O&O software

O&O SafeErase



Зміст

1 Вступ 4

2 Початок роботи 6

2.1 Огляд функцій 6

2.2 Системні вимоги 8

2.3 Інсталяція й активація 10

2.4 Стирання першого файлу 12

2.5 Інтерфейс користувача 13

3 Основні поняття 15

3.1 Як працює безпечне стирання 15

3.2 Методи стирання та SSD 17

3.3 Звіти та акти стирання 19

4 Стирання даних 20

4.1 Стирання файлів і папок 20

4.2 Безпечне очищення кошика 22

4.3 Очищення вільного місця 23

4.4 Стирання слідів роботи браузерів і Windows 25

4.5 Збереження файлів cookie вибраних вебсайтів 28

4.6 Стирання дисків і розділів 29

4.7 Стирання з Провідника 31

4.8 Відстеження та скасування стирання 32

5 Стерти весь вміст комп'ютера 34

5.1 Налаштування й запуск режиму «Фортеця» 34

5.2 Стирання всього ПК 36

5.3 Збереження журналів після стирання ПК 38

6 Звіти та сертифікати стирання 40

6.1 Керування звітами 40

6.2 Перевірка акта стирання 42

7 Параметри 44

8 Довідник 49

8.1 Командний рядок 49
8.2 Глосарій 60
9 Усунення несправностей 63
10 Поширені запитання 66
11 Що нового у версії 22 68
12 Підтримка та інші продукти O&O 70

Вступ

O&O SafeErase стирає дані без можливості відновлення: окремі файли й папки, сліди роботи браузерів і Windows, вільне місце, цілі диски та, у режимі «Фортеця», весь ПК разом із Windows. Результат документується у звітах із підписаним актом стирання.

Звичайне видалення файлу у Windows чи очищення кошика не видаляє його вміст, і програми відновлення часто можуть його повернути. Це особливо важливо перед продажем, поверненням чи утилізацією ПК або диска, а також під час щоденної роботи з конфіденційними документами. Докладніше див. у розділі Як працює безпечне стирання.

> **Стерті дані неможливо відновити**
>
> O&O SafeErase перезаписує дані без можливості відновлення. Перш ніж запускати стирання, створіть резервну копію всього потрібного на іншому диску.

З чого почати

Завдання	Розділ посібника
Випробувати O&O SafeErase на тестовому файлі	Стирання першого файлу
Стерти конфіденційні файли або папки	Стирання файлів і папок
Прибрати залишки раніше видалених файлів	Очищення вільного місця
Очистити журнал браузера, файли cookie й тимчасові файли	Стирання слідів роботи браузерів і Windows
Повністю стерти USB-накопичувач або другий диск	Стирання дисків і розділів
Підготувати ПК до продажу чи утилізації	Стирання всього ПК
Підтвердити результат стирання	Перевірка акта стирання
Стирати дані зі сценаріїв	Командний рядок

Ліцензія

O&O SafeErase — комерційна програма. Нею можна користуватися протягом пробного періоду, а надалі потрібна чинна ліцензія. У пробній версії недоступні стирання дисків і розділів та режим «Фортеця». Див. Інсталяція й активація.

Про цю довідку

Ця довідка описує O&O SafeErase 22. Знімки екрана ілюструють інтерфейс програми. Назви кнопок і параметрів виділено **жирним шрифтом** відповідно до їхніх назв у програмі.

Огляд функцій

O&O SafeErase перезаписує дані так, що програми відновлення не можуть їх повернути. На цій сторінці наведено огляд функцій і редакцій.

Функції

Функція	Призначення	Докладніше
Файли й папки	Стирає вибрані файли й папки.	Стирання файлів і папок
Вільне місце	Перезаписує залишки файлів, видалених звичайним способом, зокрема залишки кластерів і записи MFT. Наявні файли зберігаються.	Очищення вільного місця
Сліди роботи браузерів і Windows	Стирає історію, файли cookie, кеш, паролі, тимчасові файли, ескізи й інші сліди. Вибрані файли cookie можна зберегти.	Стирання слідів роботи браузерів і Windows
Диски й розділи	Стирає цілі диски чи розділи, після чого за потреби виконує ініціалізацію й форматування.	Стирання дисків і розділів
Увесь ПК	Стирає Windows та всі внутрішні диски в режимі «Фортеця» без окремого завантажувального носія.	Стирання всього ПК
Методи стирання	Шість методів — від одноразового перезапису випадковими даними відповідно до NIST 800-88 Clear / BSI CON.6 до методу Гутмана, а також SolidErase для SSD.	Методи стирання та SSD
Звіти та акти стирання	Документує кожне стирання за допомогою підписаних актів, необов’язкових позначок часу й ланцюжка актів.	Звіти та акти стирання
Рекомендації	На початковій сторінці показано час останнього стирання слідів роботи й рекомендацію щодо повторного стирання.	Інтерфейс користувача
Провідник	Стирає файли, вільне місце й вміст кошика з контекстного меню.	Стирання з Провідника
Командний рядок	Стирає дані зі сценаріїв і запланованих завдань та перевіряє акти стирання.	Командний рядок

Редакції

Редакція	Для яких систем	Відмінність
Professional Edition	ПК з Windows 10 і Windows 11	Стирає один накопичувач за раз. Не працює у Windows Server.
Server Edition	Сервери та ПК	Також працює у Windows Server. Одночасно стирає кілька накопичувачів або вільне місце на кількох накопичувачах.

Набір функцій в обох редакціях однаковий. Див. Системні вимоги.

Пробна версія

У пробній версії можна стирати файли, папки й сліди роботи та очищати вільне місце. Для стирання дисків і розділів та використання режиму «Фортеця» зі стиранням усього ПК потрібна ліцензія.

Системні вимоги

O&O SafeErase 22 працює в 64-розрядній Windows. Інші потрібні компоненти, зокрема середовище виконання .NET, установлюються разом із програмою.

Операційна система

Редакція	Підтримувані версії Windows
Professional Edition	Windows 10 і Windows 11, 64-розрядні (x64)
Server Edition	Windows 10 і Windows 11, 64-розрядні (x64), а також Windows Server 2016, 2019 і 2022. Інсталяції Server Core не підтримуються.

Professional Edition не можна встановити чи запустити у Windows Server. 32-розрядна Windows і Windows на ARM не підтримуються.

Права доступу

- Для інсталяції O&O SafeErase потрібні права адміністратора.
- Для очищення вільного місця, стирання дисків і розділів, налаштування режиму «Фортеця» та зміни інтеграції з кошиком потрібні права адміністратора. За потреби програма пропонує команду **Перезапустити від імені адміністратора**.

Режим «Фортеця»

Режим «Фортеця», потрібний для стирання системного диска й усього ПК, працює в середовищі відновлення Windows (Windows RE). Якщо Windows RE вимкнено або воно відсутнє, програма налаштування може відновити його. Якщо системний диск захищено BitLocker, підготуйте ключ відновлення.

Браузери

O&O SafeErase очищає дані наведених браузерів починаючи із зазначених версій, включно з новішими:

Браузер	Починаючи з версії
Google Chrome	115
Microsoft Edge	115
Mozilla Firefox	115
Brave	115
Opera, Opera GX	101
Vivaldi	6

Для Brave, Opera, Opera GX і Vivaldi підтримуються лише стабільні випуски. Дані Internet Explorer та попередньої версії Edge (Legacy) не очищаються.

Файлові системи

Під час очищення вільного місця **Стирати залишки в кінцях кластерів (DeepErase)** працює лише з дисками NTFS. Функція **Очищати посилання в MFT** обробляє MFT на дисках NTFS і записи каталогів на дисках FAT. Стирання дисків і розділів не залежить від файлової системи.

Інсталяція й активація

Установіть O&O SafeErase, а потім активуйте програму ліцензійним ключем або запустіть пробну версію.

Передумови: ПК відповідає системним вимогам. Ви ввійшли під обліковим записом із правами адміністратора. Для Server Edition у Windows Server використовуйте інсталяційний файл Server Edition.

Інсталяція O&O SafeErase

1. Закрийте всі запущені програми.
2. Запустіть інсталяційний файл, завантажений із вебсайту O&O.
3. Підтвердьте запит Windows на права адміністратора.
4. Прийміть ліцензійну угоду та дотримуйтеся вказівок програми інсталяції.
5. На етапі вибору компонентів залиште позначки або зніміть їх для необов’язкових частин:

- **Розширення оболонки:** команди контекстного меню Провідника.
- **Подрібнювач:** піктограма на робочому столі, на яку можна перетягувати файли й папки для стирання.
- **Командний рядок:** `OOSafeEraseCmd.exe` для сценаріїв. Див. Командний рядок.

6. Перезавантажте ПК, якщо цього вимагає програма інсталяції.

Результат: O&O SafeErase і його службу встановлено. Програма інсталяції також установлює потрібне середовище виконання .NET.

Активація ліцензії або початок пробного періоду

Під час запуску без ліцензії O&O SafeErase повідомляє, що програму ще не активовано.

1. Виберіть **Увести ліцензію**.
2. Уведіть ліцензійний ключ точно так, як у підтвердженні замовлення чи ліцензійній картці. Не плутайте цифру 1 з літерою I та цифру 0 з літерою O.
3. Підтвердьте введення або запустіть пробну версію.

Результат: O&O SafeErase активовано або запущено у пробному режимі. У пробний період повідомлення показує кількість днів, що залишилися.

У пробній версії недоступні стирання дисків і розділів та режим «Фортеця». Після завершення пробного періоду O&O SafeErase не зможе стирати дані до введення ліцензії. Команда **Придбати зараз** відкриває інтернет-магазин O&O.

Одна ліцензія діє для одного комп’ютера. З питань ліцензування кількох комп’ютерів або стирання комп’ютерів від імені клієнтів зверніться до O&O Sales або свого постачальника.

Перевірка наявності оновлень

У нижній частині панелі навігації доступні відомості про програму: встановлена версія, ліцензія та перевірка наявності оновлень. За замовчуванням O&O SafeErase також автоматично шукає оновлення. Див. Параметри > LiveUpdate.

Під час оновлення в межах тієї самої основної версії ліцензія зберігається. Для нової основної версії потрібен новий ліцензійний ключ. Якщо налаштовано режим «Фортеця», після оновлення створіть його заново.

Видалення O&O SafeErase

1. У Windows відкрийте **Налаштування** > **Програми** > **Інстальовані програми**.
2. Виберіть **O&O SafeErase** > **Видалити** та підтвердьте дію.

Якщо налаштовано режим «Фортеця», спочатку видаліть його з O&O SafeErase. Див. Повторне створення або видалення режиму «Фортеця».

Подальші дії

- Стирання першого файлу

Стирання першого файлу

Ознайомтеся з O&O SafeErase на прикладі тестового файлу: виберіть його, перевірте завдання, зітріть файл і прочитайте звіт.

Передумови: O&O SafeErase установлено й активовано або запущено пробну версію. Ви створили тестовий файл із непотрібним вмістом, наприклад текстовий файл на робочому столі.

1. На початковій сторінці виберіть **Файли й папки**.
2. Виберіть **Файли** і вкажіть тестовий файл або перетягніть його до списку.
3. Виберіть **Вигляд** > **Показати шлях** і переконайтеся, що в списку є лише тестовий файл.
4. Перейдіть до **Перевірити завдання видалення**.
5. У розділі **Що** перевірте файл, а в розділі **Як** — метод стирання. У розділі **Після цього** увімкніть **Зберегти й підписати звіт**.
6. Виберіть **Безпечно видалити зараз**.
7. Дочекайтеся появи сторінки завершення й виберіть **Показати звіт**.

Результат: тестовий файл перезаписано та видалено, минаючи кошик. Звіт містить назву файлу, застосований метод і результат **OK**.

> **Стирання не можна скасувати**
>
> Щойно стирання розпочато, повернути перезаписані дані неможливо. Перевіряйте список щоразу перед стиранням.

Подальші дії

- Стирання файлів і папок з усіма параметрами
- Стирання слідів роботи браузерів і Windows
- Очищення вільного місця для видалення залишків раніше видалених файлів

Інтерфейс користувача

O&O SafeErase відкриває початкову сторінку. До будь-якого завдання можна перейти з цієї сторінки або з панелі навігації ліворуч.

Навігація

Область	Призначення
Початок	Історія очищення, рекомендація та плитки завдань.
Безпечно видалити > **Файли й папки**	Стирання файлів і папок.
Безпечно видалити > **Вільне місце**	Очищення вільного місця.
Безпечно видалити > **Диски / розділи**	Стирання дисків і розділів.
Конфіденційність	Стирання слідів роботи браузерів і Windows.
Стерти весь комп’ютер	Режим «Фортеця» і стирання всього ПК.
Звіти	Керування звітами.
Інструменти	Довідка для командного рядка, якщо цей компонент установлено.

Унизу панелі навігації можна відкрити параметри та відомості про програму, ліцензію й оновлення. У режимі «Фортеця» там доступна команда **Вимкнути** для вимкнення ПК.

Початкова сторінка

Плитки в розділі **Безпечно видалити дані** ведуть до завдань: **Файли й папки**, **Вільне місце**, **Диски й розділи**, **Дані браузерів**, **Дані Windows і програм** та **Стерти весь комп’ютер**. Плитка зі значком замка недоступна, наприклад у пробній версії або в режимі «Фортеця». Причину вказано в повідомленні на плитці.

Над плитками вказано, коли востаннє безпечно стиралися дані браузерів і Windows, вільне місце кожного диска та вміст кошика. Це історія очищень. Програма при цьому не шукає на ПК дані, які можна відновити.

Рекомендації та спільне стирання слідів роботи

Якщо від попереднього очищення минуло більше часу, ніж передбачає рекомендований інтервал, початкова сторінка рекомендує безпечно стерти сліди роботи. Рекомендація сама по собі не запускає стирання.

Команда **Безпечно видалити сліди…** відкриває вибір даних браузерів, даних Windows, кошика й вільного місця. Області, для яких настав час очищення, уже позначено. Вільне місце позначається, лише якщо його вже колись перезаписували. Скоригуйте вибір, перевірте метод і підтвердьте дію.

Параметр **Змінити рекомендацію…** задає інтервал: 7, 14, 30, 60 чи 90 днів або **Ніколи**. Стандартне значення — 30 днів. Цей параметр також доступний у розділі Параметри > Рекомендація.

У режимі «Фортеця» історію очищення приховано. Стирання даних браузерів і Windows у цьому режимі недоступне.

Як працює безпечне стирання

Під час безпечного стирання вміст файлу або накопичувача перезаписується до звільнення місця, щоб програми відновлення не змогли відтворити дані. O&O SafeErase виконує таке стирання для файлів, папок, слідів роботи, вільного місця й цілих дисків.

Що залишається після звичайного видалення

Коли Windows видаляє файл або очищає кошик, вона лише вилучає посилання на файл із файлової системи та позначає зайняте ним місце як вільне. Вміст зберігається на диску, доки його не перезапишуть інші дані. Саме ці області читають програми відновлення.

Залишки даних також можуть міститися в розташуваннях, які не відображаються безпосередньо:

Залишки даних	Розташування
Вільне місце	Вміст файлів, видалених звичайним способом, наприклад до встановлення O&O SafeErase.
Залишки кластерів	Невикористаний простір у кінці останнього кластера наявного файлу. Він може містити частини старіших файлів.
Записи файлової системи	Імена, розміри й дати видалених файлів у головній таблиці файлів (MFT) диска NTFS. Дуже малі файли повністю зберігаються в MFT.
Сліди роботи	Журнал браузера, файли cookie, кеш, тимчасові файли, ескізи, дампи пам’яті й кошик.

Що робить O&O SafeErase

O&O SafeErase перезаписує дані з використанням вибраного методу стирання й видаляє їх. Залежно від завдання обробляються різні області:

- Файли й папки та сліди роботи: вміст вибраних об’єктів.
- Вільне місце: вільні області, залишки кластерів та записи MFT диска. Наявні файли зберігаються.
- Диски й розділи: кожен сектор вибраного розділу або диска разом з усіма файлами.
- Увесь ПК: усі внутрішні диски разом із Windows. Операція запускається в режимі «Фортеця».

Після стирання у звіті наведено оброблені об’єкти, фактично застосований метод і попередження. Результат також зафіксовано в підписаному акті стирання.

Обмеження

- Безпечне стирання неможливо скасувати. Перезаписані дані неможливо відновити навіть за допомогою O&O Software.
- Копії в резервних копіях, хмарному сховищі, вкладеннях електронної пошти або на інших дисках не змінюються. За потреби зітріть їх окремо.
- Файл, який інша програма утримує відкритим, стерти неможливо. У звіті він зазначається з попередженням.
- На SSD фізичне розташування даних визначає контролер. Програма може перезаписати лише області, до яких може звернутися Windows. Див. Методи стирання та SSD.

Методи стирання та SSD

Метод стирання визначає, як O&O SafeErase перезаписує дані: який шаблон використовує та скільки проходів виконує. Для сучасних накопичувачів підходить стандартний метод. Додаткові проходи значно подовжують операцію, не підвищуючи надійності стирання.

Стандартний метод можна задати в розділі Параметри > Метод видалення. Перед кожним стиранням у завданні відображається вибраний метод у розділі **Як**. Для поточного запуску можна вибрати інший метод.

Методи

Метод	Проходи	Шаблон
NIST 800-88 Clear / BSI CON.6 (1× випадкові дані) (за замовчуванням)	1	Випадкові дані. Відповідає рівню «Clear» у NIST SP 800-88 Rev. 2 і повному перезапису випадковими даними за вимогами модуля BSI IT-Grundschutz CON.6.
Перезаписати нулями	1	Нулі. Швидкий метод, який забезпечує лише базове стирання.
US DoD 5220.22-M (застарілий)	3	Випадкові дані, нулі, випадкові дані.
Попередня процедура BSI (застаріла)	6	00, FF, 00, FF, 00, випадкові дані.
US DoD 5220.22-M ECE (застарілий)	7	Фіксована послідовність шаблонів і випадкових даних.
Метод Гутмана (застарілий)	35	Шаблони, описані Петером Гутманом у 1996 році для тогочасних магнітних жорстких дисків.

Методи з позначкою **(застарілий)** залишаються доступними для сумісності з наявними параметрами й вимогами. Згідно з NIST SP 800-88 Rev. 2 сучасним накопичувачам не потрібні кілька проходів.

У звіті зазначено метод, фактично застосований до кожного об’єкта. Назва методу описує процедуру й не є сертифікатом стирання. Перевірте результат у звіті.

Орієнтовна тривалість завдання залежить від обсягу даних, швидкості накопичувача, методу та інших операцій на ПК.

SSD і SolidErase

На SSD фізичне розташування даних визначає контролер. Він розподіляє записи між комірками флешпам’яті й має резервні області, до яких Windows не може звернутися. Тому багаторазовий перезапис не підвищує надійності, але зношує SSD.

Якщо в розділі Параметри > SSD увімкнено **Стирати SSD за допомогою SolidErase** (стандартний стан), O&O SafeErase стирає дані на виявлених SSD за допомогою SolidErase замість вибраного методу. SolidErase один раз перезаписує дані випадковими значеннями, уникаючи зайвих циклів запису. У звіті зазначається заміна вибраного методу на SolidErase.

> **Обмеження на SSD**
>
> Програма може перезаписати лише області, які адресує Windows. Зарезервовані чи перепризначені контролером області залишаються недоступними. SolidErase не виконує команд мікропрограми Secure Erase або Sanitize та не є криптографічним стиранням.

Подальші дії

- Змінення стандартного методу
- Стирання дисків і розділів

Звіти та акти стирання

Для кожної операції стирання O&O SafeErase може створити звіт. Він показує об’єкти, застосований метод і результат. Починаючи з версії 22, разом зі звітом зберігається підписаний акт стирання, який дає змогу виявити подальші зміни звіту.

Звіт

Звіт містить завдання, час початку й тривалість, об’єкти, фактично застосований до кожного об’єкта метод, загальний результат та всі попередження й помилки. Для цілих дисків у звіті також можуть бути інвентарний номер, подальше призначення та вимога до захисту, які ви вказуєте перед стиранням, а також відомості про оператора з параметрів.

Звіти зберігаються як файли XML. Їх можна відкрити в розділі **Звіти**. Див. Керування звітами.

Акт стирання

Разом зі звітом акт стирання постачається у файлі JSON та підписаному файлі `.oose`. Зберігайте всі файли одного звіту разом.

- **Підпис**. Служба O&O SafeErase підписує акт ключем цієї інсталяції. У режимі «Фортеця» або за недоступності служби використовується тимчасовий ключ. Про це зазначено в акті. Відбиток сертифіката підпису відображається в параметрах. Замість нього можна використовувати корпоративний сертифікат.
- **Позначка часу:** якщо функцію ввімкнено, служба позначок часу підтверджує момент підписання акта відповідно до RFC 3161. Служба отримує лише хеш-значення, без самого звіту. Для акта, створеного автономно, позначку часу можна отримати пізніше. У ньому буде вказано, що її додано згодом.
- **Ланцюжок актів:** кожен новий акт посилається на попередній. Якщо акта немає і відсутня підписана примітка про його видалення, перевірка виявить розрив у ланцюжку.

Що підтверджує підпис

Чинний підпис підтверджує, що акт не змінювався після підписання. Чи було стерто кожен об’єкт, показує результат у звіті. Перевіряйте і підпис, і результат, як описано в розділі Перевірка акта стирання.

В анонімізованих звітах назви файлів і папок замінюються зірочками. Див. Параметри.

Стирання файлів і папок

Зітріть окремі файли або цілі папки з усім вмістом так, щоб дані не можна було відновити.

Передумови: файли не відкриті в інших програмах. Ви маєте резервну копію всього, що ще може знадобитися.

1. На початковій сторінці або на панелі навігації виберіть **Файли й папки**.
2. Виберіть **Файли** або **Папка** й укажіть об’єкти. Їх також можна перетягнути в список із Провідника.
3. Дочекайтеся повного додавання великих папок. Під списком відображаються загальна кількість об’єктів, кількість файлів і загальний розмір.
4. Перевірте список. Щоб показати додаткові стовпці, скористайтеся **Вигляд** > **Показати шлях** і **Показати тип**. Щоб вилучити запис зі списку, виберіть його та натисніть **Прибрати**. Сам файл залишиться на місці.
5. Перейдіть до **Перевірити завдання видалення**.
6. Перевірте вибрані об’єкти в розділі **Що** та метод стирання у розділі **Як**. У розділі **Після цього** укажіть, чи потрібно застосувати **Зберегти й підписати звіт** та **Вимкнути комп’ютер після завершення**.
7. Виберіть **Безпечно видалити зараз**.

Результат: файли перезаписано й видалено. Сторінка завершення показує кількість стертих об’єктів і попередження. Див. Відстеження та скасування стирання.

Папки з посиланнями

Папки можуть містити точки з’єднання й символічні посилання на інші розташування. За замовчуванням O&O SafeErase видаляє лише посилання, а не цільовий об’єкт. Якщо в параметрах увімкнено **Переходити за посиланнями в папках**, цільові об’єкти також буде стерто.

> **Дані поза вибраною папкою**
>
> Якщо ввімкнено **Переходити за посиланнями в папках**, посилання може вказувати на дані поза вибраною папкою. Такі дані також буде стерто. Перевірте посилання в папці перед початком.

Навіть якщо параметр увімкнено, O&O SafeErase не переходить за посиланнями на точки підключення томів, мережеві розташування, корені дисків, папки Windows і програм та папки профілів користувачів.

Подальші дії

- Щоб стерти залишки раніше видалених файлів, див. Очищення вільного місця.

- Щоб стерти файли безпосередньо з Провідника, див. Стирання з Провідника.

Безпечне очищення кошика

Під час безпечного очищення кошика Windows файли в ньому перезаписуються, а не лише вилучаються зі списку.

Передумова: ви перевірили кошик у Windows і відновили всі потрібні файли. Після безпечного очищення команда Windows **Відновити** більше не знайде їх.

1. На початковій сторінці виберіть **Безпечно видалити сліди…**.
2. Виберіть **Кошик** і зніміть позначки з областей, які не потрібно стирати зараз.
3. Перевірте метод стирання й підтвердьте вибір.

Результат: кошик порожній, а його файли перезаписано. На початковій сторінці вказано дату безпечного очищення.

Інші способи досягти того самого результату:

- У Провіднику клацніть кошик правою кнопкою миші та виберіть **Безпечно очистити Кошик**. Команда доступна, якщо її ввімкнено в розділі Інтеграція з Windows.
- У розділі **Конфіденційність** виберіть категорію **Кошик** разом з іншими слідами роботи. Див. Стирання слідів роботи браузерів і Windows.

Якщо ви вже очистили кошик звичайним способом, на диску залишилися фрагменти його вмісту. Очистьте вільне місце на цьому диску.

Подальші дії

- Стирання слідів роботи браузерів і Windows
- Очищення вільного місця

Очищення вільного місця

Перезапишіть вільне місце на диску, щоб неможливо було відновити файли, видалені звичайним способом. Наявні файли залишаться без змін.

Передумови: O&O SafeErase працює з правами адміністратора. Якщо на сторінці відображається **Перезапустити від імені адміністратора**, спочатку виберіть цей пункт. У параметрах увімкнено принаймні одне з наведених нижче підзавдань.

1. Виберіть **Вільне місце**.
2. Виберіть потрібні диски за їхніми назвами й місткістю. У підсумку вказано, скільки вільного місця буде перезаписано.
3. Відкрийте **Метод і параметри стирання** та перевірте підзавдання й **Метод для жорстких дисків**.
4. Виберіть **Стерти вільне місце зараз**.

Результат: вільні області вибраних дисків перезаписано. На початковій сторінці вказано дату очищення кожного диска.

Підзавдання

Параметр	Дія
Перезаписувати вільне місце	Перезаписує області диска, не зайняті жодним файлом.
Стирати залишки в кінцях кластерів (DeepErase)	Перезаписує невикористаний простір у кінці зайнятих кластерів.
Очищати посилання в MFT	Видаляє з файлової системи імена видалених файлів і посилання на них.

Підзавдання вмикаються або вимикаються в розділі Параметри > Вільне місце. Якщо всі підзавдання вимкнено, на сторінці з'являється повідомлення з командою **Відкрити налаштування**.

Якщо в розділі **Налаштування** > **SSD** увімкнено SolidErase, SSD обробляються цим методом. Див. Методи стирання та SSD.

Тривалість залежить насамперед від обсягу вільного місця й вибраного методу. Під час очищення уникайте запису великих обсягів даних на диск.

> **Очищення не стирає весь диск**
>
> Команда **Натомість стерти цілі диски** відкриває Стирання дисків і розділів. У цьому режимі також стираються наявні файли.

Подальші дії

- Перегляньте звіт про очищення.
- Щоб одночасно стерти сліди роботи, див. Безпечне стирання слідів роботи.

Стирання слідів роботи браузерів і Windows

Зітріть сліди роботи браузерів, Windows і програм: журнал, файли cookie, тимчасові файли, ескізи тощо.

Передумови: ви зберегли дані, введені у форми, й інші результати роботи в браузерах. Перед стиранням відкриті браузери буде закрито. Ви перевірили, які збережені паролі та закладки вам іще потрібні.

1. Виберіть **Конфіденційність** або на початковій сторінці виберіть **Дані браузерів** чи **Дані Windows і програм**.
2. Виберіть **Перевірити зараз** (або **Перевірити знову**). Список показує кількість слідів роботи в кожній категорії.
3. Розгорніть групи й виберіть категорії. Команди **Вибрати все** та **Скасувати вибір** змінюють вибір одразу для всіх категорій. Вибір зберігається до наступного запуску.
4. Ще раз перевірте вибір, особливо **Паролі й дані форм**, **Закладки** і **Налаштування браузера**.
5. Виберіть **Видалити вибрані сліди**.
6. Якщо відкрито браузери, підтвердьте, що їх можна закрити.

Результат: вибрані сліди перезаписано й видалено. На початковій сторінці вказано дати очищення даних браузерів і Windows.

Дані браузерів

O&O SafeErase очищає дані Google Chrome, Microsoft Edge, Mozilla Firefox, Brave, Vivaldi, Opera й Opera GX в усіх профілях браузерів. Підтримувані версії наведено в розділі Системні вимоги. На сторінці відображаються встановлені браузери та їхні версії. Дані версії з позначкою про відсутність підтримки не очищаються.

Категорія	Що буде видалено
Історія	Відвідані вебсайти.
Історія завантажень	Список завантажених файлів. Самі файли залишаються.
Файли cookie	Сеанси входу й збережені дані сайтів. Ви вийдете з облікових записів на сайтах. Щоб зберегти файли cookie певних сайтів, див. Збереження файлів cookie вибраних вебсайтів.
Кеш	Кешовані сторінки й зображення.
Паролі й дані форм	Збережені паролі й дані форм. Вони видаляються остаточно.
Закладки	Збережені закладки.
Налаштування браузера	Початкова сторінка, пошукова система та інші параметри скидаються.

У Brave і Vivaldi немає категорії **Налаштування браузера**. В Opera та Opera GX немає ані **Закладки**, ані **Налаштування браузера**.

Дані, що зберігаються

Brave, Vivaldi, Opera й Opera GX зберігають дані деяких власних функцій у тих самих файлах, що й параметри та закладки. O&O SafeErase ніколи не стирає наведені нижче дані незалежно від вибраних категорій:

- **Brave:** Brave Wallet і Brave Rewards.
- **Vivaldi:** нотатки, пошта й канали, календар, контакти та збережені сеанси. Плитки експрес-панелі (Speed Dial) у Vivaldi є закладками, тому вони стираються разом із **Закладки**.
- **Opera й Opera GX:** експрес-панель (Speed Dial), параметри VPN і бічної панелі, дані месенджерів бічної панелі та дощок (Pinboards), а також GX Mods. Стирання **Файли cookie** однаково завершує сеанси входу в месенджерах.

Дані Windows і програм

Категорія	Що буде видалено
Нещодавні документи	Ярлики в папці «Останні». Самі документи залишаються.
Тимчасові файли Windows	Вміст `%TEMP%` і `Windows\Temp`.
Кеш ескізів	Ескізи зображень у Провіднику.
Кошик	Видалені об’єкти в кошику.
Дампи пам’яті	Дампи ядра після системних збоїв.
Файли CheckDisk	Фрагменти, відновлені CheckDisk (`*.chk`).
Збережені облікові дані FTP	Облікові дані FTP, збережені в Провіднику.

У режимі «Фортеця» неможливо стерти сліди роботи браузерів і Windows.

Подальші дії

- Збереження файлів cookie вибраних вебсайтів
- Як вибрати браузери для очищення: Параметри

Збереження файлів cookie вибраних вебсайтів

Збережіть файли cookie сайтів, якими регулярно користуєтеся, щоб не довелося знову входити на них після стирання файлів cookie за допомогою O&O SafeErase.

Передумова: перед початком закрийте браузери. O&O SafeErase не може прочитати файли cookie відкритого браузера й тому не відобразить його домени.

1. Відкрийте **Налаштування** > **Файли cookie для збереження**.
2. Виберіть **Додати…**.
3. Введіть частину доменного імені, наприклад `bank.example`. У списку з’являться відповідні домени, для яких браузери зберегли файли cookie. Можна також увести домен, якого немає в списку.
4. У розділі **Застосовується до** виберіть **Лише цей домен** або **Цей домен і всі піддомени**. Діалогове вікно покаже, скільки наявних файлів cookie буде збережено.
5. Виберіть **Додати** і підтвердьте параметри кнопкою **OK**.

Результат: під час наступного стирання файли cookie цього домену буде збережено в усіх підтримуваних браузерах.

Щоб знову стирати файли cookie певного домену, вилучіть його зі списку. Якщо список порожній, стираються всі файли cookie вибраних браузерів.

> **Примітка**
>
> Список захищає лише файли cookie. Історія перегляду, кеш та інші вибрані категорії того самого сайту й далі стираються. Збереження сеансу входу залежить і від самого сайту.

Подальші дії

- Стирання слідів роботи браузерів і Windows

Стирання дисків і розділів

Зітріть цілий диск або один розділ разом з усіма файлами, наприклад перед продажем чи утилізацією накопичувача.

> **Усі дані на накопичувачі буде втрачено**
>
> Вибір цілого диска охоплює всі його розділи, зокрема без букви диска, як-от розділи Linux або відновлення. Створіть резервну копію потрібних даних на іншому диску. Перевірте модель, номер і місткість диска.

Передумови: для O&O SafeErase активовано ліцензію і програму запущено з правами адміністратора. Вибраний накопичувач не є системним. Системний диск можна стерти лише в режимі «Фортеця».

1. Виберіть **Диски / розділи**. Якщо ви підключили чи від’єднали накопичувач, виберіть **Оновити**.
2. Виберіть цілий диск або окремі розділи. Команда **Вигляд** > **Показати нерозмічені області** показує області без розділів.
3. Відкрийте **Метод і параметри стирання** і перевірте метод. Для цілого диска ввімкніть **Після стирання ініціалізувати й форматувати**, якщо хочете знову використовувати диск у Windows відразу після стирання.
4. Виберіть **Стерти диск…**.
5. У вікні підтвердження ще раз перевірте диск. Там також наведено розділи, які не відображалися у списку.
6. Для цілих дисків за потреби вкажіть інвентарний номер, подальше призначення та вимогу до захисту для акта стирання.
7. Якщо на диску є операційна система, введіть показаний код безпеки. Потім виберіть **Безповоротно стерти зараз**.

Результат: кожен сектор вибраного накопичувача перезаписано. Без форматування на диску не залишиться розділів і він не відображатиметься в Провіднику.

Ініціалізація й форматування після стирання

Якщо ввімкнено **Після стирання ініціалізувати й форматувати**, після повного стирання O&O SafeErase створює один розділ на весь диск, виконує швидке форматування й призначає букву диска:

Диск	Стиль розділів і файлова система
Внутрішній диск	GPT, NTFS
USB-накопичувач, карта пам’яті	exFAT, для дисків до 2 ТБ — MBR

Параметр початково вимкнено, він діє лише для поточного запуску. Він недоступний у режимі «Фортеця» і для завдання Стирання всього ПК. Якщо форматування не вдалося, O&O SafeErase повідомить про це попередженням. Саме стирання вже завершено. Потім можна ініціалізувати диск у засобі «Керування дисками» Windows.

Якщо накопичувач змінився

Якщо після вибору диска підключити або від’єднати інший, номери дисків можуть змінитися. У такому разі O&O SafeErase не стиратиме накопичувач і повідомить, що він змінився. Виберіть **Оновити** та знову вкажіть потрібний накопичувач.

Подальші дії

- Перевірка акта стирання
- Стирання системного й усіх внутрішніх дисків: Стирання всього ПК

Стирання з Провідника

Контекстне меню Провідника дає змогу стирати файли й папки, вільне місце диска та вміст кошика.

Передумова: команди ввімкнено. Відкрийте **Налаштування** > **Інтеграція з Windows**, увімкніть **Контекстне меню провідника** і, для кошика, **Кошик** та підтвердьте кнопкою **OK**. Windows запитає права адміністратора. Команду кошика можна змінювати, лише коли O&O SafeErase працює з правами адміністратора.

1. У Провіднику виберіть файли або папки.
2. Клацніть вибрані об’єкти правою кнопкою миші та виберіть **Безпечно видалити**. Для диска виберіть **Стерти вільне місце**, а для кошика — **Безпечно очистити Кошик**.
3. У діалоговому вікні перевірте об’єкти й метод. Команда **Інші параметри…** відкриває O&O SafeErase з поточним вибором.
4. Запустіть стирання.

Результат: об’єкти стерто методом, показаним у діалоговому вікні. Операція очищення також з’явиться на початковій сторінці O&O SafeErase.

У Windows 11 команди доступні в компактному контекстному меню. Якщо їх там немає, виберіть **Показати додаткові параметри** та перевірте параметр у розділі **Інтеграція з Windows**.

З контекстного меню не можна стерти весь накопичувач. Див. Стирання дисків і розділів.

Подальші дії

- Змінення стандартного методу стирання

Відстеження та скасування стирання

Стежте за поточним стиранням, за потреби виконуйте іншу роботу, а після завершення перевірте результат.

Під час стирання O&O SafeErase показує перебіг, кількість об’єктів, поточний прохід, витрачений і орієнтовний залишковий час. Не вимикайте ПК під час стирання.

Робота під час стирання

- Команда **Продовжити у фоні** приховує сторінку, але стирання продовжується. Перебіг відображається у верхній частині вікна. Команда **Показати** знову відкриває сторінку.
- Команда **Вимкнути після завершення** вимикає ПК після стирання. Заздалегідь збережіть потрібні звіт і журнали.

Одночасно може виконуватися лише одне стирання. Перш ніж запускати нове, дочекайтеся завершення поточного або скасуйте його.

Скасування стирання

1. Виберіть **Скасувати зараз**.
2. Дочекайтеся, доки на сторінці з’явиться повідомлення про скасування стирання.

Результат: обробку зупинено. Уже стерті об’єкти залишаються стертими. Об’єкти, які не було оброблено або було оброблено частково, ще можуть піддаватися відновленню.

> **Скасування стирання накопичувача**
>
> Після часткового стирання диск чи розділ не містить ані повного набору старих даних, ані придатної до використання файлової системи. Виконайте повне стирання повторно. Якщо скасувати стирання системного диска в режимі «Фортеця», Windows зазвичай більше не запускається.

Перевірка результату

На сторінці завершення вказано, чи виконано стирання успішно, завершено з попередженнями, не виконано для певних об’єктів або скасовано.

1. Відкрийте **Журнал** та ввімкніть **Лише попередження й помилки**.
2. Перевірте кожен запис. Типова причина проблеми — файл, який інша програма утримує відкритим.
3. Щоб переглянути всі подробиці, виберіть **Показати звіт**.
4. Усуньте причину, наприклад закрийте відповідну програму, і повторіть стирання решти об’єктів.

Результат: ви знаєте, які об’єкти стерто. Якщо є попередження чи помилки, стерто не всі об’єкти.

Подальші дії

- Керування звітами
- Після стирання всього ПК див. Збереження журналів

Налаштування й запуск режиму «Фортеця»

Налаштуйте режим «Фортеця» і перезавантажте в ньому ПК. У цьому режимі O&O SafeErase працює в середовищі відновлення Windows (Windows RE), а не в установленій Windows. Файли не блокуються запущеною системою, тому можна стерти системний диск або весь ПК.

Передумови:

- Для O&O SafeErase активовано ліцензію. Режим «Фортеця» недоступний у пробній версії.
- O&O SafeErase запущено з правами адміністратора. В іншому разі виберіть **Перезапустити від імені адміністратора** на цій сторінці.
- На ПК доступне середовище Windows RE. Якщо його вимкнено, програма налаштування може його відновити.
- Наразі не виконується стирання.

Налаштування режиму «Фортеця»

1. Виберіть **Стерти весь комп’ютер**. Картка **Режим «Фортеця»** показує стан, версію, стан Windows RE і розташування.
2. Виберіть **Налаштувати Режим «Фортеця»**.
3. Зачекайте, доки на картці з’явиться **Налаштовано**. Налаштування триває кілька хвилин і не перезавантажує ПК.

Результат: режим «Фортеця» налаштовано в середовищі відновлення Windows і можна запустити будь-коли.

Запуск режиму «Фортеця»

1. Збережіть відкриті документи та закрийте всі програми.
2. Виберіть **Запустити Режим «Фортеця»** та підтвердьте перезавантаження.
3. Якщо системний диск захищено BitLocker, підтвердьте призупинення захисту до наступного звичайного запуску Windows. Підготуйте ключ відновлення BitLocker.

Результат: ПК перезавантажиться, і O&O SafeErase відкриється в режимі «Фортеця». Продовжуйте за інструкцією Стирання всього ПК або зітріть окремі диски й розділи, зокрема системний диск.

У режимі «Фортеця» недоступне стирання слідів роботи браузерів і Windows. Якщо перезавантажити ПК, не стерши Windows, система знову запуститься у звичайному режимі.

Повторне створення або видалення режиму «Фортеця»

Після оновлення O&O SafeErase на картці відображається **Рекомендовано оновлення** або **Невідомо**. Виберіть **Створити знову**, щоб режим «Фортеця» використовував установлену версію.

Команда **Прибрати** видаляє запис завантаження й папку режиму «Фортеця». Його можна будь-коли налаштувати знову.

Подальші дії

- Стирання всього ПК
- Збереження журналів після стирання ПК

Стирання всього ПК

Зітріть усі внутрішні диски ПК разом із Windows та програмами, наприклад перед продажем, поверненням або утилізацією комп’ютера.

> **Буде стерто Windows та всі внутрішні диски**
>
> Усі дані, програми й операційну систему буде перезаписано без можливості відновлення. Внутрішні диски стираються завжди. Після цього ПК не зможе завантажити Windows.

Передумови:

- Створено резервні копії всіх потрібних файлів і ліцензійних ключів установлених програм на зовнішньому диску.
- Від’єднано зовнішні диски, які не потрібно стирати, крім диска для збереження журналів.
- Налаштовано режим «Фортеця», і ПК вже перезавантажено в цьому режимі.

Вибір дисків

1. У режимі «Фортеця» виберіть **Стерти весь комп’ютер**.
2. Перевірте назву, місткість і тип кожного диска в списку. Внутрішні диски вибрано завжди.
3. Виберіть зовнішні диски, які також потрібно стерти.
4. У розділі **Зберегти журнали в:** виберіть зовнішній диск, який не буде стерто, або **Мережева спільна папка…**. Див. Збереження журналів. Команда **Оновити** повторно шукає диски, наприклад після підключення USB-накопичувача.
5. Перевірте метод. Якщо в параметрах увімкнено SolidErase, для SSD використовується цей метод.
6. Виберіть **Далі**.

Підтвердження та запуск

1. Перевірте підсумкові відомості й останнє попередження.
2. За потреби вкажіть для акта стирання **Інвентарний номер**, **Подальше призначення носія** й **Потрібний рівень захисту даних**.
3. Введіть показаний код безпеки.
4. Виберіть **Стерти весь комп’ютер зараз**.

Результат: усі вибрані диски перезаписано. Наприкінці O&O SafeErase копіює журнали й звіт у вибране місце.

Перш ніж вимикати чи перезапускати ПК, перевірте результат і збережені журнали. Журнали, що залишаються лише в пам’яті, буде втрачено під час перезавантаження. Збережіть їх за допомогою **Зберегти журнали…**.

Команда **Після стирання ініціалізувати й форматувати** для цього завдання недоступна. Щоб знову скористатися диском, ініціалізуйте його в новій системі, наприклад у засобі «Керування дисками» Windows.

Подальші дії

- Збереження журналів після стирання ПК
- Перевірка акта стирання

Збереження журналів після стирання ПК

Зберігайте звіт і журнали стирання всього ПК на диску, який не буде стерто, щоб мати підтвердження результату.

Під час стирання журнали зберігаються в оперативній пам’яті. Наприкінці O&O SafeErase копіює журнал стирання, звіт, журнал програми й журнал служби до місця, вибраного в розділі **Зберегти журнали в:**.

Збереження на зовнішньому диску

1. Підключіть USB-накопичувач, який не буде стерто.
2. У розділі **Зберегти журнали в:** виберіть **Оновити**, а потім — диск.

Диск не має бути вибраний для стирання. Якщо зовнішній диск не підключено або всі зовнішні диски стираються, зберегти журнали на зовнішньому диску неможливо.

Збереження на спільному мережевому ресурсі

Передумова: ПК підключено до мережі, а середовище відновлення Windows має драйвер мережевого адаптера.

1. У розділі **Зберегти журнали в:** виберіть **Мережева спільна папка…**.
2. Укажіть **Спільна папка:** у форматі `\\server\share` або `\\server\share\folder`.
3. Укажіть **Ім’я користувача:** у форматі `DOMAIN\user` та введіть **Пароль:**. Якщо доступ до ресурсу не потребує імені користувача, залиште відповідне поле порожнім.
4. Підтвердьте введені дані. O&O SafeErase перевірить з’єднання, вхід і право запису.

Результат: після завершення стирання журнали зберігаються в папці `OOSE-Logs\<computer>_<timestamp>` на спільному ресурсі. Пароль не зберігається.

Якщо перевірка не вдалася, у повідомленні буде зазначено причину: немає мережі, сервер не знайдено, неправильне ім’я користувача чи пароль або відсутнє право запису. Виправте дані чи виберіть USB-накопичувач або **Не зберігати**.

Збереження журналів після операції

Якщо вибрано **Не зберігати** або копіювання не вдалося, журнали залишаться в пам’яті до перезавантаження ПК.

1. Підключіть USB-накопичувач.
2. На сторінці завершення виберіть **Зберегти журнали…**.
3. Виберіть диск і збережіть журнали.

4. Перш ніж вимикати ПК, переконайтеся, що файли є на диску.

Результат: журнали й звіт збережено на USB-накопичувачі.

> **Відомості для служби підтримки**
>
> Якщо диска немає під рукою, на сторінці завершення в розділі **Інформація для підтримки** показано код. Сфотографуйте його смартфоном і надішліть до O&O Support. Код не містить персональних даних і не замінює звіт або акт стирання.

Подальші дії

- Перевірка акта стирання

Керування звітами

Знайдіть звіт про стирання, перевірте результат і збережіть, експортуйте або видаліть потрібні звіти.

1. Виберіть **Звіти**. Для кожного збереженого звіту в списку зазначено дату, тривалість, обсяг операції, метод і стан.
2. Виберіть **Фільтр**, щоб відфільтрувати список за **Тип**, **Стан** та **Період**. Команда **Скинути** знову показує всі звіти.
3. Відкрийте звіт.
4. Перевірте загальний результат і результат для кожного об’єкта, а потім перегляньте журнал щодо попереджень і помилок.
5. Якщо звіт має акт стирання, перевірте підпис. Див. Перевірка акта стирання.

Результат: ви з’ясували, чи завершено стирання повністю. Стан **OK** означає, що стерто всі об’єкти. Стани **Попередження**, **Помилка** і **Скасовано** означають, що деякі об’єкти не стерто.

Імпорт та експорт звітів

- Команда **Імпортувати** додає до списку звіти з іншої папки чи ПК, наприклад звіти після стирання всього ПК. Після імпорту O&O SafeErase показує кількість чинних, змінених, непідписаних і відсутніх актів стирання.
- Команда **Експортувати в Excel** зберігає дані звіту у форматі електронної таблиці для подальшої обробки. Експорт не замінює звіт і підписаний акт стирання.

Зберігайте разом звіт XML та відповідні файли JSON і `.oose`.

Видалення звітів

Команда **Безпечно видалити звіт** стирає один звіт, а **Безпечно видалити все** — усі звіти. Відповідні акти також стираються. У ланцюжку актів це фіксується підписаною приміткою про видалення.

> **Видалені звіти неможливо відновити**
>
> Звіти стираються безпечно. Перед видаленням архівуйте звіти, які потрібно зберегти для підтвердження результатів.

Подальші дії

- Папка звітів, автоматичне збереження й анонімізація: Параметри

- Перевірка акта стирання

Перевірка акта стирання

Перевірте, чи залишився акт стирання незмінним, щоб використовувати звіт як підтвердження стирання.

Передумова: звіт XML, файл JSON і відповідний файл `.oose` містяться в одній папці. Звіти з іншого ПК слід спочатку імпортувати.

1. Виберіть **Звіти** і відкрийте звіт.
2. Перегляньте рядок **Підпис**. У ньому наведено стан, сертифікат підпису та його відбиток SHA-256, а також позначку часу.
3. Зіставте стан із таблицею нижче.
4. У цьому самому звіті перевірте результат стирання.

Результат: ви з'ясували, чи справжній акт і чи повністю виконано стирання. Обидві перевірки потрібні: чинний підпис не означає, що стерто кожен об'єкт.

Стан	Значення
Акт стирання дійсний	Після підписання акт не змінювався.
Акт стирання дійсний, без часової позначки	Акт не змінювався. Служба позначок часу не підтвердила час підписання.
Акт стирання змінено	Вміст більше не відповідає підпису. Збережіть файл без змін для перевірки.
Акт стирання не підписано	Акт не має підпису, який можна перевірити. Причину зазначено у звіті.
Прогалина в ланцюжку актів стирання	Попередній акт видалено без примітки про видалення.
Без підпису (старий звіт)	Звіт створено попередньою версією, яка не створювала актів стирання.

Перевірка з командного рядка

Командний рядок дозволяє перевірити акт без ліцензії, нічого не стираючи:

```
.\OOSafeEraseCmd.exe verify "C:\Reports\Report_example.oose"
```

Результат позначається кодом завершення. Див. Командний рядок. Перевірити ланцюжок актів можна, лише якщо попередні акти доступні на цьому ПК.

Подальші дії

- Звіти та акти стирання
- Дані оператора, сертифікат підпису й позначки часу: Параметри

Параметри

На цій сторінці наведено всі параметри діалогового вікна, їхнє призначення й стандартні значення. Відкрийте діалогове вікно внизу панелі навігації та підтвердьте зміни кнопкою **OK**.

Параметри, які адміністратор задав за допомогою групової політики, заблоковані й мають відповідну позначку. Деякі сторінки приховано в режимі «Фортеця».

Програма

Загальні

Параметр	Значення	За замовчуванням
Мова	Мова програми. Зміна набуває чинності після перезапуску програми.	Використовувати системний параметр
Режим відображення	Світлий, темний або один із двох режимів високої контрастності.	Використовувати системний параметр
Згортати в область сповіщень	Під час стирання згортає вікно в область сповіщень.	Вимкнено
Закривати програму, запущену з контекстного меню, після видалення	Закриває програму після стирання, запущеного з контекстного меню Провідника. Звіти зберігаються автоматично.	Вимкнено

Інтеграція з Windows

Ці параметри містяться на сторінці **Загальні відомості**. Вони застосовуються після натискання **OK**. Windows запитує права адміністратора. У режимі «Фортеця» ці параметри не відображаються.

Параметр	Значення	За замовчуванням
Контекстне меню провідника	Додає **Безпечно видалити** та **Стерти вільне місце** до контекстного меню Провідника. Див. Стирання з Провідника.	Як налаштовано на цьому ПК
Кошик	Додає **Безпечно очистити Кошик** до контекстного меню кошика. Змінити можна лише в програмі, запущеній з правами адміністратора.	Як налаштовано на цьому ПК

Якщо прав адміністратора немає, на сторінці доступна команда **Перезапустити від імені адміністратора**.

LiveUpdate

Параметр	Значення	За замовчуванням
Автоматично перевіряти оновлення	Регулярно перевіряє наявність нової версії та пропонує її встановити.	Увімкнено
Не показувати поточне оновлення	Приховує повідомлення про поточне доступне оновлення. Повідомлення про наступні оновлення з'являтимуться.	Вимкнено
Не показувати подальші оновлення	Приховує всі повідомлення про оновлення. Наявність оновлень можна й надалі перевіряти у відомостях про програму.	Вимкнено

Додатково

Параметр	Значення	За замовчуванням
Розблокувати диск	Визначає дію, якщо диск для стирання використовується: **Завжди запитувати**, **Завжди ігнорувати** чи **Завжди розблоковувати**. Розблокування активного диска може спричинити втрату даних у програмах, які його використовують.	Завжди запитувати
Увімкнути ведення журналу	Записує докладний журнал служби O&O SafeErase для підтримки. Коли вимкнено, записуються лише попередження й помилки. Після зміни служба перезапускається.	Вимкнено

Стирання

Метод видалення

Стандартний метод стирання для нових завдань. Його можна змінити окремо для кожного завдання.

Параметр	За замовчуванням
Метод стирання	**NIST 800-88 Clear / BSI CON.6 (1× випадкові дані)**

Файли й папки

Параметр	Значення	За замовчуванням
Переходити за посиланнями в папках	Також стирає цільові об’єкти точок з’єднання та символічних посилань у вибраних папках. Програма ніколи не переходить за посиланнями на точки підключення, мережеві об’єкти, корені дисків або папки Windows, програм і профілів користувачів.	Вимкнено

Вільне місце

Підзавдання очищення вільного місця. Якщо одне з них вимкнено, у діалоговому вікні з’являється попередження. Якщо вимкнено всі, очистити вільне місце неможливо.

Параметр	Значення	За замовчуванням
Безпечно стерти вільне місце	Перезаписує області, не зайняті жодним файлом.	Увімкнено
DeepErase у кластерах	Перезаписує залишки кластерів у кінці зайнятих кластерів (NTFS).	Увімкнено
Видаляти посилання на видалені файли	Видаляє з файлової системи записи видалених файлів: записи MFT у NTFS і записи каталогів у FAT.	Увімкнено

SSD

Параметр	Значення	За замовчуванням
Стирати SSD за допомогою SolidErase	Замість вибраного методу стирає виявлені SSD за допомогою SolidErase. Див. Методи стирання та SSD.	Увімкнено

Аналіз і звіти

Рекомендація

Параметр	Значення	За замовчуванням
Рекомендувати безпечне видалення через	Інтервал, після якого початкова сторінка рекомендує повторно стерти дані браузерів і Windows та очистити вільне місце: 7, 14, 30, 60 чи 90 днів або **Ніколи**.	30 днів

Браузер

Для кожного підтримуваного браузера є окремий перемикач. У розділі Конфіденційність очищаються лише вибрані браузери. Не можна вибрати браузер, який не встановлено.

Параметр	За замовчуванням
Окремий перемикач для кожного браузера	Усі ввімкнено

Файли cookie для збереження

Список доменів, чиї файли cookie зберігаються під час очищення. Див. Збереження файлів cookie вибраних вебсайтів. Команда **Додати…** додає домен, а **Прибрати** вилучає його зі списку.

Параметр	За замовчуванням
Список доменів	Порожній список: стираються всі файли cookie

Звіти

Параметр	Значення	За замовчуванням
Автоматично зберігати звіти	Зберігає звіт кожної операції в папці звітів.	Вимкнено
Знеособлювати імена файлів і папок	Замінює в нових звітах назви папок і файлів зірочками, наприклад `C:\*\*\*`. Дані оператора також не включаються до акта стирання. Наявні звіти не змінюються.	Вимкнено
Створювати повний журнал	Додає до звіту кожен оброблений об’єкт, а не лише попередження та помилки.	Увімкнено
Показувати у звіті не більше 10 000 записів	Обмежує кількість записів про файли, що відображаються у звіті.	Увімкнено
Місце	Папка для звітів. Команда **Огляд…** дає змогу вибрати іншу папку, доступну для запису.	`Documents\OO Software\OO SafeErase\Reports` у профілі користувача

Акт стирання

Відомості про оператора записуються в кожен акт стирання. Усі поля початково порожні (**Не вказано**).

Параметр	Значення
Ім’я	Ім’я особи, яка виконує стирання.
Посада або функція	Посада або роль цієї особи.
Організація	Компанія чи організація.
Місце	Місце проведення стирання.
Контакт (телефон або електронна пошта)	Контакт для запитань про стирання.

Підпис актів стирання

Параметр	Значення	За замовчуванням
Сертифікат підпису	Показує сертифікат, яким служба підписує акти, та його відбиток SHA-256. Лише для довідки.	Ключ цієї інсталяції
Сертифікат компанії (відбиток)	Відбиток сертифіката із закритим ключем у сховищі сертифікатів цього комп’ютера. Служба використовуватиме його для підпису замість ключа цієї інсталяції.	Порожньо
Додати часову позначку (RFC 3161)	Служба позначок часу підтверджує, коли підписано кожен акт. Надсилається лише хеш-значення підпису. Для актів, створених автономно, позначку часу буде отримано пізніше.	Вимкнено
Центр часових позначок (URL)	Адреса служби позначок часу, наприклад кваліфікованої служби відповідно до eIDAS.	Порожнє поле: DigiCert

Командний рядок

`OOSafeEraseCmd.exe` стирає файли, папки, вільне місце, диски та вміст кошика з командного рядка. Файл установлюється в папку O&O SafeErase, якщо під час інсталяції вибрано компонент **Командний рядок**. Його вибрано за замовчуванням. Програма інсталяції не додає його до `PATH`.

Запустіть командний рядок або PowerShell із правами адміністратора й перейдіть у папку програми або вкажіть повний шлях до неї. У PowerShell для запуску з поточної папки додайте перед іменем `.\`. Плитка **Командний рядок** на сторінці **Інструменти** відкриває цю довідку. Без підключення до Інтернету вона показує ту саму довідку, що й `--help`.

```
.\OOSafeEraseCmd.exe <command> [options]
```

Команди стирають справжні дані

`wipe-file` і `secure-move` стирають без додаткового запиту. Інші команди стирання зазвичай запитують підтвердження, якщо його не вимкнено параметром `--yes`. Спершу перевірте сценарій на тестових даних. Параметр `--analyze-only` доступний лише для наведених нижче команд і не є універсальним тестовим режимом.

Команди

Команда	Призначення
`wipe-file`	Стерти один файл.
`wipe-folder`	Стерти папку та весь її вміст.
`wipe-freespace`	Очистити вільне місце тому.
`wipe-disk`	Стерти цілий диск.
`wipe-region`	Стерти розділ або область диска.
`list`	Стерти всі файли й папки, зазначені в текстовому файлі.
`wipe-trash`	Безпечно очистити свій кошик.
`list-trash`	Вивести список об’єктів у своєму кошику. Дані не стираються.
`secure-move`	Скопіювати файли чи папки до цільової папки, а потім безпечно стерти джерело.
`list-disks`	Показати диски та їхні розділи, номери, серійні номери й розміри. Дані не стираються.
`list-methods`	Показати методи стирання.
`verify <file>`	Перевірити акт стирання (`.oose` або `.json`) чи акт, розташований поруч зі звітом XML.
`license`	Показати, активувати або перевірити ліцензію.

Також підтримуються назви `wipe-directory` , `wipe-partition` , `wipe-recyclebin` і `list-recyclebin` .

Спільні параметри

Параметр	Значення
`--method`, `-m <method>`	Метод стирання, див. Методи. Стандартне значення: `Random`.
`--verbose`	Докладне виведення.
`--quiet`, `-q`	Не виводити перебіг виконання. Запити, які потребують відповіді, усе одно відображаються.
`--help`, `-h`, `/?`	Показати довідку.
`--version`	Показати версію.

Параметри перевіряються до початку стирання. Недопустимий для команди чи повторений параметр, відсутнє значення або невідомий метод завершують команду з кодом 1.

Параметри окремих команд

Команда	Параметр	Значення
`wipe-file`	`--file`, `-f <path>`	Файл для стирання.
`wipe-folder`	`--directory`, `-d <path>` (або `--folder`, `-f`)	Папка для стирання.
`list`	`--list-file`, `-l <path>`	Текстовий файл з одним шляхом у кожному рядку. Рядки, що починаються з `#`, є коментарями. Якщо хоча б один рядок містить неприпустимий шлях, стирання не виконується.
`wipe-file`, `wipe-folder`, `list`	`--force`	Також дозволити стирання в папках Windows, програм або профілі користувача. Див. Шляхи до файлів і папок.
`wipe-folder`, `list`	`--follow-links`	Також стирати цільові об’єкти точок з’єднання й символічних посилань. За замовчуванням видаляються лише посилання. Програма ніколи не переходить за посиланнями на точки підключення, мережеві об’єкти, корені дисків або папки Windows, програм і профілів користувачів.
`wipe-freespace`	`--volume`, `-v <path>`	Том, наприклад `C:\`.
`wipe-freespace`	`--free-space`, `--cluster-tips`, `--fs-records`	Перезаписати вільне місце, залишки кластерів і записи файлової системи. Якщо жодного з цих параметрів не вказано, перезаписується лише вільне місце.
`wipe-disk`, `wipe-region`	`--disk`, `-d <id>`	Номер диска з виводу `list-disks`, наприклад `0` для `\\.\PhysicalDrive0`.
`wipe-region`	`--region`, `-r <id>`	Номер розділу або області з виводу `list-disks`.
`wipe-disk`, `wipe-region`	`--serial <serial number>`	Стирати лише диск із цим серійним номером.
`wipe-disk`, `wipe-region`	`--expect-size <bytes>`	Стирати лише диск, розмір якого в байтах точно відповідає заданому.
`wipe-disk`	`--format`	Після стирання створити один розділ і швидко його відформатувати. Для внутрішніх дисків використовуються

Команда	Параметр	Значення
		GPT/NTFS, для USB-накопичувачів і карт пам’яті — exFAT із MBR до 2 ТБ. Недоступно в режимі «Фортеця».
`wipe-disk`, `wipe-region`	`--ignore-ssd`	Не показувати примітку про SSD.
`wipe-trash`, `list-trash`	`--all-users`	Кошики всіх користувачів на всіх дисках замість власного кошика.
`list-trash`	`--drives-only`	Показати лише диски, у кошиках яких є об’єкти.
`wipe-disk`, `wipe-region`, `list`, `wipe-trash`	`--analyze-only`	Виконати лише аналіз, нічого не стирати.
`wipe-folder`, `list`, `wipe-disk`, `wipe-region`, `wipe-trash`	`--yes`, `-y`	Не запитувати підтвердження перед стиранням. Див. Підтвердження.
`secure-move`	`--source`, `-s <paths>`	Шляхи до джерел через крапку з комою.
`secure-move`	`--target`, `-t <path>`	Цільова папка.

Методи

Назва для `--method`	Проходи	Метод
`Random` (синоніми `NistClear` і `BsiCon6`)	1	NIST 800-88 Clear / BSI CON.6, випадкові дані. Стандартний метод.
`Zeros`	1	Перезапис нулями.
`Solid`	1	SolidErase для SSD.
`Nsa3`	3	US DoD 5220.22-M (застарілий).
`Bsi`	6	Попередня процедура BSI (застаріла), відмінна від BSI CON.6.
`Nsa7`	7	US DoD 5220.22-M ECE (застарілий).
`Gutmann`	35	Метод Гутмана (застарілий).

Див. Методи стирання та SSD.

Ліцензія

Командний рядок використовує ліцензію O&O SafeErase на цьому комп’ютері та не має окремої ліцензії. Для стирання потрібна активована ліцензія або чинна пробна версія. На відміну від графічної програми, командний рядок у пробний період також дає змогу стирати диски. Команди стирання виводять кількість днів до завершення пробного періоду в потік помилок, якщо не задано `--quiet`. Команди `license`, `list-disks`, `list-methods`, `verify`, `--help` і `--version` працюють без ліцензії.

Команда	Значення
`license status`	Показати ліцензію на цьому комп’ютері.
`license activate <license key>`	Активувати ліцензію за допомогою ключа. Зручно на комп’ютері без графічного вікна програми, наприклад на сервері.
`license validate`	Перевірити ліцензію через службу ліцензування O&O.

Шляхи до файлів і папок

Команди `wipe-file`, `wipe-folder` і `list` перед стиранням перевіряють усі шляхи та показують повний шлях до об’єкта:

- Відносний шлях, наприклад `old_data`, обчислюється від поточної папки.

- Самостійний запис `C:`, а також `C:folder` і `\folder` не приймаються, оскільки залежать від неявної поточної папки. Укажіть повний шлях, наприклад `C:\Data\Old`.
- Корінь диска або спільного ресурсу, наприклад `C:\` чи `\\server\share`, не приймається. Для стирання цілого накопичувача використовуйте `wipe-disk` або `wipe-region`.
- Стирання папок Windows, програм, профілів користувачів та їхніх батьківських папок дозволено лише за наявності `--force`.

Підтвердження

Перед стиранням команди `wipe-folder`, `list`, `wipe-disk`, `wipe-region` і `wipe-trash --all-users` показують цільові об’єкти та чекають натискання клавіші. Ctrl+C скасовує операцію. Якщо запит вимкнено параметром `--yes`, такої можливості перевірити вибір не буде.

Диск або розділ з операційною системою можна стерти, лише ввівши показаний код безпеки в консолі, як і в графічній програмі. Параметр `--yes` не замінює код. Диск чи розділ, з якого запущено Windows, стерти неможливо. Для цього потрібен режим «Фортеця».

Якщо потрібне підтвердження, але відповісти нікому, наприклад через переспрямування вводу в запланованому завданні, команда завершується з кодом 5 і нічого не стирає.

Диски й розділи

Команда `list-disks` показує для кожного диска номер, модель, розмір, серійний номер і розділи та позначає диск із запущеною Windows. Для кожного диска також виводяться параметри `--serial` і `--expect-size` із відповідними значеннями.

Номери дисків можуть змінюватися, зокрема після підключення USB-накопичувача. Параметри `--serial` і `--expect-size` дають змогу перевірити диск перед виконанням `wipe-disk` та `wipe-region`. Якщо за номером виявлено інший диск, стирання не виконується й команда завершується з кодом 1.

Для SSD команди `wipe-disk` й `wipe-region` попереджають, що перезапис не охоплює резервної області SSD. Див. Методи стирання та SSD. Параметр `--ignore-ssd` приховує цю примітку.

Акти стирання та служба

Якщо службу O&O SafeErase запущено, командний рядок, як і графічна програма, виконує стирання через неї. Служба перевіряє запит, а під час стирання створюється підписаний акт стирання. Після завершення командний рядок показує розташування акта. Для стирання через службу завжди потрібна консоль, запущена з правами адміністратора.

Якщо службу не запущено, командний рядок повідомляє про це й виконує стирання у власному процесі з правами консолі. Акт стирання не створюється. Без прав адміністратора можна стерти лише файли й папки, які має право видаляти поточний обліковий запис. Для дисків, розділів і вільного місця потрібні права адміністратора.

Якщо версії командного рядка та служби не збігаються, наприклад після незавершеного оновлення, нічого не стирається, а команда завершується з кодом 4. Повторно встановіть O&O SafeErase.

Сценарії та заплановані завдання

- Викликайте `OOSafeEraseCmd.exe` із повним шляхом до файлу.
- Для планової інвентаризації використовуйте команду перегляду дисків. Для перевірки актів доступна команда перевірки підпису.
- Якщо потрібне підтвердження, а ввід переспрямовано, операція завершується з кодом 5. Параметр `--yes` прибирає звичайний запит, тому не використовуйте його під час перевірки цільового об’єкта.
- Ідентифікуйте диски за `--serial` і `--expect-size`. Стерти диск або розділ з операційною системою зі сценарію неможливо, оскільки потрібен код безпеки.
- Перевіряйте код завершення, а не текст виводу. Примітки й помилки надходять до потоку помилок.

Нижче наведено приклад перевірки цільового диска лише для читання. Він виводить відомості про накопичувачі й не змінює даних. Перед окремою операцією стирання звірте модель, серійний номер і розмір цільового диска. Сам номер диска після підключення чи від’єднання накопичувачів може змінитися.

```
# Перевірка цілі без запису: показати номери, розміри та серійні номери дисків
$cmd = "<program folder>\OOSafeEraseCmd.exe"
& $cmd list-disks
if ($LASTEXITCODE -ne 0) {
 Write-Error "Помилка перевірки дисків. Код: $LASTEXITCODE"
}
```

Приклади

```
# Стерти файл стандартним методом
.\OOSafeEraseCmd.exe wipe-file --file "C:\temp\secret.txt"

# Стерти папку методом Гутмана
.\OOSafeEraseCmd.exe wipe-folder --directory "C:\temp\old_data" --method Gutmann

# Очистити вільне місце диска C: разом із залишками кластерів
.\OOSafeEraseCmd.exe wipe-freespace --volume "C:\" --free-space --cluster-tips

# Показати диски, їхні номери, серійні номери й розміри
.\OOSafeEraseCmd.exe list-disks

# Стерти диск 2 (USB-накопичувач) і відформатувати його після стирання
.\OOSafeEraseCmd.exe wipe-disk --disk 2 --format

# Стерти розділ 1 на диску 2
.\OOSafeEraseCmd.exe wipe-region --disk 2 --region 1

# Безпечно очистити кошик поточного користувача
.\OOSafeEraseCmd.exe wipe-trash

# Активувати ліцензію
.\OOSafeEraseCmd.exe license activate <license key>

# Перевірити акт стирання
.\OOSafeEraseCmd.exe verify "C:\Reports\Report_20261019_083000.oose"
```

Коди завершення

Код	Значення
0	Успіх. Для `verify`: акт чинний, зокрема за відсутності позначки часу.
1	Неправильне використання: недопустимий, невідомий чи повторений параметр, не знайдено файл або цільовий об’єкт, шлях відхилено чи диск не відповідає `--serial` або `--expect-size`. Нічого не стерто.
2	Немає чинної ліцензії: її не активовано, пробний період минув або ліцензія втратила чинність.
3	Не вдалося виконати операцію.
4	Версії командного рядка й служби не збігаються.
5	Потрібне підтвердження, але ввід переспрямовано. Нічого не стерто.
6	Операцію завершено, проте не кожен об’єкт перезаписано: видалено лише посилання, ім’я жорсткого посилання чи покажчик місця заповнення хмарного файлу. Такі об’єкти наведено у списку.
7	Заборонено політикою адміністратора (`wipe-disk`, `wipe-freespace`).
20	`verify`: акт було змінено.
21	`verify`: розрив у ланцюжку актів.
22	`verify`: непідписаний акт або звіт старого формату без акта.
99	Неочікувана помилка.
130	Скасовано, наприклад через Ctrl+C або неправильний код безпеки.

Команди oosecmd

Попередні версії O&O SafeErase містили засіб командного рядка `oosecmd.exe`. Засіб `OOSafeEraseCmd.exe` не приймає його параметрів. Відповідність для наявних сценаріїв наведено нижче:

oosecmd	OOSafeEraseCmd.exe
Файли й папки без параметра, `--match`	`wipe-file --file <path>`, `wipe-folder --directory <path>`. Для кількох шляхів: `list --list-file <file>`
`--security <level>`	`--method <method>`: `highest` → `Gutmann`, `high` → `Nsa7`, `medium` → `Bsi`, `low` → `Nsa3`, `lowest` → `Random`, `zero` → `Zeros`
`--freespace <drive>`	`wipe-freespace --volume <drive>:\`
`--deletedrive <number>`	`wipe-disk --disk <number>`
`--deletevolume <drive letter>`	`wipe-region --disk <number> --region <number>`. Команда `list-disks` показує номери
`--showdisks`, `-w`	`list-disks`
`--tempfiles recyclebin`	`wipe-trash`
`--tempfiles`, `--internetfiles`	Команди немає. Стирайте сліди роботи браузерів і Windows у графічній програмі
`--analyse`, `--autoclean`	Команди немає
`--register "user:… company:… serial:…"`	`license activate <license key>`
`--createreport`, `-r`, `--reportname`	Параметра немає. Акт стирання створюється, якщо працює служба. Див. Акти стирання та служба
`--yes`, `-y`	`--yes`, `-y`
`--silent`, `-s`	`--quiet`, `-q`
`--verbose`, `-v`	`--verbose`. Параметр `-v` тепер означає `--volume`

Сліди роботи браузерів і Windows можна стерти лише в графічній програмі. Див. Стирання слідів роботи браузерів і Windows.

Глосарій

У глосарії пояснено терміни, які використовуються в O&O SafeErase і цьому посібнику.

Термін	Значення
Кластер	Найменша одиниця, якою файлова система виділяє місце на диску.
Залишок кластера	Невикористане місце в кінці останнього кластера файлу. Воно може містити фрагменти старіших файлів. **Стирати залишки в кінцях кластерів (DeepErase)** перезаписує це місце.
DeepErase	Підзавдання очищення вільного місця, що перезаписує залишки кластерів.
Метод стирання	Процедура перезапису даних, яка визначає шаблон і кількість проходів. Див. Методи стирання та SSD.
Акт стирання	Підписаний файл (`.oose`), який супроводжує звіт і дає змогу виявляти зміни. Див. Звіти та акти стирання.
Режим «Фортеця»	Робота O&O SafeErase у середовищі відновлення Windows, де встановлена Windows не блокує файли. Потрібна для стирання системного диска та всього ПК.
Вільне місце	Області диска, не зайняті жодним файлом. Вони можуть містити вміст файлів, видалених звичайним способом.
MFT	Головна таблиця файлів (Master File Table) — каталог диска NTFS. Зберігає імена та посилання на видалені файли й вміст дуже малих файлів.
Прохід	Один повний перезапис даних. Деякі методи виконують кілька проходів із різними шаблонами.
Ланцюжок актів	Послідовність актів стирання на ПК. Кожен акт посилається на попередній, тому видалення акта можна виявити.
Звіт	Файл XML із цільовими об’єктами, застосованим методом і результатом стирання.
Безпечне стирання	Перезапис даних до звільнення зайнятого ними місця, щоб запобігти їхньому відновленню.
SolidErase	Метод O&O для SSD: один прохід із випадковими даними, що дає змогу уникнути зайвих циклів запису.
SSD	Твердотільний накопичувач на основі флешпам’яті. Фізичне розташування даних визначає його контролер.
Позначка часу	Підтвердження часу підписання акта стирання службою позначок часу за стандартом RFC 3161.
Сліди роботи	Дані, що залишаються після роботи браузерів, Windows і програм: журнал, файли cookie, кеш, тимчасові файли тощо.
TRIM	Команда, за допомогою якої Windows повідомляє SSD, які області більше не використовуються.

Термін	Значення
Windows RE	Середовище відновлення Windows: мінімальна версія Windows в окремому розділі, призначена для відновлення системи та роботи режиму «Фортеця».

Усунення несправностей

Знайдіть відповідну ознаку нижче та виконайте наведені кроки. Якщо проблему не усунуто, зверніться до O&O Support.

Функцію заблоковано

Причина: потрібна ліцензія або права адміністратора, чи функція недоступна в режимі «Фортеця». Причину вказано на заблокованій плитці або сторінці.

Розв’язання:

1. Якщо в повідомленні є команда **Перезапустити від імені адміністратора**, виберіть її.
2. Для стирання дисків і використання режиму «Фортеця» у пробній версії введіть ліцензію. Див. Інсталяція й активація.
3. Стирайте сліди роботи браузерів і Windows у самій Windows. У режимі «Фортеця» ця функція недоступна.

Не вдається очистити вільне місце

Причина: O&O SafeErase запущено без прав адміністратора або вимкнено всі підзавдання очищення вільного місця.

Розв’язання:

1. Виберіть **Перезапустити від імені адміністратора**.
2. Якщо сторінка повідомляє, що очищення вільного місця вимкнено, виберіть **Відкрити налаштування** та ввімкніть принаймні один параметр у розділі **Вільне місце**.

Файл не було стерто

Причина: інша програма утримує файл відкритим або Windows забороняє доступ.

Розв’язання:

1. Відкрийте журнал стирання й прочитайте попередження щодо файлу.
2. Закрийте програму, що використовує файл. Якщо її не вдається визначити, перезапустіть Windows.
3. Повторіть стирання файлу.

Не вдається закрити браузер

Причина: браузер або один із його фонових процесів не завершує роботу на запит O&O SafeErase.

Розв’язання:

1. Збережіть результати роботи в браузері й закрийте його вручну.
2. Переконайтеся в диспетчері завдань, що всі процеси браузера завершено.
3. Знову виберіть **Видалити вибрані сліди**.

Версія браузера не підтримується

Причина: версія встановленого браузера новіша або старіша за версії, що їх може очищати O&O SafeErase. Сліди роботи цього браузера не стираються.

Розв’язання: установіть найновіше оновлення O&O SafeErase, а потім виберіть **Перевірити знову**.

Диск не стерто, оскільки він змінився

Причина: після вибору підключено або від’єднано диск, унаслідок чого змінилися номери дисків.

Розв’язання:

1. Виберіть **Оновити**.
2. Знову виберіть накопичувач і перевірте назву, номер та місткість.
3. Повторно запустіть стирання.

Стертий диск не відображається у Провіднику

Причина: після повного стирання на диску немає розділів.

Розв’язання: ініціалізуйте диск і створіть розділ у засобі «Керування дисками» Windows або для наступного стирання ввімкніть **Після стирання ініціалізувати й форматувати**. Див. Стирання дисків і розділів.

Режим «Фортеця» не запускається

Причина: режим «Фортеця» не налаштовано, налаштовано іншою версією програми, Windows RE вимкнено або ще триває стирання.

Розв’язання:

1. Виберіть **Стерти весь комп’ютер** і перевірте картку **Режим «Фортеця»**.
2. Виберіть **Налаштувати Режим «Фортеця»** або **Створити знову**. Програма налаштування відновить вимкнене середовище Windows RE.
3. Дочекайтеся завершення поточних стирань і виберіть **Запустити Режим «Фортеця»**.

Не вдається зберегти журнали на спільному мережевому ресурсі

Причина: у режимі «Фортеця» немає мережі (часто через відсутність драйвера мережевого адаптера), сервер недоступний, облікові дані неправильні або обліковий запис не має права запису до ресурсу.

Розв'язання:

1. Прочитайте повідомлення: у ньому вказано причину.
2. Виправте шлях до ресурсу, ім'я користувача або пароль.
3. Якщо мережа недоступна, виберіть USB-накопичувач.

> **Під час перезавантаження журнали в оперативній пам'яті втрачаються**
>
> Якщо журнали не вдалося зберегти, перед вимкненням чи перезавантаженням ПК виберіть **Зберегти журнали…**. Див. Збереження журналів.

Бракує звіту

Причина: автоматичне збереження звітів вимкнено, до папки звітів неможливо записати дані або звіт приховано фільтром.

Розв'язання:

1. У розділі **Звіти** виберіть **Фільтр** > **Скинути**.
2. Перевірте папку звітів і автоматичне збереження в розділі Параметри > Звіти.

Версії служби та програми не збігаються

Причина: версії програми та служби O&O SafeErase різняться, наприклад після незавершеного оновлення.

Розв'язання: повторно встановіть O&O SafeErase з актуального інсталяційного файлу. Програма й служба завжди встановлюються разом.

Поширені запитання

Короткі відповіді на поширені запитання. До кожної відповіді додано посилання на докладніші відомості.

Чи можна скасувати безпечне стирання?

Ні. Перезаписані дані не відновить навіть O&O Software. Скасування операції також не поверне вже перезаписаних даних. Спочатку створіть резервні копії всього потрібного. Див. Як працює безпечне стирання.

Як стерти файли, які вже видалено звичайним способом?

Очистьте вільне місце на диску. Це перезапише залишки видалених файлів і збереже наявні файли. Див. Очищення вільного місця.

Чи видаляє очищення вільного місця наявні файли?

Ні. Перезаписуються лише області, не зайняті жодним файлом. Щоб стерти диск разом із файлами, скористайтеся функцією Стирання дисків і розділів.

Чи означає рекомендація на початковій сторінці, що знайдено дані?

Ні. Вона лише показує, коли востаннє виконувалося безпечне очищення. При цьому програма не сканує ПК й не запускає стирання. Див. Інтерфейс користувача.

Чому після очищення завершилися сеанси входу на сайтах?

Стирання файлів cookie видаляє дані входу. Додайте сайти, на яких хочете залишитися в обліковому записі, до списку Файли cookie для збереження.

Чому у звіті зазначено SolidErase замість вибраного методу?

Якщо відповідний параметр увімкнено, для SSD використовується SolidErase. У звіті зазначено фактичний метод. Див. Методи стирання та SSD.

Який метод стирання вибрати?

Стандартний метод NIST 800-88 Clear / BSI CON.6 один раз перезаписує дані випадковими значеннями. Цього достатньо для сучасних жорстких дисків. Методи з більшою кількістю проходів потребують значно більше часу. Див. Методи стирання та SSD.

Чи стираються підключені USB-накопичувачі під час стирання всього ПК?

Лише якщо ви їх виберете. Внутрішні диски стираються завжди. Для журналів використовуйте диск, який не буде стерто. Див. Стирання всього ПК.

Чи підтверджує чинний акт стирання, що все стерто?

Він підтверджує, що акт не змінювали. Чи стерто кожен об’єкт, показує результат у звіті. Перевіряйте і підпис, і результат. Див. Перевірка акта стирання.

Чи допомагає O&O SafeErase виконувати вимоги GDPR?

O&O SafeErase стирає персональні дані без можливості відновлення та документує стирання підписаними актами. Яких саме заходів потребує ваша організація, визначаєте ви. Програма не замінює оцінювання захисту даних.

Що можна робити у пробній версії?

Можна стирати файли, папки й сліди роботи та очищати вільне місце. Для стирання дисків і розділів та використання режиму «Фортеця» потрібна ліцензія. Див. Інсталяція й активація.

Де розташована версія для командного рядка?

Якщо компонент установлено, `OOSafeEraseCmd.exe` міститься в папці програми O&O SafeErase. Див. Командний рядок.

Що нового у версії 22

У O&O SafeErase 22 оновлено інтерфейс і додано документування стирання підписаними актами. На цій сторінці наведено зміни порівняно з версією 21.

Нові можливості

- **Новий інтерфейс:** панель навігації ліворуч, початкова сторінка з історією й рекомендаціями, перегляд завдання перед стиранням і нове подання перебігу. Доступні світлий, темний і два висококонтрастні режими та підтримка програм невізуального доступу. Див. Інтерфейс користувача.
- **Підписані акти стирання:** до кожного звіту можна додати підписаний акт із необов'язковою позначкою часу RFC 3161 та ланцюжком актів. Відомості про оператора задаються в **Налаштування** > **Звіти**. Див. Звіти та акти стирання.
- **Стерти весь комп'ютер**. Журнали можна зберігати на спільному мережевому ресурсі, для кожного стирання можна вказати інвентарний номер, подальше призначення та вимогу до захисту. Після стирання з'являється код для підтримки. Див. Стирання всього ПК.
- **Після стирання ініціалізувати й форматувати**. Після стирання цілого диска O&O SafeErase може створити й відформатувати розділ. Див. Стирання дисків і розділів.
- **Додаткові браузери:** окрім Chrome, Edge та Firefox підтримуються Brave, Vivaldi, Opera й Opera GX. Очищаються всі профілі браузерів.
- **Файли cookie для збереження**. Під час стирання файлів cookie можна зберігати їх для вибраних вебсайтів. Див. Збереження файлів cookie вибраних вебсайтів.
- **Командний рядок:** `OOSafeEraseCmd.exe` стирає дані зі сценаріїв, використовує ліцензію програми, створює акти стирання через службу й перевіряє їх. Параметри попереднього засобу `oosecmd.exe` не підтримуються. Див. Командний рядок.

Зміни

- **Новий стандартний метод:** NIST 800-88 Clear / BSI CON.6 один раз перезаписує дані випадковими значеннями. Методи DoD, попередню процедуру BSI та метод Гутмана позначено як **застарілі**. Див. Методи стирання та SSD.
- **Посилання в папках:** точки з'єднання й символічні посилання в папках за замовчуванням більше не обробляються з переходом до цілі. Перехід можна ввімкнути новим параметром **Переходити за посиланнями в папках**.
- **Інтеграція з Windows**. Команди контекстного меню тепер налаштовуються в **Налаштування** > **Загальні відомості**.
- Параметр **Увімкнути ведення журналу** тепер керує журналом служби O&O SafeErase.
- Параметр **Режим «Фортеця»** тепер міститься в розділі **Стерти весь комп'ютер**.

- Програма містить потрібне їй середовище виконання .NET.

Вилучено

- Перевірку безпеки, яка шукала на ПК дані для відновлення, вилучено. Тепер початкова сторінка показує історію очищення.
- Файли cookie Adobe Flash Player та дані Internet Explorer більше не очищаються.
- Перевірку оновлень і відомості для служби підтримки переміщено з **Інструменти** до відомостей про програму.

Підтримка та інші продукти O&O

На цій сторінці пояснюється, як зв’язатися з O&O Support, які відомості прискорять розгляд звернення та де знайти ліцензії, оновлення й інші продукти O&O.

Зв’язок із O&O Support

Скористайтеся формою на сторінці підтримки O&O або напишіть на support@oo-software.com. З питань ліцензій і замовлень також можна звертатися через сторінку підтримки.

Додайте такі відомості:

- Версію й редакцію продукту та версію Windows. Вони відображаються у відомостях про програму внизу панелі навігації.
- Завдання та тип цільового об’єкта, наприклад файл, вільне місце, диск або весь ПК.
- Точний текст повідомлення про помилку та кроки для її відтворення.
- Звіт і журнал стирання.
- Де виконувалося стирання: у Windows чи в режимі «Фортеця».

Після стирання всього ПК в розділі **Інформація для підтримки** на сторінці завершення відображається код зі стислим технічним підсумком. Якщо немає диска для журналів, надішліть фото коду.

> **Примітка**
>
> Звіти можуть містити назви файлів і дисків та дані оператора. Перевірте їх перед надсиланням. Не публікуйте й не надсилайте на знімках екрана ліцензійні ключі чи паролі.

Ліцензії й оновлення

O&O SafeErase — комерційна програма. Нею можна користуватися протягом пробного періоду, а надалі потрібна чинна ліцензія. У пробній версії недоступні стирання дисків і розділів та режим «Фортеця».

Оновлення в межах тієї самої основної версії, наприклад із 22.0 до 22.1, зазвичай безкоштовні. Для нової основної версії потрібен новий ліцензійний ключ. Як увести ліцензію й перевірити наявність оновлень, див. Інсталяція й активація.

Інші продукти O&O

O&O Software розробляє засоби для Windows, зокрема для резервного копіювання, оптимізації й захисту конфіденційності. Огляд усіх продуктів наведено на вебсайті O&O.