ІНФОРМАТИКА

Налаштовування 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	Конфіденційність	Цілісність
Забезпечення доступу до загальнодоступних даних усім користувачам, захист цих даних від спотворення та блокування зловмисниками.	Забезпечення доступу до даних на основі розподілу прав доступу.	Захист даних від зловмисного або випадкового видалення чи спотворення.

Розділ 4
§ 4.1

Класифікація загроз інформаційній безпеці

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.

Розділ 4
§ 4.1

Класифікація загроз інформаційній безпеці

Розглядають й інші класифікації загроз:

За метою	*За місцем виникнення*	*За походженням*
зловмисні, випадкові	*зовнішні, внутрішні*	*природні, техногенні, зумовлені людиною*

Розділ 4
§ 4.1

Класифікація загроз інформаційній безпеці

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

Розділ 4
§ 4.1

Шкідливі програми, їх види та принципи дії

За рівнем небезпечності дій шкідливі програми розподіляють на:

Безпечні	Небезпечні	Дуже небезпечні
проявляються відео- та звуковими ефектами, не змінюють файлову систему, не ушкоджують файли й не виконують шпигунських дій;	призводять до перебоїв у роботі комп'ютерної системи: зменшують розмір доступної оперативної пам'яті, перезавантажують комп'ютер тощо;	знищують дані з постійної та зовнішньої пам'яті, виконують шпигунські дії тощо.

Розділ 4
§ 4.1

Шкідливі програми, їх види та принципи дії

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

- **Комп'ютерні віруси**
  - дискові (завантажувальні) віруси
  - файлові віруси
- **Хробаки (черв'яки) комп'ютерних мереж**
- **Троянські програми**
- **Рекламні модулі, або Adware**
- **Інші**
  - Руткіти
  - Експлойти
  - Бекдори
  - Завантажувачі

Розділ 4
§ 4.1

Засоби боротьби зі шкідливими програмами

найпопулярнішими комерційними антивірусними програми є:

ESET NOD 32	Kaspersky Internet Security	BitDefender тощо

Розділ 4
§ 4.1

Засоби боротьби зі шкідливими програмами

Майже не поступаються їм за ефективністю безкоштовні програми:

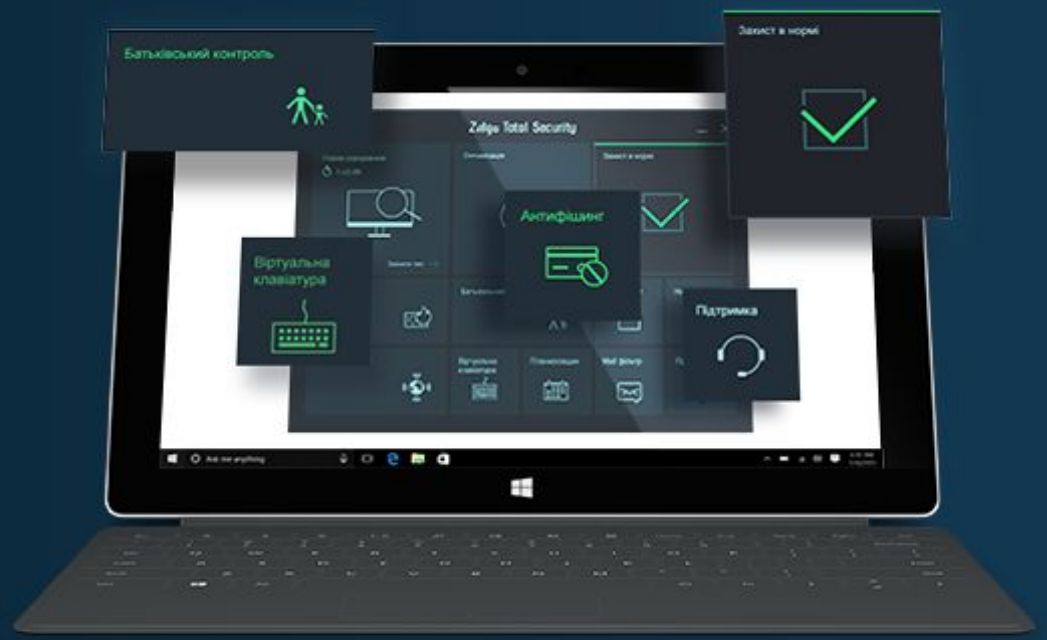
Avast Free Antivirus	***360 Total Security***	***Avira Free Antivirus***	***Panda Free Antivirus та інші***

Розділ 4
§ 4.1

Засоби боротьби зі шкідливими програмами

9

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

Розділ 4
§ 4.2

Загрози, що виникають під час роботи в інтернеті

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;***

Розділ 4
§ 4.2

Загрози, що виникають під час роботи в інтернеті

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;*

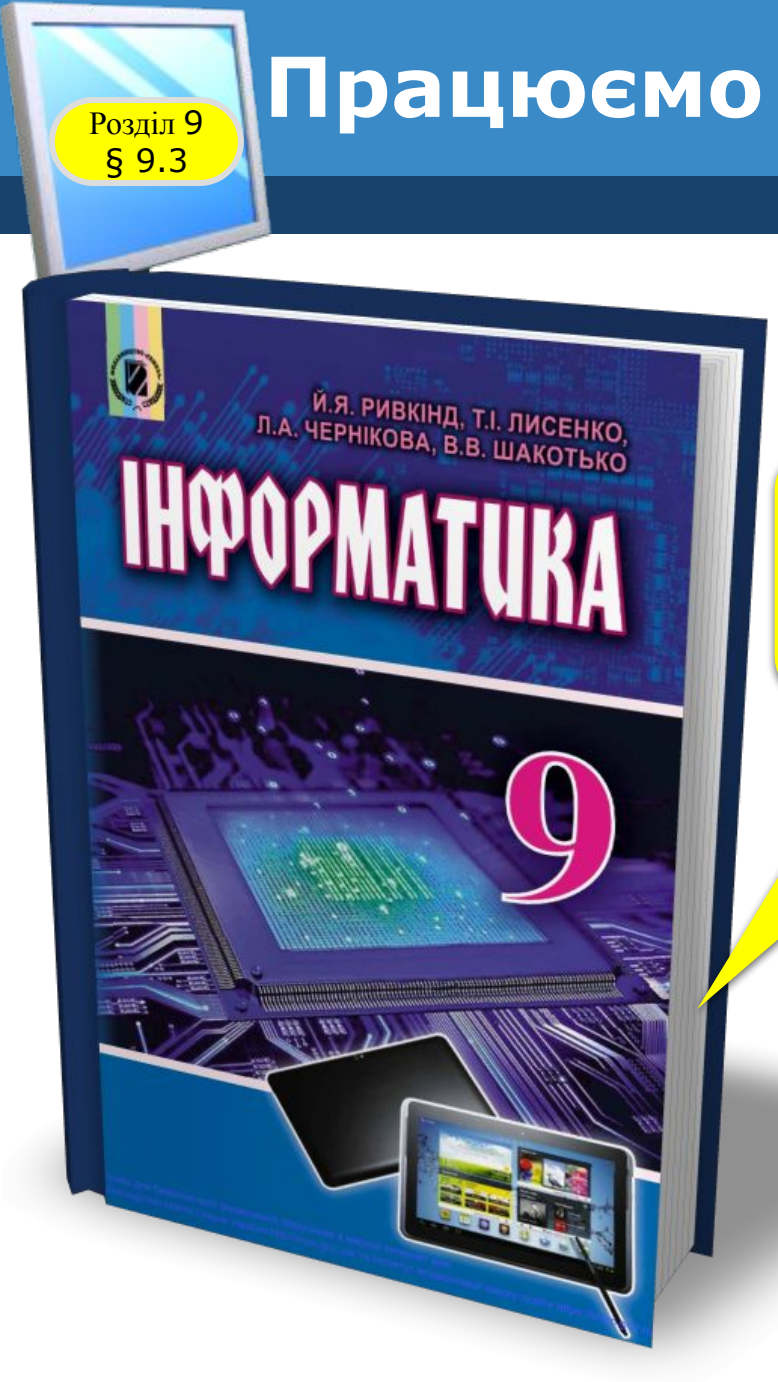
Працюємо за комп’ютером

Практична робота

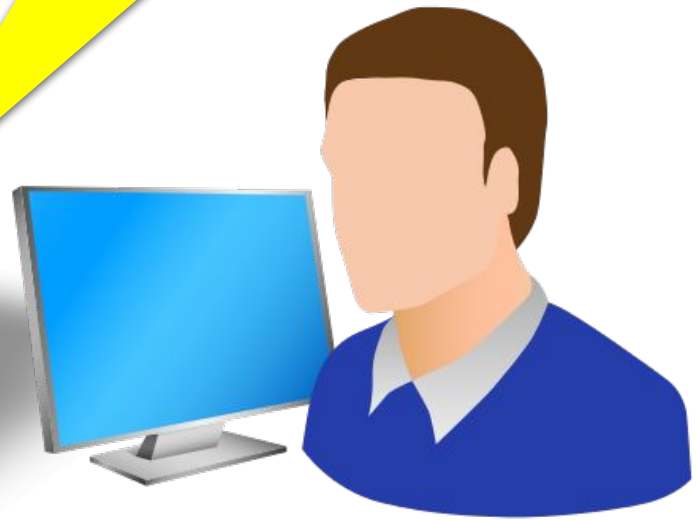
Налаштовування параметрів безпеки в середовищі браузера

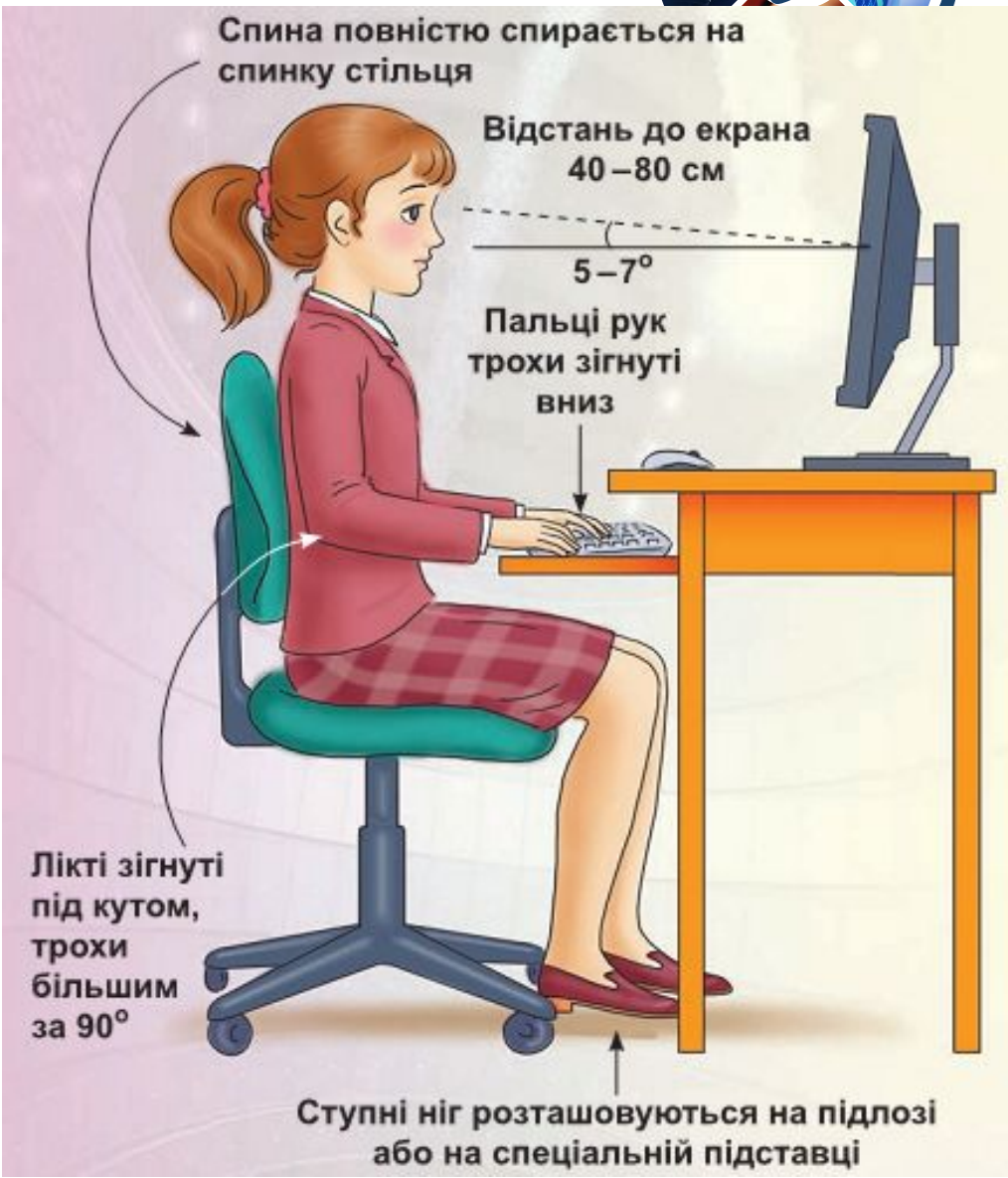
Розділ 9
§ 9.3

Працюємо за комп’ютером



Сторінка 131



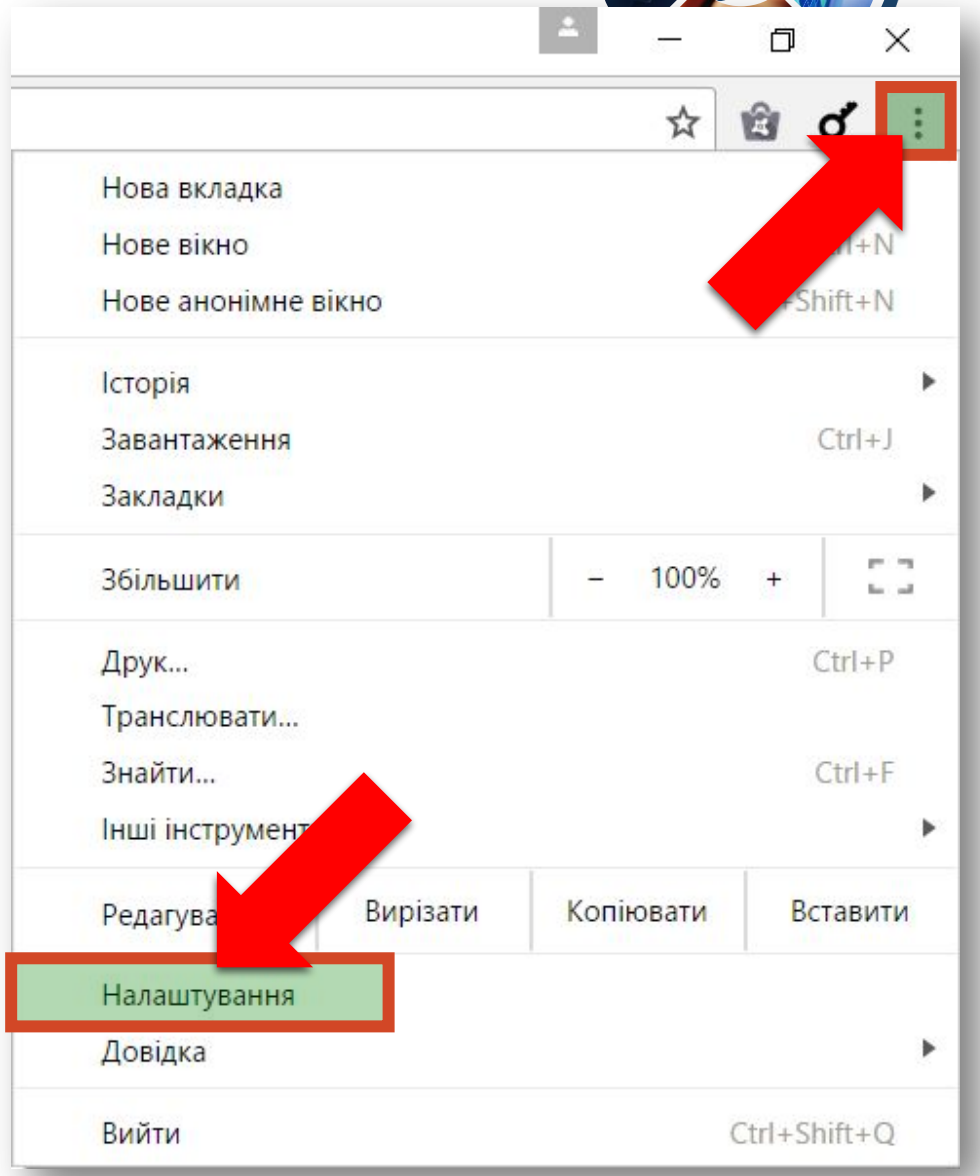


Розділ 4
§ 4.2

Засоби браузера, призначені для гарантування безпеки

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.

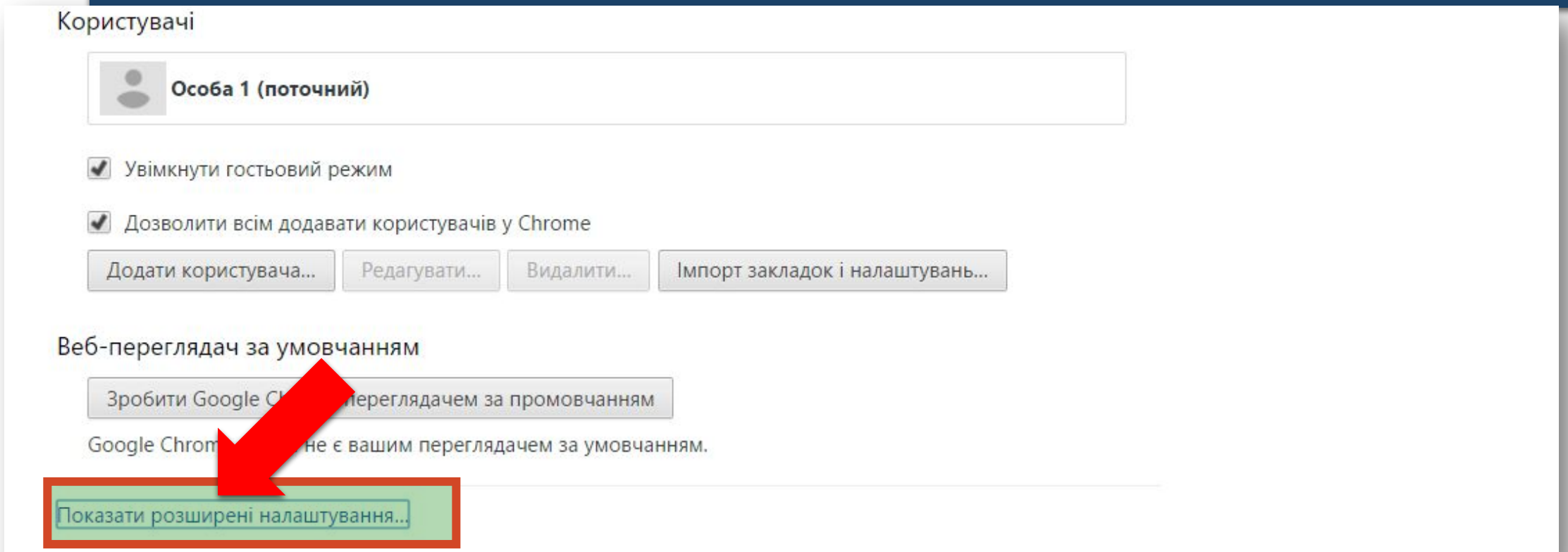


Розділ 4
§ 4.2

Практичне завдання

Вибрати засоби браузера, призначені для гарантування безпеки,

на сторінці налаштувань вибрати посилання Показати розширені налаштування.

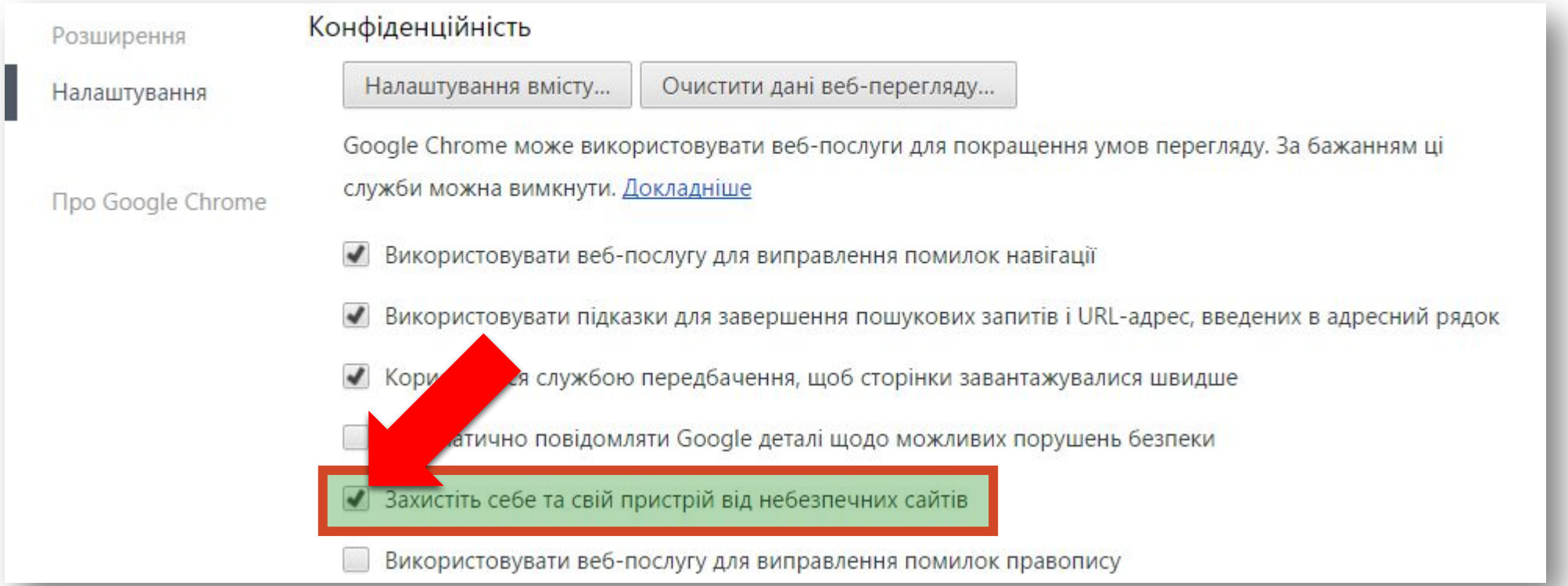


Розділ 4
§ 4.2

Практичне завдання

9

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.

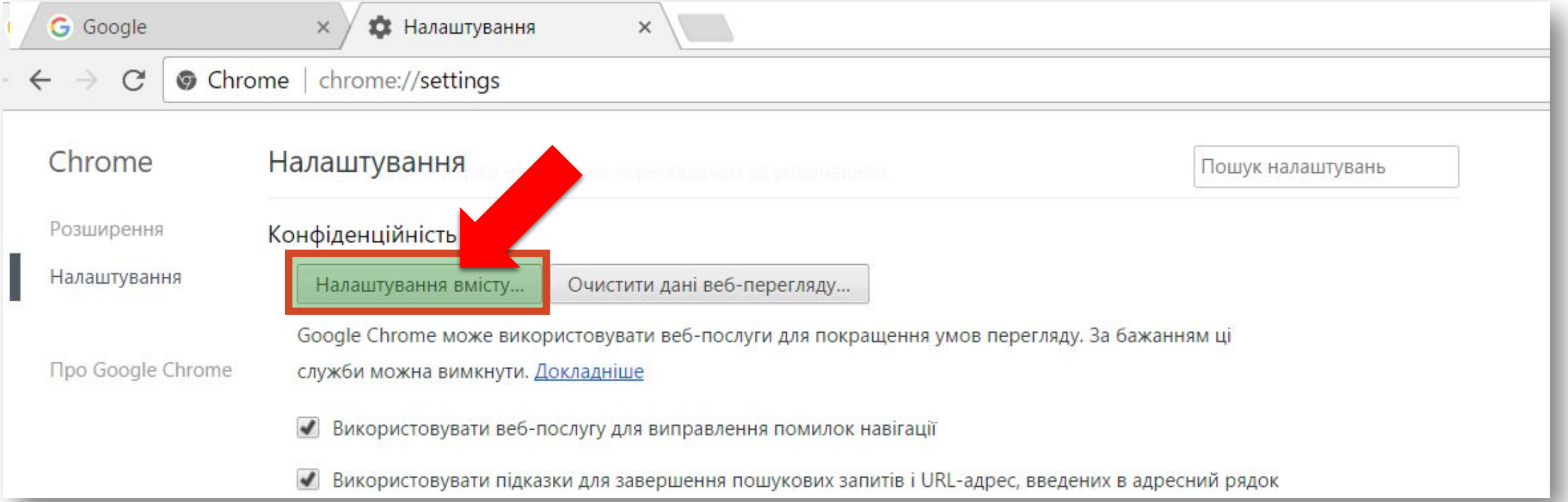


Розділ 4
§ 4.2

Практичне завдання

9

Для подальших налаштувань безпеки потрібно вибрати кнопку Налаштування вмісту.



Розділ 4
§ 4.2

Захист від спаму

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****.*

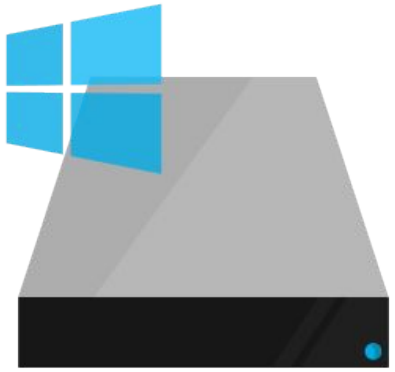
Розділ 4
§ 4.2

Безпечне зберігання даних. Резервне копіювання та відновлення даних

9

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

На диску С	На решті дисків
встановлюють операційну систему і програмне забезпечення	зберігають інші дані



Розділ 4
§ 4.2

Безпечне зберігання даних. Резервне копіювання та відновлення даних

9

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.

Розділ 4
§ 4.2

Безпечне видалення даних

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

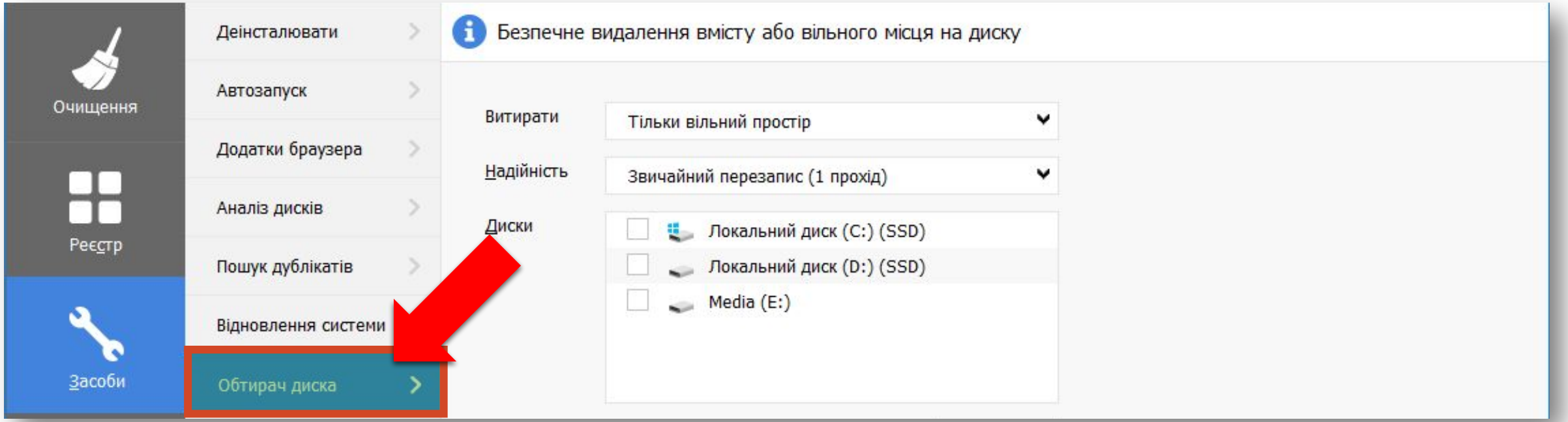
CCleaner
PROFESSIONAL

Розділ 4
§ 4.2

Безпечне видалення даних

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

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



Розділ 4
§ 4.2

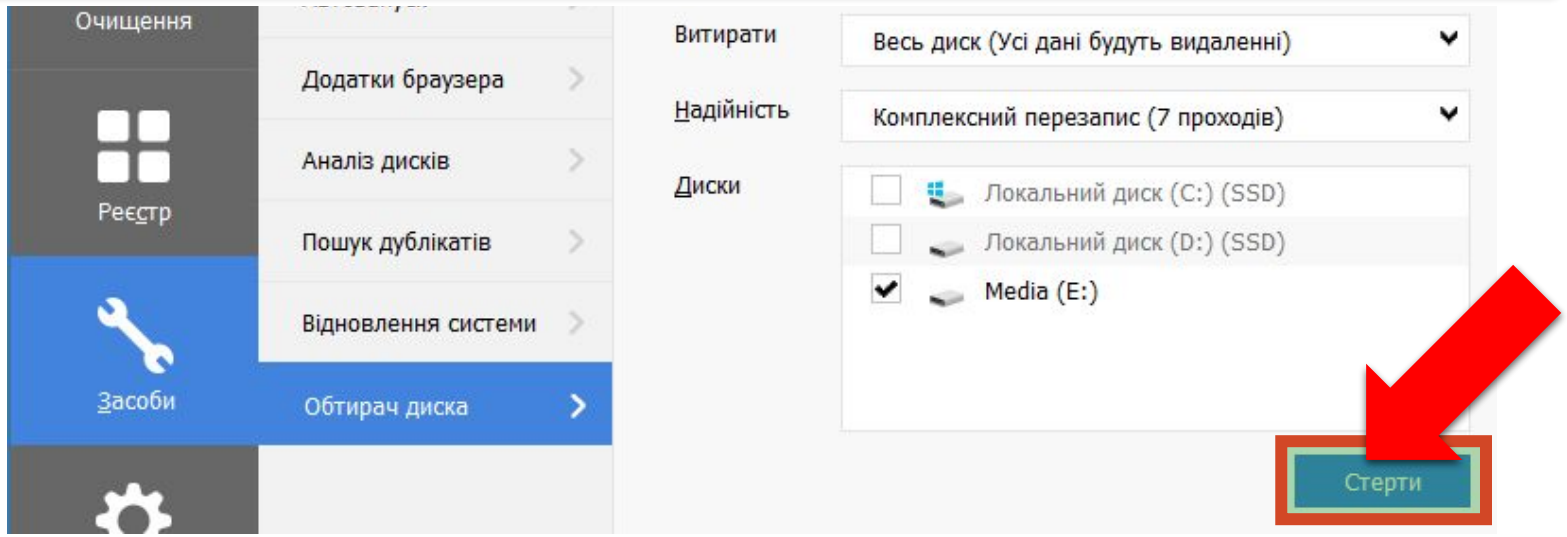
Безпечне видалення даних

3. Вибрати у списку **Диски** носій даних для безпечного видалення.

4. Установити у списку **Витирати** область для безпечного видалення даних — напкрилкад **Увесь диск**.

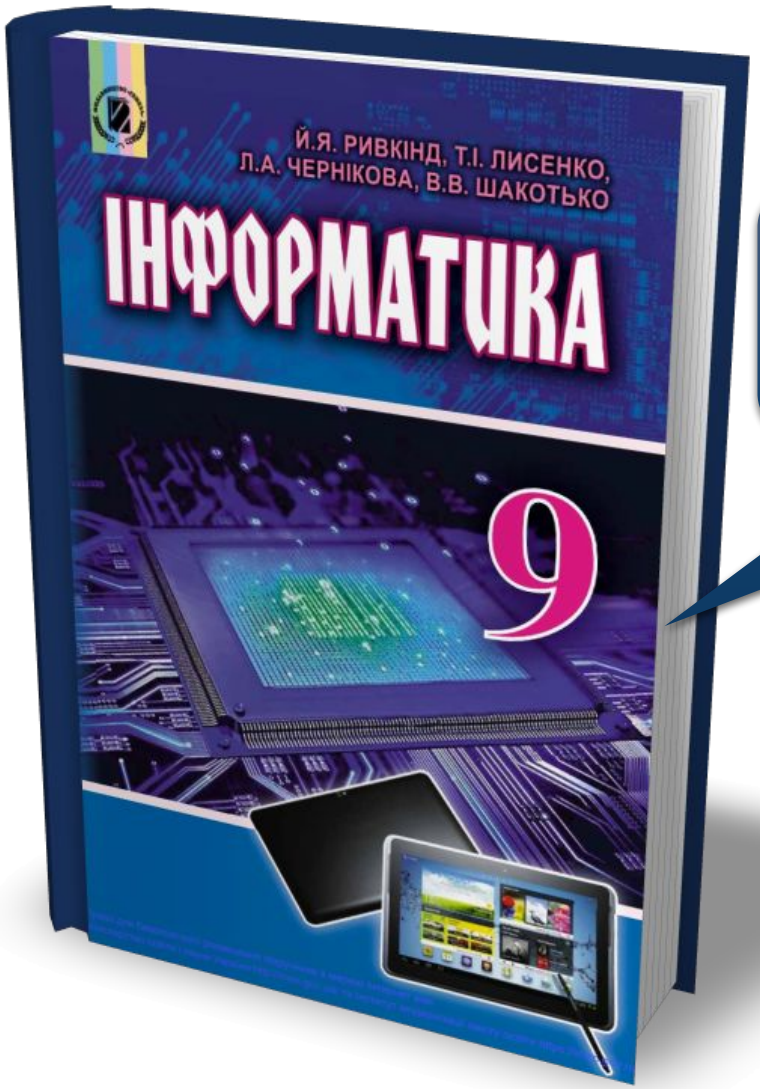
5. Вибрати у списку **Надійність** режим видалення даних, наприклад **Комплексний перезапис** (7 проходів).

6. Вибрати кнопку **Стерти**.



Розділ 9
§ 9.3

Домашнє завдання



Проаналізувати
§ 4.2, ст. 131

Дякую за увагу!

За навчальною програмою 2017 року