштування» → «Сповіщення» → «Показ мініатюр» → «Без блокування».

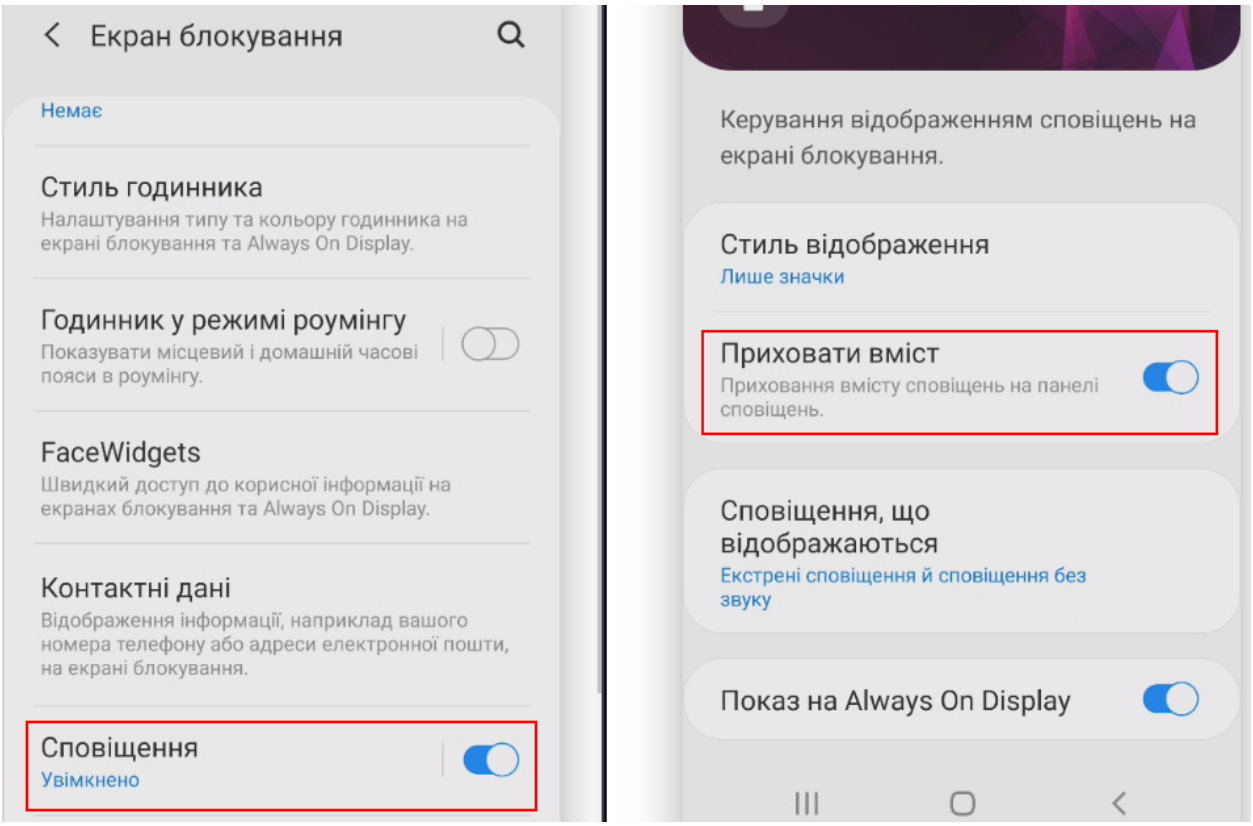


Рис. 3. Вимкнення повідомлень

Слід пам’ятати, що окремі налаштування стосуються не тільки самого мобільного пристрою, але й облікового запису. Враховуючи це потрібно переглянути налаштування безпеки облікового запису та встановити відповідні параметри.

Одним з прикладів такого налаштування є встановлення двофакторної автентифікації (рис. 4).

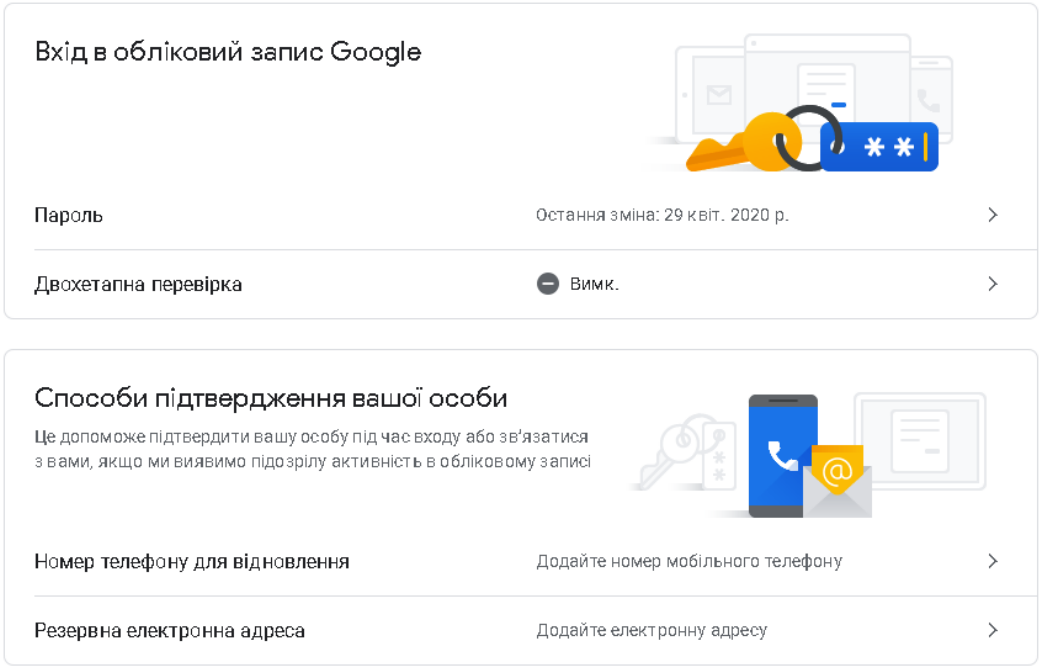


Рис. 3. Налаштування безпеки облікового запису

Для виконання розглянутого завдання на iPhone: «Сайт Apple ID» → «Двофакторна ідентифікація» → «Увімкнути»; «Безпека» → «Перевірені номери телефонів» → «Змінити» → «Додати номер телефону з можливістю приймання текстових повідомлень».

Для заборони відслідковування своїх дій після авторизації в обліковому записі можна встановити спеціальне розширення (https://tools.google.com/dlpage/gaoptout?hl=ru).

Залежно від конкретних умов слід правильно налаштувати синхронізацію даних. Якщо Ви не бажаєте зберігати відомості на віддаленому ресурсі, потрібно вимкнути автоматичну синхронізацію даних у налаштуваннях відповідного облікового запису в мобільному пристрої (рис. 4).

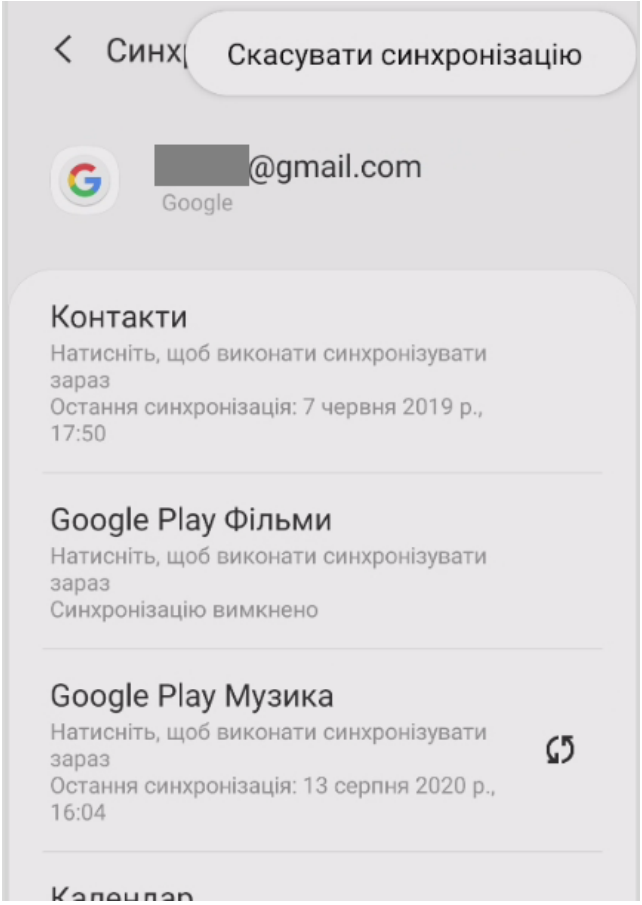


Рис. 4. Налаштування синхронізації

Для виконання розглянутого завдання на iPhone: «Налаштування» → «Apple ID, iCloud, медіаматеріали» → «iCloud» → «iCloud Drive» → «Фото».

Крім наведеного, слід також вимкнути автоматичне підключення до Wi-Fi мереж (рис. 5). Якщо у Вас налаштоване автопідключення до відомих точок доступу Wi-Fi, то Ви так само автоматично можете бути під'єднаним до підробленої точки доступу. У подальшому весь трафік Інтернет може бути пропущений через обладнання зловмисника. Це дозволяє порушнику примусово перенаправляти запити з Вашого пристрою на свої ресурси. При цьому Ви можете навіть нічого не помітити.

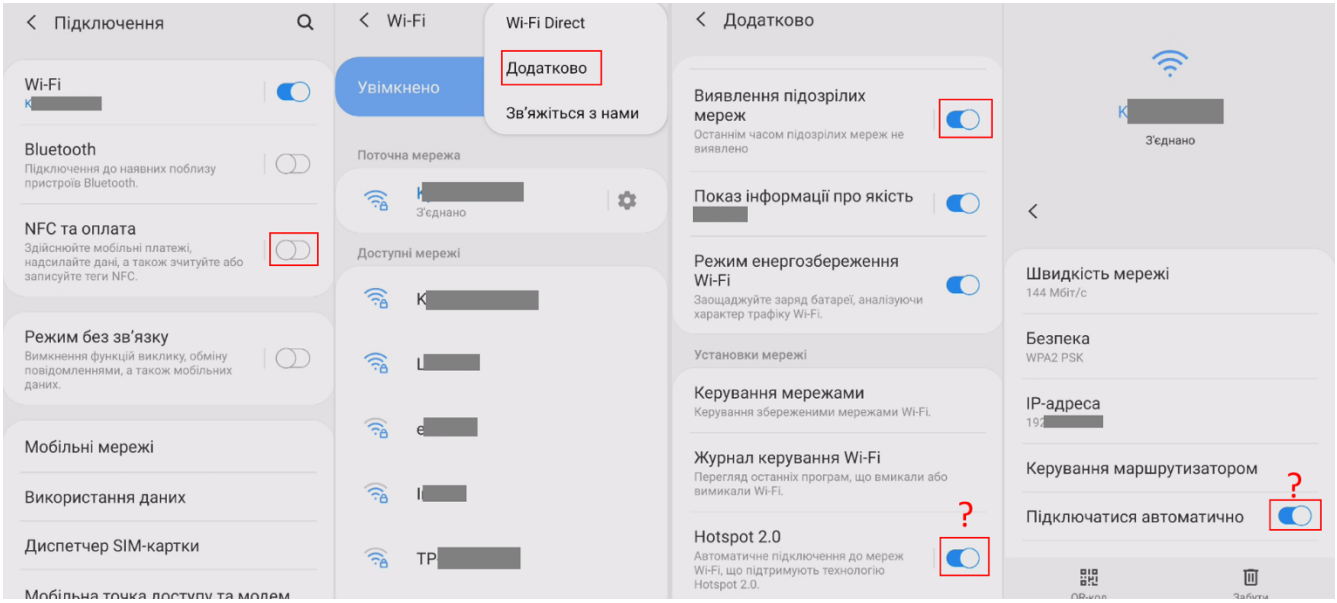


Рис. 5. Налаштування Wi-Fi

Для виконання розглянутого завдання на iPhone: «Налаштування» → «Wi-Fi» → Обрати відповідну мережу → «Автопідключення» → «Вимкнути».

Що стосується налаштувань окремих застосунків, то тут слід передусім звернути увагу на обмеження їх доступу до чутливих даних: файлів на телефоні, контактів, геолокації тощо (рис. 6).

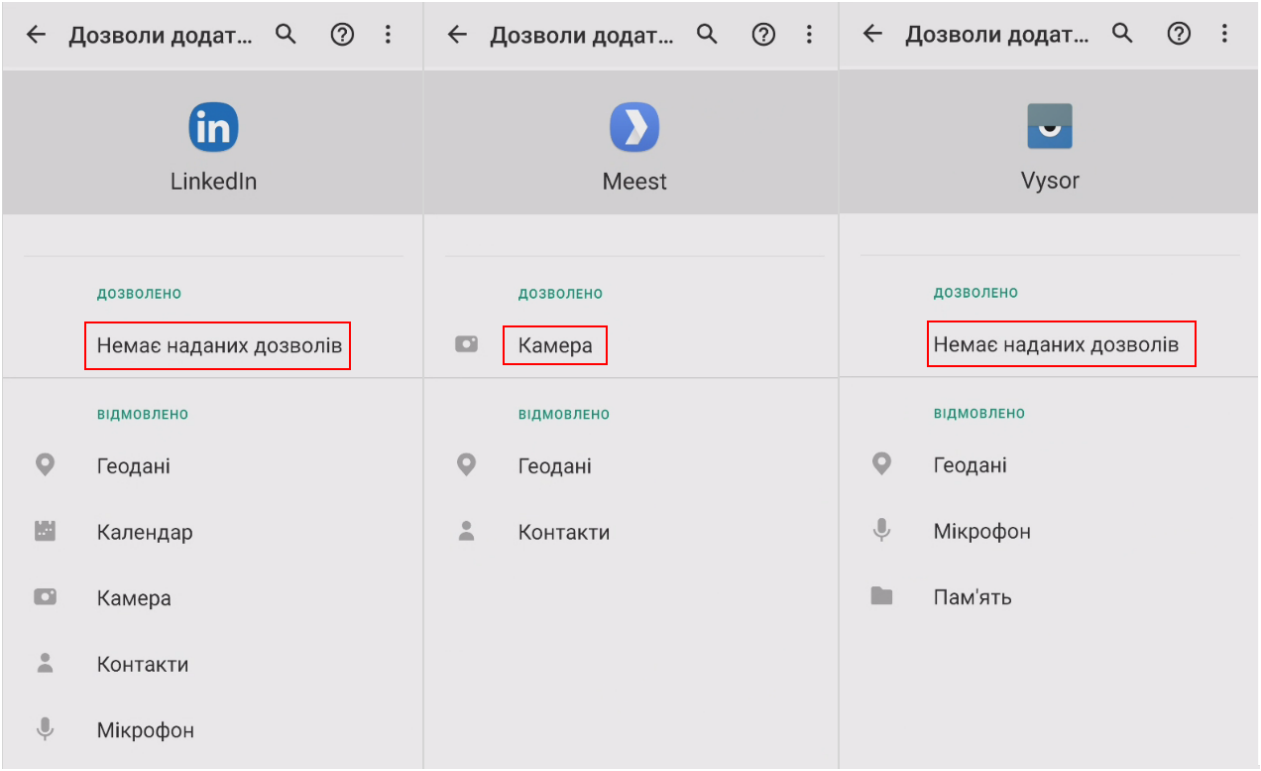


Рис. 6. Налаштування прав доступу для застосунків

Для виконання розглянутого завдання на iPhone: «Налаштування» → «Конфіденційність» → «Геолокація», «Відслідковування» → поставити «Вимкнути» у налаштуваннях відповідних застосунків.

У використовуваних браузерах також слід налаштувати відповідну безпеку. Наприклад, у Google Chrome це можна зробити як на рис. 7.

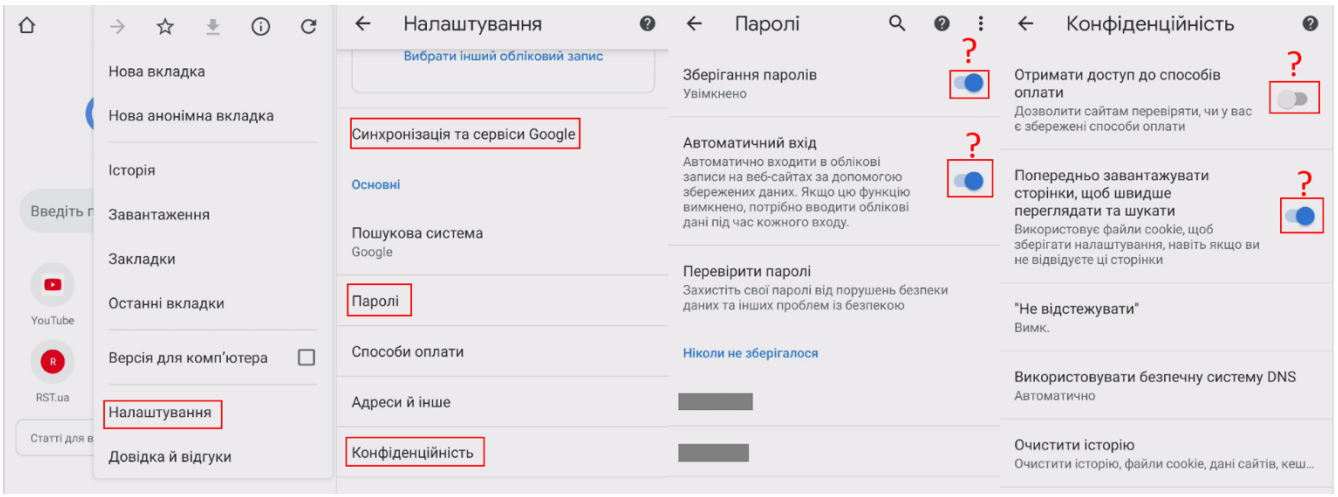


Рис. 7. Налаштування безпеки браузера

Важливою частиною захисту мобільного пристрою є правильне налаштування програм для спілкування (месенджерів). Найбільш поширеними такими рішеннями на теперішній час є Telegram (рис. 8), Viber (рис. 9), WhatsApp (рис. 10).

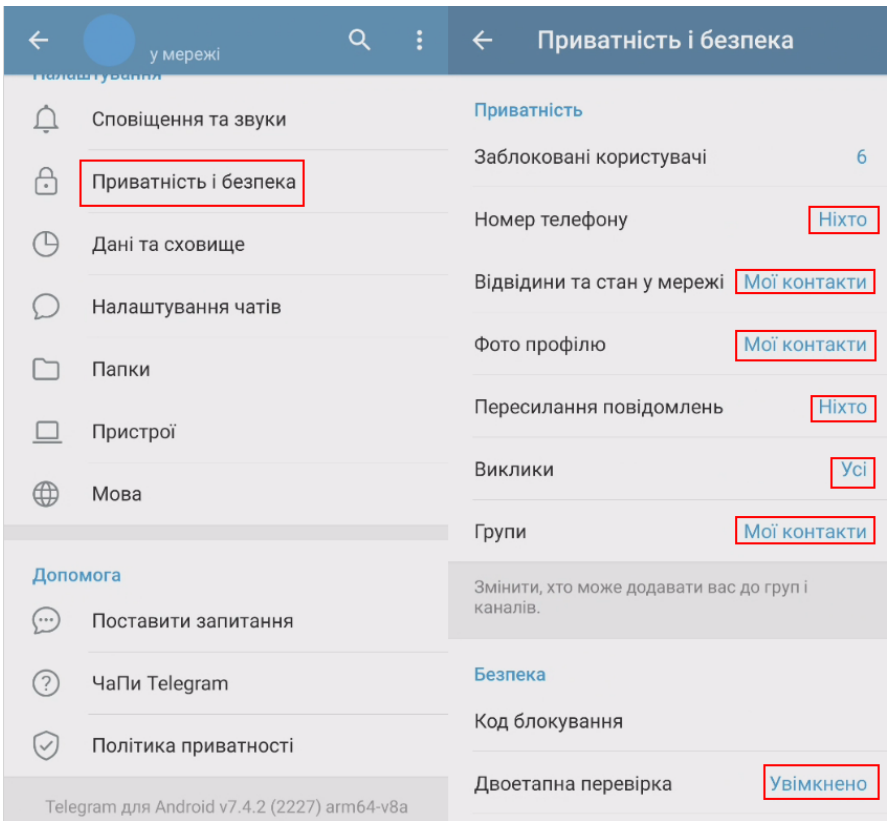


Рис. 8. Налаштування безпеки браузера «Telegram»

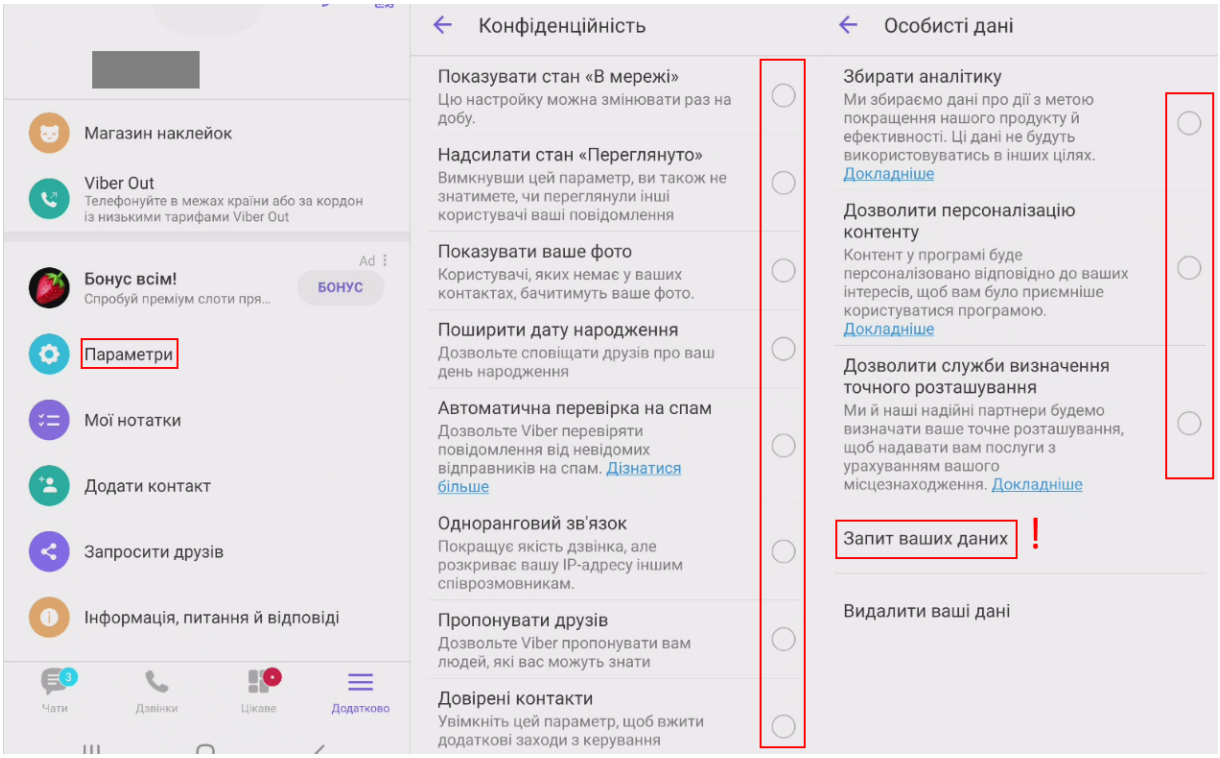


Рис. 9. Налаштування безпеки браузера «Viber»

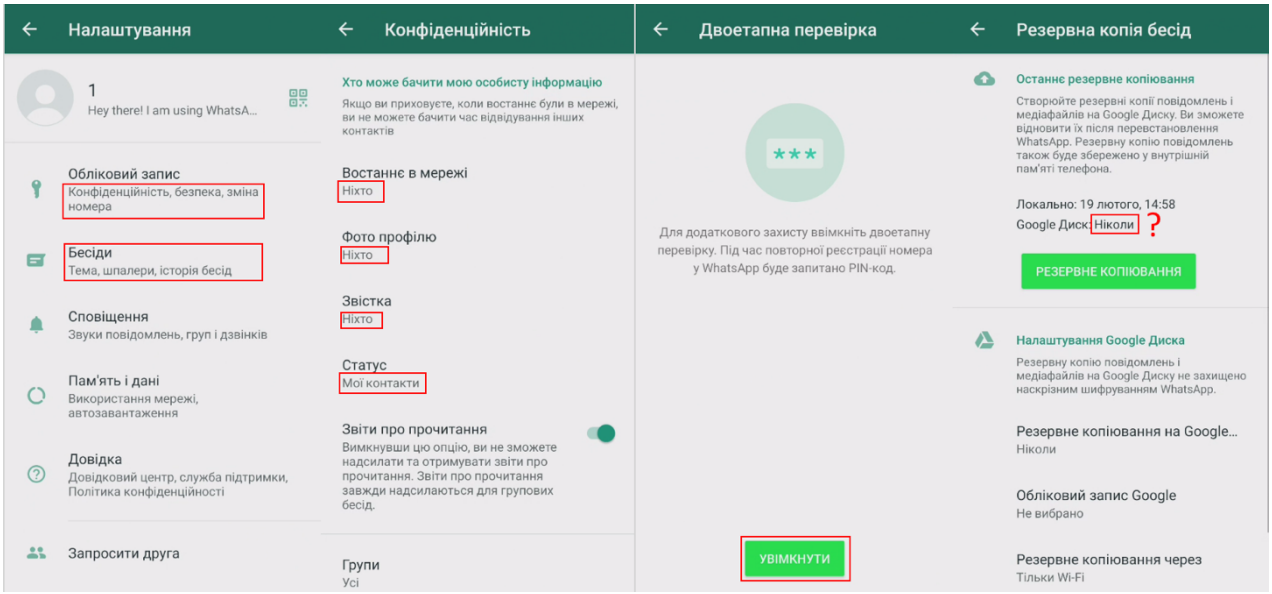


Рис. 10. Налаштування безпеки браузера «WhatsApp»

Щодо налаштувань резервного копіювання даних в різних застосунках, то тут рішення користувач має прийняти самостійно з урахуванням існуючих ризиків.

Завдання

1. Налаштуйте параметри безпеки для:
- операційної системи свого мобільного пристрою;
- облікових записів, прив'язаних до мобільного пристрою;
- встановлених на мобільному пристрої застосунків.

Практичне заняття «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: 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», 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).

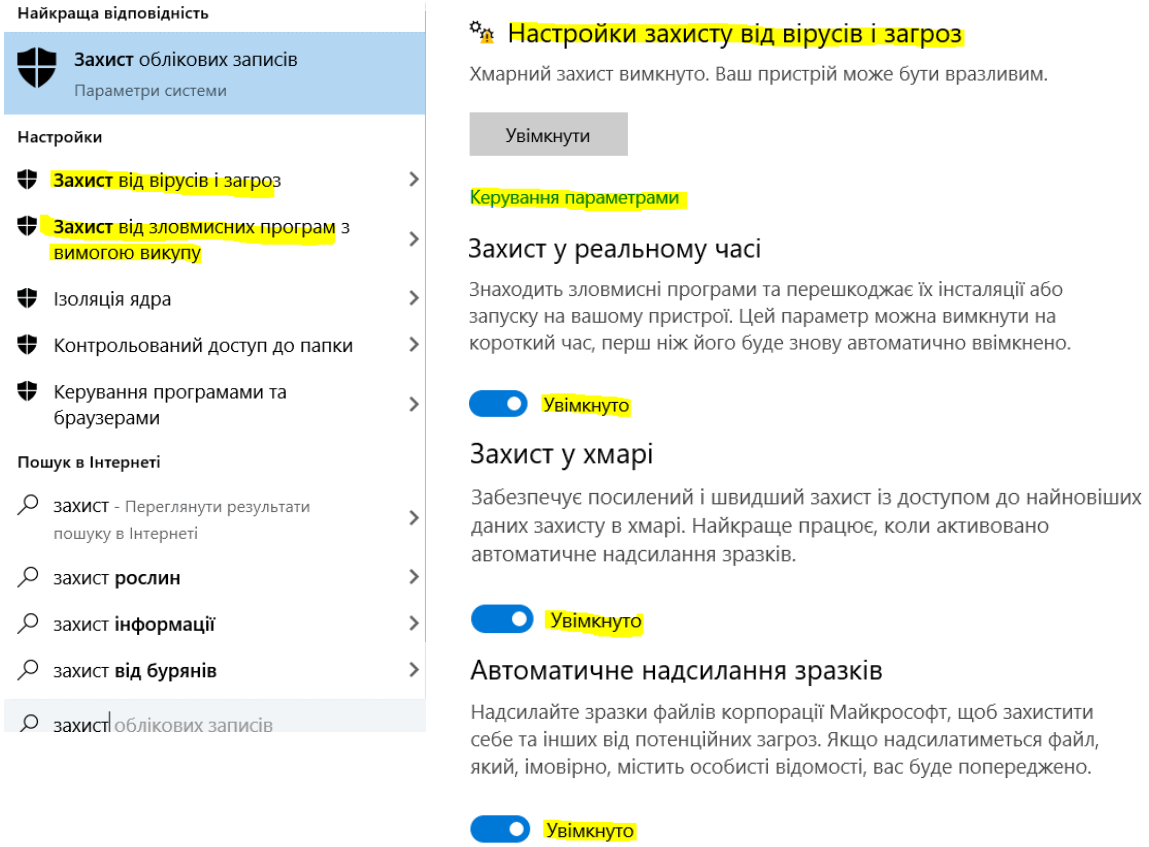


Рис. 1. Налаштування захисту від вірусів

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 домену», «Приватна мережа», «Загальнодоступна мережа») та ввімкнути брандмауер.

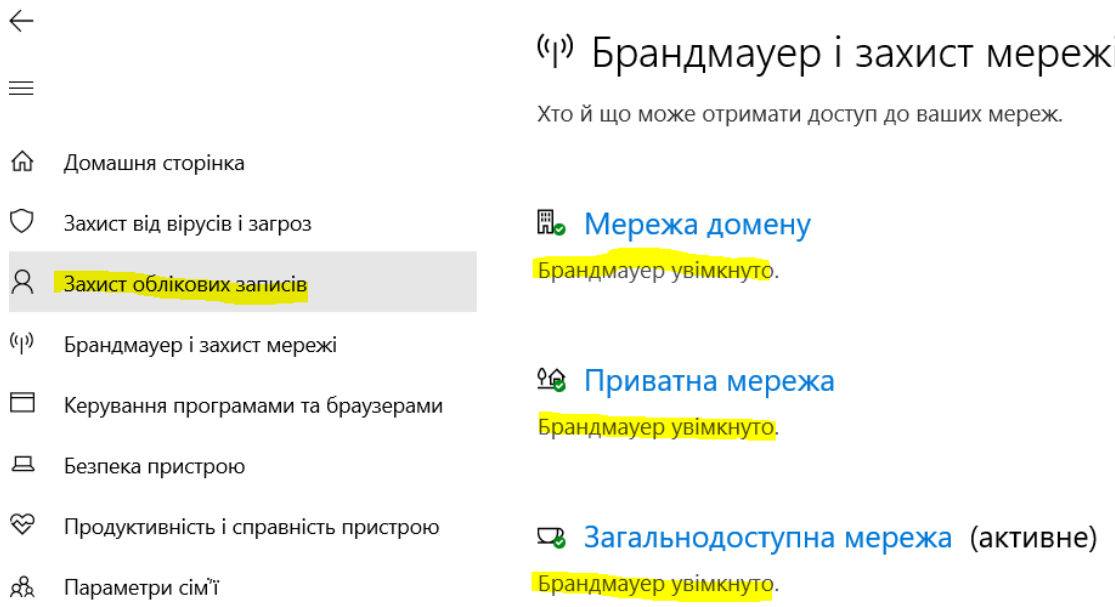


Рис. 2. Налаштування захисту мережі

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».

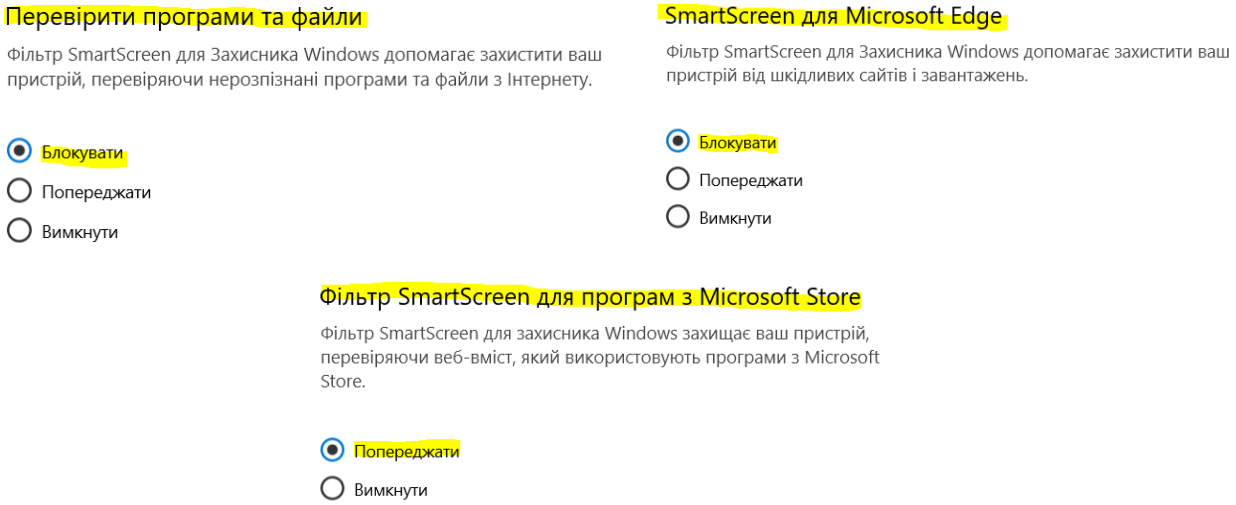


Рис. 3. Налаштування SmartScreen

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

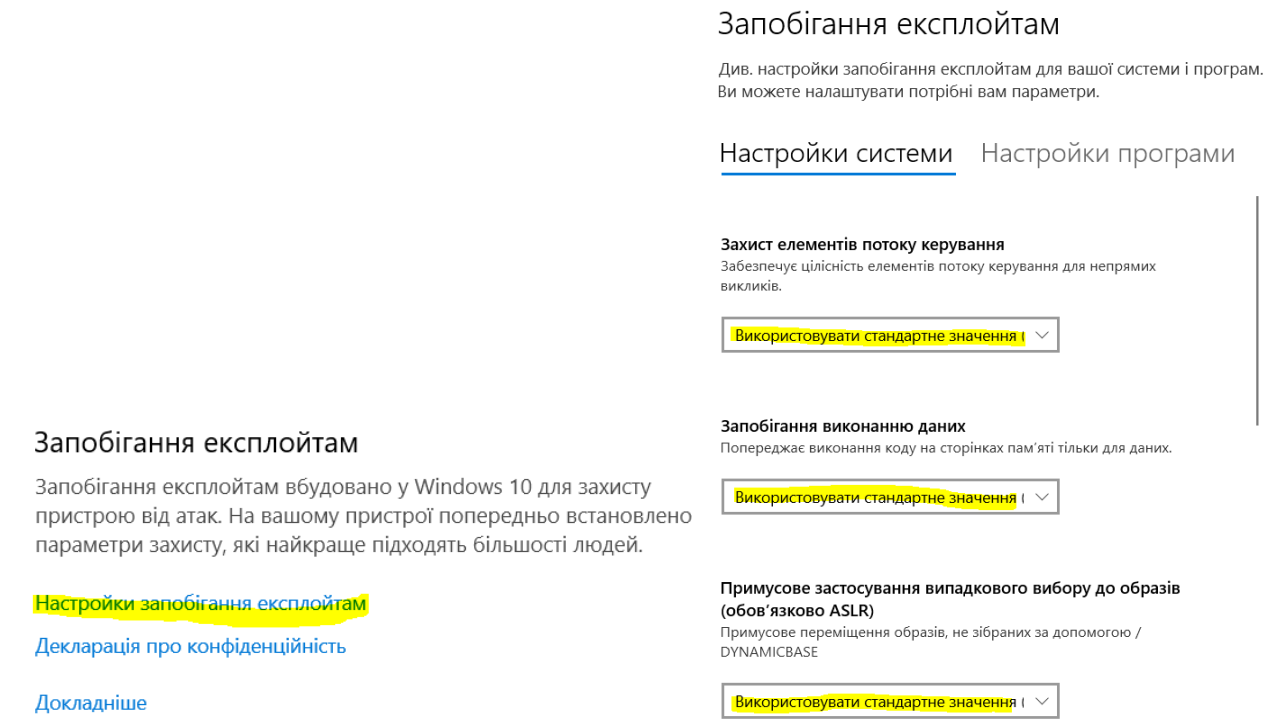


Рис. 4. Налаштування «Настройки запобігання експлойтам»

Після здійснення усіх дій вийти із меню налаштувань системи.

У налаштуваннях веббраузеру 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.

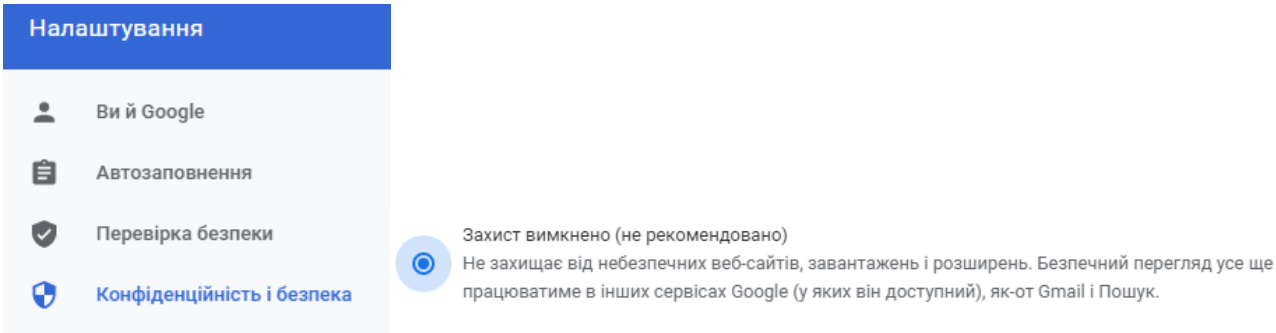


Рис. 5. Вимкнення захисту у веббраузері Google Chrome

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

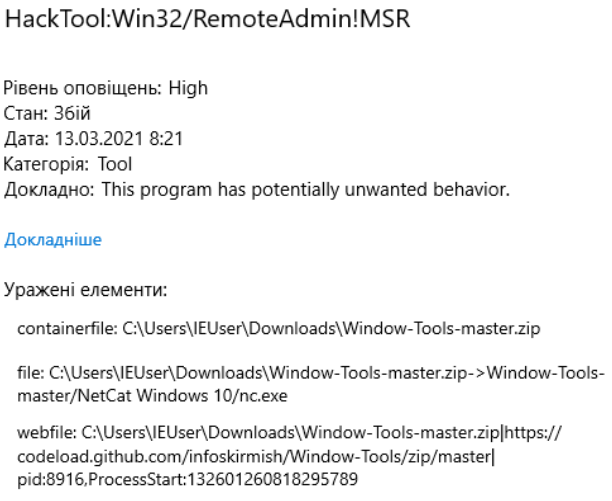


Рис. 6. Виявлення та блокування шкідливого файлу

Практичне заняття «Антивірусні програми ”Zillya!” та ”ZoneAlarm”»

Навчальна мета заняття: встановити і перевірити ефективність антивірусів «Zillya!» та ”ZoneAlarm”.

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».

Порядок проведення заняття

Завантажити і виконати встановлення демонстраційної версії Zillya! Total Security (https://zillya.ua/zillya-total-security). Відкрити антивірус, в меню «Швидкі налаштування» встановити Режим повідомлень: Діалоговий (рис. 1).

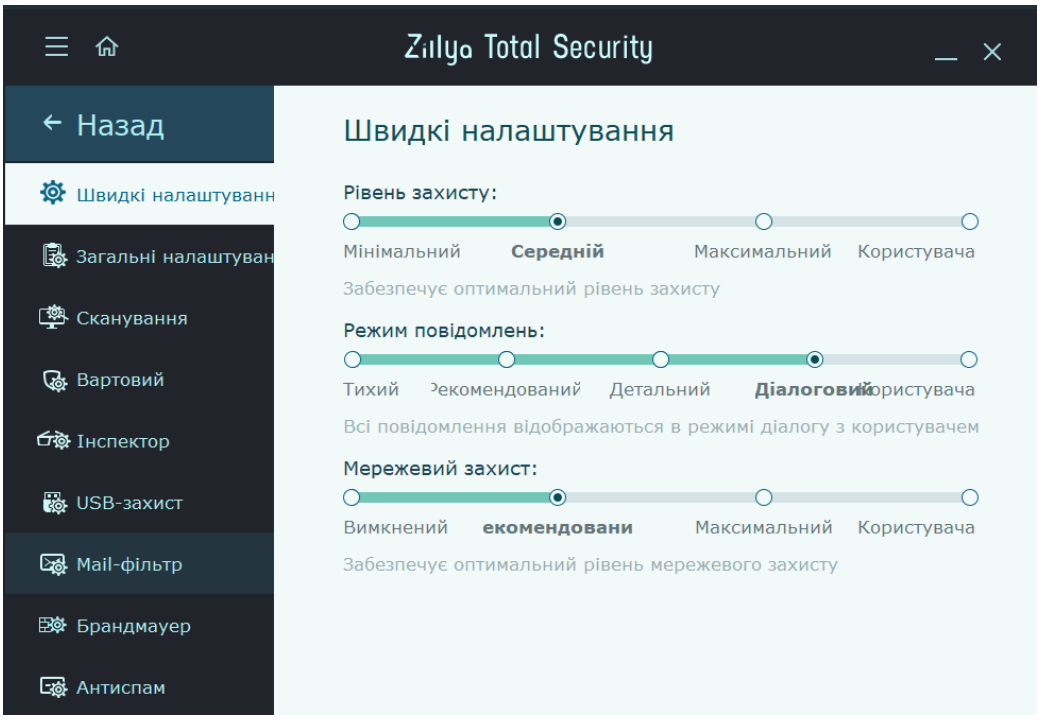


Рис. 1. Встановлення діалогового режиму повідомлень

Завантажити будь-який доступний у мережі файл зі шкідливим кодом, наприклад, за посиланням is.gd/7Xad5B. Встановити факт виявлення шкідливого файлу (рис. 2).

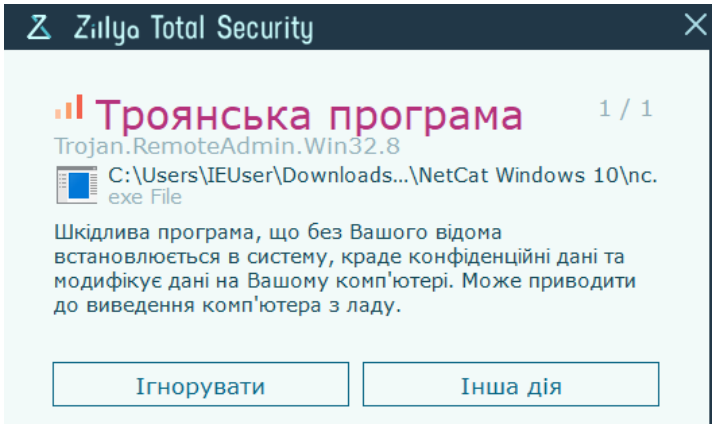


Рис. 2. Виявлення шкідливої програми

Відкрити браузер та перейти на сайт https://www.virustotal.com/gui/home/upload (рис. 3).

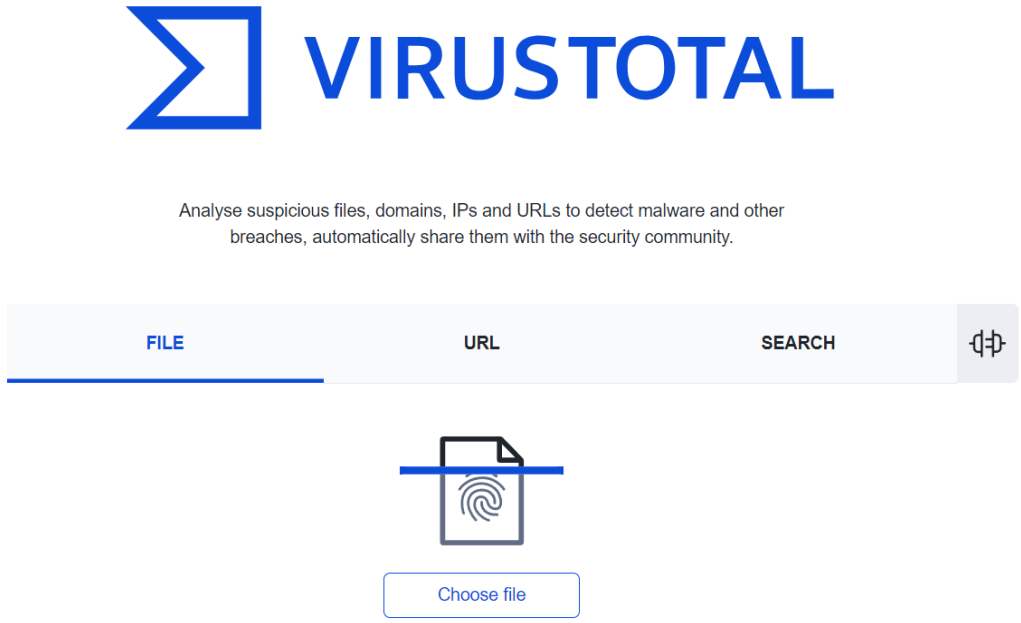


Рис. 3. Сервіс перевірки файлів на наявність шкідливого коду

Завантажити на сайт або шкідливий файл або посилання на нього та переконатися у наявності вірусу (рис. 4).

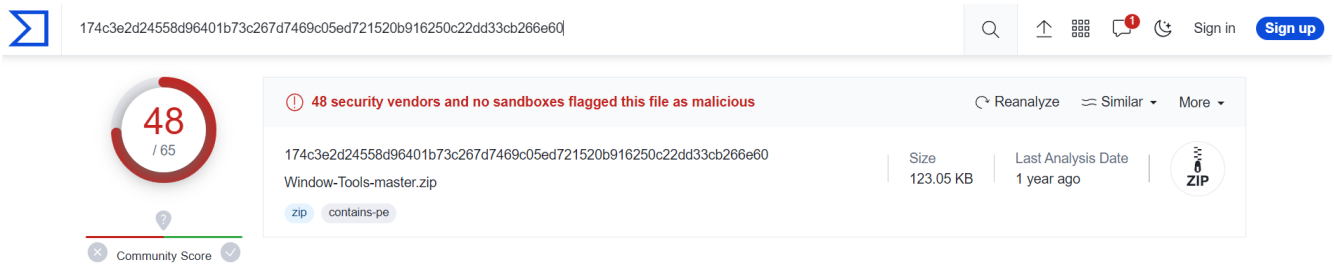


Рис. 4. Результат перевірки файлу на наявність шкідливого коду

Завантажити і виконати встановлення антивірус ZoneAlarm Free Antivirus (https://www.zonealarm.com/software/free-antivirus) (рис. 3).

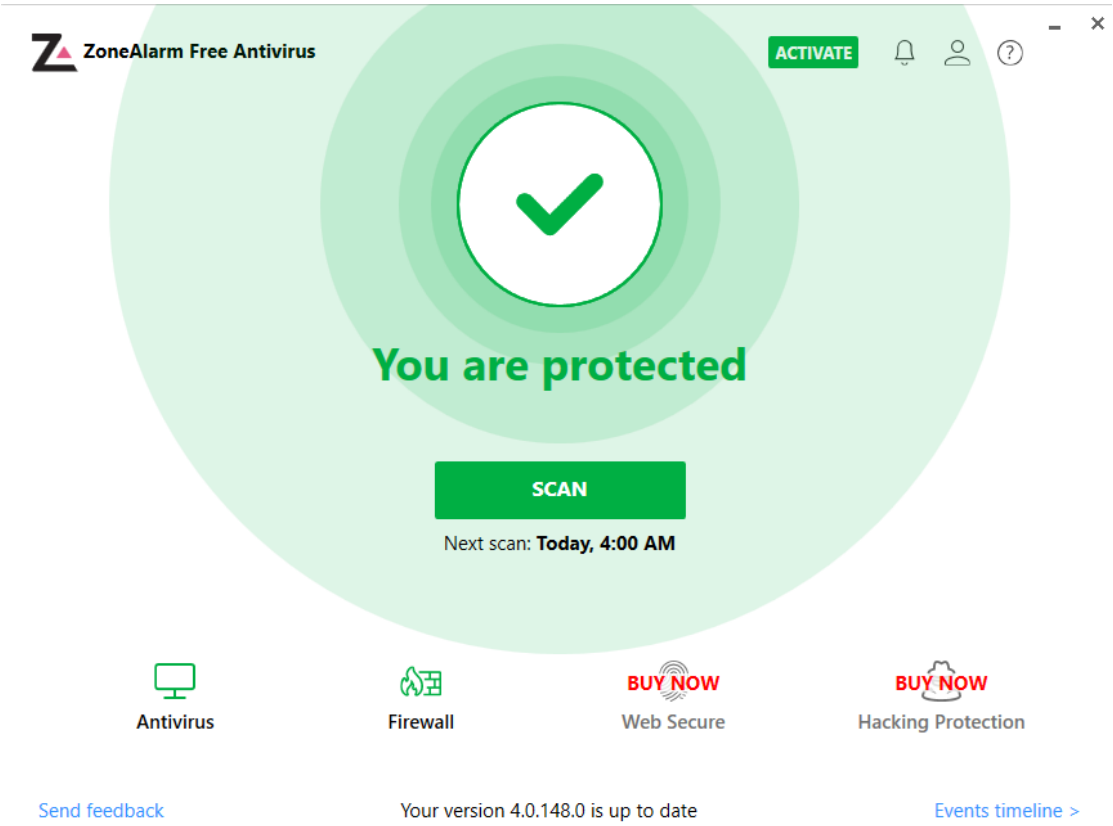


Рис. 3. Головне меню ZoneAlarm Free Antivirus

Завантажити будь-який доступний у мережі файл-зразок ШПЗ, наприклад, архів Backdoor.MSIL.Tyupkin.zip (is.gd/diFvPU), який розпакувати (пароль: infected). Встановити факт виявлення шкідливого файлу (рис. 4).

Рис. 4. Виявлення ШПЗ антивірусом ZoneAlarm Free Antivirus

Практичне заняття «Створення захищеного флеш-накопичувача»

Навчальна мета заняття: створити захищений флеш-накопичувач за допомогою вбудованого в ОС Windows 7/10 Pro/10 Enterprise сервісу BitLocker To Go та програми VeraCrypt.

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», флеш-накопичувачі за кількістю слухачів, особисті смартфони у слухачів.

Порядок проведення заняття

Створити захищений флеш-накопичувач за допомогою вбудованого в ОС Windows 7/10 Pro/10 Enterprise сервісу BitLocker To Go, який повністю шифрує вміст флеш-накопичувача на рівні файлової системи. У випадку фізичної втрати флеш-накопичувача дані залишаться недоступними для читання.

Вставити флеш-накопичувач у USB порт та відкрити «Провідник файлів». Увімкнути BitLocker для диску флеш-накопичувача: клацнути правою кнопкою миші диск у вікні «Провідника файлів», а потім вибрати команду «Увімкнути BitLocker». Якщо немає цього параметра у контекстному меню, то, ймовірно, у вас не Windows Pro або Enterprise, і знадобиться шукати інше рішення для шифрування (рис. 1).

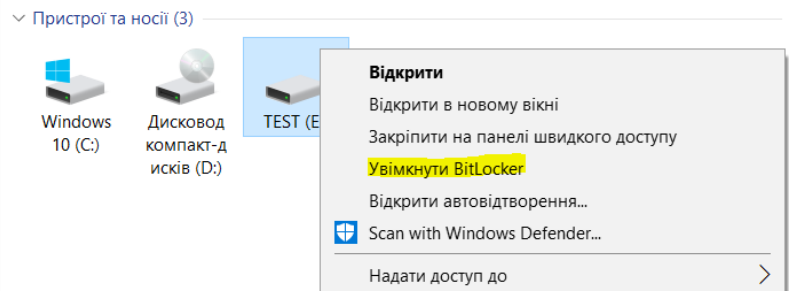


Рис. 1. Увімкнення BitLocker

Зачекати, поки BitLocker здійснить ініціалізацію диску, далі обрати спосіб розблокування диску – за допомогою паролю, обрати надій пароль (рис. 2).

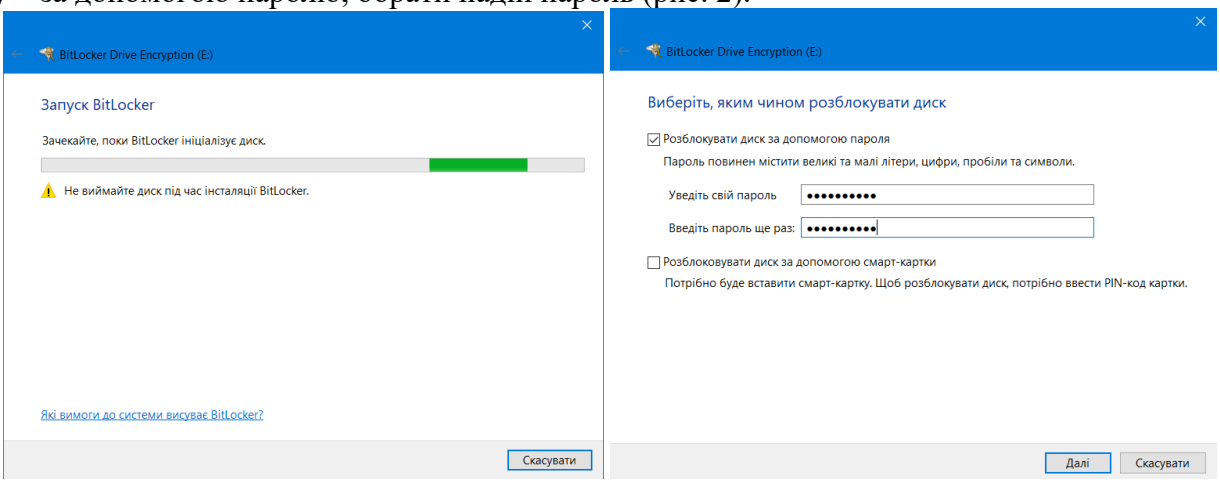


Рис. 2. Ініціалізація BitLocker та вибір способу розблокування диску

Далі BitLocker надає можливість створити ключ відновлення, який можна використовувати для доступу до зашифрованих файлів, якщо ви, наприклад, забудете пароль (рис.3). Ключ відновлення можна зберегти у своєму обліковому записі Microsoft, на диску USB, файлі або навіть

роздрукувати. Ці параметри є однаковими, якщо ви шифруєте системний або несистемний диск. Зберегти ключ відновлення у файл – зміст цього файлу можна скопіювати у парольний менеджер та видалити файл.

Далі обрати шифрування всього диску (рис. 3), режим сумісності для різних версій Windows та запустити шифрування диску (рис. 4).

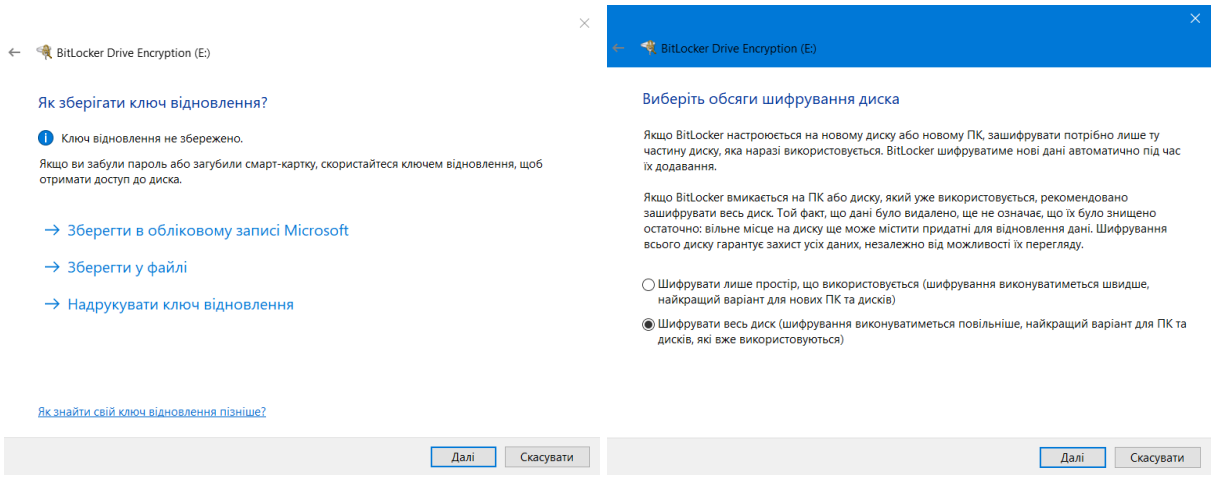


Рис. 3. Збереження ключа відновлення та вибір обсягу шифрування диску

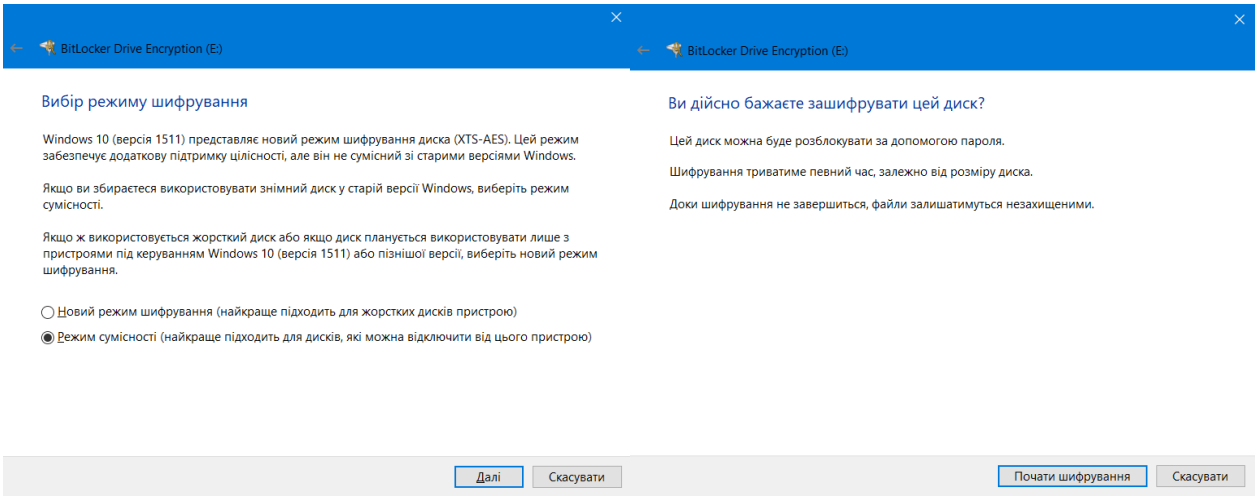


Рис. 4. Вибір режиму шифрування та початок шифрування

Після завершення шифрування у «Провіднику файлів» з’явися відповідна піктограма розшифрованого диску, яка зміниться, якщо витягти диск і знову вставити, а також з’явиться запрошення ввести пароль для розшифрування диску (рис. 5).

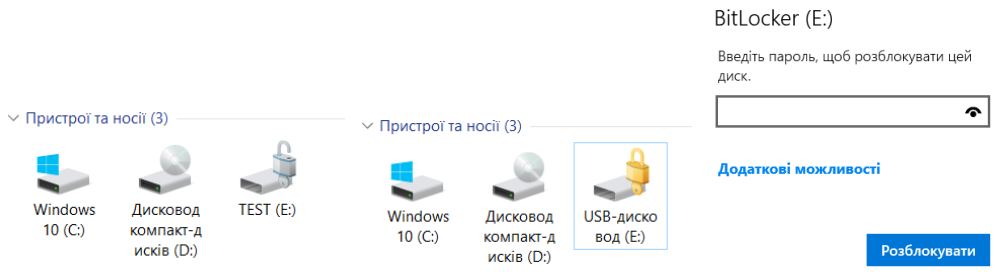


Рис. 5. Піктограми розшифрованого та зашифрованого диску, запрошення ввести пароль

Записати на розшифрований диск довільні файли, витягнути флеш-накопичувач та повторити процедуру розблокування, щоб переконатися у цілісності файлів після розшифрування.

Створити захищений флеш-накопичувач за допомогою безкоштовної утиліти з відкритим кодом «VeraCrypt», яка побудована на базі останньої версії TrueCrypt.

VeraCrypt використовує так званий контейнер. Стосовно VeraCrypt, контейнер – це оболонка, в якій у зашифрованому вигляді зберігаються всі файли. Фізично контейнер – це один файл. Отримати доступ до файлів, які лежать всередині контейнера-оболонки можна тільки одним способом – ввівши правильний пароль. Процедура введення пароля і підключення контейнера називається «монтуванням».

Файли у VeraCrypt шифруються не по одному, а контейнерами. Коли програма підключає контейнер (монтує його), то контейнер виглядає як флешка – з'являється новий диск, з яким можна робити будь-які операції – копіювати туди файли, відкривати файли, видаляти файли, редагувати файли. Роблячи це, не потрібно думати про шифрування – все, що всередині контейнера, вже надійно зашифровано і зберігається / шифрується в реальному часі. І як тільки вимкнути контейнер, то вхід до нього надійно закриється.

Завантажити архів портативної версії утиліти (portable version for Windows, https://www.veracrypt.fr/en/Downloads.html) та запустити розпакування.

З теки VeraCrypt запустити файл VeraCrypt-x64.exe та у меню 'Settings' змінити мову програми на українську. Для цього клацнути на меню 'Settings', там вибрати 'Language ...' та обрати «Українська». Далі натиснути «Створити том» (том – це те ж саме що і контейнер) (рис. 6).

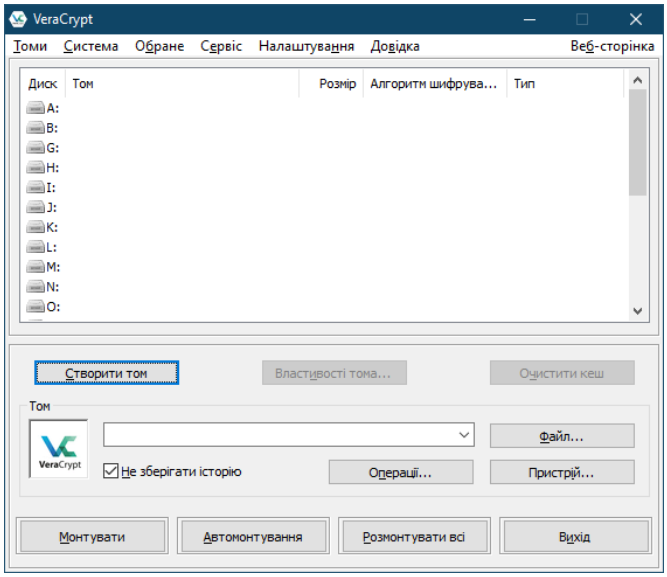
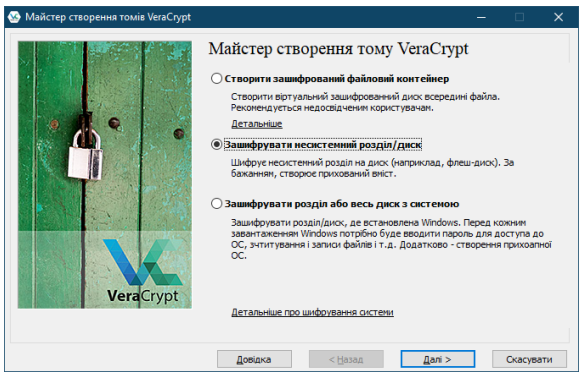
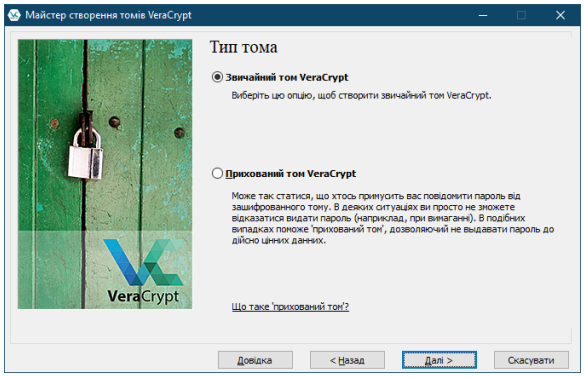


Рис. 6. Головне вікно VeraCrypt

Обрати «Зашифрувати несистемний розділ/диск», «Звичайний том VeraCrypt». Вибрати розміщення тому, вказавши як пристрій флеш-накопичувач. **ВАЖЛИВО: перевірити правильність вибору пристрою, який потім буде форматуватися.** Вибрати режим створення тому «Створити зашифрований том і відформатувати його» (рис. 7).





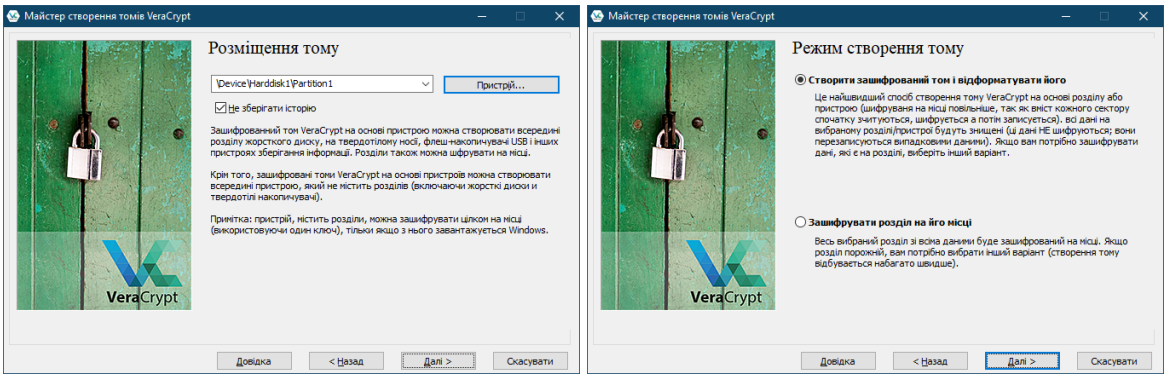


Рис. 7. Майстер створення тому

Налаштування шифрування залишити за замовчуванням. Встановити пароль тому дотримуючись рекомендацій, що будуть запропоновані у вікні вибору паролю. Важливо запам’ятати пароль і ніде не записувати. Як рекомендація – взяти перші (останні) літери улюбленої довгої фрази із заміною деяких літер цифрами і символами. Для форматування тому випадковим чином рухати мишею деякий час, а потім ініціювати форматування носія.

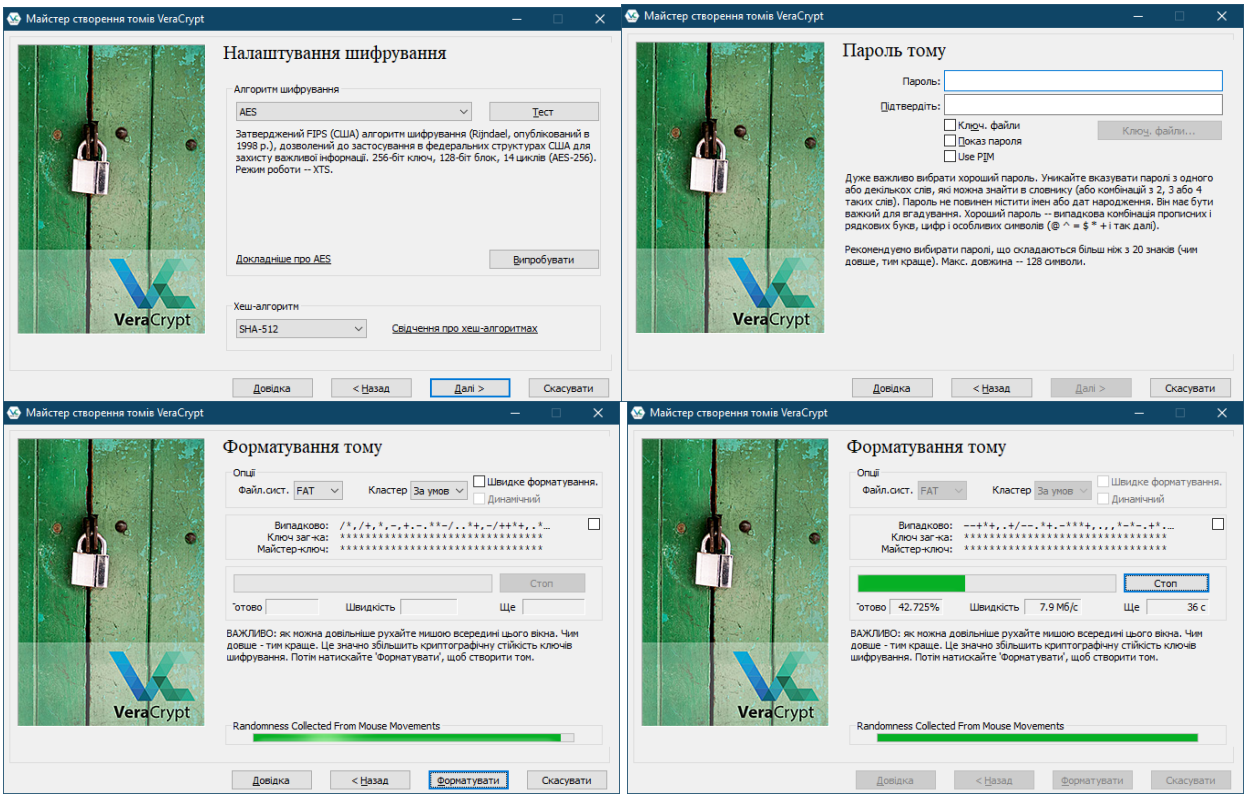


Рис. 8. Налаштування шифрування та форматування тому

Після форматування ознайомитися із порядком монтування тому. Захищений флеш-накопичувач створено.

Для користуванням захищеним носієм у головному вікні VeraCrypt вибрати у розділі «Пристрій» диск флеш-накопичувача, вільну літеру для диску, що буде змонтований, та натиснути «Монтувати» або «Автомонтування» (рис. 9).

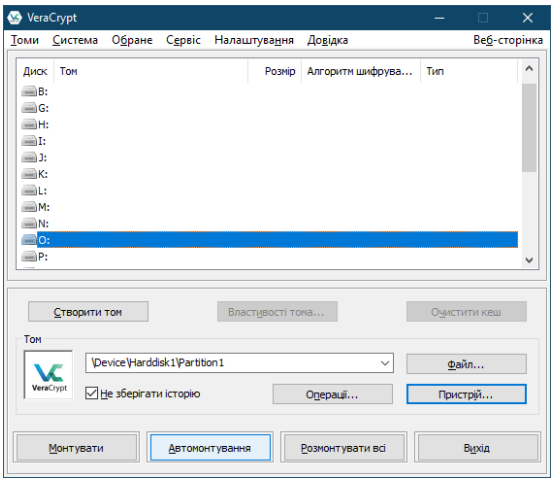


Рис. 9. Підключення зашифрованого диску

На запит ввести пароль і буде створений новий логічний диск, з яким можна працювати: записувати і редагувати файли, запускати програми.

По закінченні роботи із змонтованим диском у головному вікні VeraCrypt натиснути «Розмонтувати всі».

Перевірити надійність захисту інформації здійснити шляхом обміну змінними носіями і спробою відкрити диски.

Практичне заняття «Блокування доступу до операційної системи за відсутності активності»

Навчальна мета заняття: налаштувати блокування ОС Windows за відсутності активності.

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», флеш-накопичувачі за кількістю слухачів, особисті смартфони у слухачів.

Порядок проведення заняття

Налаштувати та перевірити функціонування автоматичного блокування ОС Windows після 5 хвилин відсутності активності.

На панелі задач у полі пошуку ввести запит «блокування», вибрати «Налаштування екрана блокування» – «Налаштування часу очікування екрана» та встановити «…вимикати через 5 хвилин» (рис. 1).

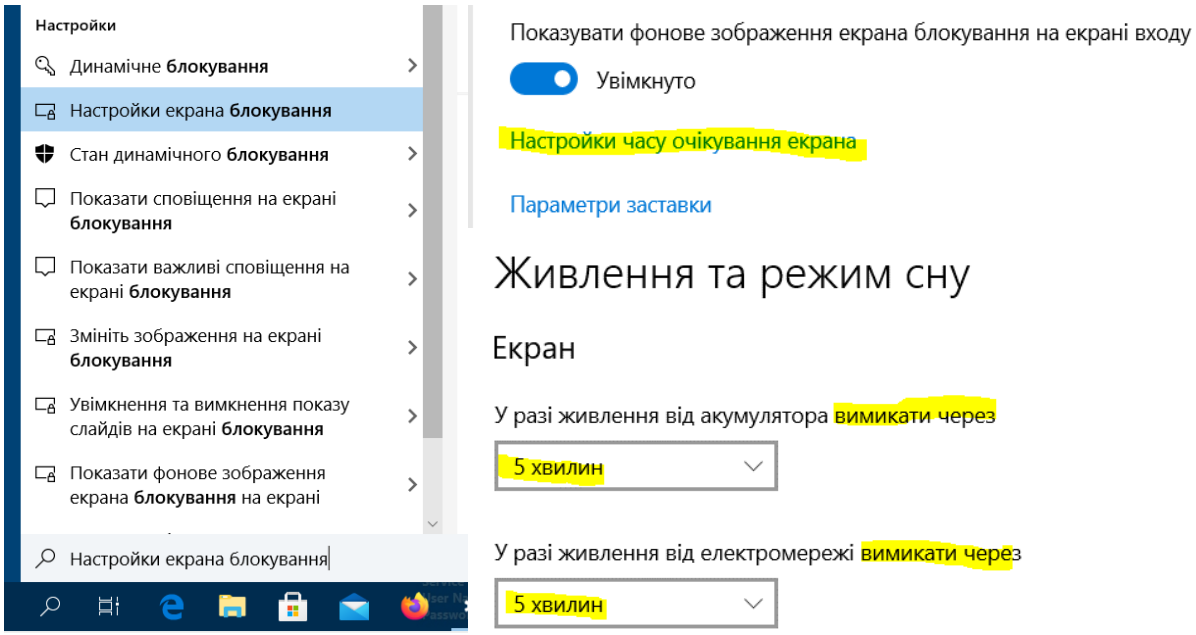


Рис. 1. Налаштування автоматичного блокування ОС Windows після 5 хвилин відсутності активності

Налаштувати та перевірити роботу функції «Динамічне блокування» Windows, яка буде вмикати блокування, коли пристрої, з'єднанні з комп'ютером, опиняться за межами досяжності.

У смартфоні та комп'ютері включити Bluetooth, з'єднати пристрої між собою через відповідні налаштування Bluetooth (рис. 2). Шляхом тестової передачі довільного файлу зі смартфона до комп'ютера переконатися у встановленому з'єднанні.

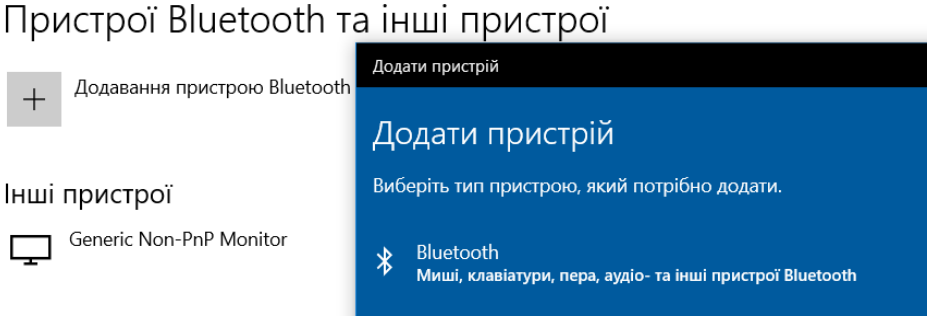


Рис. 2. Підключення Bluetooth пристрою до комп'ютеру

На панелі задач у полі пошуку ввести запит «динамічне», обрати «Динамічне блокування» та ввімкнути «Дозволити Windows автоматично блокувати пристрій, коли вас немає поруч» (рис. 3). Дочекатися, коли система знайде і відобразить графічно встановлене Bluetooth-підключення зі смартфоном.

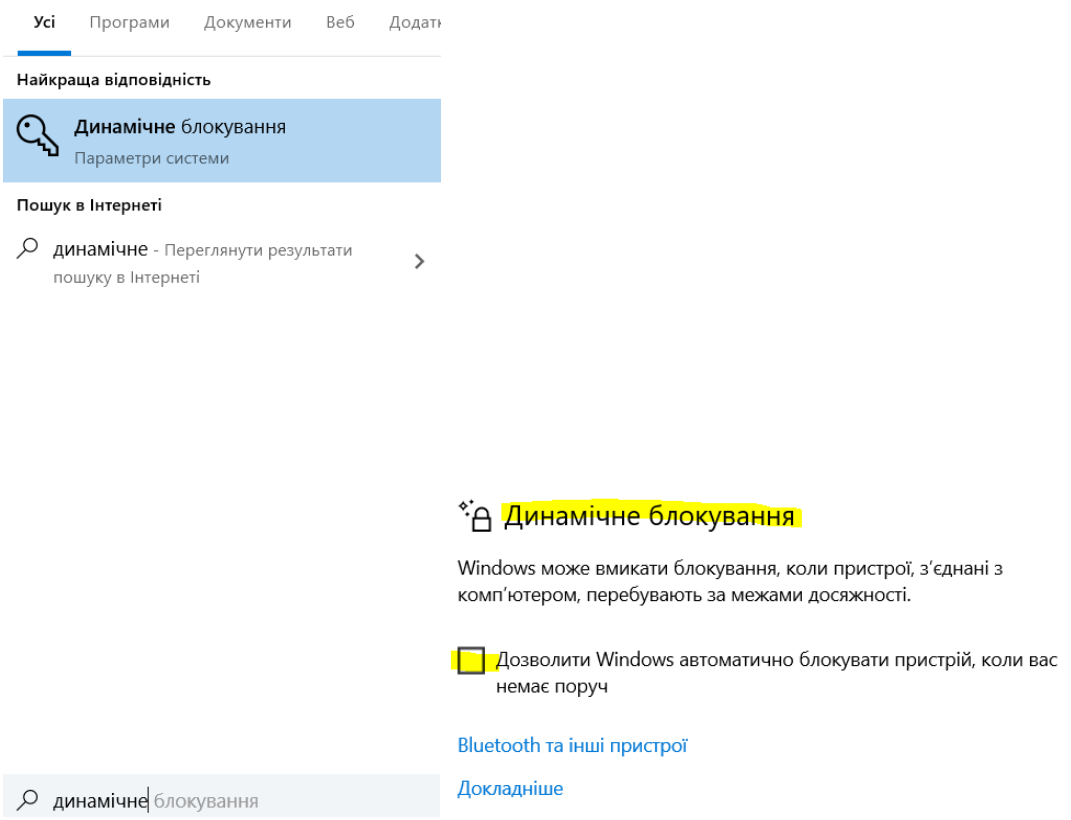


Рис. 3. Налаштування «Динамічне блокування» Windows

Розірвати з'єднання смартфона з комп'ютером, відключивши Bluetooth-адаптер смартфона, і дочекатися автоматичного блокування екрана (приблизно через 1 хвилину).

Блокування доступу до операційної системи за допомогою флеш-накопичувача.

Завантажити архів утиліти USB Raptor (https://sourceforge.net/projects/usbraptor) та видобути із нього файли. Запустити файл USB Raptor.exe, погодитись із ліцензійною угодою (рис. 4).

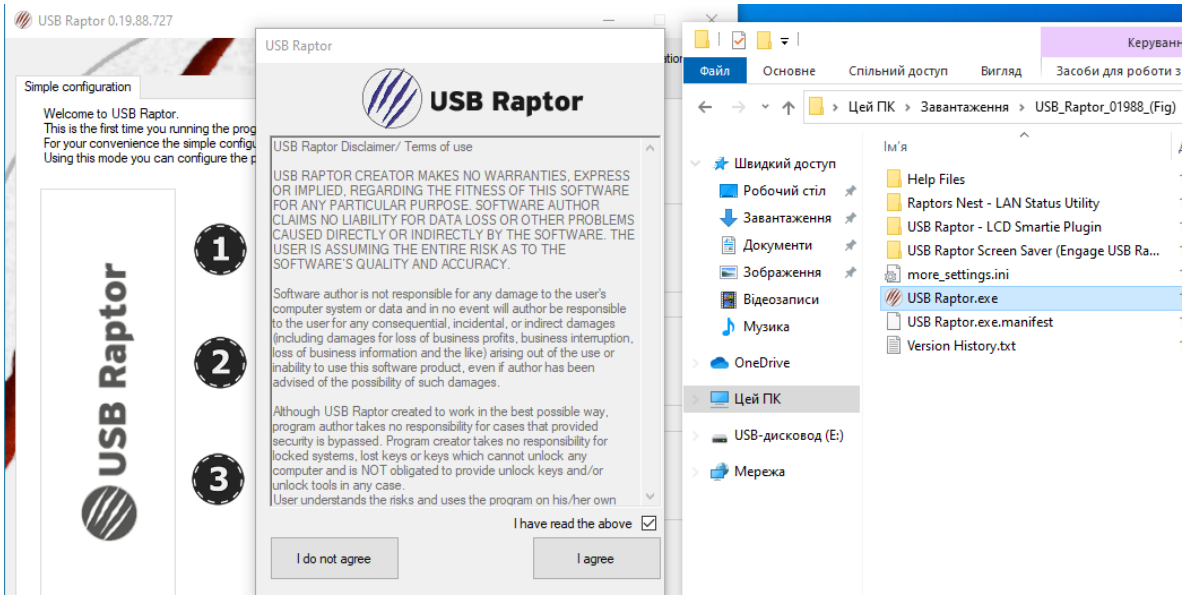


Рис. 4. Запуск утиліти USB Raptor

Вставити у комп’ютер флеш-накопичувач і через головне меню програми встановити пароль резервного розблокування системи при виході із ладу флеш-накопичувача, створити файл розблокування unlock.k3y та увімкнути USB Raptor (рис. 5).

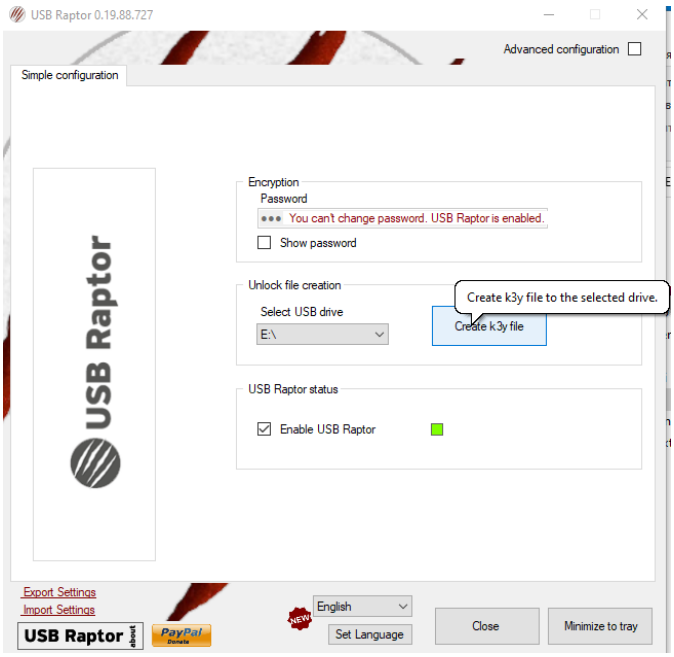


Рис. 5. Налаштування і увімкнення USB Raptor

Перевірити функціонування автоматичного блокування/розблокування ОС Windows після вилучення/підключення флеш-накопичувача.

Здійснити спробу розблокування без флеш-накопичувача через введення паролю.

Практичне заняття «Інструменти виявлення неправдивих повідомлень»

Навчальна мета заняття: навчитися перевіряти окремі відомості в мережі «Інтернет» на достовірність.

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».

Порядок проведення заняття

Для перевірки повідомлень та інших матеріалів на предмет їх актуальності та достовірності можуть бути використані різні аналітичні методи. Для полегшення цього процесу також варто застосовувати і низку технічних рішень. Серед подібних інструментів можна виділити такі.

Розширення **Fake Profile Detector (Deepfake, GAN)** – інструмент, який працює в браузерах на базі Chrome або Chromium і дає змогу ідентифікувати зображення, створені з використанням штучного інтелекту (рис. 1). Саме тому, якщо обличчя реальної людини додано до іншого зображення, воно теж визначатиметься як справжнє. Розширення доступне за посиланням https://chrome.google.com/webstore/detail/fake-profile-detector-dee/jbpcgcnnhmjmajjkgdaogpgefbnokpcc/related?hl=en-US

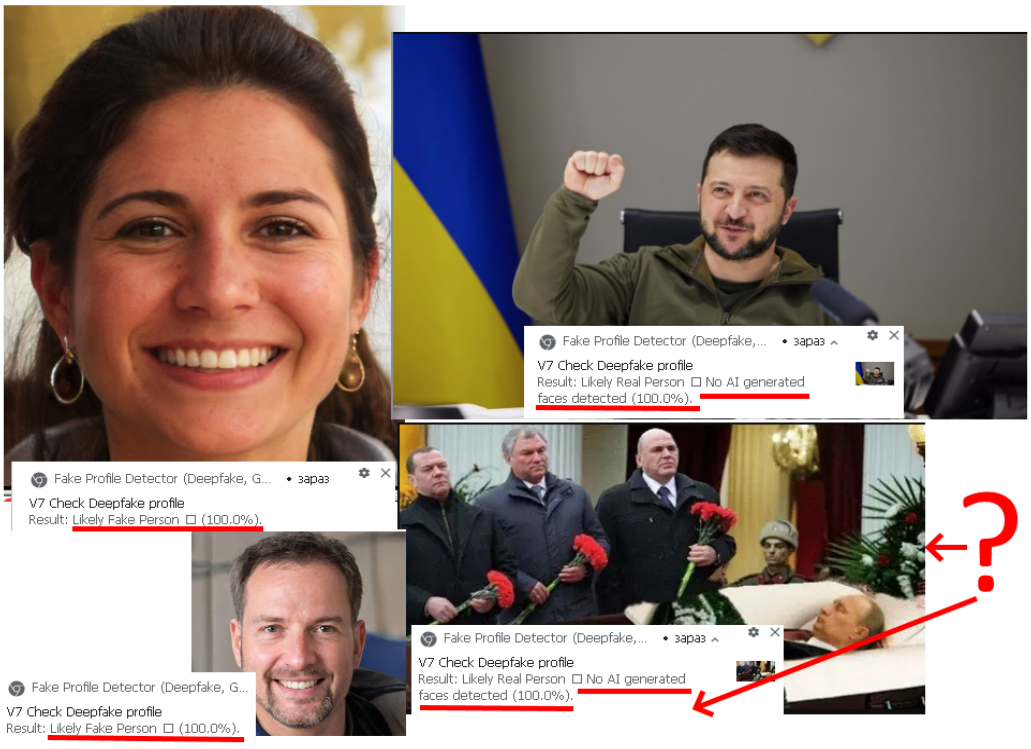


Рис. 1. Результат роботи розширення з виявлення діпфейків

Сервіси **Sensity** (https://platform.sensity.ai/login?redirect=%2Fdeepfake-detection), **Is your image GAN generated?** (https://gan-detector-mayachitra.azurewebsites.net/), **AI or Not** (https://aiornot.optic.xyz/#home) та **Illuminarty** (https://app.illuminarty.ai/#/) виконують подібну функцію (рис. 2).

Сервіс **Forensically** (29a.ch/photo-forensics) дозволяє з використанням нескладних методів аналізу спробувати зрозуміти, чи вносилися до зображення якісь зміни.

Розширення **Deepfake Detection** (https://github.com/deep2universe/DeepFakeChrome) призначено для виявлення DeepFake відео в сервісі YouTube. Також для ідентифікації фейкового відео призначено сервіс **Scan & Detect Deepfake Videos** (https://scanner.deepware.ai).

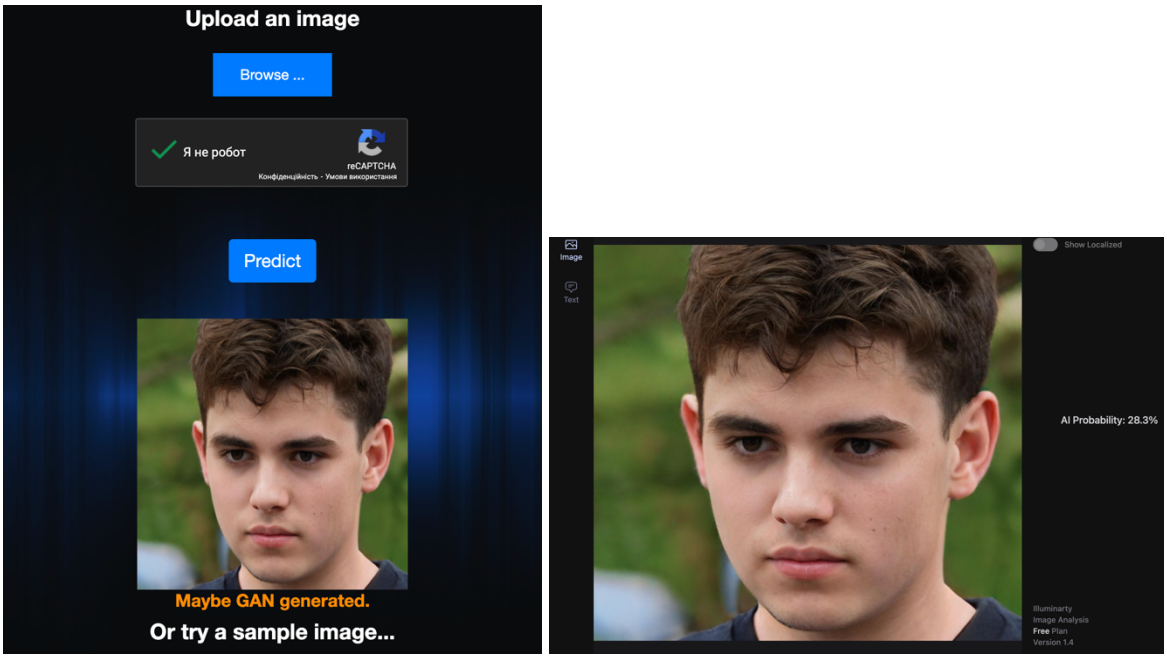


Рис. 2. Результат роботи сервісів з виявлення зображень, згенерованих за допомогою системи штучного інтелекту

Зображення можуть не мати ознак маніпуляцій, проте використовуватися у неправдивих повідомленнях у різних контекстах. Для того, щоб знайти першоджерело відповідних малюнків можна використовувати розширення **Who stole my pictures** (рис. 3).

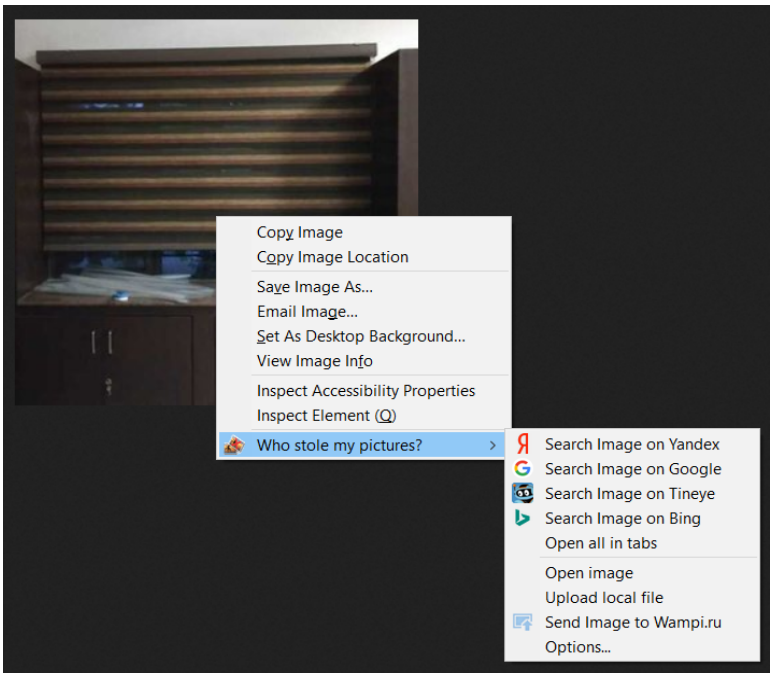


Рис. 3. Використання розширення для пошуку зображень

Завантажити описане розширення можна за адресами:

- для браузеру «Chrome» (https://chrome.google.com/webstore/detail/who-stole-my-pictures/mcdbnfhkikiofkkicppioekloflmaibd);
- для браузеру «Firefox» (https://addons.mozilla.org/ru/firefox/addon/who-stole-my-pictures/).

Подібним до описаного розширення є «**Fake news debunker by InVID & WeVerify**» (https://www.invid-project.eu/tools-and-services/invid-verification-plugin/).

Для аналізу тексту на предмет його свтрення за допомогою штучного інтелекту можна використати ресурс **GPTZero** (github.com/BurhanUlTayyab/GPTZero, gptzero.me).

Створіть декілька зображень за допомогою ресурсу thispersondoesnotexist.com або generated.photos/faces та розмістіть їх у своєму профілі в соціальній мережі.

За опомогою описаних програмних продуктів спробуйте перевірити завантажені Вами зображення на справжність. Спробуйте здійснити перевірку із зображеннями, опрацьованими Телеграм-ботом **@Pix2MixV2Bot**.

Для різних фотознімків самостійно опрацюйте сервіс **Am I Real**? (https://seintpl.github.io/AmIReal/).

Перейдіть за посиланням olx.com та знайдіть декілька оголошень з продажу ігрових приставок. За допомогою розширення «Who stole my pictures» або «Fake news debunker by InVID & WeVerify» перевірте, чи нема серед фотографій у знайдених оголошеннях, зображень, завантажених з інших сайтів.

Згенеруйте текст за допомогою однієї з систем генеративного штучного інтелекту, перевірте його за допомогою gptzero.me.

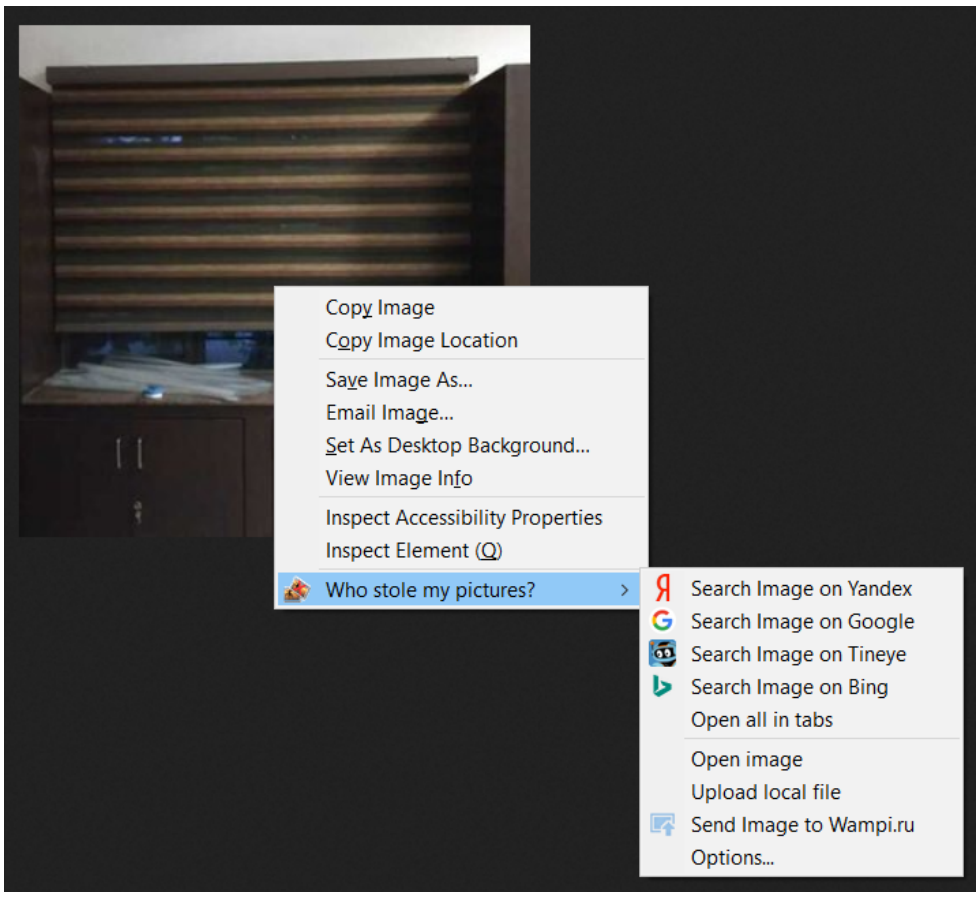


Рис. 3. Використання розширення для пошуку зображень

Завантажити описане розширення можна за адресами:

- для браузеру «Chrome» (https://chrome.google.com/webstore/detail/who-stole-my-pictures/mcdbnfhkikiofkkicppioekloflmaibd);
- для браузеру «Firefox» (https://addons.mozilla.org/ru/firefox/addon/who-stole-my-pictures/).

1. Створіть декілька зображень за допомогою ресурсу thispersondoesnotexist.com або generated.photos/faces, а також завантажте декілька медіафайлів із соціальних мереж.

2. Дослідіть роботу описаних програмних інструментів. Для відпрацювання розширення «Fake Profile Detector» використовуйте зображення, розміщені на онлайн-ресурсах.

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.