МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

Кафедра інформаційних технологій

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних та самостійних робіт
з дисципліни

«Безпека персональної інформації в мережі Інтернет»

для підготовки здобувачів вищої освіти
галузі знань 12 «Інформаційні технології»

Одеса 2020

УДК 004.43

Укладач:

Задерейко О.В. – кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Рекомендовано навчально-методичною радою
Національного університету «Одеська юридична академія»,
протокол № 2 від 4 грудня 2020 р.

Рецензенти:

Троянський О.В. – кандидат технічних наук, доцент, директор інституту інституту інформаційної безпеки, радіоелектроніки та телекомунікацій Одеського національного політехнічного університета

Кухаренко С.В. – кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Розглянуто основні методи і засоби захисту інформаційно-телекомунікаційних систем та мереж від витоків конфіденційних даних.

Містить завдання до лабораторних та самостійних занять, які виконуються у комп'ютерному класі в межах навчальної дисципліни.

Призначено для студентів з метою закріплення лекційного матеріалу і підготовки до лабораторних та самостійних занять з дисципліни «Безпека персональної інформації в мережі Інтернет».

Методичні вказівки до виконання лабораторних та самостійних робіт з дисципліни «Безпека персональної інформації в мережі Інтернет» для здобувачів вищої освіти галузі знань 12 «Інформаційні технології» / Уклад.: О.В.Задерейко. – О.: НУ «ОЮА», 2020. – 69 с.

ПЕРЕДМОВА

Дисципліна «Безпека персональної інформації в мережі Інтернет» вивчається студентами академії за напрямом бакалаврської підготовки з галузі знань 12 «Інформаційні технології» на першому курсі навчання.

Метою викладання навчальної дисципліни «Безпека персональної інформації в мережі Інтернет» є засвоєння базових знань та практичних навичок з захисту персональних даних від витоків з інформаційно-телекомунікаційних систем та мереж.

Безпека персональної інформації – це сукупність методів захисту від витоків персональної інформації заснованих на використанні програмних та апаратних засобів. Програмне забезпечення для захисту персональної інформації та вміння його використати є, поза сумнівом, важливою складовою для захиста будь-якої інформаційно-телекомунікаційної системи, комп'ютера або пристрою комунікації.

Оволодіння курсом «Безпека персональної інформації в мережі Інтернет» передбачає читання лекцій, проведення лабораторних занять, виконання самостійної роботи та складання заліку. Особлива увага приділяється прищепленню студентам практичних навичок із застосування сучасних технологій захисту персональної та конфіденційної інформації у майбутній професійній діяльності.

Згідно з вимогами освітньо-професійної програми після вивчення дисципліни «Безпека персональної інформації в мережі Інтернет» студенти повинні:

– **знати** основні вразливості інформаційно-телекомунікаційних систем;

– **знати** принципи пошуку витоків персональної інформації в операційних системах;

– **володіти** методиками резервування персональних даних користувачів;

– **вміти** блокувати витоки конфіденційної інформації з пристроїв комунікації;

– **вміти** аналізувати результати пошуку витоків в інформаційно-телекомунікаційних системах;

– **вміти** блокувати витоки прикладного програмного забезпечення у пристроях комунікації.

Перелік тем лабораторних занять та самостійних робіт

Тема 1. Поняття персональних даних

Самостійна робота 1. Захист персональних даних держави

Тема 2. Витоки персональних даних

Лабораторна робота 1. Аналіз мережевих витоків операційної системи

Тема 3. Резервування персональних даних

Лабораторна робота 2. Резервування персональних даних в операційних системах

Тема 4. Відновлення персональних даних

Лабораторна робота 3. Відновлення персональних данних з носіїв різного типу

Тема 5. Технології збору персональних даних

Самостійна робота 2. Операторний збір персональних даних

Самостійна робота 3. Методи збору персональних даних

Тема 6. Захист персональних даних

Лабораторна робота 4. Криптографічний захист персональних даних

Лабораторна робота 5. Захист веб-браузерів Mozilla Firefox та Tor від витоків персональних даних

Лабораторна робота № 6. Захист персональних даних в операційних системах

Самостійна робота 4. Захист від витоків і збору інформації при веб-серфингу в інтернет

ЗМІСТ

ТЕМА 1. ПОНЯТТЯ ПЕРСОНАЛЬНИХ ДАНИХ 7
САМОСТІЙНА РОБОТА № 1 7
ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ДЕРЖАВІ 7
КОНТРОЛЬНІ ПИТАННЯ 7
ТЕМА 2. ВИТОКИ ПЕРСОНАЛЬНИХ ДАНИХ 9
ЛАБОРАТОРНА РОБОТА № 1 9
АНАЛІЗ МЕРЕЖЕВИХ ВИТОКІВ ОПЕРАЦІЙНОЇ СИСТЕМИ 9
ЗАВДАННЯ 9
КОНТРОЛЬНІ ПИТАННЯ 13
ТЕМА 3. РЕЗЕРВУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ 14
ЛАБОРАТОРНА РОБОТА № 2 14
РЕЗЕРВУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ В ОПЕРАЦІЙНИХ СИСТЕМАХ 14
ЗАВДАННЯ 14
КОНТРОЛЬНІ ПИТАННЯ 15
ТЕМА 4. ВІДНОВЛЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ 17
ЛАБОРАТОРНА РОБОТА № 3 17
ВІДНОВЛЕННЯ ПЕРСОНАЛЬНИХ ДАННИХ З НОСІЇВ РІЗНОГО ТИПУ 17
ЗАВДАННЯ 17
КОНТРОЛЬНІ ПИТАННЯ 22
ТЕМА 5. ТЕХНОЛОГІЇ ЗБОРУ ПЕРСОНАЛЬНИХ ДАНИХ 24
САМОСТІЙНА РОБОТА № 2 24
ОПЕРАТОРНИЙ ЗБІР ПЕРСОНАЛЬНИХ ДАНИХ 24
КОНТРОЛЬНІ ПИТАННЯ 25
САМОСТІЙНА РОБОТА № 3 26
МЕТОДИ ЗБОРУ ПЕРСОНАЛЬНИХ ДАНИХ 26
КОНТРОЛЬНІ ПИТАННЯ 26
ТЕМА 6. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ 28
ЛАБОРАТОРНА РОБОТА № 4 28
КРИПТОГРАФІЧНИЙ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ 28

ЗАВДАННЯ 28
КОНТРОЛЬНІ ПИТАННЯ 36
ЛАБОРАТОРНА РОБОТА № 5 37
ЗАХИСТ ВЕБ-БРАУЗЕРІВ MOZILLA FIREFOX та TOR ВІД ВИТОКІВ ПЕРСОНАЛЬНИХ ДАНИХ 37
ЗАВДАННЯ 37
КОНТРОЛЬНІ ПИТАННЯ 50
ЛАБОРАТОРНА РОБОТА № 6 51
ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ОПЕРАЦІЙНИХ СИСТЕМАХ 51
ЗАВДАННЯ 51
КОНТРОЛЬНІ ПИТАННЯ 54
САМОСТІЙНА РОБОТА № 4 55
ЗАХИСТ ВІД ВИТОКІВ І ЗБОРУ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ВЕБ-СЕРФИНГУ В ІНТЕРНЕТ 55
ЗАВДАННЯ 55
КОНТРОЛЬНІ ПИТАННЯ 58

ТЕМА 1. ПОНЯТТЯ ПЕРСОНАЛЬНИХ ДАНИХ

Самостійна робота 1. Захист персональних даних держави

САМОСТІЙНА РОБОТА № 1

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ДЕРЖАВІ

Мета заняття – вивчити особливості формування інформаційного, та цифрового суверенітетів держави і правові особливості їх законодавчої реалізації в Україні.

Навчальні питання

1. Особливості захисту персональних даних в державі.
2. Складові захисту персональних даних держави.

ЗАВДАННЯ

1. Ознайомитись з вмістом лекції №1 на тему «ЗАГАЛЬНІ ПОНЯТТЯ ПРО ПЕРСОНАЛЬНІ ДАНІ», лекції №2 «МОДЕЛЬ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ GDPR В ЕС».
2. Підготувати оглядову доповідь, об'ємом 5 - 15 сторінок на тему «Захист персональних даних в Україні» з вказівкою використаних джерел.
3. Підготувати відповідь на контрольне питання, номер якого повинен відповідати порядковому номеру в списку групи.
4. Оформити звіт з самостійної роботи і надіслати його для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Чим забезпечується традиційний захист персональних даних в державі?
2. Що приводить до трансформації традиційної концепції захисту персональних даних держави?
3. Які основні законодавчі ініціативи України по формуванню захиста персональних даних?
4. Які заходи у цифровому просторі здійснюються для захисту персональних даних в Україні.
5. Які складові ідеального захисту персональних даних існують?

6. Чим обумовлено ослаблення захисту персональних даних держави?
7. У чому полягають суперечності законодавчих ініціатив України в питаннях формування захисту персональних даних?

ТЕМА 2. ВИТОКИ ПЕРСОНАЛЬНИХ ДАНИХ

ЛАБОРАТОРНА РОБОТА № 1

АНАЛІЗ МЕРЕЖЕВИХ ВИТОКІВ ОПЕРАЦІЙНОЇ СИСТЕМИ

Мета заняття – проаналізувати мережеві з‘єднання операційної системи з зовнішними хостами, та виявити потенційно шкідливі з‘єднання, що можуть привести до витоків конфіденційної інформації користувача.

Навчальні питання

1. Аналізатори мережевих пакетів.
2. Принципи роботи пакетних сніфферів.
3. Функції пакетних сніфферів.
4. Програмне забезпечення для моніторингу мережевого трафіку та його можливості.

ЗАВДАННЯ

1. Встановити, веб-браузери **Wireshark**. Для цього завантажити інсталяцію програмного забезпечення за адресою - https://1.eu.dl.wireshark.org/win64/Wireshark-win64-3.4.0.exe.
2. Встановити програмне забезпечення **Wireshark**.

Примітка: При істаляції обов‘язково виконати встановлення модулів **Npcap X.X** та **USBcap X.X.X.X.** (рис.4.1)

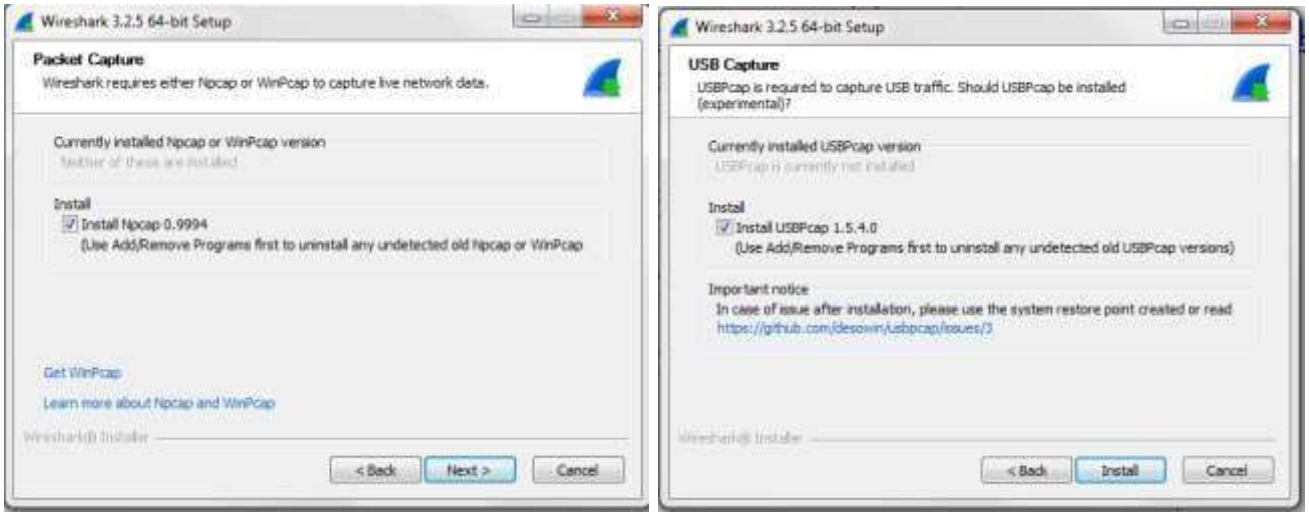
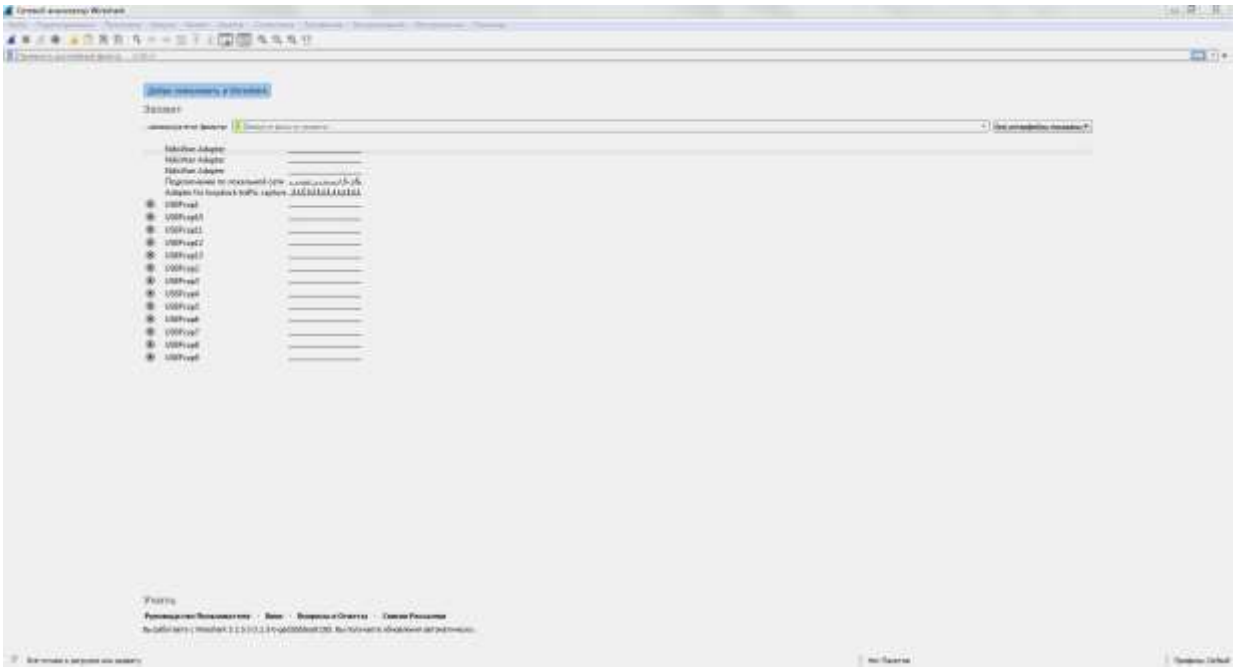
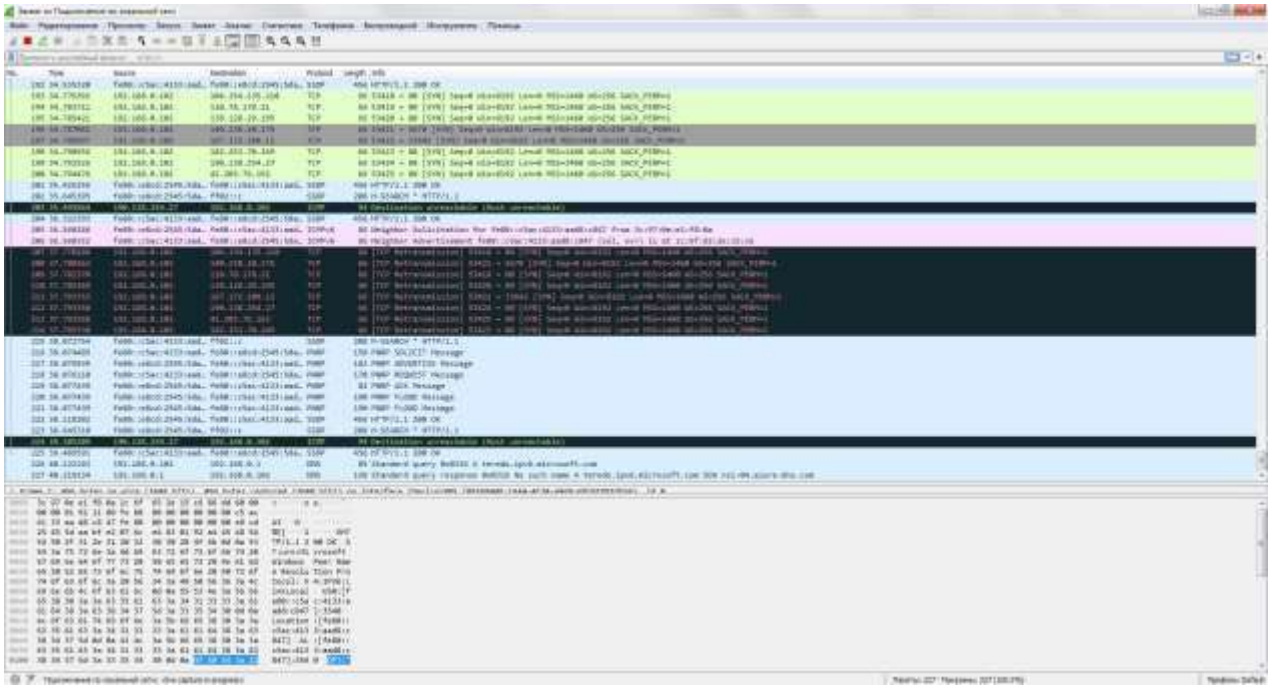


Рис.4.1. Встановлення модулів Npcap X.X та USBcap X.X.X.X.

3. Після успішного закінчення процесу інсталяції виконати перезагрузку операційної системи.
4. Виконати перевірку на наявність витоків (несанкціонованих мережевих зовнішних з‘єднань) операційної системи:
    4.1. Запустити програмне забезпечення **Wireshark**. Відкриється вікно:



    4.2. Встановити курсор Миши на мережевий інтерфейс «**Подключение к локальной сети**» и натиснути її ліву кнопку два рази. Відкриється вікно:



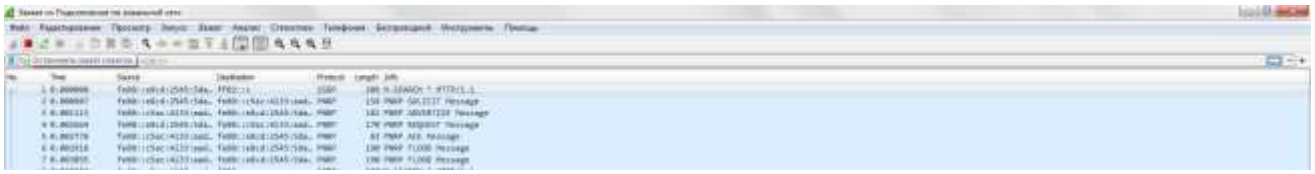
4.3. Виконати моніторінг мережевих з‘єднань операційної системи протягом щонайменше півгодини.

Примітка: Під час моніторінгу не запускати будь-якє програмне забезпечення (веб-браузери, редактори і інше). Це важливо, з точки зору виявленя несанкціонованих з‘єднань операційної системи, які не ініційовані користувачем.

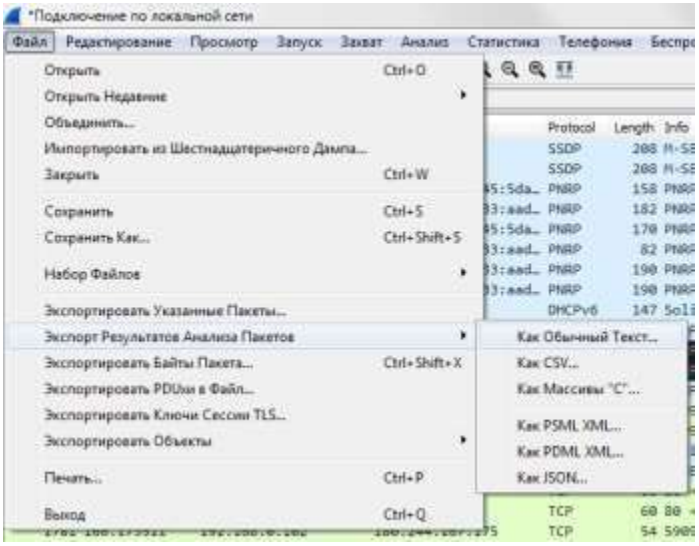
Перезагрузити компютер для ініцюювання мережевих процессів. (запустить в автозагрузке Wireshark).

4.4. Зберегти результати моніторінгу мережевих з‘єднань операційної системи:

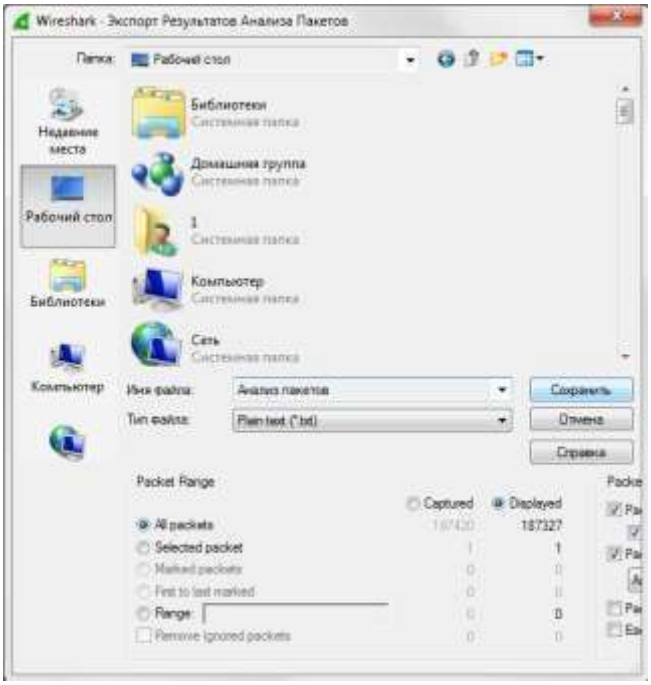
4.4.1. Зупинити моніторінг мережевих з‘єднань операційної системи, для чого на панелі інструментів натиснути на кнопку  (див. вікно нижче):



4.4.2. Виконати збереження результатів моніторінгу мережевих з‘єднань операційної системи у текстовий файл (див. вікно нижче):



4.4.3. Після встановлення курсору в положення «**Как Обычный текст**», натиснути ліву кнопку Миши. Відкриється вікно:



4.4.4. Присвоїти назву «**Аналіз пакетів**» файлу з результатами моніторінгу мережевих з‘єднань операційної системи і натиснути кнопку «**Сохранить**».

4.5. Виконати аналіз мережевих з‘єднань операційної системи, що містяться в отриманому файлі «**Аналіз пакетів.txt**»:

4.5.1. Занести всі з‘єднання, що виконані по протоколу DNS до таблиці 1.

Таблиця 1. Мережеві з‘єднання операційної системи

DNS з‘єднання операційної системи			
№	**Source**	**Destination**	**Info**
1.			
2.			
3.			
...			

5. Проаналізувати результати, отримані у таблиці 1 та виявити несанкціоновані мережеві з‘єднання, зробити висновки щодо програмного забезпечення, яке можливо їх викликало та занести їх до звіту.
6. В додаток звіту помістити файл «**Аналіз пакетів.txt**».
7. Оформити звіт з лабораторної роботи і надіслати його для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Як отримати інформацію о мережевих з‘єднаннях операційної системи?
2. Які типи мережевих з‘єднань існують?
3. Як отримати інформацію про несанкціновані мережеві з‘єднання операційної системи?
4. Які критерії застосовуються для визначення несанкцінованих мережевих з‘єднань операційної системи?
5. Які протоколи використовуються для встановлення несанкцінованих мережевих з‘єднань операційної системи?

ТЕМА 3. РЕЗЕРВУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ

ЛАБОРАТОРНА РОБОТА № 2

РЕЗЕРВУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ В ОПЕРАЦІЙНИХ СИСТЕМАХ

Мета заняття - ознайомитися з основними прийомами резервування даних користувачів при експлуатації стаціонарного комп'ютерного устаткування.

Навчальні питання

1. Принципи резервування даних.
2. Програмне забезпечення для резервування даних.

ЗАВДАННЯ

1. Створити робочий каталог на диску за узгодженням з викладачем.
2. Викачати програмне забезпечення **WinToFlash** і **ISO образ програмного забезпечення Acronis True Image** в попередньо створений каталог на жорскому диску.
3. Встановити програмне забезпечення **WinToFlash** на комп‘ютер.

   Примітка: Викачати програму **WinToFlash** та її опис за посиланням - https://bit.ly/306AfUr.
4. Створити завантажувальний Flash-накопичувач, з використанням програмного забезпечення **WinToFlash** з ISO образом програмного забезпечення **Acronis True Image**.

   Примітка: Викачати ISO образ програмного забезпечення **Acronis True Image** та його опис за посиланням - https://bit.ly/3mC5i4m.
5. Завантажити комп'ютер із завантажувального Flash-накопичувача за допомогою відповідного режиму BIOS.
6. Запустити програмне забезпечення **Acronis True Image**.
7. Зробити резервну копію системного розділу операційної системи. Назву файлу резервної копії - **system403XX.tib**, де в імені файлу замість символів «**XX**» вказати своє прізвище. Файл зберегти на доступний диск (**D:\, E:\). Режим збереження резервної копії файлу вибрати «зашифрований»**.

Примітка: вибір розділів для резервування рекомендовано виконувати за попередньою рекомендацією викладача.

8. Перевірити наявність створеного файлу резервної копії даних на вибраному диску комп'ютера за допомогою файлового менеджеру і зафіксуйте його розмір у звіті.
9. Створіть зону безпеки «**Acronis**» з урахуванням розміру отриманого файлу резервної копії даних.
10. Створити акаунт на хмарному сховищі Mega.nz.
11. Завантажити створений файл резервної копії **system403XX.tib** в хмарне сховище.
12. Надіслати викладачу реквізити доступу від хмарного сховища (логін, пароль) на вказану електронну адресу.
13. Зробити резервну копію системного диску у зону безпеки «**Acronis**».
14. Перезавантажити комп'ютер в звичайному режимі (з жорсткого диска).
15. Внести зміни в операційну систему: встановити відсутній браузер або інше програмне забезпечення на власний розсуд і вийти з операційної системи.
16. Завантажити комп'ютер із створеного завантажувального Flash-накопичувача.
17. Запустити програмне забезпечення **Acronis True Image**.
18. Відновити системний розділ жорсткого диска з раніше створеного файлу **system403XX.tib** резервної копії в режимі з «перевіркою помилок».
19. Після закінчення процесу відновлення системного розділу операційної системи перезавантажити комп'ютер в звичайному режимі з жорсткого диска і переконатися у відсутності внесених змін в операційну систему.
20. У звіті підготувати відповідь на контрольне питання, номер якого повинен відповідати порядковому номеру в списку групи.
21. Оформити звіт з лабораторної роботи і надіслати його для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

6. Наведіть приклади коли необхідно застосовувати резервне копіювання даних?

7. Наведіть приклади програмного забезпечення для створення завантажувальних Flash-накопичувачів.
8. Наведіть приклади програмного забезпечення, що може бути використано для резервування даних.
9. З якими форматами образів може працювати програмне забезпечення WinToFlash?
10. Які файли можна виключати при створенні резервної копії даних?
11. У чому полягає відмінність інкрементної резервної копії даних в програмному забезпеченні Acronis True Image.
12. У чому полягає відмінність повної резервної копії даних в програмному забезпеченні Acronis True Image?
13. У чому полягає відмінність інкрементної резервної копії даних?
14. У яких випадках слід використовувати криптографічне шифрування файлу резервної копії даних?
15. Які переваги надає можливість створення зони безпеки «Acronis»?
16. За яким критерієм слід вибирати розмір зони безпеки «Acronis»?
17. На яких розділах жорсткого диску можна створювати резервні копії даних?
18. Поясніть доцільність або необхідність включення MBR (Master Boot Record) при відновленні з резервної копії данних?

ТЕМА 4. ВІДНОВЛЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ

ЛАБОРАТОРНА РОБОТА № 3

ВІДНОВЛЕННЯ ПЕРСОНАЛЬНИХ ДАННИХ З НОСІЇВ РІЗНОГО ТИПУ

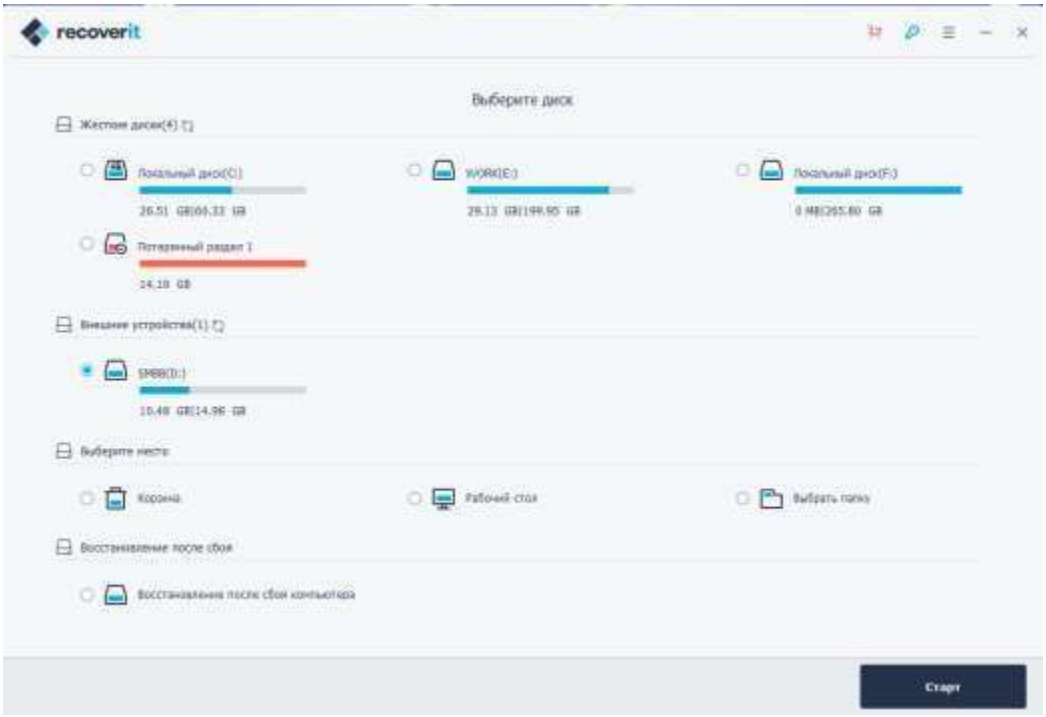
Мета заняття - отримати практичні навички з відновлення видалених даних з носіїв різного призначення з використанням спеціалізованого програмного забезпечення.

Навчальні питання

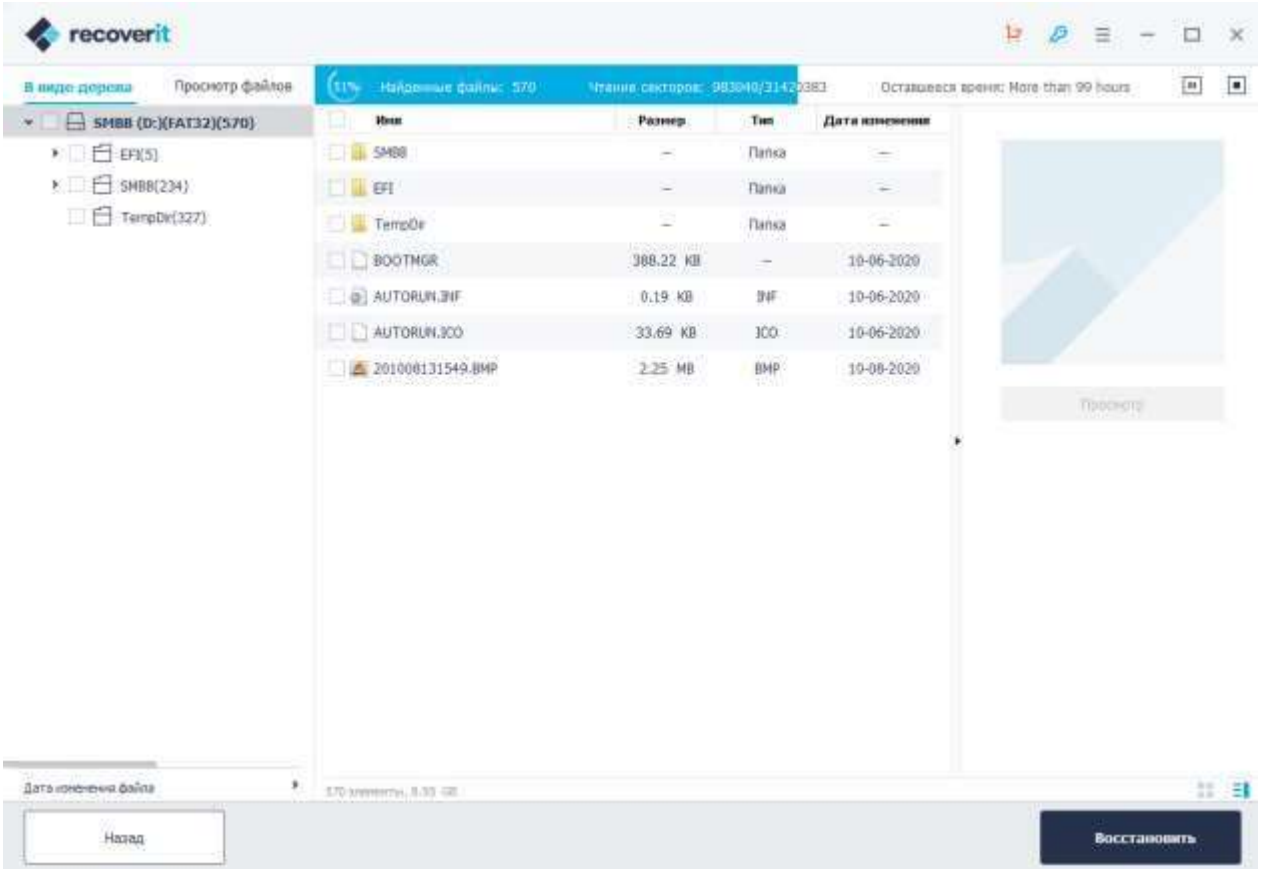
1. Технології відновлення даних.
2. Програмне забезпечення для відновлення даних.

ЗАВДАННЯ

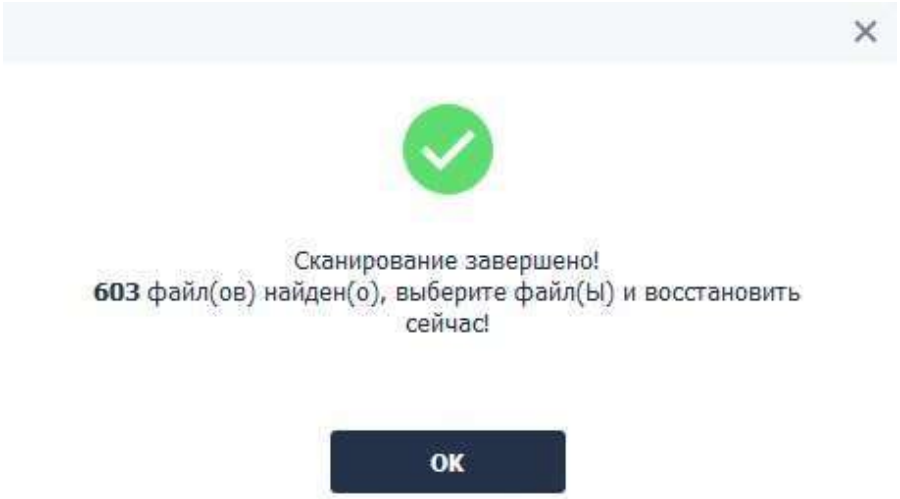
1. **Виконати відновлення всіх видалених файлів с Flash-карти:**
   1.1. Викачати архів з спеціалізованим програмним забезпеченням **Wondershare Recoverit** за адресою: https://bit.ly/34ImWLz і розпакувати його на диску, вказаному викладачем.
   1.2. Запустити виконуємий файл **_Silent Install.bat**
   1.3. Дочекатися встановлення програмного забезпечення.
   1.4. Вставити в USB порт Flash-карту пам‘яті.
   1.5. Запустити програму **Wondershare Recoverit.** Відкриється вікно:



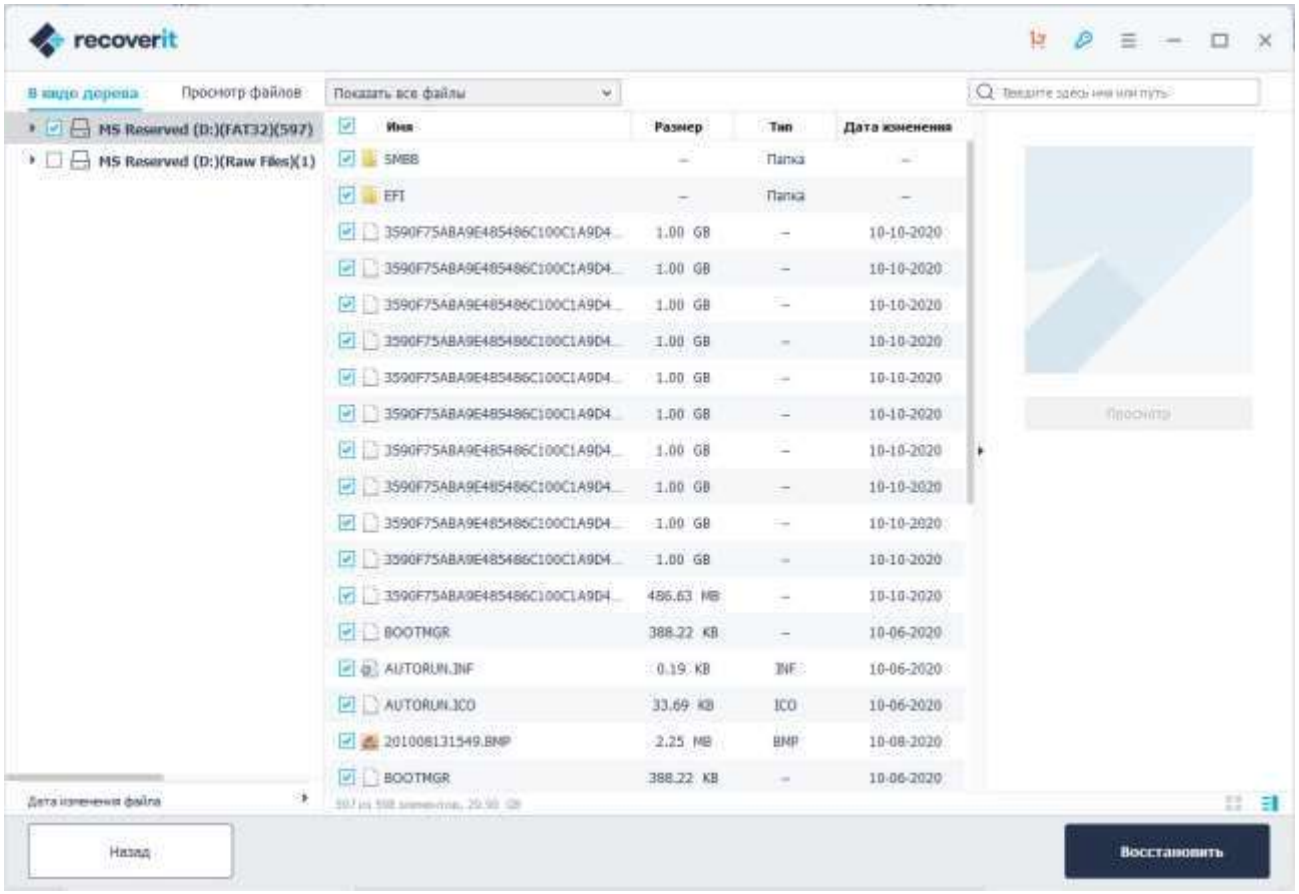
1.6. У списку дисків обрати розділ **Внешнее устройство**, де встановити маркер напроти **Flash-карти пам‘яті**. Нажати кнопку **СТАРТ**. Відкриється вікно:



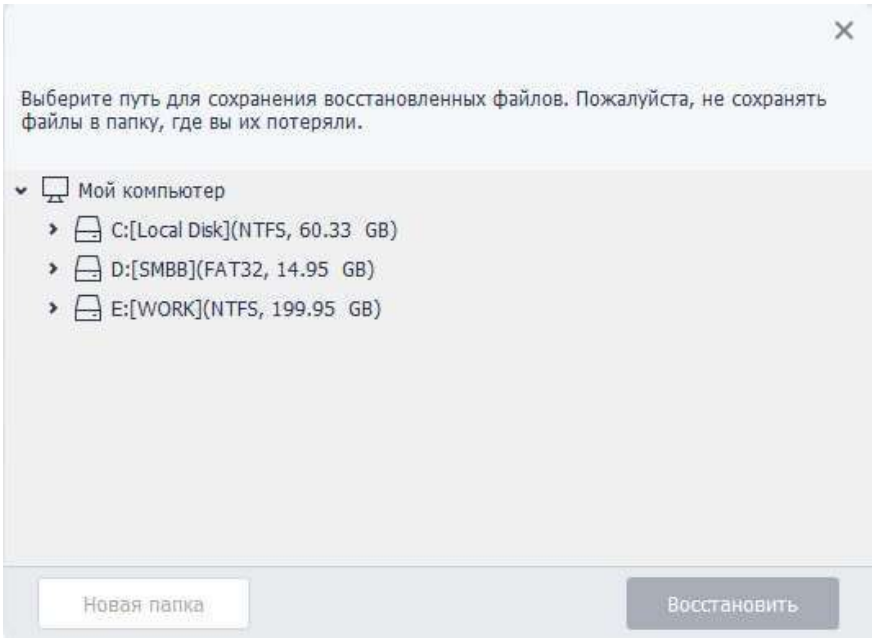
1.7. Дочекатися закінчення процесу сканування видалених файлів. Відкриється вікно:



1.8. Нажати кнопку **ОК**. Відкриється вікно:

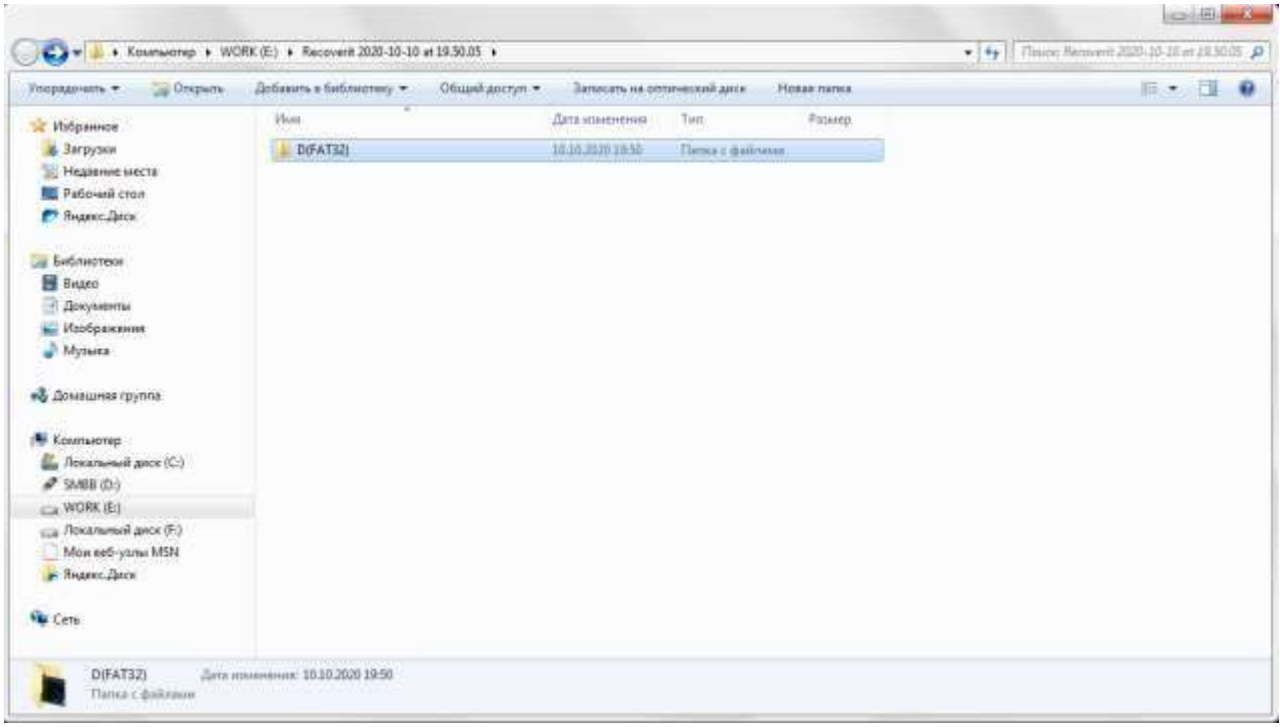


1.9. У графі «**Имя**» встановити маркер √, що автоматично виділить всі видалені файли. Нажати кнопку «**Восстановить**». Відкриється вікно:



1.10. Вибрати диск (за вказівкою викладача), на який будуть відновлені знайдені видалені файли і натиснути кнопку **Восстановить.** Відкриється вікно:

1.11. Дочекатися закінчення процесу відновлення файлів. Відкриється вікно:



1.12. Ознайомитися з вмістом папки **Recoverit __-__-__ at __.__.**, в якій розташовані відновлені файли. Вибірково перевірити цілісність відновлених файлів. Результати перевірки занести до звіту

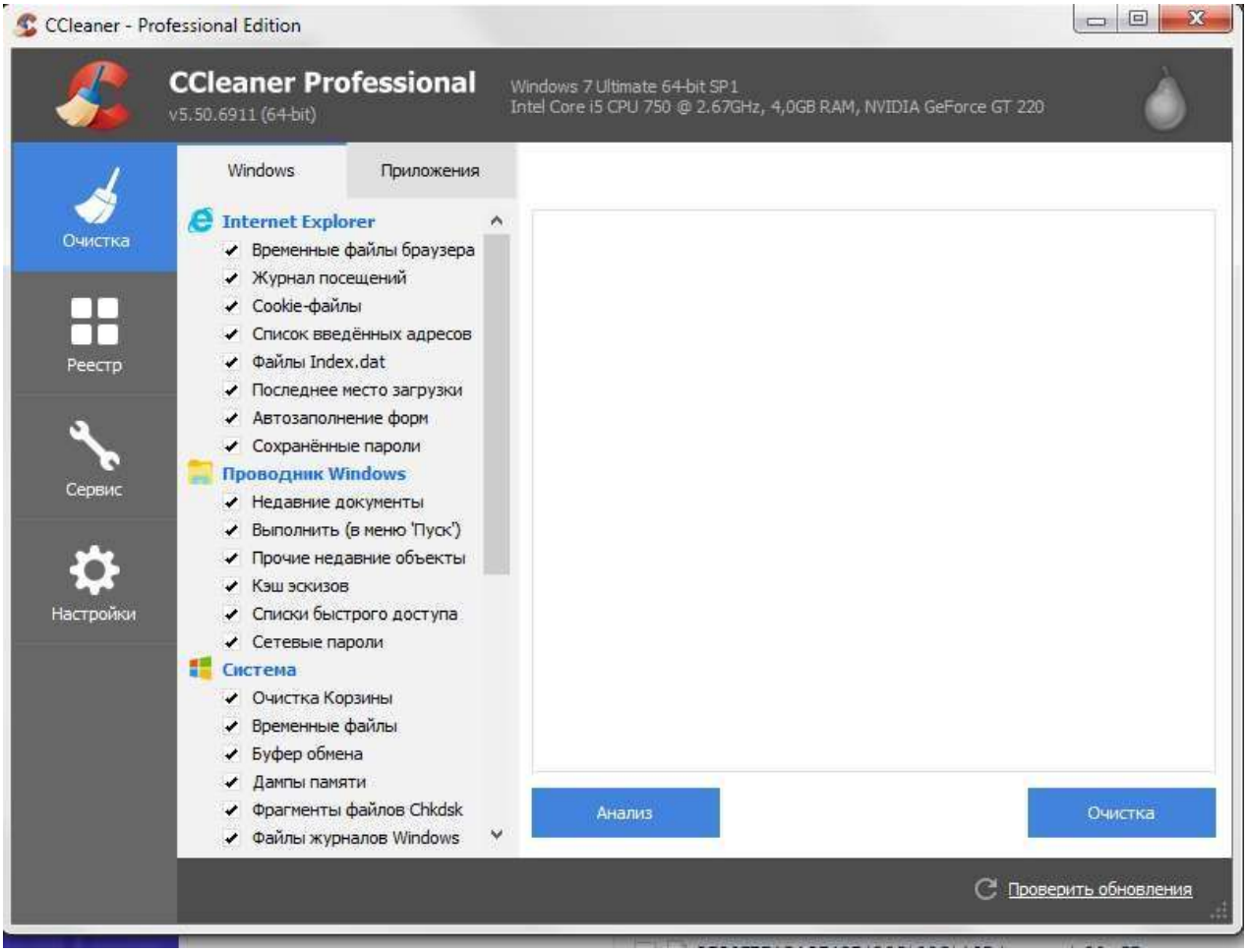
2. Виконати примусове очищення вільного простору Flash-карти:

2.1. Викачати архів з спеціалізованим програмним забезпеченням **CCleaner** за адресою: https://bit.ly/2GLI3EP і розпакувати архів на диску, вказаному викладачем.

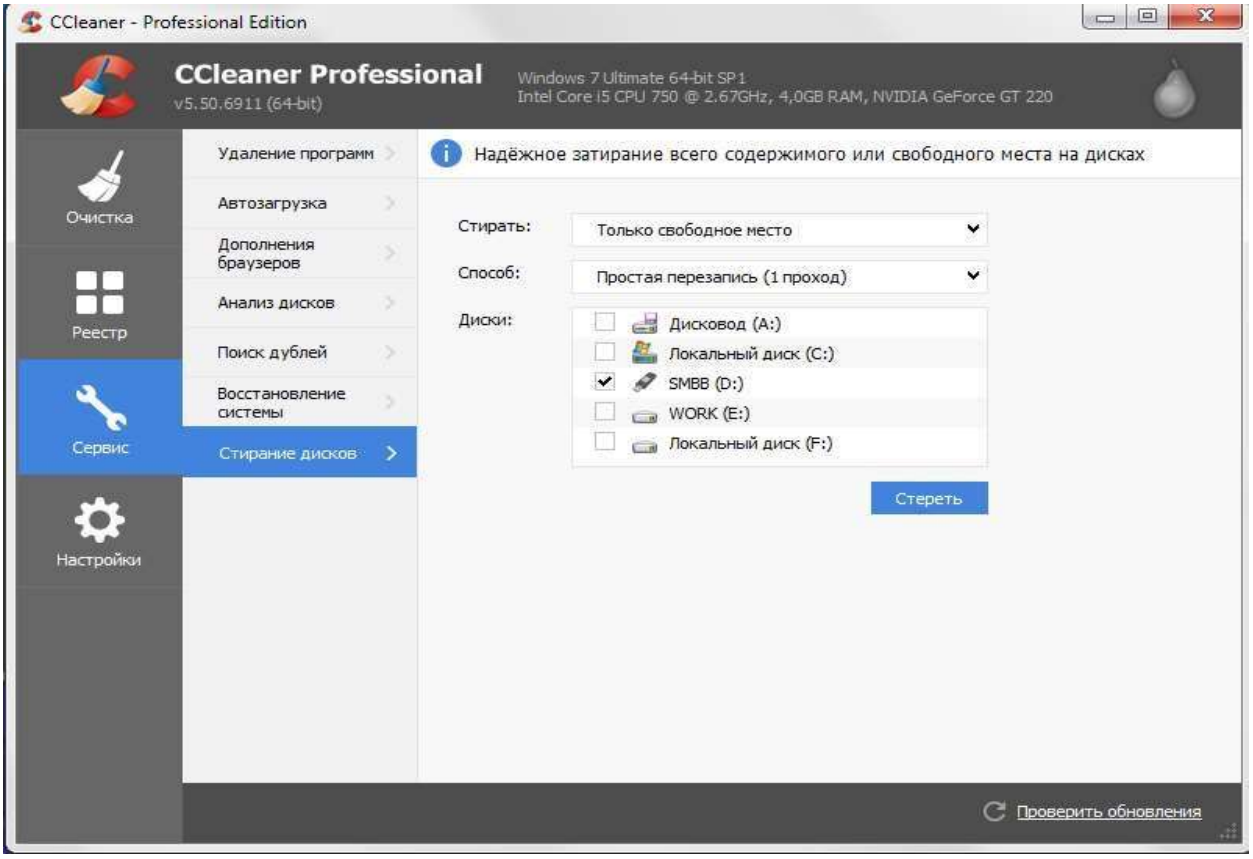
2.2. Запустити файл **ccsetup571.exe**.

2.3. Дочекатися закінчення процесу встановлення програмного забезпечення.

2.4. Запустити програму **CCleaner**. Відкриється вікно:



2.5. Вибрати режим «**Сервис**» ⇒ «**Стирание дисков**».



2.6. У графі «**Стирать:**» вибрати режим «**Только свободное место**», у графі «**Способ:**» вибрати режим «**Только свободное место**», у графі «**Диски:**» встановити маркер √ поруч з **Flash-картою.**

2.7. Нажати кнопку «**Стереть**». Дочекатися закінчення процесу затирання вільного простору **Flash-карти.**

3. Повторно виконати відновлення всіх видалених файлів с Flash-карти:

3.1. Виконати пункти 1.1 – 1.6.

4. Ознайомитися з вмістом другої папки **Recoverit__-__- at__.__.**, в якій розташовані відновлені файли. Порівняти вміст обох папок з відновленими файлами. Для цього необхідно заповнити таблицю 1.

Таблиця 1

Recoverit___-__-__at __.__.					
(1 папка)	**Тип файлу 1**	**Тип файлу 2**	**Тип файлу 3**	**Тип файлу 4**	**Тип файлу …**
Загальна сума відновлених файлів по типам					
Recoverit___-__-__at __.__.					
(2 папка)	**Тип файлу 1**	**Тип файлу 2**	**Тип файлу 3**	**Тип файлу 4**	**Тип файлу …**
Загальна сума відновлених файлів по типам					

5. Проаналізувати отримані кількісні та якісні результати відновлення файлів у таблиці 1, зробити висновки та занести їх до звіту.
1. У звіті підготувати відповідь на контрольне питання, номер якого повинен відповідати порядковому номеру в списку групи.
2. Оформити звіт з лабораторної роботи і надіслати його для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Які режими відновлення файлів доступні в спеціалізованому програмному забезпеченні Wondershare Recoverit?

2. У яких випадках необхідно використовувати режим попереднього перегляду для відновлюємих документів-фото і зображень?
3. З яких носіїв можливе відновлення файлів в спеціалізованому програмному забезпеченні Wondershare Recoverit?
4. Які формати відновлюємих файлів підтримує спеціалізоване програмне забезпечення Wondershare Recoverit?
5. Які переваги і недоліки відкриває користувачеві режим очищення вільного простору носія?

ТЕМА 5. ТЕХНОЛОГІЇ ЗБОРУ ПЕРСОНАЛЬНИХ ДАНИХ

САМОСТІЙНА РОБОТА № 2

ОПЕРАТОРНИЙ ЗБІР ПЕРСОНАЛЬНИХ ДАНИХ

Мета заняття - навчити користувача виконувати пошук інформації з використанням внутрішньої мови запитів пошукових систем.

Навчальні питання

1. Оперативний пошук інформації в пошукових системах.
2. Фільтрація пошукової видачі за необхідними критеріями пошуку.

Завдання на самостійну роботу:

1. Виконати пошук документів WORD, що містять в назві ключове слово "`захист даних`" в пошукової системі Google.
2. Зберегти першу інтернет-сторінку з результатами пошукової видачі з назвою **Прізвище_Ім‘я_результати_пошуку_doc_google.html**.

Примітка: Сторінки з результатами пошуку повинні бути збережені в режимі "Тільки сторінка HTML".

3. Виконати пошук документів **Adobe Acrobat**, що містять в назві ключове слово "`захист даних`" в пошуковій системі Google.

   3.1. Зберегти першу інтернет-сторінку з результатами пошукової видачі з назвою **Прізвище_Ім‘я_результати_пошуку_pdf_google.html**.

4. Виконати пошук документів **WORD**, розташованих на інтернет-ресурсі https://onua.edu.ua в пошуковій системі Google.

   4.1. Зберегти першу інтернет-сторінку з результатами пошукової видачі з назвою **Прізвище_Ім‘я_результати_пошуку_ONUA_DOC.html**

5. Виконати пошук документів **Adobe Acrobat**, розташованих на інтернет-ресурсі https://onua.edu.ua в пошуковій системі Google.

   5.1. Зберегти першу інтернет-сторінку з результатами пошукової видачі з назвою **Прізвище_Ім‘я_результати_пошуку_ONUA_PDF.html**

6. У звіті підготувати відповідь на контрольне питання, номер якого повинен відповідати порядковому номеру в списку групи.

7. Оформити звіт з самостійної роботи і надіслати його для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Які оператори застосовуються для пошуку файлів необхідного типу в пошуковій системі Google?
2. Які оператори застосовуються для локального пошуку файлів на інтернет-ресурсі в пошуковій системі Google?
3. У чому полягає перевага операторного пошуку перед звичайним пошуком?

САМОСТІЙНА РОБОТА № 3

МЕТОДИ ЗБОРУ ПЕРСОНАЛЬНИХ ДАНИХ

Мета заняття – вивчити технології збору інформації про користувача у віртуальному Інтернет-просторі.

Навчальні питання

1. Принципи збору інформації в Інтернет.
2. Системи збору статистики, що вживаються на інтернет-ресурсах.
3. Системи збору інформації про користувачів у соціальних мережах.

Завдання на самостійну роботу:

1. Ознайомитись з вмістом лекції № 5 на тему «СИСТЕМИ ЗБОРУ ДАНИХ КОРИСТУВАЧА В ІНТЕРНЕТ».
2. Підготувати оглядову доповідь, об'ємом 5 - 15 сторінок на тему «Технології збору персональних даних користувачів мережі Інтернет» з вказівкою використаних джерел.
3. У звіті підготувати відповідь на контрольне питання, номер якого повинен відповідати порядковому номеру в списку групи.
4. Оформити звіт з самостійної роботи і надіслати його для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Які системи аналізу відвідуваності інтернет-ресурсів існують?
2. Для чьго використовуються файли cookie в HTTP заголовках?
3. Яку базову інформацію о користувачах дозволяють отримати системи збору статистики?
4. Які основні параметри відвідуваності інтернет-ресурсів існують?
5. Яку інформацію про користувачів збирають соціальні мережі?
6. Поясніть принцип збору інформації з використанням плагинів соціальних мереж?
7. Поясніть принцип збору інформації про користувача пошуковими машинами?

8. Поясніть уразливості використання Flash cookies?
9. Наведіть класифікацію файлів cookie.
10. Які параметри відвідуваності інтернет-ресурсів існують?
11. Які дані збирають соціальні плагіни?
12. Які персональні дані збираються мобільними додатками соціальних мереж?
13. Поясніть принцип пошуку і аналізу персональних даних користувачів в соціальних мережах.

ТЕМА 6. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

ЛАБОРАТОРНА РОБОТА № 4

КРИПТОГРАФІЧНИЙ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

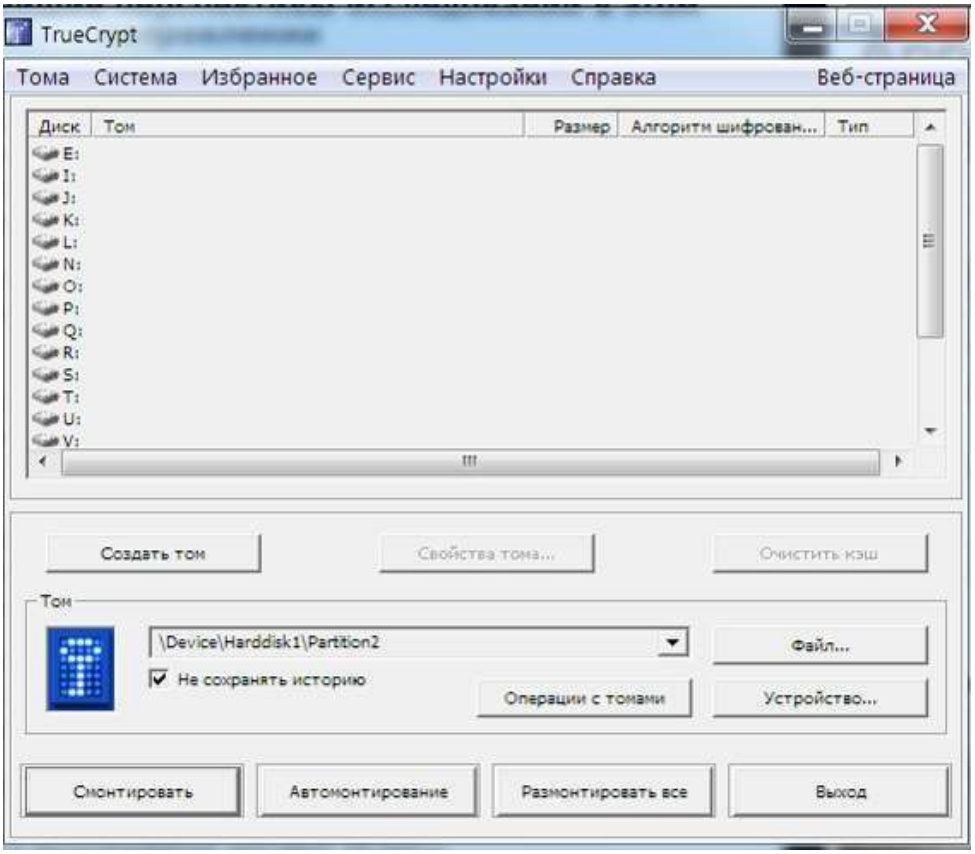
Мета заняття - отримати практичні навички з захисту даних користувача від несанкціонованого доступу з використанням криптографічного програмного забезпечення.

Навчальні питання

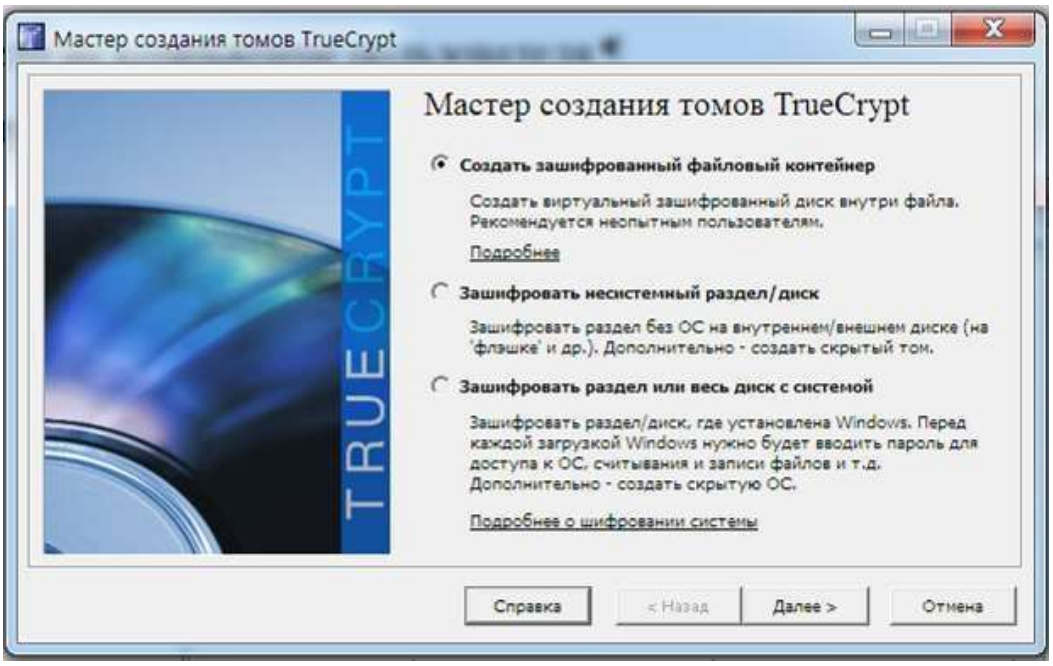
1. Технології криптографічного захисту даних.
2. Програмне забезпечення для криптографічного захисту даних.

ЗАВДАННЯ

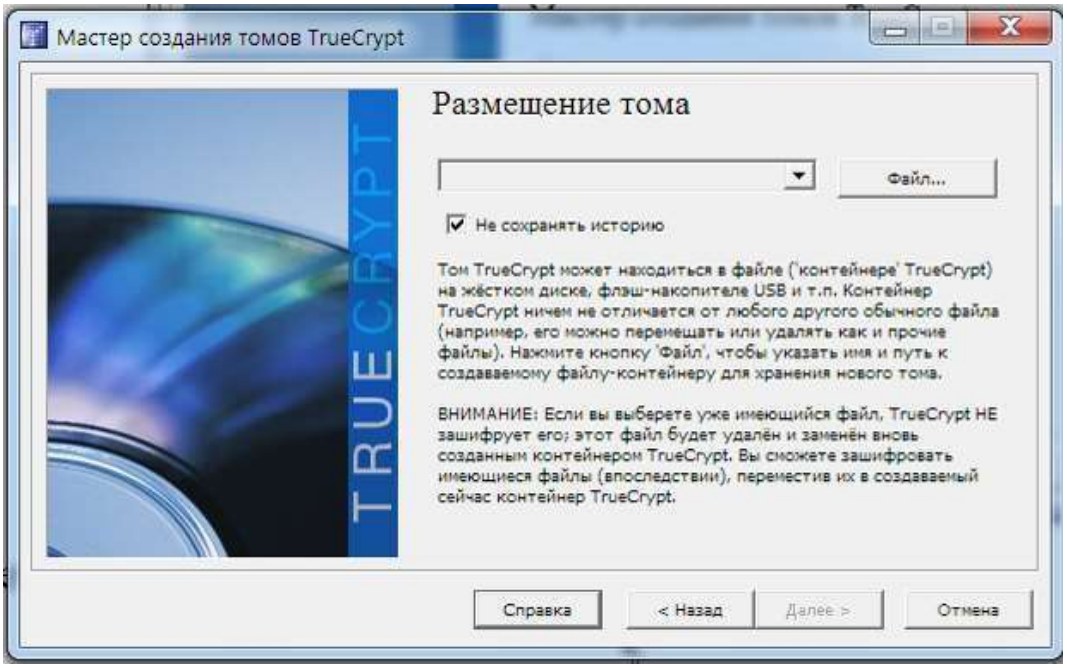
3. **Створити криптостійкий файловий контейнер з даними користувача.**
   3.1. Викачати криптографічне програмне забезпечення **Truecrypt** за адресою: https://bit.ly/36zRVvR і розпакувати архів на диску, вказаному викладачем.
   3.2. Запустити виконуємий файл **Truecrypt.exe**. Відкриється вікно:



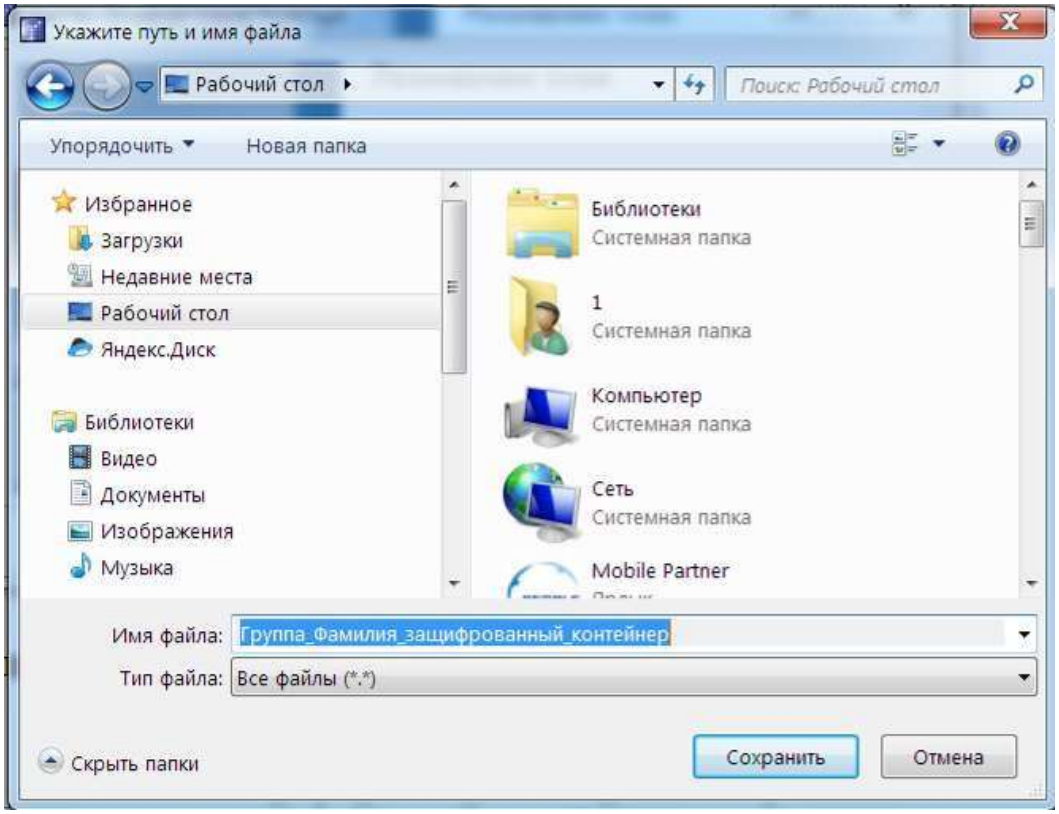
3.3. В верхньому меню «**Тома**» натиснути «**Создать новый том**». Відкриється вікно:



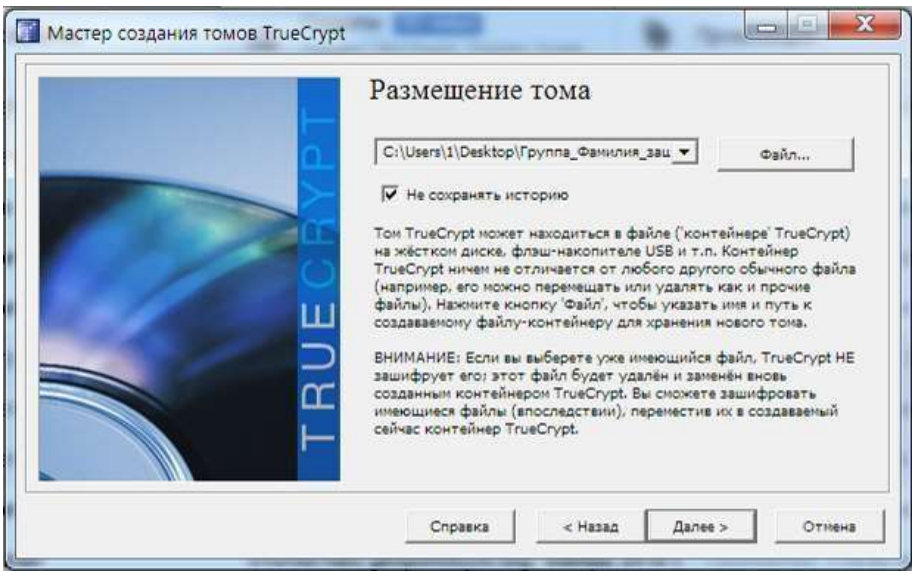
3.4. Встановити маркер в положення «**Создать зашифрованный файловый контейнер**» курсор Натиснути кнопку **Далі**. Відкриється вікно:



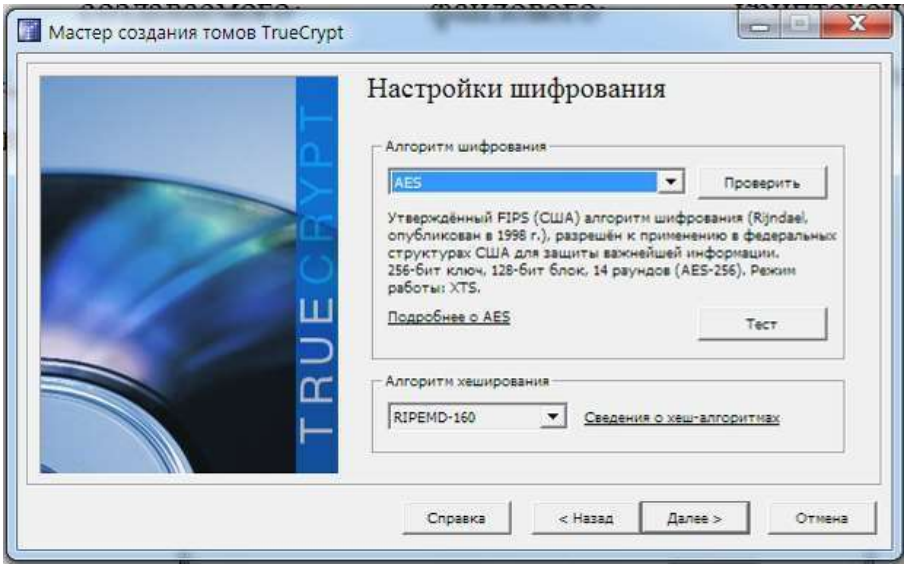
3.5. Натиснути кнопку **Файл**. Відкриється вікно:



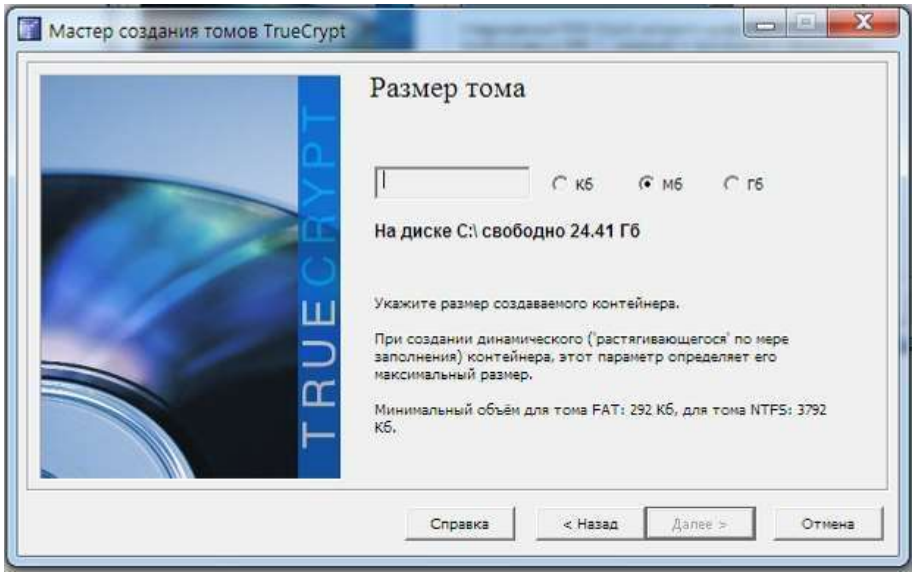
У вікні «**Укажите путь и имя файла**» в **графі «Імя файла**» необхідно вказати шлях до створюємого файлового криптоконтейнера. Присвоїти ім'я файловому криптоконтейнеру – **usercontainer** (де замість "**user**" вказати своє прізвище) і шлях до нього. Натиснути кнопку **Сохранить.** Відкриється вікно:



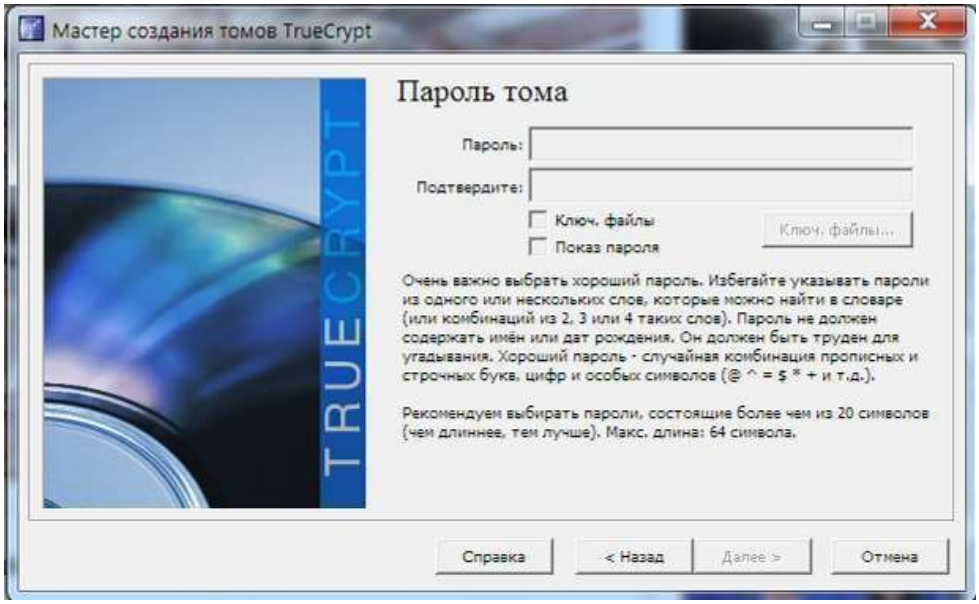
3.6. Натиснути кнопку **Далее.** Відкриється вікно:



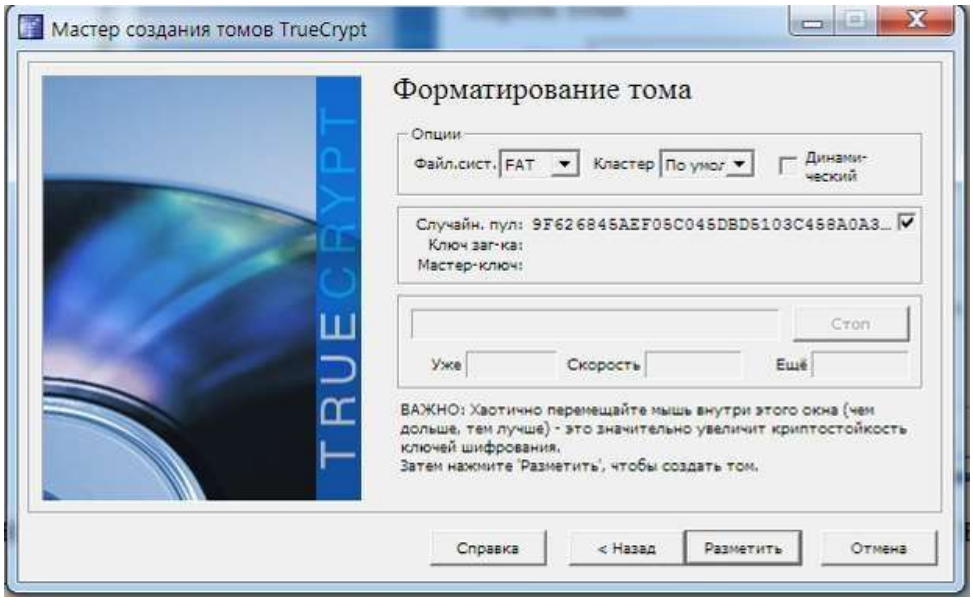
3.7. Вибрати бажаємий алгоритм шифрування і натиснути кнопку **Далі**. Відкриється вікно:



3.8. Ввести в поле «**Размер тома**» встановити значення 100 і виставити маркер в положення **мБ**, і натиснути кнопку **Далее**. Відкриється вікно:



3.9. Ввести в поля «**Пароль:**» і «**Подтвердите:**» бажаний пароль і натисніть кнопку **Далее**. Відкриється вікно:

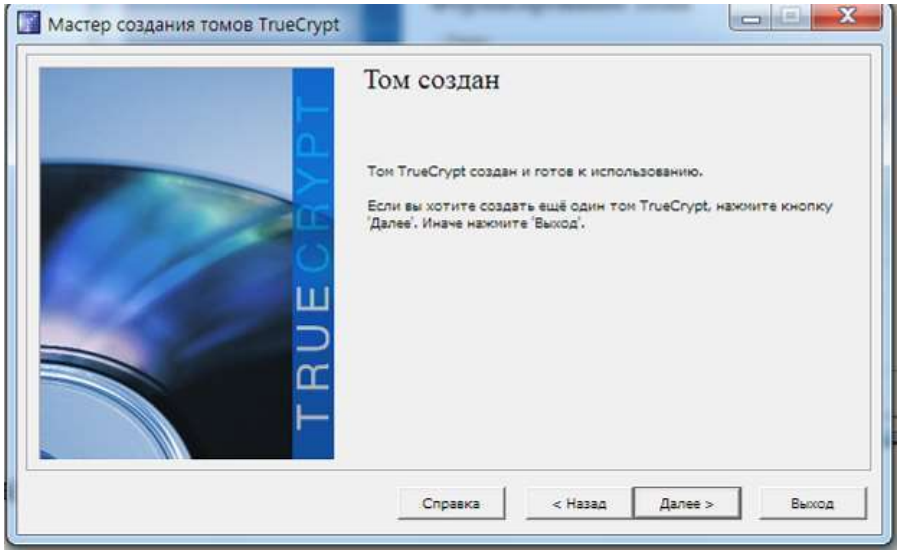


3.10. Вибрати файлову систему **FAT абоNTFS** і розмір кластеру. Встановити маркер напроти «**Динамический**».

Примітка: Динамічний файловий криптоконтейнер можна створювати тільки на фізичних розділах з NTFS форматуванням.

3.11. Виконати випадкове переміщення курсора миши у вікні «**Случайн. пул: /Ключ заголовка: / Мастер ключ:**», протягом, що найменше хвилини.

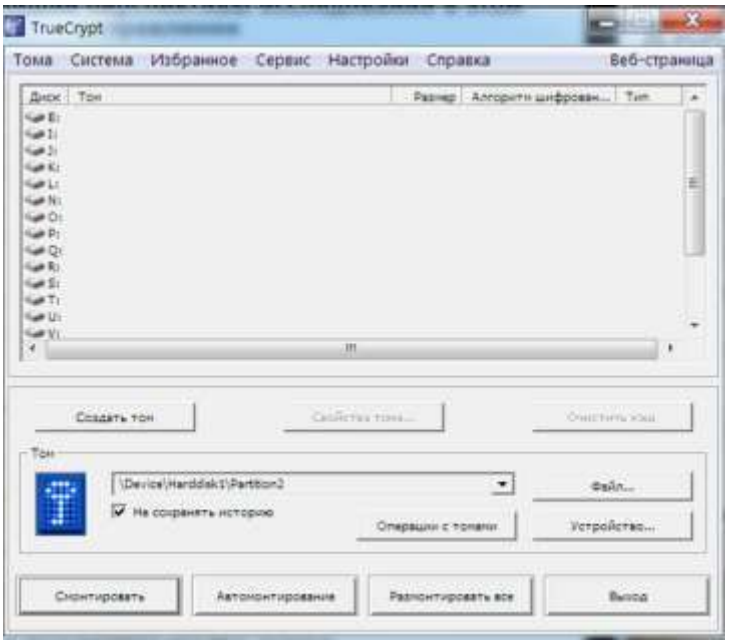
3.12. Натиснути кнопку **Розмітити** і дочекатися закінчення процесу створення файлового криптоконтейнеру. Після закінчення процесу відкриється вікно:



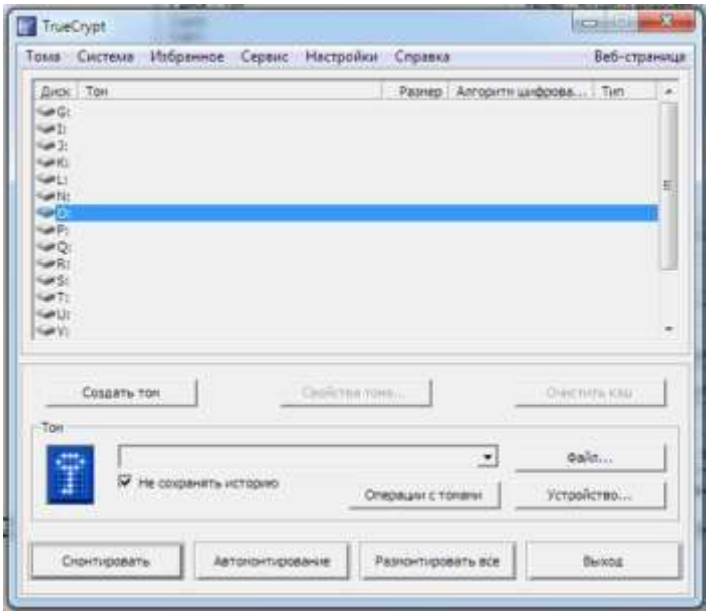
3.13. Натиснути кнопку **Выход**.

4. Змонтувати створений файловий криптоконтейнер **«usercontainer»** у диск:

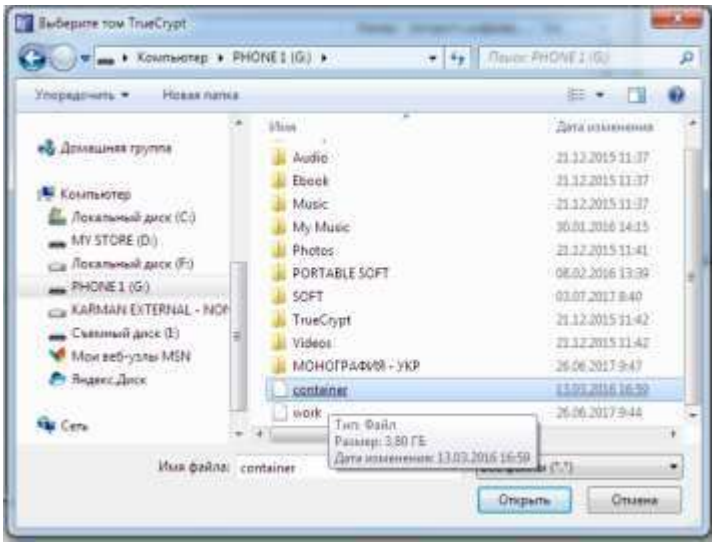
4.1. Запустити **Truecrypt.exe**. Відкриється вікно:



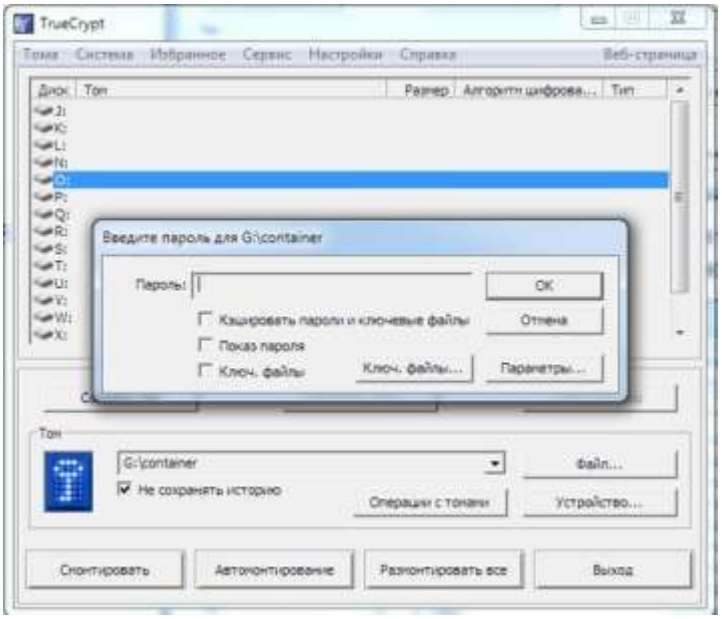
4.2. Встановити курсор на бажаний диск (наприклад **O:)**, як показано нижче



4.3. Натиснути кнопку **Файл**. Відкриється вікно «**Выберите том Truecrypt**», в якому необхідно вибрати курсором створений файловий криптоконтейнер «**usercontainer**» і натиснути кнопку **Открыть** (див. вікно нижче):



4.4. Змонтувати створений файловий криптоконтейнер в диск **О**. Для цього необхідно встановити курсор миші на диск **О** і клацнути клавішею миші. Відкриється вікно:

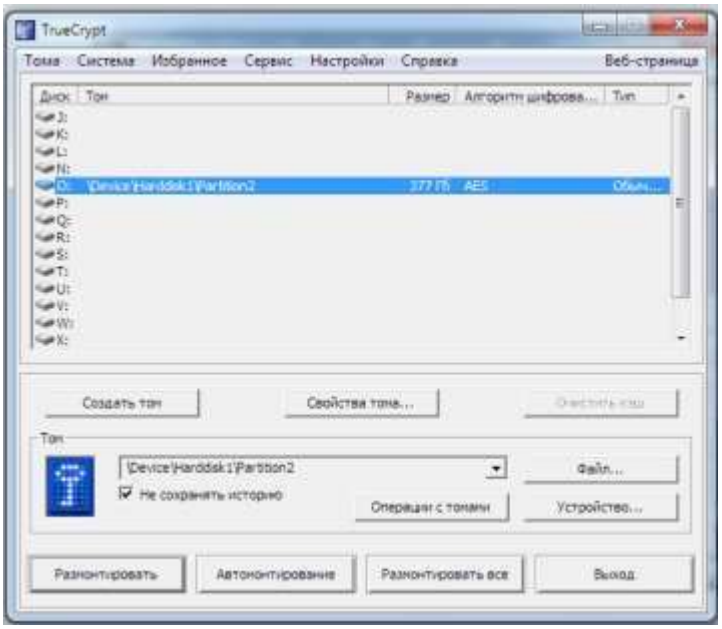


4.5. У вікні «**Введите пароль**» ввести пароль, який використовувався при створенні криптоконтейнера і натиснути кнопку **ОК**.

Відкрити **Мій комп'ютер** в операційній системі і переконатися в появі нового диска **О** з розміром, рівним заданому, при створенні файлового контейнера.

4.6. Виконати копіювання будь-яких даних користувача за вказівкою викладача в створений файловий криптоконтейнер засобами операційної системи.

4.7. Розмонтувати диск (зашифрувати криптоконтейнер). Для цього необхідно натиснути кнопку **Размонтировать.** (див. нижче вікно).



5. Завантажити створений файловий криптоконтейнер в хмарне сховище файлів (по вибору Google Disk, Microsoft Onedrive, Mega.nz або інше).

Примітка: Якщо користувач не має авторизованого доступу до хмарного сховища, він повинен виконати реєстрацію у обраному хмарному сховищі самостійно.

6. Надіслати на електронну поштову скриньку викладача посилання для «скачування» завантаженого файлового криптоконтейнеру **usercontainer**, а також пароль на його монтування.
7. У звіті підготувати відповідь на контрольне питання номер якого повинен відповідати порядковому номеру в списку групи.
8. Оформити звіт з лабораторної роботи і надіслати його для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Для чого використовуються операції монтування/розмотування файлового криптоконтейнеру?
2. Поясніть особливості створення динамічного файлового криптоконтейнеру.
3. Як підвищити критостійкість створюємого файлового криптоконтейну?
4. Як працює шифрування-на-льоту в програмному забезпеченні Truecrypt?
5. Де зберігає дані у незашифрованому вигляді програмне забезпечення TrueCrypt?
6. Поясніть призначення програмного забезпечення TrueCrypt?
7. Поясніть переваги програмного забезпечення TrueCrypt?
8. Що трапиться з файлами при використанні програмного забезпечення TrueCrypt, у разі перезавантаження операційної системи?
9. Які алгоритми шифрування використовуються у програмному забезпеченні TrueCrypt?

ЛАБОРАТОРНА РОБОТА № 5

ЗАХИСТ ВЕБ-БРАУЗЕРІВ MOZILLA FIREFOX та TOR ВІД ВИТОКІВ ПЕРСОНАЛЬНИХ ДАНИХ

Мета заняття - забезпечення максимального рівня приватності користувача при веб-серфінгу за рахунок конфігурування веб-браузерів **Mozilla FireFox** та **TOR**.

Навчальні питання

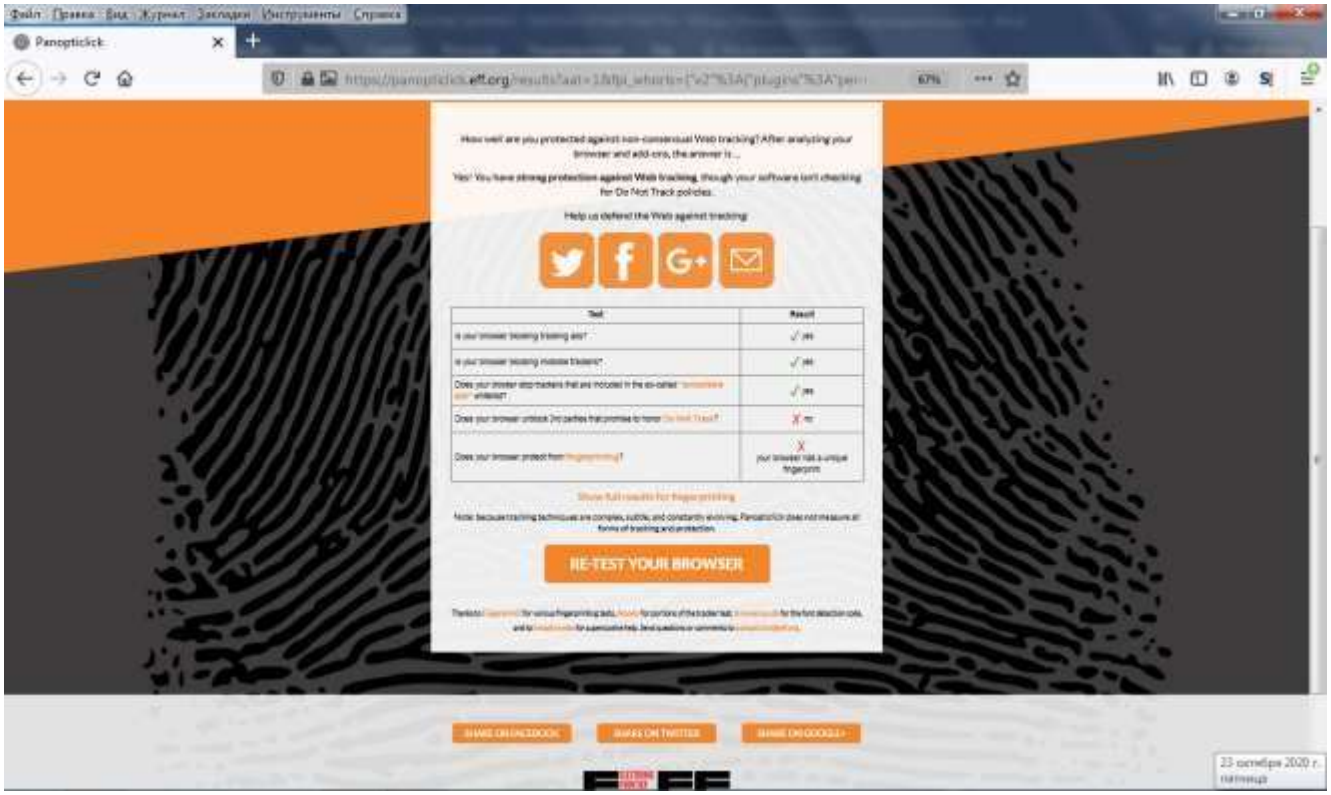
1. Витоки персональних даних в веб-браузерах.
2. Технології захисту від витоків персональних даних в веб-браузерах.

ЗАВДАННЯ

1. Встановити, веб-браузери **Mozilla Firefox** і **TOR**. Для цього завантажити інсталяції програмного забезпечення за адресами - https://www.mozilla.org/ru/ и https://www.torproject.org/download/.
2. Виконати перевірку веб-браузерів **Mozilla Firefox** и **TOR** на наявність витоків.

   2.1. В адресному рядку веб-браузера ввести адресу - https://panopticlick.eff.org/. Відкриється вікно:

2.2. Нажати кнопку «**TEST ME**». Відкриється вікно:

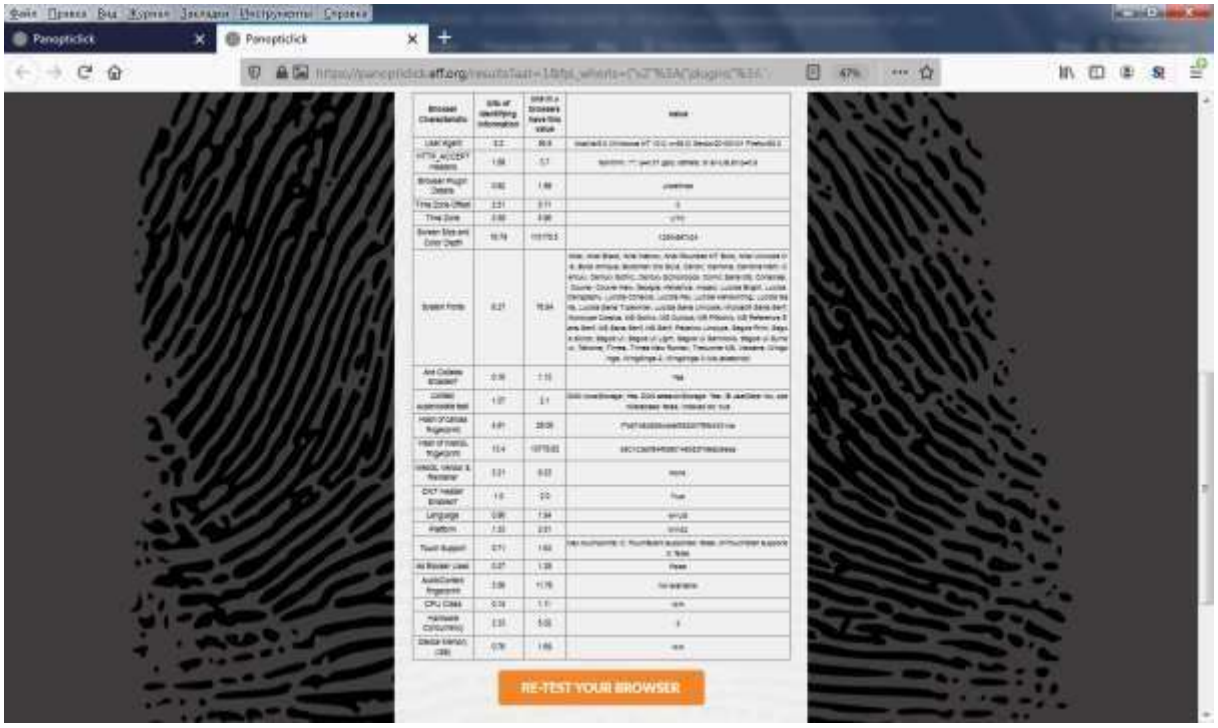


3. Отримані результати занести в таблицю 1.

Таблиця 1. Результати тестування веб-браузерів до очищення

Вид тесту		**Результати тестування (+ / -)**	
		MOZILLA FIREFOX	**TOR**
1	Is your browser blocking tracking ads?		
2	Is your browser blocking invisible trackers?		
3	Does your blocker stop trackers that are included in the so-called “acceptable ads” whitelist?		

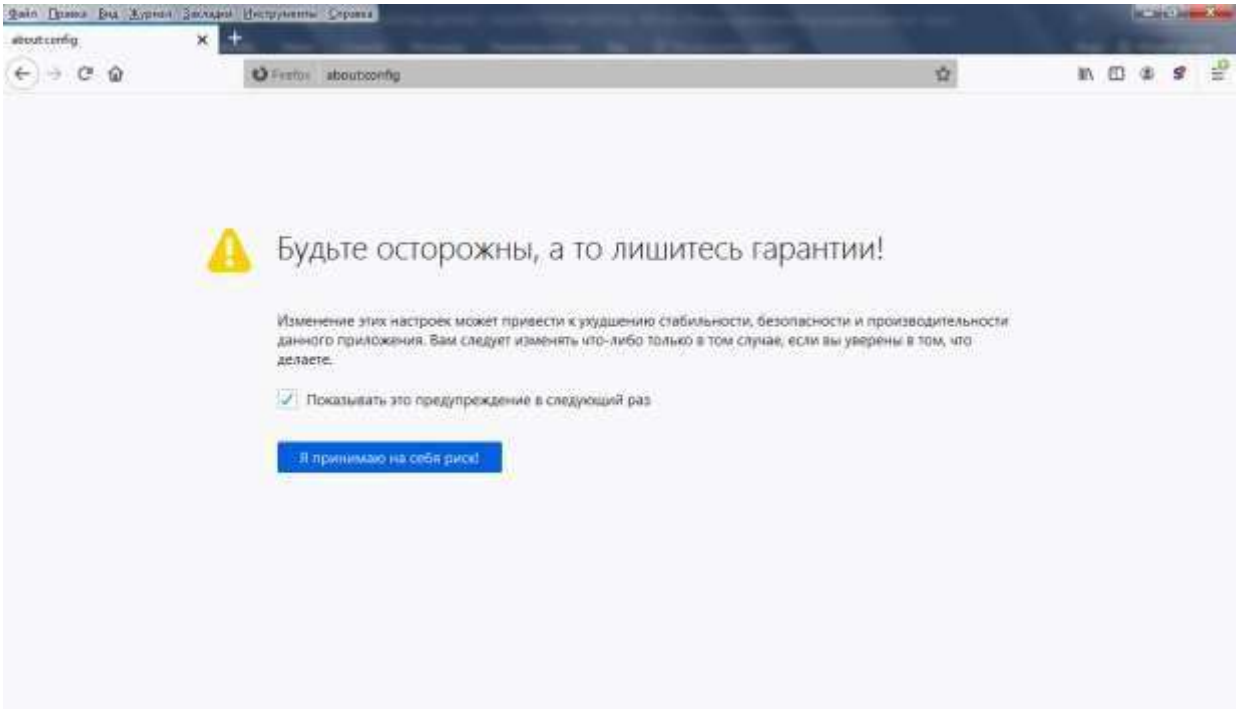
3.1. Натиснути кнопку/посилання «**Show full results for fingerprinting**». Відкриється вікно:



3.2. Результати повного тестування для веб-браузерів **Mozilla FireFox** і **TOR** скопіювати в таблицю 2 (див. додаток 1). Скачати додаток можна за посиланням - https://bit.ly/35QbUEC.

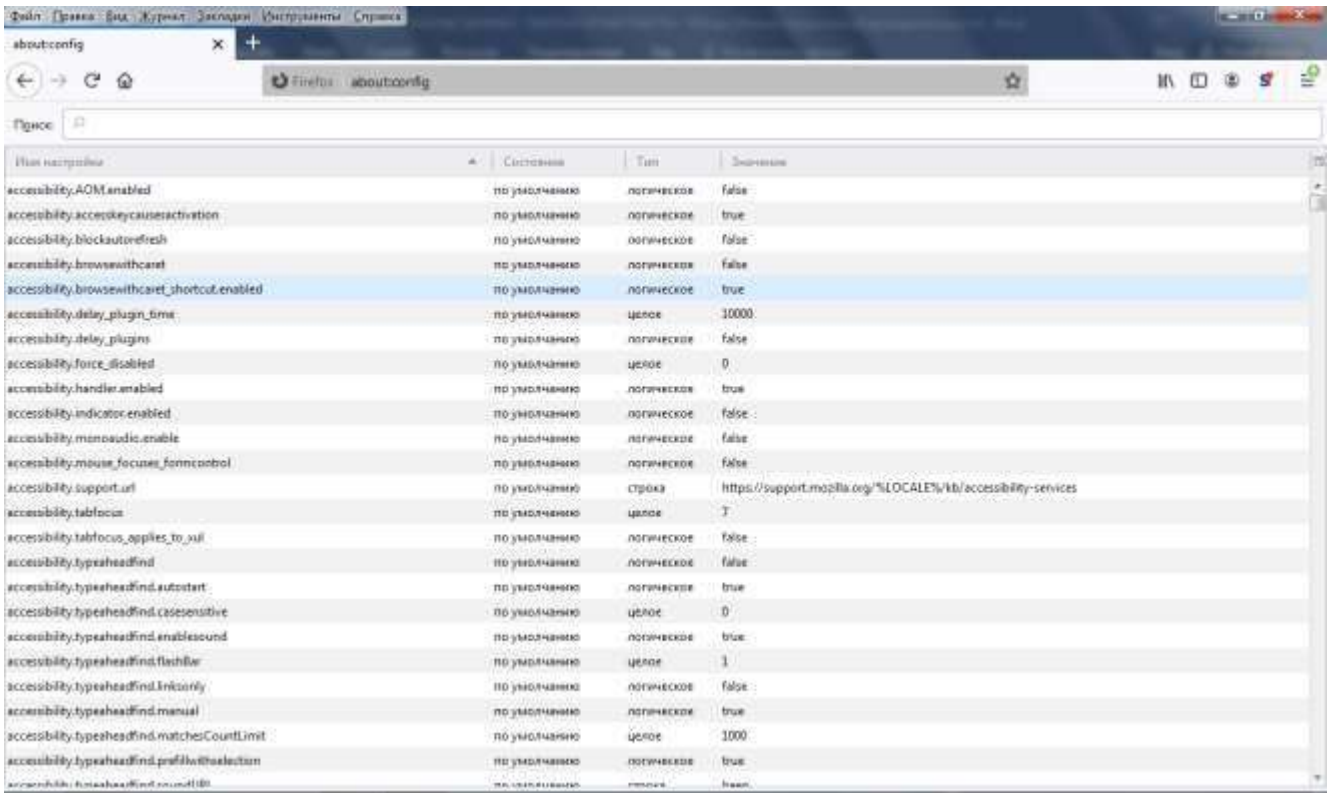
4. Виконати тонке налаштування веб-браузерів **Mozilla FireFox** и **TOR**:

4.1. По черзі відкрити веб-браузери **Mozilla Firefox** и **TOR**. В адресному рядку набрати команду **about:config**. Нажати клавішу **Enter**. Відкриється вікно:



Примітка: Після введення цієї команди з'явиться повідомлення про те, що потрібно бути обережним з настроюванням, так як існує можливість позбавлення гарантії на програмний продукт веб-браузер **Mozilla Firefox** і **TOR** відповідно.

4.2.Нажати кнопку **«Я принимаю на себя риск».** Відкриється вікно настроювань:



Примітка: У вікні налаштувань, в рядку пошуку (але не в адресному рядку!), як це показано вище необхідно ввести необхідну команду. Після появи необхідного рядка необхідно натиснути на нього правою клавішею миші і в випадаючому меню вибрати перший пункт «**Переключить**». Після переключення в полі «**Значение**» переконатися у наявності параметру «**False**» або «**Enable**». Якщо необхідно ввести параметри: **"", "[]", 0, "US".**

4.3.Порівняти наявність наведених нижче команд у веб-браузерах **Mozilla Firefox и TOR** Результати порівняння оформити у вигляді таблиці 3 (див. додаток 2). Скачати таблицю можна за посиланням - https://bit.ly/2HUV3sl.

4.4.Відключити сервіс **Pocket**[1]. Для цього по черзі ввести команди і внести зміни:

extensions.pocket.api", ""
extensions.pocket.enabled", false
extensions.pocket.site", ""
extensions.pocket.oAuthConsumerKey", ""

4.5.Відключити **WebRTC**[2]. Для цього по черзі ввести команди і внести зміни:

media.peerconnection.enabled", false
media.peerconnection.ice.default_address_only", true
media.peerconnection.ice.no_host", true
media.peerconnection.ice.relay_only", true
media.peerconnection.ice.tcp", false
media.peerconnection.identity.enabled", false
media.peerconnection.turn.disable", true
media.peerconnection.use_document_iceservers", false
media.peerconnection.video.enabled", false
media.peerconnection.default_iceservers", "[]"

4.6.Відключити **доступ к геолокації**. Для цього по черзі ввести команди і внести зміни:

geo.enabled", false
geo.providerms-windows-location", false
geo.wifi.uri", ""

4.7.Відключити **збір статистичних даних**:

4.7.1. Відключити **відправку звітів о стабільності і продуктивності**. Для цього по черзі ввести команди і внести зміни:

datareporting.healthreport.service.enabled, false
datareporting.healthreport.uploadEnabled, false

[1] **Pocket -** сервіс дозволяє користувачеві відзначати вподобану сторінку за допомогою відповідної кнопки і зберігає її в хмарному сервісі Mozilla Firefox.
[2] **WebRTC** - технологія використовується для створення з'єднань з одноранговою мережею в режимі реального часу, і потрібна для того, щоб користувачі через свої пристрої обмінювалися трафіком без додаткового програмного забезпечення.

4.7.2. Відключити **відсилання статистики, по технології Snippets**[3]. Ввести команду и внести изменения:

browser.aboutHomeSnippets.updateUrl, ""

4.7.3. Відключити **асинхронні запити аналітики**. Для цього по черзі ввести команди і внести зміни:

beacon.enabled", false
browser.send_pings", false
browser.send_pings.require_same_host", false

4.7.4. Відключити **метрики продуктивності**. Для цього по черзі ввести команди і внести зміни:

dom.enable_performance", false
dom.enable_performance_observer", false
dom.enable_performance_navigation_timing", false
browser.slowStartup.notificationDisabled", false
network.predictor.enabled", false
network.predictor.enable-hover-on-ssl", false
network.prefetch-next", false
network.http.speculative-parallel-limit", 0

4.7.5. Відключити **надсилання інформації про встановлені доповнення**. Для цього по черзі ввести команди і внести зміни:

extensions.getAddons.cache.enabled", false

4.7.6. Відключити **доступ к давачам**[4]. Для цього по черзі ввести команди і внести зміни:

device sensors enabled", false
device sensors orientation.enabled", false
device sensors motion.enabled", false
device sensors proximity.enabled", false
device sensors ambientLight.enabled", false

[3] **Технология Snippets** - сніпети є частиною браузера Mozilla Firefox і пропонують короткі поради. Firefox регулярно отримує колекцію сніпетів зі своїх серверів, яка адаптована до технічних параметрів веб-браузера Mozilla Firefox.
[4] **Давачі** – стаціонарний комп'ютер оснащений датчиками температури і т.д.

4.8. Відключити і**дентифікацію веб-браузера**. Для цього по черзі ввести команди і внести зміни:

dom.webaudio.enabled", false

privacy.resistfingerprinting", true

4.9. Відключити **передачу інформації про мережеве з'єднання**. Для цього по черзі ввести команди і внести зміни:

dom.netinfo.enabled", false

dom.network.enabled", false

4.10. Відключити **використання пристроїв і передачу медіа**[5]. Для цього по черзі ввести команди і внести зміни:

dom.gamepad.enabled", false

dom.gamepad.non_standard_events.enabled", false

dom.imagecapture.enabled", false

dom.presentation.discoverable", false

dom.presentation.discovery.enabled", false

dom.presentation.enabled", false

dom.presentation.tcp_server.debug", false

media.getusermedia.aec_enabled", false

media.getusermedia.audiocapture.enabled", false

media.getusermedia.browser.enabled", false

media.getusermedia.noise_enabled", false

media.getusermedia.screensharing.enabled", false

media.navigator.enabled", false

media.navigator.video.enabled", false

media.navigator.permission.disabled", true

media.video_stats.enabled", false

dom.battery.enabled", false

dom.vibrator.enabled", false

dom.vr.require-gesture", false

dom.vr.poseprediction.enabled", false

dom.vr.openvr.enabled", false

[5] Відключення використання через веб-браузер камер, мікрофонів, геймпадів, окулярів віртуальної реальності і разом з пристроями (передачу різного медіаконтенту) і розпізнавання мови.

dom.vr.oculus.enabled", false

dom.vr.oculus.invisible.enabled", false

dom.vr.enabled", false

dom.vr.test.enabled", false

dom.vr.puppet.enabled", false

dom.vr.osvr.enabled", false

dom.vr.external.enabled", false

dom.vr.autoactivate.enabled", false

media.webspeech.synth.enabled", false

media.webspeech.test.enable", false

media.webspeech.synth.force_global_queue", false

media.webspeech.recognition.force_enable", false

media.webspeech.recognition.enable", false

4.11. Відключити **телеметрію і відправку звітів розробникам**. Для цього по черзі ввести команди і внести зміни:

toolkit.telemetry.archive.enabled", false

toolkit.telemetry.bhrPing.enabled", false

toolkit.telemetry.cachedClientID", ""

toolkit.telemetry.firstShutdownPing.enabled", false

toolkit.telemetry.hybridContent.enabled", false

toolkit.telemetry.newProfilePing.enabled", false

toolkit.telemetry.previousBuildID", ""

toolkit.telemetry.reportingpolicy.firstRun", false

toolkit.telemetry.server", ""

toolkit.telemetry.server_owner", ""

toolkit.telemetry.shutdownPingSender.enabled", false

toolkit.telemetry.unified", false

toolkit.telemetry.updatePing.enabled", false

datareporting.healthreport.infoURL", ""

datareporting.healthreport.uploadEnabled", false

datareporting.policy.dataSubmissionEnabled", false

datareporting.policy.firstRunURL", ""

browser.tabs.crashReporting.sendReport", false

browser.tabs.crashReporting.email", false

browser.tabs.crashReporting.emailMe", false

breakpad.reportURL", ""

security.ssl.errorReporting.automatic", false

toolkit.crashreporter.infoURL", ""

network.allow-experiments", false

dom.ipc.plugins.reportCrashUR", false

dom.ipc.plugins.flash.subprocess.crashreporter.enabled", false

4.12. Включити **стандартний пошук веб-браузера без відправки місця розташування**. Для цього по черзі ввести команди і внести зміни:

browser.searchgeoSpecificDefaults", false

browser.searchgeoSpecificDefaults.url", ""

browser.search.geoip.url", ""

browser.search.region", "US"

browser.search.suggest.enabled", false

browser.search.update", false

4.13. Відключити **push-уведомления**[6]. Для цього по черзі ввести команди і внести зміни:

dom.push.enabled", false

dom.push.connection.enabled", false

dom.push.serverURL", ""

4.14. Включити **захист від витоку DNS**[7]. Для цього по черзі ввести команди і внести зміни:

network.dns.disablePrefetch", true

network.dns.disableIPv6", true

network.security.esni.enabled", true

network.trr.mode", 2

network.trr.uri", "https://cloudflare-dns.com/dns-query"

4.15. Відключити **перенаправлення**[8]. Для цього по черзі ввести команди і внести зміни:

[6] **push-повідомлення** - можуть працювати навіть тоді, коли закрита інтернет-сторінка.
[7] Можливий виток DNS по IPv6, попереджувальна відправка DNS, настройка Dns (DNS over HTTPS).
[8] З'єднання з detectportal.firefox.com встановлюється при кожному запуску Mozilla Firefox.

network.captive-portal-service.enabled", false

network.captive-portal-service.maxInterval", 0

captivedetect.canonicalURL", ""

4.16. Відключити **передачу даних на сервери Google**[9]. Для цього по черзі ввести команди і внести зміни:

browser.safebrowsing.allowOverride", false

browser.safebrowsing.blockedURIs.enabled", false

browser.safebrowsing.downloads.enabled", false

browser.safebrowsing.downloads.remote.block_dangerous", false

browser.safebrowsing.downloads.remote.block_dangerous_host", false

browser.safebrowsing.downloads.remote.block_potentially_unwanted", false

browser.safebrowsing.downloads.remote.block_uncommon", false

browser.safebrowsing.downloads.remote.enabled", false

browser.safebrowsing.malware.enabled", false

browser.safebrowsing.phishing.enabled", false

browser.safebrowsing.downloads.remote.url", ""

browser.safebrowsing.provider.google.advisoryName", ""

browser.safebrowsing.provider.google.advisoryURL", ""

browser.safebrowsing.provider.google.gethashURL", ""

browser.safebrowsing.provider.google.reportMalwareMistakeURL", ""

browser.safebrowsing.provider.google.reportPhishMistakeURL", ""

browser.safebrowsing.provider.google.reportURL", ""

browser.safebrowsing.provider.google.updateURL", ""

browser.safebrowsing.provider.google4.advisoryName", ""

browser.safebrowsing.provider.google4.advisoryURL", ""

browser.safebrowsi ng.provider.google4.dataSharingURL", ""

browser.safebrowsi ng.provider.google4.gethashURL", ""

browser.safebrowsing.provider.google4.reportMalwareMistakeURL", ""

4.17. Відключити **передачу історії серфінгу в Google**[10]. Ввести команду и внести изменения:

browser.safebrowsing.malware.enabled", false

[9] Налаштування за замовчуванням дозволяє Google захищати веб-браузер від вірусів і фішингу.

[10] Потрібне попередження, що відключення **Safe Browsing** підвищує ризик зараження в результаті відвідування шкідливого сайту.

4.18. Відключити **DRM**[11]. Для цього по черзі ввести команди і внести зміни:

browser.eme.ui.enabled", false

media.eme.enabled", false

media.gmp-eme-adobe.enabled", false

4.19. Відключити **підключення до сторонніх серверів**[12]. Ввести команду и внести изменения:

loop.enabled", false

4.20. Відключити **пошукові підказки**[13]. Ввести команду и внести изменения:

browser.search.suggest.enabled", false

4.21. Включить **захист від стеження з боку сайтів**[14]. Ввести команду и внести изменения:

privacy.trackingprotection.enabled", false

4.22. Відключити **відсилання статистики, пов'язаної з технологією Snippets**[15]. Ввести команду и внести изменения:

browser.aboutHomeSnippets.updateUrl, ""

5. Закрити веб-браузери **Mozilla Firefox** и **TOR**.

6. Виконати очищення веб-браузерів **Mozilla Firefox** и **TOR:**

6.1. Викачати архів з спеціалізованим програмним забезпеченням **CCleaner** за адресою: https://bit.ly/2GLI3EP і розпакувати архів на диску, вказаному викладачем.

6.2. Запустити файл **ccsetup571.exe**.

---

[11] **DRM** - бінарне розширення з невідомим вихідним кодом. Дозволяє відтворювати зашифрований медіаконтент і використовувати Netflix і ін. без Microsoft Silverlight. Якщо повністю видалити DRM, то буде потрібно встановити версію EME-free веб-браузера Mozilla Firefox.

[12] Веб-браузер Mozilla Firefox підключається до сторонніх серверів (Telefonica) без дозволу.

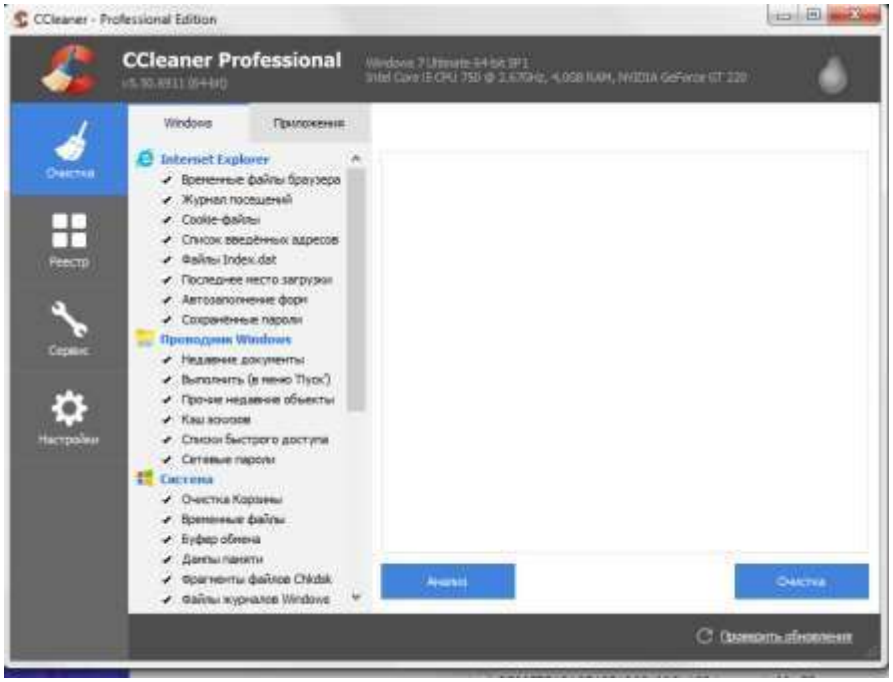
[13] **Пошукові підказки** - все набране в рядку пошуку відправляється пошуковій системі. Після відключення цієї опції підказки продовжать роботу, але тільки на основі локальної історії пошуку.

[14] **Захист від стеження з боку сайтів** - виконується активне блокування сайтів, які відомі своєю некоректною поведінкою щодо стеження за користувачами.

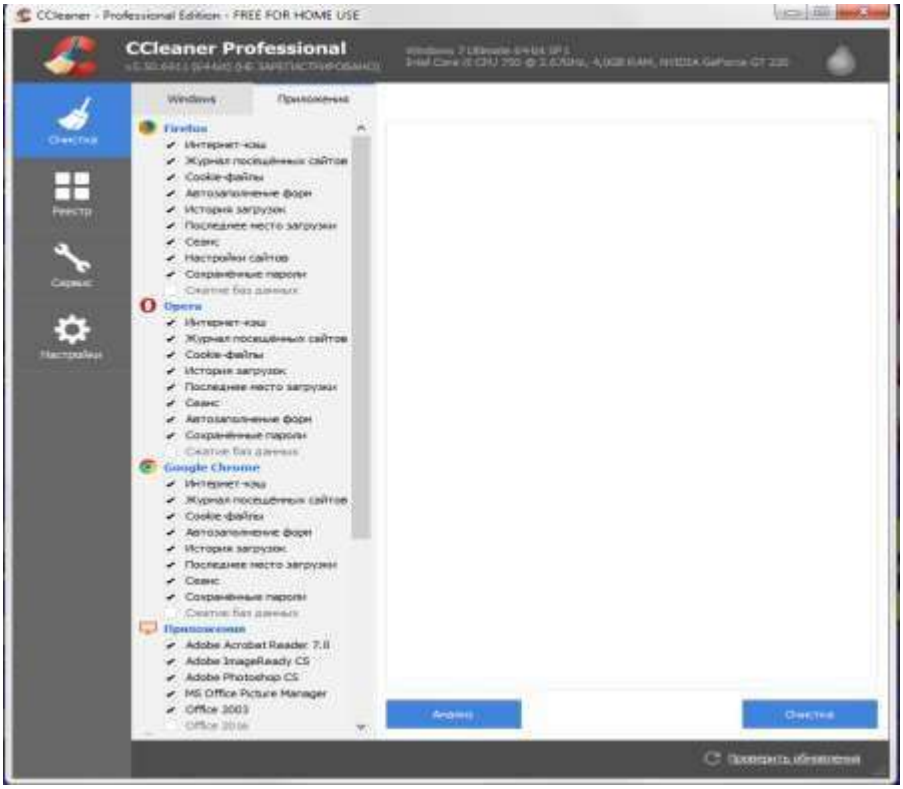
[15] **Статистика, повязана з технологією Snippets** - домашня сторінка веб-браузера, містить вбудований механізм показу рекламної інформації та стеження за користувацькими уподобаннями.

6.3. Дочекатися закінчення процесу встановлення програмного забезпечення.

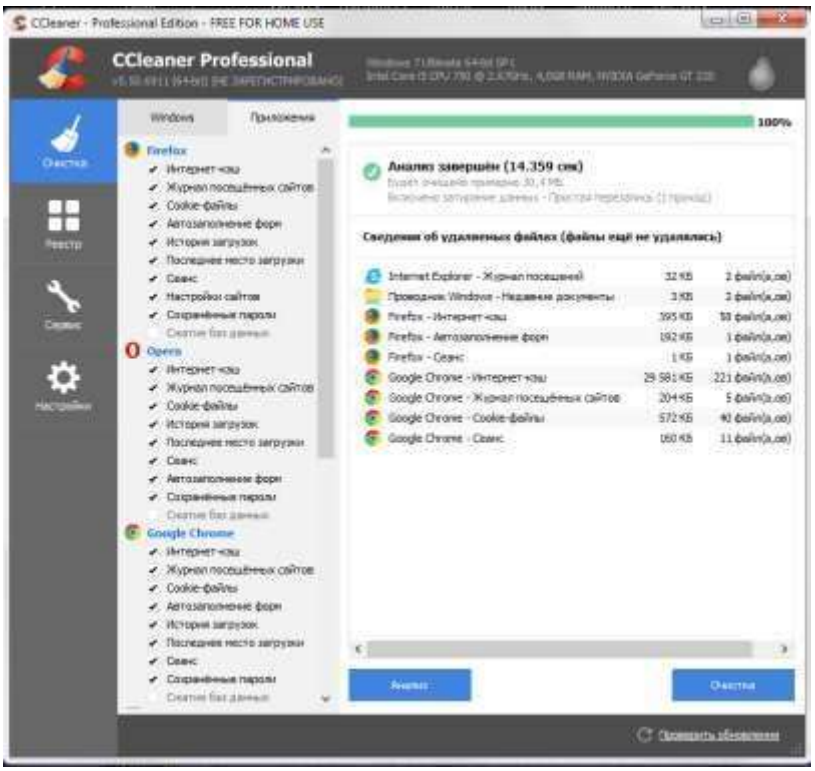
6.4. Запустити програму **CCleaner**. Відкриється вікно:



6.5. Вибрати режим «**Очистка**» ⇒ «**Приложения**». Встановити маркери √ в положення, вказане нижче:



6.6. Нажати кнопку «**Анализ**» і дочекатися закінчення його виконання, як показано нижче:



6.7. Нажати кнопку «**Очистка**» і дочекатися закінчення процедури очищення даних у веб-браузерах.

7. Повторно виконати перевірку веб-браузерів **Mozilla Firefox** и **TOR** на наявність витоків (див. вище п.2 и п.3).

7.1. Отримані результати занести в таблицю 2.

Таблиця 2. Результати тестування веб-браузерів після очищення

Вид тесту		**Результати тестування** (+ / -)	
		MOZILLA FIREFOX	**TOR**
1	Is your browser blocking tracking ads?		
2	Is your browser blocking invisible trackers?		
3	Does your blocker stop trackers that are included in the so-called “acceptable ads” whitelist?		

8. Проаналізувати отримані результати про цифрові відбитки веб-браузерів Mozilla Firefox і TOR у таблицях 1-3, зробити висновки та занести їх до звіту.
9. У звіті підготувати відповідь на контрольне питання, номер якого повинен відповідати порядковому номеру в списку групи.

10. Оформити звіт з лабораторної роботи і надіслати його для перевірки на електронну поштову скриньку викладача.

КОНТРОЛЬНІ ПИТАННЯ

1. Які види витоків існують у веб-браузерах?
2. Які статистичні дані відсилаються, пов'язані з технологією Snippets?
3. У чому полягає можлива загроза використання бінарного розширення DRM?
4. Чим відрізняються режими стандартного і локального пошуку у веб-браузері?
5. Чим пояснюється можливість витоків даних у веб-браузері через Push повідомлення?
6. У чому полягає можливий витік DNS по IPv6?
7. Що дозволяє реалізувати налаштування протоколу DNS over HTTPS (DoH)?
8. Які витоки даних характерні для сервісу Pocket?
9. Які загрози несе для користувача технологія WebRTC у веб-браузерах?

ЛАБОРАТОРНА РОБОТА № 6

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ОПЕРАЦІЙНИХ СИСТЕМАХ

Мета заняття – навчити користувача захищати операційну систему комп'ютера від витоків конфіденційної інформації.

Навчальні питання

1. Аналіз витоків персональних даних в операційних системах.
2. Протидія накопичуванню персональних даних в операційних системах.

ЗАВДАННЯ

1. Ознайомитись з вмістом лекції №10 на тему “ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ВІД ЗБОРУ І ВИТОКІВ».
2. Виконати пошук інформації про дії користувача в операційній системі. Для цього необхідно:
   - 2.1. Викачати програмне забезпечення **LastActivityView** за адресою: http://www.nirsoft.net/utils/computer_activity_view.html
   - 2.2. Розпакувати вміст zip-архива в папку з назвою **LastActivityView** на диск, вибраний по розсуду користувача.
   - 2.3. Виконати пошук і збереження інформації про дії користувача в операційній системі за допомогою програмного забезпечення LastActivityView. Для цього необхідно:
     - 2.3.1. У теці **LastActivityView** запустити програмний файл **LastActivityView.exe**.
     - 2.3.2. Зберегти весь список дій користувача у файл **СДК_Група__Прізвище_І‘мя.txt**.
     - 2.3.3. Вислати створений файл **СДК_Група__Прізвище_І‘мя.txt** на електронну поштову скриньку викладача на перевірку.
3. Викачати програмне забезпечення WIPE за адресою: https://privacyroot.com/software/www/ru/wipe.php.
   - 3.1. Виконати встановлення програмного забезпечення WIPE, запустивши файл **setup_wipe.exe**.

Примітка: Під час встановлення програмного забезпечення комп'ютер має бути підключений до мережі Інтернет.

3.2. За допомогою програмного забезпечення WIPE виконати повне очищення операційної системи. Для цього необхідно:

3.2.1. Запустити програмне забезпечення WIPE.

3.2.2. У режимі **Деталі** необхідно встановити всі прапорці напроти категорій, що очищаються, у вікні **Докладні відомості про елементи очищення**.

3.2.3. Натиснути кнопку **Видалити** та дочекатися завершення процесу очищення операційної системи.

3.3. Виконати повторний пошук і збереження інформації про дії користувача в операційній системі. Для цього необхідно:

3.3.1. У папці **LastActivityView** запустити програмний файл **LastActivityView.exe**.

3.3.2. Зберегти весь список дій користувача у файл **СДК_clean_Група__Прізвище_І‘мя.txt**.

3.4. Порівняти списки дій користувача у файлах **СДК_Група__Прізвище_І‘мя.txt** і **СДК_clean_Група_Прізвище_І‘мя.txt** і зробити виводи.

4. Виконати «заморожування» операційної системи. Для цього необхідно:

4.1. Викачати програмне забезпечення **Toolwize Time Freeze** за адресою: http://www.toolwiz.com/products/toolwiz-time-freeze/.

4.2. Виконати встановлення програмного забезпечення Toolwize Time Freeze, запустивши файл **Setup_Timefreeze.exe** і перезавантажити операційну систему.

4.3. Запустити програмне забезпечення **Toolwize Time Freeze**.

4.4. У робочому вікні програмного забезпечення **Toolwize Time Freeze** Натиснути кнопку **Start Time Freeze** для активізації процесу «заморожування» операційної системи.

4.5. Виконати наступні дії на **Робочому столі** операційної системи:

4.5.1. Створити набір з 2-х довільних ярликів.

4.5.2. Створити довільний текстовий документ «Блокнот» і заповнити його інформацією на свій розсуд.

4.5.3. Створити довільний документ Word і заповнити його інформацією на свій розсуд.

4.6. Виконати пошук і збереження інформації про дії користувача в операційній системі. Для цього необхідно:

4.6.1. У папці **LastActivityView** запустити програмний файл **LastActivityView.exe**.

4.6.2. Зберегти весь список дій користувача у файл **СДК_no_freeze_Група__Прізвище_І‘мя.txt**.

4.7. Виконати перезавантаження операційної системи і переконатися у відсутності на **Робочому столі** створених файлів.

4.8. Виконати пошук і збереження інформації про дії користувача в операційній системі. Для цього необхідно:

4.8.1. У папці **LastActivityView** запустити програмний файл **LastActivityView.exe**.

4.8.2. Зберегти весь список дій користувача у файл **СДК_freeze_Група__Прізвище_І‘мя.txt**.

4.9. Порівняти списки дій користувача у файлах **СДК_no_freeze_Група__Прізвище_І‘мя.txt** і **СДК_freeze_Група_Прізвище_І‘мя.txt** та зробити виводи.

4.10. Вислати створені файли:

СДК_Група__Прізвище_І‘мя.txt, СДК_clean_Група__Прізвище_І‘мя.txt, СДК_no_freeze_Група__Прізвище_І‘мя.txt, СДК_freeze_Група__Прізвище_І‘мя.txt на електронну поштову скриньку викладача на перевірку.

5. Виконати захист комп'ютера користувача за допомогою мережевого екрану Comodo Firewall. Для цього необхідно:

5.1. Викачати програмне забезпечення Comodo Firewall за адресою: https://bit.ly/2OOf3Qo.

5.2. Виконати встановлення програмного забезпечення Comodo Firewall, запустивши файл **cmd_fw_installer.exe** і перезавантажити операційну систему.

КОНТРОЛЬНІ ПИТАННЯ

1. Поясніть відмінність протоколів дій користувача у файлах **СДК_Група_Прізвище_І‘мя.txt** та **СДК_clean_Група_Прізвище_І‘мя.txt**.
2. Поясніть відмінність протоколів дій користувача у файлах **СДК_no_freeze_Група_Прізвище_І‘мя.txt** та **СДК_freeze_Група_Прізвище_І‘мя.txt**.
3. Яка інформація про користувача може збиратися операційною системою?
4. Які способи захисту застосовуються для запобігання витоків персональних даних в операційних системах?
5. Якого ефекту дозволяє досягти «заморожування» операційної системи?
6. Які переваги відкриває використання портативного програмного забезпечення?
7. Які види портативного програмного забезпечення існують?
8. Які переваги відкриває застосування мережевих екранів?
9. Які різновиди мережевих екранів існують?
10. Чому слід застосовувати очищення операційної системи від слідів роботи користувача?

САМОСТІЙНА РОБОТА № 4

ЗАХИСТ ВІД ВИТОКІВ І ЗБОРУ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ВЕБ-СЕРФИНГУ В ІНТЕРНЕТ

Мета заняття – навчити користувача захищати свій комп'ютер від збору конфіденційних даних при роботі в мережі Інтернет.

Навчальні питання

1. Принципи захисту веб-браузерів від витоків конфіденційної інформації в Інтернет.
2. Очищення веб-браузерів від слідів перебування користувача в Інтернет.
3. Способи блокування витоків персональних даних при веб-серфінгу.
4. Способи заміни реальної IP-адреси користувача при веб-серфінгу.

ЗАВДАННЯ

1. Ознайомитись з вмістом лекції № 10 на тему «ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ВІД ЗБОРУ І ВИТОКІВ У ВІРТУАЛЬНОМУ СЕРЕДОВИЩІ ІНТЕРНЕТ».
2. Виконати налаштування веб-браузерів, що забезпечують конфіденційну роботу користувача в мережі Інтернет. Для цього необхідно:
   2.1. Викачати і встановити інсталяційні пакети веб-браузерів: **Opera** (посилання для викачування - https://www.opera.com/ru/computer/thanks?ni=stable&os=windows, **Mozilla Firefox** (посилання для викачування - https://www.mozilla.org/ru/firefox/new/).
   2.2. Відключити автозаповнення і збереження паролів у веб-браузерах:
   - Для **Opera**: режим «**Налаштування**» - «**Безпека**» - «**Автозаповнення**» - зняти прапорець, якщо він встановлений;
   - Для **Mozilla Firefox**: режим «**Налаштування**» - «**Захист**» - «**Паролі**» - в рядку «**Запам'ятовувати паролі для сайтів**» прибрати прапорець, якщо він встановлений, в рядку «**Використовувати майстер-пароль**» встановити прапорець і ввести бажаний пароль;

- Для перевірки викладачем виконаного завдання вислати на електронну пошту викладача скриншоти виконаних налаштувань для кожного з браузеров у вигляді графічних файлів:

  - **Група_Прізвище_І‘мя_mozilla_паролі.jpg;**

  - **Група____Прізвище_І‘мя_opera_паролі.jpg;**

2.3. Відключити виконання **JavaScript** у веб-браузерах:

- Для **Opera**: режим «**Налаштування»** - «**Сайти»** - «**Заборонити виконання Javascript»** - встановити прапорець, якщо він не встановлений;
- Для перевірки викладачем виконаного завдання вислати на електронну поштову скриньку скриншоти виконаних налаштувань для кожного з веб-браузерів у вигляді графічних файлів:

  - **Група_Прізвище_І‘мя_opera_javascript.jpg**.

  - **Група__Прізвище_І‘мя_mozilla_javascript.jpg**.

2.4. Відключити режим відображення **спливаючих вікон** у веб-браузерах:

- Для **Opera**: режим «**Налаштування»** - «**Сайти»** - «**Спливаючі вікна»** - «**Блокувати спливаючі вікна»** встановити прапорець, якщо він не встановлений;
- Для **Mozilla Firefox**: режим «**Налаштування»** - «**Вміст»** - «**Спливаючі вікна»** - «**Блокувати спливаючі вікна»** встановити прапорець, якщо він не встановлений;
- Для перевірки викладачем виконаного завдання вислати на електронну пошту викладача скриншоти виконаних налаштувань для кожного з веб-браузерів у вигляді графічних файлу **Група__Прізвище_І‘мя_Opera_вікна.jpg** та **Група_Прізвище_І‘мя_Mozilla_вікна.jpg;**

2.5. Виконати налаштування веб-браузерів для безпечної роботи з файлами **cookies**:

- Для **Opera**: режим «**Налаштування**» - «**Безпека**» - «**Файли cookie**» - «**Зберігати локальні дані до виходу з браузера**» встановити прапорець, якщо він не встановлений; встановити прапорець в режим **«Блокувати сторонні файли cookie і дані сайтів»**.

2.6. Виконати настроювання режиму автоматичного очищення слідів роботи користувача на комп'ютері та в Інтернет. **Для цього необхідно**:

- Викачати програмне забезпечення **Cleaner** за адресою: https://www.piriform.com/ccleaner/download.
- Виконати встановлення програмного забезпечення **Ccleaner**, запустивши файл **ccsetup.exe**. Після закінчення встановлення перезавантажити операційну систему.
- Запустити програмне забезпечення **Ccleaner**.
- У робочому вікні програмного забезпечення **Ccleaner** Натиснути кнопку **Налаштування** і встановити маркер в положення **Режим очищення – Безпечне видалення – Простий перезапис (1 прохід)**.
- У робочому вікні програмного забезпечення **Ccleaner** Натиснути кнопку **Очищення** для виконання операції очищення операційної системи та слідів роботи користувача в Інтернет.
- У робочому вікні програмного забезпечення **Ccleaner** у закладках **Windows** і **Програми** встановити прапорці напроти всіх позицій за виключенням **Очищення вільного місця**.
- У робочому вікні програмного забезпечення **Ccleaner** натиснути кнопку **Очищення** (у правому нижньому кутку екрану).

2.7. Виконати захист веб-браузерів від збору конфіденційних даних Інтернет:

- Перейти на сторінку встановлення розширення **Adguard антибанер** для веб-браузера за адресою:

https://adguard.com/ru/download.html. Виконати встановлення розширення.

2.8. Виконати заміну своєї **реальної IP-адреси**. **Для цього необхідно**:

- Відкрити **Yandex браузер** і перевірити свою **реальну IP-адресу**, набравши в його адресному рядку **http://2ip.ru**;
- Створити скриншот сторінки, що відкрилася, і зберегти його у вигляді графічного файлу **Група_Прізвище_І'мя_реальна_IP_адреса.jpg**.
- і виконати встановлення розширення **CyberGhost VPN - Free Proxy**.
- Активізувати розширення **CyberGhost VPN - Free Proxy** натисканням кнопки .
- Виконати повторну перевірку своєї **IP-адреси**, набравши в адресному рядку веб-браузера **http://2ip.ru**;
- Створити скриншот сторінки, що відкрилася, і зберегти його у вигляді графічного файлу **Група_Прізвище_І'мя_віртуальна_ip_адреса.jpg**.
- Вислати створені скриншоти файлів **Група_Прізвище_І'мя_реальна_ip_адреса.jpg** і **Група_Прізвище_І'мя_віртуальна_ip_адреса.jpg** на електронну поштову скриньку викладача на перевірку викладачеві.

КОНТРОЛЬНІ ПИТАННЯ

1. Чим небезпечна синхронізація аккаунтов користувача у веб-браузерах?
2. Яку загрозу несуть користувачеві спливаючі вікна на інтернет-ресурсах?
3. Поясніть особливості збору інформації за допомогою плагинів (кнопок) соціальних мереж на сторінках інтернет-ресурсів?
4. Яку небезпеку для користувача несе для користувачів можливість збереження паролів і форм у веб-браузерах?
5. Які способи блокування систем збору інтернет-статистики існують?

6. Яка інформація про користувача збирається в соціальних мережах?
7. Поясніть призначення файлів cookies при роботі веб-браузера з інтернет-ресурсами.
8. Поясніть принцип заміни реальної IP-адреса користувача.
9. Поясніть призначення проксі сервера.
10. Дайте класифікацію проксі серверів і поясніть їх особливості.
11. Поясніть принцип функціонування програмного забезпечення для заміни реальної IP-адреси користувача.
12. На які обставини необхідно звернути увагу при виборі способу заміни реальної IP-адреса користувача.

Перелік рекомендованої літератури та інформаційних джерел

Базова література

1. 1. Концептуальні основи захисту інформаційного суверенітету України: монографія / О.В. Задерейко, О.В. Троянський, Р.І. Чанишев.– Одеса: Фенікс, 2018. – 110 с.
2. Захист інформації в автоматизованих системах управління: навчальний посібник/ І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир: ЖДУ ім. І. Франка, 2015. – 226 с.
3. Бем М. В. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник / М. В. Бем, І. М. Городиський, Г. Саттон, О. М. Родіоненко – Київ: К.І.С., 2015. – 220 с. 3. Грищук Р. В. Основи кібернетичної безпеки : монографія / Р. В. Грищук, Ю. Г. Даник ; під заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.
4. Захист даних в інформаційних системах. Методичні вказівки до лабораторних робіт для студентів денної форми навчання спеціальності 6.010104.36 "Професійна освіта. Комп'ютерні технології в управлінні та навчанні" (Частина 1) /Упор. О. С. Горянська.– Стаханов: СНІГОТ УІПА, 2012.– 120 стор.
5. Захист даних в інформаційних системах. Методичні вказівки до лабораторних робіт для студентів денної форми навчання спеціальності 6.010104.36 "Професійна освіта. Комп'ютерні технології в управлінні та навчанні" (Частина 2) /Упор. О. С. Горянська.– Стаханов: СНІГОТ УІПА, 2012.– 76 стор.
6. Захарченко М.В. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум. Частина 1 – Комплекси засобів захисту інформації від НСД: навч. посіб. / М.В. Захарченко, В.Г. Кононович, В.Й. Кільдішев, Д.В. Голев // За ред. ак. МАІ М.В. Захарченка.– Одеса: ОНАЗ ім. О.С. Попова, 2011. – 168 с.
7. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків : ХНЕУ, 2010. – 316 с.

Допоміжна література

1. Кібербезпека України: аналіз сучасного стану / Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Задерейко О.В. // Захист інформації. – Київ: Національний авіаційний університет. – 2019. – Т. 21. – №3. – С. 150–157.
2. Моніторинг рівня кібербезпеки України у світових рейтингах / Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Задерейко О.В. // Інформаційна безпека людини, суспільства, держави. – Київ: Національна академія Служби безпеки України. – 2019. – №3(27). – С. 100–107.2.
3. Задерейко, А.В. Проблемные аспекты деперсонализации цифровых изображений / А.В. Задерейко, А.В. Троянский, Н. И. Логинова, Е.Г. Трофименко // Інформатика та математичні методи в моделюванні. - 2017. - Том 7, № 1-2. - С. 37 - 46.
4. Program-Technical Aspects of Encryption Protection of Users' Data / Natalia Loginova, Elena Trofimenko, Olexander Zadereyko, Rashid Chanyshev // TCSET'2016, XIIIth International Conference "Modern Problems of Radio Engineering, Telecommunications, and Computer Science" (February 23 – 26, 2016, Lviv-Slavsko, Ukraine). – Lviv: Publishing House of Lviv Polytechnic, 2016. – P.443–445.
5. The implementation of depersonalization algorithm of digital images. A. Zadereyko, N. Loginova, A. Troyanskiy, E. Trofimenko. 2nd International Conference on Advanced Information and Communication Technologies-2017 (AICT-2017), Lviv, Ukraine, July 4-7, 2017, p. 56 – 61.
6. Проблемные аспекты защиты информационного суверенитета государства и перспективы его защиты в Украине / Задерейко А.В., Троянский А.В., Чечельницкий В.Я. // Програмна інженерія журнал. - 2017. - № 2. - С. 10 – 13.
7. Algorithm of user's personal data protection against data leaks in Windows 10 OS / Olexander V. Zadereyko, Olena G. Trofymenko, Nataliia I. Loginova // Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. – 2019, vol.9, - p. 41 – 44.

8. A. Zadereyko, A. Troyanskiy, N. Loginova, E. Trofimenko. “The implementation of depersonalization algorithm of digital images”, in 2nd International Conference on Advanced Information and Communication Technologies (AICT), Lviv, 2017, pp. 56 – 61.
9. Задерейко О.В. Анализ утечек данных пользователей в мобильных приложениях / Кібербезпека в сучасному світі : матеріали ІІ Всеукраїнської науково-практичної конференції (м. Одеса, 20 листопада 2020 р.) / за ред. О. В. Дикого ; уклад.: Н.І. Логінова, В.Д. Бойко, М.О. Флюнт. – Одеса : Видавничий дім «Гельветика», 2020. – С. 108 - 114.
10. А.В. Задерейко. Защита от скрытого сбора персональных данных пользователей при веб-серфинге в Интернет / Кібербезпека в сучасному світі: актуальні виклики. Матеріали всеукраїнської науково-практичної конференції (м. Одеса, 29 листопада 2019 р.) / за ред. О.В. Дикого; уклад.: Я.І. Кузьма, Т.Ф. Стоянова, Ю.Ю. Пастернак, - Одеса: Видавничий дім "Гельветика". 2019, - С. 95 - 100.
11. Задерейко О.В., Трофименко О.Г., Логінова Н.І. Захист персональних даних в ОС Windows 10. Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаціиних системах. VII Міжнародна науково-практична конференція (8 - 10 листопада 2018 р.). Чернівецький національний університет імені Юрія Федьковича. м. Чернівці, Україна.
12. Сучасне кіберсередовище як театр бойових дій. Задерейко О.В., Логінова Н.І., Троянский О.В. // Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 17 листопада 2017 р. – Одеса : ОДУВС, 2017. С. 72–74.
13. Проблемні аспекти забезпечення конфіденційності цифрового медіаконтенту / Задерейко О.В. // Захист інформації і безпека інформаційних систем: матеріали VI Міжнар. наук. - 3-22 техн. конф. - Львів : Видавництво Львівської політехніки, 2017. – С. 148 – 149.
14. Основи комп’ютерної техніки: навч.-метод. посібник / О.Г. Трофименко, О.В. Задерейко, Н.І. Логінова. – Одеса, 2017. – 148 с.

15. Козловський, А. В. Комп'ютерна техніка та інформаційні технології [Текст] : навчальний посібник для студ. вищ. навч. закладів: рек. МОНУ / А. В. Козловський, Ю. М. Паночишин, Б. В. Погріщук. – 2-ге вид., стереотип. – К. : Знання, 2012. – 463 с.

Інформаційні ресурси

1. https://it.inf.od.ua – сайт кафедри інформаційних технологій, на якому розміщено робочі матеріали з курсу «Безпека персональної інформації в мережі Інтернет»
2. http://dspace.onua.edu.ua – eNUOLAIR – депозитарій (архів) НУ ОЮА

Додаток 1

Таблиця 1. Результати повного тестування для веб-браузерів **Mozilla FireFox и TOR**

Browser Characteristic	**bits of identifying information**	**one in *x* browsers have this value**	**value**	
			Mozilla FireFox	**TOR**
User Agent	5.2	36.8	Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0	Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
HTTP_ACCEPT Headers	1.89	3.7	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.5	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.5
Browser Plugin Details	0.92	1.89	undefined	undefined
Time Zone Offset	2.51	5.71	0	0
Time Zone	2.58	5.96	UTC	UTC
Screen Size and Color Depth	16.79	113175.5	1280x667x24	1000x600x24
System Fonts	6.27	76.94	Arial, Arial Black, Arial Narrow, Arial Rounded MT Bold, Arial Unicode MS, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century, Century Gothic, Century Schoolbook, Comic Sans MS, Consolas, Courier, Courier New, Georgia, Helvetica, Impact, Lucida Bright, Lucida Calligraphy, Lucida Console, Lucida Fax, Lucida Handwriting, Lucida Sans, Lucida Sans Typewriter, Lucida Sans Unicode, Microsoft Sans Serif, Monotype Corsiva, MS Gothic, MS Outlook, MS PGothic, MS Reference Sans Serif, MS Sans Serif, MS Serif, Palatino Linotype, Segoe Print, Segoe Script, Segoe UI, Segoe UI Light, Segoe UI Semibold, Segoe UI Symbol, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3 (via javascript)	Arial, Arial Black, Arial Narrow, Cambria Math, Courier, Courier New, Georgia, Helvetica, Lucida Console, MS Gothic, MS PGothic, MS Sans Serif, MS Serif, Segoe UI, Segoe UI Light, Segoe UI Semibold, Tahoma, Times, Times New Roman, Verdana (via javascript)
Are Cookies Enabled?	0.16	1.12	Yes	Yes
Limited supercookie test	1.07	2.1	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No, openDatabase: false, indexed db: true	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No, openDatabase: false, indexed db: true
Hash of canvas fingerprint	4.81	28.05	f7b57c6c925c4daf352807f8fd4331ca	randomized
Hash of WebGL fingerprint	13.4	10778.62	d9c1c3e0f54f0860149382f196a35eea	randomized

WebGL Vendor & Renderer	3.21	9.23	None	None
DNT Header Enabled?	1.0	2.0	True	False
Language	0.96	1.94	en-US	en-US
Platform	1.33	2.51	Win32	Win32
Touch Support	0.71	1.63	Max touchpoints: 0; TouchEvent supported: false onTouchStart supported: false	Max touchpoints: 0; TouchEvent supported: false onTouchStart supported: false
Ad Blocker Used	0.37	1.29	False	False
AudioContext fingerprint	3.56	11.76	not available	not available
CPU Class	0.15	1.11	N/A	N/A
Hardware Concurrency	2.33	5.02	2	2
Device Memory (GB)	0.76	1.69	N/A	N/A

Додаток 2

Таблиця 2. Порівняння наявності команд у веб-браузерах Mozilla FireFox і TOR

КОМАНДА	Mozilla FireFox	TOR
	(+ / -)	(+ / -)
Сервіс Pocket		
extensions.pocket.api", ""		
extensions.pocket.enabled", false		
extensions.pocket.site", ""		
extensions.pocket.oAuthConsumerKey", ""		
WebRTC		
media.peerconnection.enabled", false		
media.peerconnection.ice.default_address_only", true		
media.peerconnection.ice.no_host", true		
media.peerconnection.ice.relay_only", true		
media.peerconnection.ice.tcp", false		
media.peerconnection.identity.enabled", false		
media.peerconnection.turn.disable", true		
media.peerconnection.use_document_iceservers", false		
media.peerconnection.video.enabled", false		
media.peerconnection.default_iceservers", "[]"		
Геолокація		
geo.enabled",false		
geo.providerms-windows-location", false		
geo.wifi.uri", ""		
Звіти про стабільність і продуктивність		
datareporting.healthreport.service.enabled, false		
datareporting.healthreport.uploadEnabled, false		
Технологія Snippets		
browser.aboutHomeSnippets.updateUrl, ""		
Асинхронні запити аналітики		
beacon.enabled", false		
browser.send_pings", false		
browser.send_pings.require_same_host", false		
Метрики продуктивності		
dom.enable_performance", false		
dom.enable_performance_observer", false		
dom.enable_performance_navigation_timing", false		
browser.slowStartup.notificationDisabled", false		
network.predictor.enabled", false		
network.predictor.enable-hover-on-ssl", false		
network.prefetch-next", false		
network.http.speculative-parallel-limit", 0		
Інформація про встановлені доповнення		
extensions.getAddons.cache.enabled", false		
Доступ до давачів		

user_pref('device sensors enabled", false		
user_pref('device Sensors orientation.enabled", false		
user_pref('device sensors motion.enabled", false		
user_pref('device sensors proximity.enabled", false		
user_pref('device sensors ambientLight.enabled", false		
Ідентифікація веб-браузера		
dom.webaudio.enabled", false		
privacy.resistfingerprinting", true		
Передача інформації про мережеве з'єднання		
user_pref(dom.netinfo.enabled", false		
user_pref(dom.network.enabled", false		
Використання пристроїв і передача медіа		
dom.gamepad.enabled", false		
dom.gamepad.non_standard_events.enabled", false		
dom.imagecapture.enabled", false		
dom.presentation.discoverable", false		
dom.presentation.discovery.enabled", false		
dom.presentation.enabled", false		
dom.presentation.tcp_server.debug", false		
media.getusermedia.aec_enabled", false		
media.getusermedia.audiocapture.enabled", false		
media.getusermedia.browser.enabled", false		
media.getusermedia.noise_enabled", false		
media.getusermedia.screensharing.enabled", false		
media.navigator.enabled", false		
media.navigator.video.enabled", false		
media.navigator.permission.disabled", true		
media.video_stats.enabled", false		
dom.battery.enabled", false		
dom.vibrator.enabled", false		
dom.vr.require-gesture", false		
dom.vr.poseprediction.enabled", false		
dom.vr.openvr.enabled", false		
dom.vr.oculus.enabled", false		
dom.vr.oculus.invisible.enabled", false		
dom.vr.enabled", false		
dom.vr.test.enabled", false		
dom.vr.puppet.enabled", false		
dom.vr.osvr.enabled", false		
dom.vr.external.enabled", false		
dom.vr.autoactivate.enabled", false		
media.webspeech.synth.enabled", false		
media.webspeech.test.enable", false		
media.webspeech.synth.force_global_queue", false		
media.webspeech.recognition.force_enable", false		
media.webspeech.recognition.enable", false		
Телеметрія і відправка звітів розробникам		
toolkit.telemetry.archive.enabled", false		
toolkit.telemetry.bhrPing.enabled", false		
toolkit.telemetry.cachedClientID", ""		

toolkit.telemetry.firstShutdownPing.enabled", false		
toolkit.telemetry.hybridContent.enabled", false		
toolkit.telemetry.newProfilePing.enabled", false		
toolkit.telemetry.previousBuildID", ""		
toolkit.telemetry.reportingpolicy.firstRun", false		
toolkit.telemetry.server", ""		
toolkit.telemetry.server_owner", ""		
toolkit.telemetry.shutdownPingSender.enabled", false		
toolkit.telemetry.unified", false		
toolkit.telemetry.updatePing.enabled", false		
datareporting.healthreport.infoURL", ""		
datareporting.healthreport.uploadEnabled", false		
datareporting.policy.dataSubmissionEnabled", false		
datareporting.policy.firstRunURL", ""		
browser.tabs.crashReporting.sendReport", false		
browser.tabs.crashReporting.email", false		
browser.tabs.crashReporting.emailMe", false		
breakpad.reportURL", ""		
security.ssl.errorReporting.automatic", false		
toolkit.crashreporter.infoURL" , ""		
network.allow-experiments", false		
dom.ipc.plugins.reportCrashUR", false		
dom.ipc.plugins.flash.subprocess.crashreporter.enabled", false		
Стандартний пошук веб-браузера без відправки місця розташування		
user_pref(browser.searchgeoSpecificDefaults", false		
user_pref(browser.searchgeoSpecificDefaults.url", ""		
user_pref(browser.search.geoip.url", ""		
user_pref(browser.search.region", "US"		
user_pref(browser.search.suggest.enabled", false		
user_pref(browser.search.update", false		
push-повідомлення		
dom.push.enabled", false		
dom.push.connection.enabled", false		
dom.push.serverURL", ""		
Захист від витоків DNS		
network.dns.disablePrefetch", true		
network.dns.disableIPv6", true		
network.security.esni.enabled", true		
network.trr.mode", 2		
network.trr.uri", "https://cloudflare-dns.com/dns-query"		
Перенаправлення		
network.captive-portal-service.enabled", false		
network.captive-portal-service.maxInterval", 0		
captivedetect.canonicalURL", ""		
Передача даних на сервери Google		
browser.safebrowsing.allowOverride", false		
browser.safebrowsing.blockedURIs.enabled", false		
browser.safebrowsing.downloads.enabled", false		
browser.safebrowsing.downloads.remote.block_dangerous", false		
browser.safebrowsing.downloads.remote.block_dangerous_host", false		

browser.safebrowsing.downloads.remote.block_potentially_unwanted", false		
browser.safebrowsing.downloads.remote.block_uncommon", false		
browser.safebrowsing.downloads.remote.enabled", false		
browser.safebrowsing.malware.enabled", false		
browser.safebrowsing.phishing.enabled", false		
browser.safebrowsing.downloads.remote.url", ""		
browser.safebrowsing.provider.google.advisoryName", ""		
browser.safebrowsing.provider.google.advisoryURL", ""		
browser.safebrowsing.provider.google.reportMalwareMistakeURL", ""		
browser.safebrowsing.provider.google.reportPhishMistakeURL", ""		
browser.safebrowsing.provider.google.reportURL", ""		
browser.safebrowsing.provider.google.updateURL", ""		
browser.safebrowsing.provider.google4.advisoryName", ""		
browser.safebrowsing.provider.google4.advisoryURL", ""		
browser.safebrowsi ng.provider.google4.dataSharingURL", ""		
browser.safebrowsi ng.provider.google4.gethashURL", ""		
user pref ("browser.safebrowsing.provider.google4.reportMalwareMistakeURL", ""		
browser.safebrowsing.provider.google.gethashURL", ""		
Передача історії серфінгу в Google		
browser.safebrowsing.malware.enabled", false		
DRM		
browser.eme.ui.enabled", false		
media.eme.enabled", false		
media.gmp-eme-adobe.enabled", false		
Підключення до сторонніх серверів		
loop.enabled", false		
Пошукові підказки		
browser.search.suggest.enabled", false		
Захист від стеження з боку сайтів		
privacy.trackingprotection.enabled", false		
Відсилання статистики, пов'язаної з технологією Snippets		
browser.aboutHomeSnippets.updateUrl, ""		