

ІНФОРМАТИКА

Налаштування параметрів безпеки в середовищі браузера



За навчальною програмою 2017 року



Урок 7



Пригадайте

- ✓ Які можуть виникати загрози безпеці даних в Інтернеті;
- ✓ які засоби використовують для захисту даних і безпечної роботи на комп'ютері;
- ✓ як налаштувати параметри безпеки в середовищі браузера.

Пам'ятайте

Під час виконання практичних завдань пам'ятай про **правила безпеки** життєдіяльності при роботі з комп'ютером!



Інформаційна безпека базується на таких принципах

Інформаційна безпека

Доступність

Забезпечення доступу до загальнодоступних даних усім користувачам, захист цих даних від спотворення та блокування злоумисниками.

Конфіденційність

Забезпечення доступу до даних на основі розподілу прав доступу.

Цілісність

Захист даних від злоумисного або випадкового видалення чи спотворення.



Залежно від результату шкідливих дій, загрози інформаційній безпеці можна поділити на такі види:

отримання доступу до секретних або конфіденційних даних;

порушення або повне припинення роботи комп'ютерної інформаційної системи;

отримання доступу до керування роботою комп'ютерної інформаційної системи.



Розглядають й інші класифікації загроз:

За метою

За місцем виникнення

За походженням

**зловмисні,
випадкові**

**зовнішні,
внутрішні**

**природні,
техногенні,
зумовлені
людиною**






Перелік основних загроз інформаційній безпеці

 *Знищення та спотворення даних*

 *Отримання доступу до секретних і конфіденційних даних*

 *Пошкодження пристроїв інформаційної системи*

 *Отримання прав на виконання дій, що передбачені тільки для окремих керівних осіб*

 *Отримання доступу до здійснення фінансових операцій замість власників рахунків*

 *Отримання повного доступу до керування інформаційною системою*



За **рівнем небезпечності дій** шкідливі програми розподіляють на:

Безпечні

проявляються відео- та звуковими ефектами, не змінюють файлову систему, не ушкоджують файли й не виконують шпигунських дій;

Небезпечні

призводять до перебоїв у роботі комп'ютерної системи: зменшують розмір доступної оперативної пам'яті, перезавантажують комп'ютер тощо;

Дуже небезпечні

знищують дані з постійної та зовнішньої пам'яті, виконують шпигунські дії тощо.



За **принципами розповсюдження та функціонування** шкідливі програми розподіляють на:

Комп'ютерні віруси

**Хробаки
(черв'яки)
комп'ютерних мереж**

Троянські програми

**Рекламні модулі, або
Adware**

Інші

**ДИСКОВІ
(завантажувальні)
віруси**

**файлові
віруси**



Руткіти

Експлойти

Бекдори

Завантажувачі

Засоби боротьби зі шкідливими програмами

Розділ 4
§ 4.1



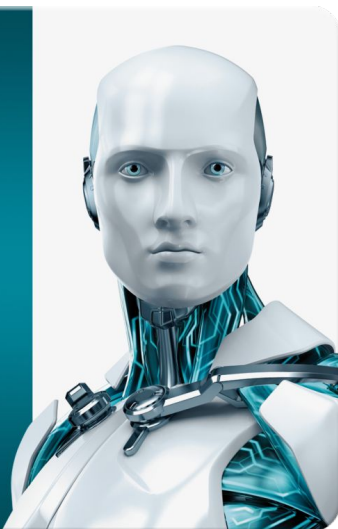
найпопулярнішими комерційними антивірусними програми є:

ESET NOD 32

*Kaspersky
Internet Security*

BitDefender тощо

eset
NOD32
ANTIVIRUS



Засоби боротьби зі шкідливими програмами

Розділ 4
§ 4.1



**Майже не поступаються їм за ефективністю
безкоштовні програми:**

*Avast Free
Antivirus*

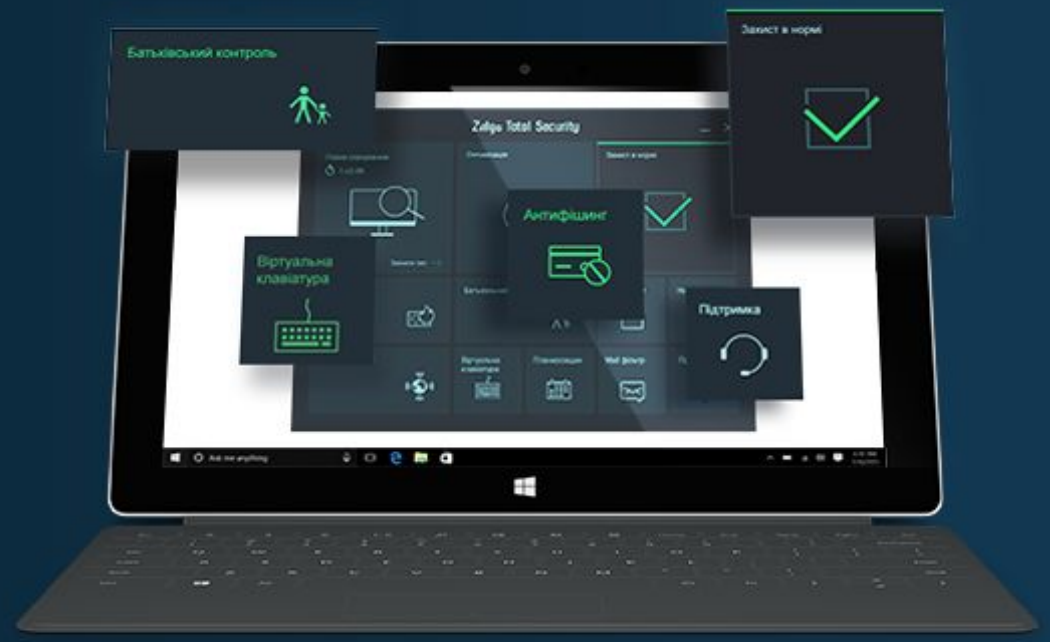
*360 Total
Security*

*Avira Free
Antivirus*

*Panda Free
Antivirus та
інші*



Наприклад, Українська антивірусна лабораторія пропонує кілька варіантів свого антивірусу *Zillya!*



Zillya! Total Security

Максимальний захист від існуючих кіберзагроз!



Менеджер процесів



Батьківський контроль



Приватність даних



Менеджер автозапуску

Покращено існуючий функціонал



Антифішинг



Брандмауер



Антиспам



Комплексний захист



Серед основних загроз використання комп'ютерних мереж для користувачів, особливо підлітків, виділяють:

□ комунікаційні ризики — ризики, що пов'язані зі спілкуванням у мережі та використанням онлайн-ігор:

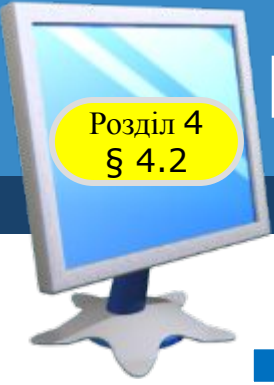
- **булінг** — залякування, приниження, цькування, переслідування, компрометація людей з використанням особистих або підробних матеріалів, розміщених в Інтернеті, надсилання повідомлень з використанням різних сервісів. Майже кожна п'ята дитина в Європі, що використовує Інтернет, стала жертвою булінга;



Продовження...

- **компрометувати** — виставляти в негарному вигляді, шкодити добрій славі;
- **кібер-грумінг** — входження в довіру людини для використання її в сексуальних цілях;
- **надмірне захоплення іграми в мережі** — може призвести до втрати реальності, нерозуміння та несприйняття норм і правил людського співіснування, комп'ютерної залежності;





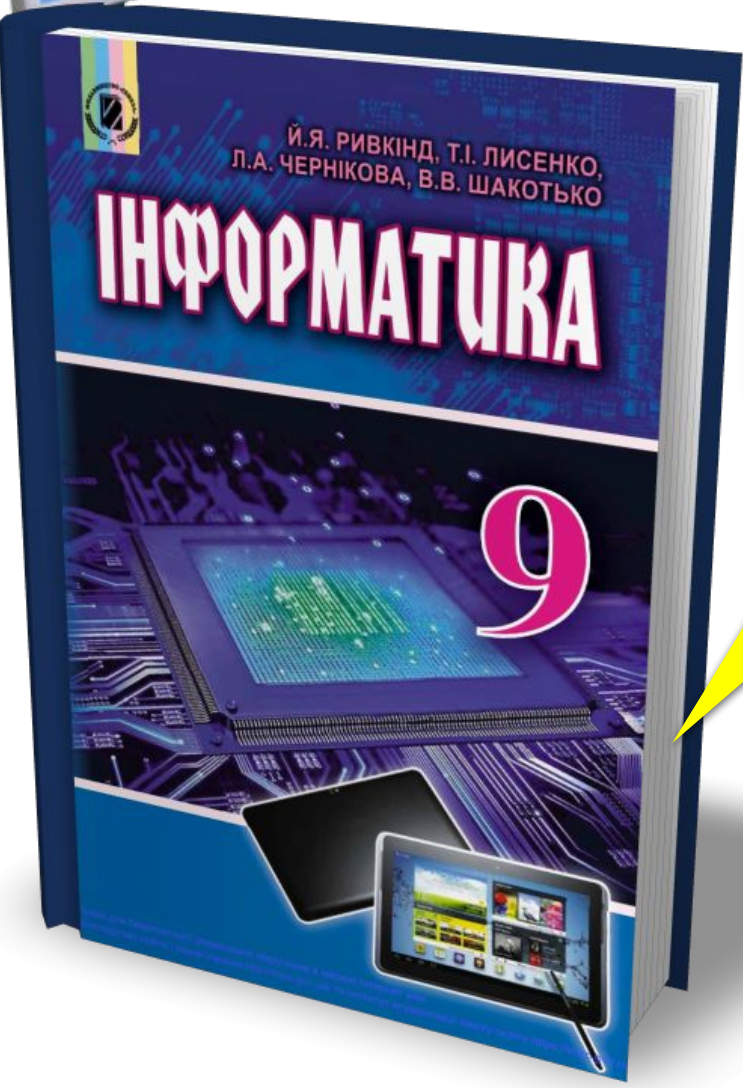
Практична робота

***Налаштовування
параметрів безпеки в
середовищі браузера***

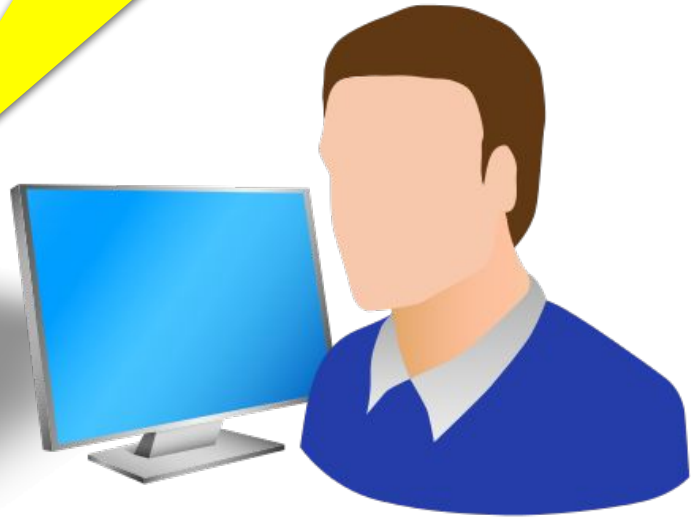


Працюємо за комп'ютером

Розділ 9
§ 9.3



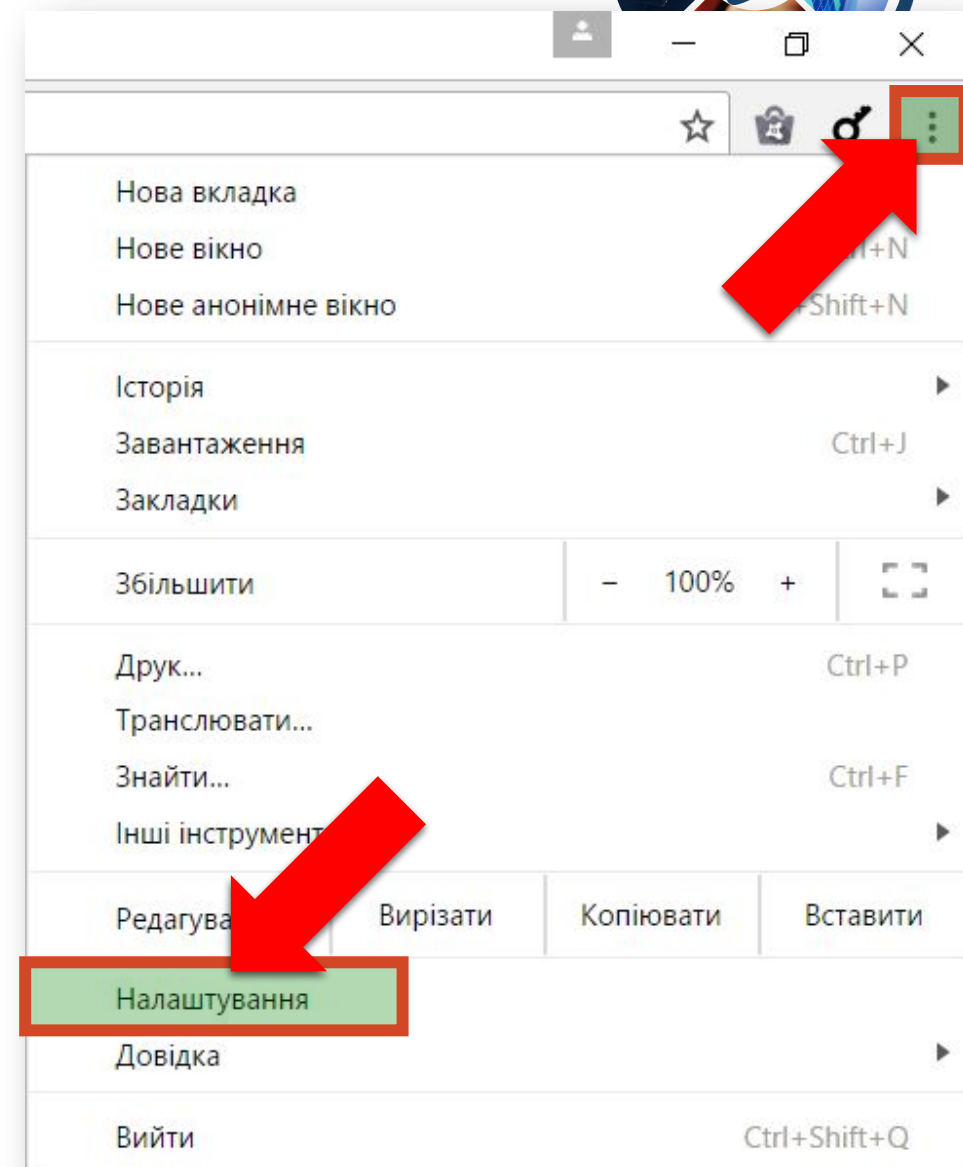
**Сторінка
131**





*Перш за все слід переглянути та за потреби змінити налаштування браузера розділу меню, у якому зібрано властивості, пов'язані з безпекою. Наприклад, у браузері **Google Chrome** для їх перегляду треба виконати*

Налаштування та керування Google Chrome ⇒ Налаштування.





*Вибрати засоби браузера, призначені для гарантування безпеки, на сторінці налаштувань вибрати посилання **Показати розширені налаштування.***

Користувачі

 **Особа 1 (поточний)**

- Увімкнути гостьовий режим
- Дозволити всім додавати користувачів у Chrome

Додати користувача...

Редагувати...

Видалити...

Імпорт закладок і налаштувань...

Веб-переглядач за умовчанням

Зробити Google Chrome веб-переглядачем за промовчанням

Google Chrome не є вашим переглядачем за умовчанням.

Показати розширені налаштування...



Відобразиться більш повний список налаштувань браузера, серед яких у групі **Конфіденційність слід перевірити, чи встановлено позначку прапорця **Захистіть себе і свій пристрій від небезпечних сайтів**.**

Розширення

Налаштування

Про Google Chrome

Конфіденційність

Налаштування вмісту... Очистити дані веб-перегляду...

Google Chrome може використовувати веб-послуги для покращення умов перегляду. За бажанням ці служби можна вимкнути. [Докладніше](#)

- Використовувати веб-послугу для виправлення помилок навігації
- Використовувати підказки для завершення пошукових запитів і URL-адрес, введених в адресний рядок
- Користуватися службою передбачення, щоб сторінки завантажувалися швидше
- Автоматично повідомляти Google деталі щодо можливих порушень безпеки
- Захистіть себе та свій пристрій від небезпечних сайтів**
- Використовувати веб-послугу для виправлення помилок правопису

Практичне завдання

Розділ 4
§ 4.2



Для подальших налаштувань безпеки потрібно вибрати кнопку *Налаштування вмісту*.

The screenshot shows the Google Chrome settings interface. The browser tabs at the top include 'Google' and 'Налаштування'. The address bar shows 'chrome://settings'. On the left sidebar, 'Налаштування' is selected. The main content area is titled 'Налаштування' and 'Конфіденційність'. A red arrow points to the 'Налаштування вмісту...' button, which is highlighted with a red box. To its right is the 'Очистити дані веб-перегляду...' button. Below these buttons, there is a paragraph of text and two checked checkboxes.

Chrome Налаштування Пошук налаштувань

Розширення

Налаштування **Налаштування вмісту...** Очистити дані веб-перегляду...

Про Google Chrome

Конфіденційність

Google Chrome може використовувати веб-послуги для покращення умов перегляду. За бажанням ці служби можна вимкнути. [Докладніше](#)

- Використовувати веб-послугу для виправлення помилок навігації
- Використовувати підказки для завершення пошукових запитів і URL-адрес, введених в адресний рядок



Спам — це розсилання повідомлень, як правило, рекламного характеру великій кількості користувачів.

Ці повідомлення надсилаються користувачам без їхньої згоди на це. Більшість спаму йде через електронну пошту, тому часто поштові сервери мають у своєму складі модуль захисту від спаму, який відстежує і накопичує відомості про адреси, з яких ідуть спамові розсилки, та направляє такі листи у спеціальну папку — **Спам**.

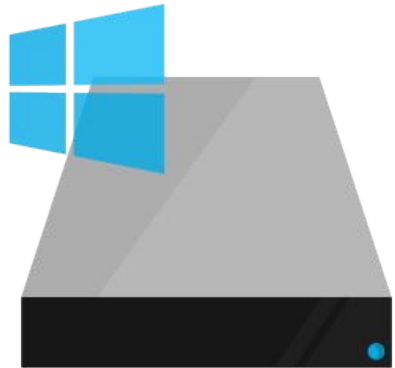




Зазвичай жорсткий диск ділять на кілька дисків **C, **D** і так далі.**

На диску **C**

встановлюють операційну систему і програмне забезпечення



На решті дисків

зберігають інші дані





Резервне копіювання завжди проводять на інші носії:

DVD-диск



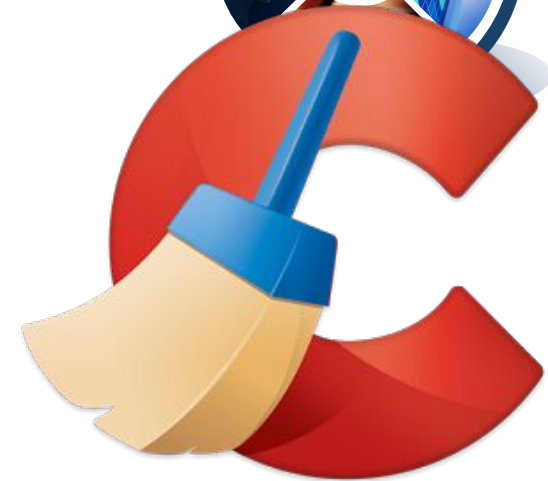
Флеш-накопичувач



Мережеві ресурси



Відмінні від тих, з яких копіюють. Неможна розміщувати резервну копію файлів на тому самому диску або диску, де встановлена операційна система.



Популярною програмою для безпечного видалення й очистки комп'ютера від невживаних і тимчасових файлів є **CCleaner (piriform.com/ccleaner).**

Програма має:

Базову безкоштовну версію

**Платні версії з додатковими
МОЖЛИВОСТЯМИ**



CCleaner
FREE

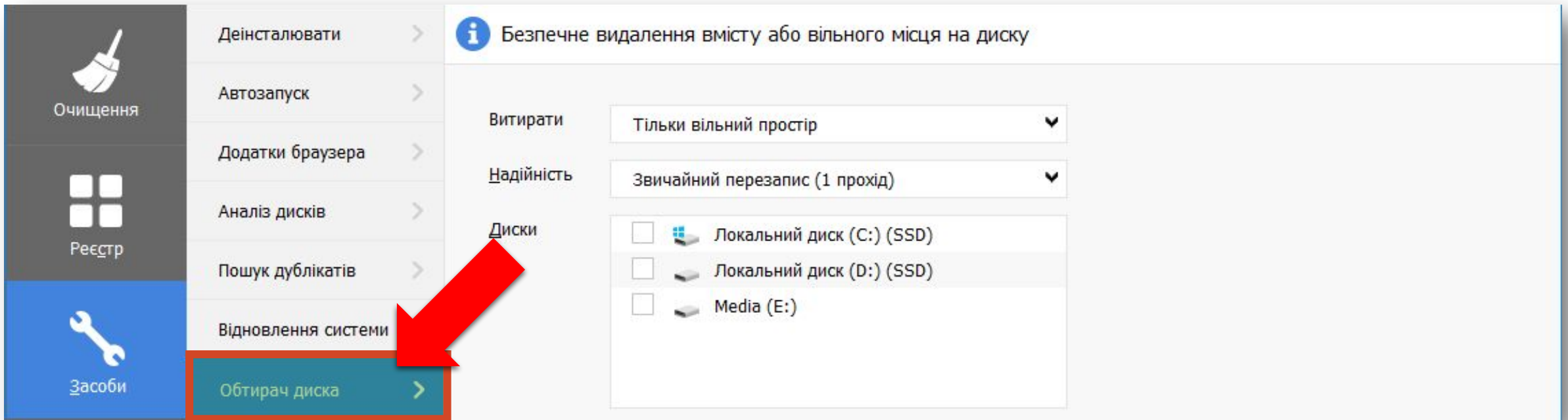


CCleaner
PROFESSIONAL



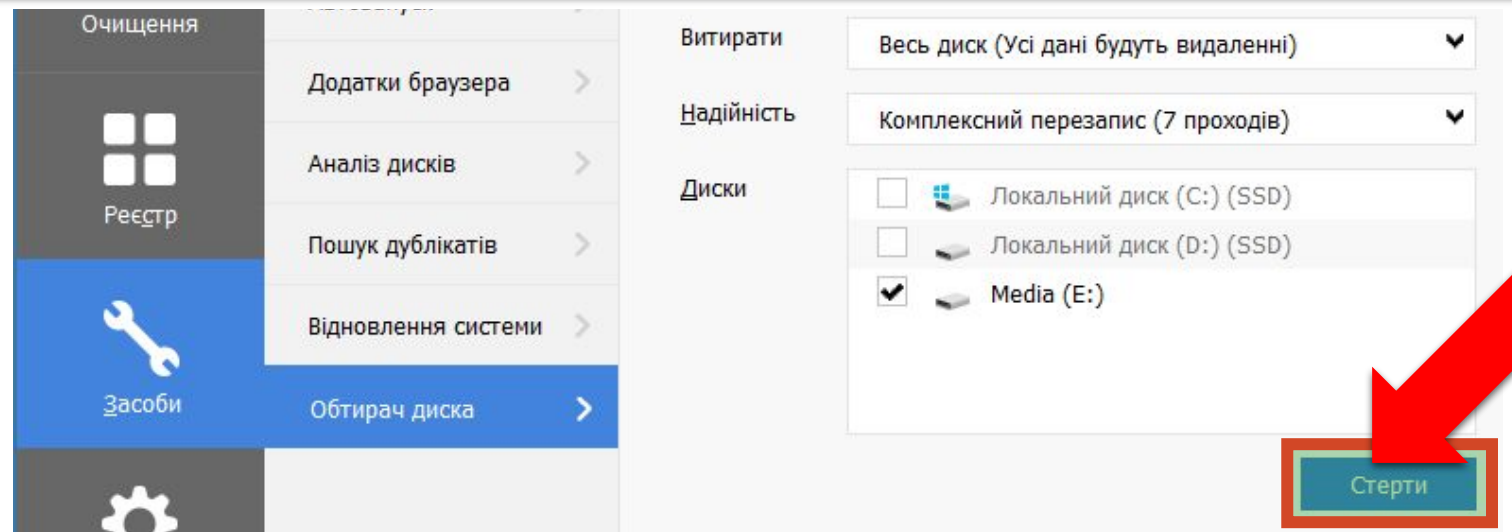
Для повного видалення даних з певного диска у програмі **CCleaner Free** потрібно:

1. Вибрати кнопку **Засоби** 
2. Вибрати кнопку **Обтирач диска.**



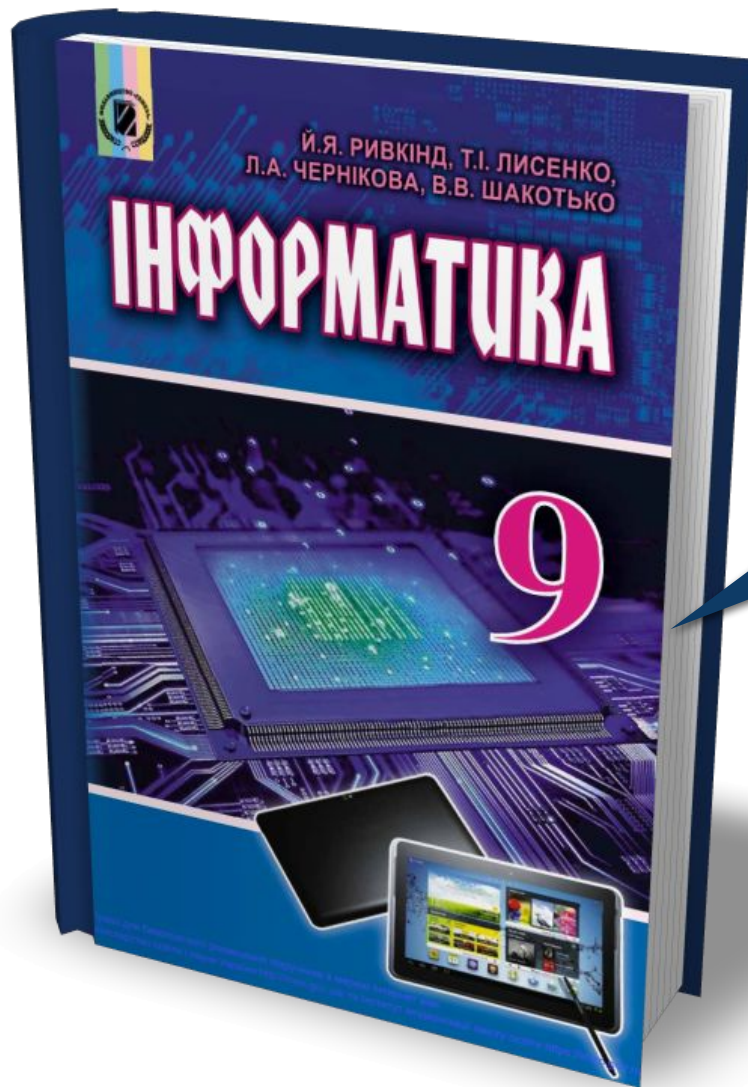


3. Вибрати у списку **Диски** носій даних для безпечного видалення.
4. Установити у списку **Витирати** область для безпечного видалення даних — наприклад **Увесь диск**.
5. Вибрати у списку **Надійність** режим видалення даних, наприклад **Комплексний перезапис (7 проходів)**.
6. Вибрати кнопку **Стерти**.



Домашнє завдання

Розділ 9
§ 9.3



Проаналізувати
§ 4.2, ст. 131

ІНФОРМАТИКА

Дякую за увагу!



За навчальною програмою 2017 року

