INFORMATION TECHNOLOGY

Anna Kalinichenko
Detachable Subdivision "Nizhinsky Professional College of National University of Life and Environmental Sciences of Ukraine", Nizhin, Ukraine
ORCID iD: 0000-0001-8676-7031

ENSURING PERSONAL COMPUTER RESILIENCE TO SUDDEN POWER LOSS

Abstract. The risks of data loss and disruption to personal computer operation caused by sudden power loss are analysed. Based on technical documentation, the effects of caching and delayed writes on data preservation are examined. The capabilities and limitations of NTFS journaling and SSD power loss protection are identified. The combined use of an uninterruptible power supply, automatic shutdown, document saving features, and backups is justified. A multilayer protection algorithm covering system preparation, response to a power outage, and recovery is proposed. Criteria for evaluating its effectiveness are defined: the amount of lost changes, successful shutdown and file restoration, and the time required to resume work.
Keywords: personal computer, power supply, uninterruptible power supply, data protection, backup.

Анна Калініченко
Відокремлений структурний підрозділ "Ніжинський фаховий коледж Національного університету біоресурсів і придокористування України", м. Ніжин, Україна
ORCID iD: 0000-0001-8676-7031

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА ДО РАПТОВОГО ПРИПИНЕННЯ ЕЛЕКТРОЖИВЛЕННЯ

Анотація. Проаналізовано ризики втрати даних і порушення роботи персонального комп'ютера внаслідок раптового припинення електроживлення. На основі технічної документації розглянуто вплив кешування та відкладеного запису на збереження інформації. Визначено можливості й обмеження журналювання NTFS та захисту SSD від втрати живлення. Обґрунтовано доцільність поєднання джерела безперебійного живлення, автоматичного завершення роботи, засобів збереження документів і резервного копіювання. Запропоновано алгоритм багаторівневого захисту, який охоплює підготовку системи, реагування на знеструмлення та відновлення роботи. Визначено критерії оцінювання його ефективності: обсяг утрачених змін, успішність завершення роботи й відновлення файлів та час повернення до виконання робочих завдань.
Ключові слова: персональний комп'ютер, електроживлення, джерело безперебійного живлення, захист даних, резервне копіювання.

Раптове припинення електроживлення становить загрозу для безперервності роботи персонального комп'ютера (ПК) та збереження інформації. Особливого

значення ця проблема набуває під час підготовки документів, виконання обчислень, програмування й опрацювання навчальних матеріалів. Наслідки знеструмлення можуть охоплювати втрату незбережених змін, переривання операцій запису та необхідність відновлення робочого середовища. Тому забезпечення стійкості ПК потребує узгодженого застосування апаратних і програмних засобів, які діють до виникнення збою, під час втрати живлення та після його відновлення.

Метою роботи є обґрунтування комплексу апаратних і програмних заходів для зменшення ризику втрати даних та скорочення часу відновлення роботи персонального комп'ютера після раптового припинення електроживлення. Методологічною основою є аналіз технічної документації Microsoft, Eaton і Kingston та порівняння описаних у ній механізмів захисту. Стійкість у межах дослідження розглядається як здатність системи зберегти критично важливі дані, коректно завершити роботу за наявності резервного живлення та відновити працездатність після повернення електропостачання.

Для визначення способів захисту необхідно враховувати механізми запису інформації. За документацією Microsoft, Windows використовує системний файловий кеш: дані спочатку можуть записуватися в оперативну пам'ять, а їх перенесення на накопичувач відбувається пізніше. Такий підхід підвищує продуктивність, проте створює проміжок часу, протягом якого змінені дані ще не перебувають на енергонезалежному носії. Якщо живлення припиняється до завершення запису, відповідні зміни можуть бути втрачені [1]. Отже, оцінюючи захищеність інформації, потрібно враховувати весь шлях її проходження: від прикладної програми через системний кеш до накопичувача.

Певний рівень відновлюваності забезпечує файлова система NTFS. Вона використовує журнал транзакцій і контрольні точки для відновлення узгодженості файлової системи після збою [2]. Водночас відновлення її структури та збереження останніх змін у відкритому документі є різними завданнями. З огляду на механізм відкладеного запису, журналювання не слід трактувати як гарантію збереження всіх поточних даних користувача [1; 2]. Тому можливості файлової системи мають доповнюватися засобами резервного живлення та захисту файлів.

На рівні накопичувача важливим є захист від втрати живлення — Power Loss Protection (PLP). У технічних матеріалах Kingston описано апаратні механізми, які використовують запас енергії конденсаторів для завершення критичних операцій SSD, зокрема перенесення даних із внутрішнього кешу до NAND-пам'яті та збереження службових структур. Програмні механізми накопичувача можуть забезпечувати перевірку й відновлення внутрішніх таблиць після некоректного вимкнення [3]. При цьому наявність і повнота захисту залежать від конкретної моделі SSD. Можливості серверних накопичувачів із апаратним PLP не можна автоматично поширювати на всі споживчі пристрої. Крім того, захист

SSD охоплює дані, які вже надійшли до накопичувача, і не забезпечує збереження інформації, що залишається лише в оперативній пам'яті ПК.

Основним засобом підтримання роботи комп'ютера після зникнення основного живлення є джерело безперебійного живлення (ДБЖ). Його вибір потребує врахування топології, допустимого навантаження та необхідного часу автономної роботи. У технічному довіднику Eaton розглянуто відмінності між типами ДБЖ, активною потужністю у ватах і повною потужністю у вольт-амперах, а також чинники, що впливають на стан акумуляторів [4]. Для конкретного ПК необхідно перевіряти відповідність навантаження обом граничним показникам ДБЖ. Час автономної роботи слід визначати за характеристиками обраної моделі для відповідного навантаження [5]. У межах запропонованого підходу резерв енергії має бути достатнім для збереження роботи та завершення роботи ОС із часовим запасом.

Окремого значення набуває взаємодія ДБЖ з операційною системою. Якщо завершення роботи залежить лише від користувача, захист може виявитися недостатнім за його відсутності. Тому доцільно застосовувати ДБЖ із підтримуваним інтерфейсом обміну даними та сумісним програмним забезпеченням. Прикладом є Eaton Intelligent Power Protector, який забезпечує автоматичне коректне завершення роботи під час тривалого порушення електропостачання [6]. Умови запуску цієї процедури потрібно визначати з урахуванням доступної автономності та часу завершення роботи конкретної системи. Автоматизація має залишати запас енергії для виконання необхідних операцій.

На рівні прикладних програм необхідно розрізняти регулярне збереження, автозбереження та автовідновлення. У документації Microsoft описано можливості AutoSave й AutoRecover, умови застосування яких залежать від програми, її версії та розташування файлу [7]. Ці функції допомагають зменшити ризик втрати результатів роботи, проте не дають підстав гарантувати відновлення кожної останньої зміни. Тому налаштування відповідних механізмів має супроводжуватися перевіркою їх роботи на контрольному документі та регулярним збереженням важливих результатів.

Самостійним складником захисту є резервне копіювання. Його завдання полягає у створенні доступної для відновлення копії даних на випадок втрати або пошкодження робочих файлів. Зокрема, засіб File History у Windows дає змогу зберігати версії особистих файлів на зовнішньому накопичувачі або в мережевому розташуванні та відновлювати їх за потреби [8]. Для забезпечення практичної цінності резервування потрібно визначити перелік захищених папок, періодичність копіювання й порядок перевірки відновлення. Успішне створення копії доцільно підтверджувати пробним відновленням контрольного файлу.

На основі проведеного аналізу пропонується наступний алгоритм забезпечення стійкості ПК, який охоплює три етапи. Підготовчий етап

передбачає визначення критично важливих даних, добір ДБЖ, налаштування автоматичного завершення роботи, збереження документів і резервного копіювання. На етапі припинення електроживлення система отримує сигнал від ДБЖ, повідомляє користувача та за визначених умов запускає процедуру завершення роботи. Після повернення електропостачання перевіряються запуск ОС, доступність робочих файлів і потреба у відновленні інформації. Така послідовність поєднує запобігання втратам із підготовкою до їх можливого усунення.

Для аналізу наслідків збою можуть використовуватися журнали подій Windows. Зокрема, подія Kernel-Power із кодом 41 свідчить про те, що попереднє завершення роботи було некоректним. Водночас Microsoft наголошує, що цього запису недостатньо для однозначного встановлення причини: він може бути пов’язаний із припиненням живлення, системною помилкою або іншими обставинами [9]. Тому діагностичний висновок потрібно робити шляхом зіставлення системних подій, журналу ДБЖ та відомостей про фактичне порушення електропостачання.

Ефективність запропонованого комплексу заходів доцільно оцінювати за обсягом утрачених змін, успішністю автоматичного завершення роботи, можливістю відновлення контрольних файлів і тривалістю повернення до виконання робочих завдань. У цій роботі зазначені показники запропоновано як основу подальшої практичної перевірки; кількісне оцінювання потребує випробувань конкретної конфігурації ПК, ДБЖ та програмного середовища.

Під час організації захисту від раптового знеструмлення необхідно враховувати помилки у визначенні складу обладнання, яке потребує резервного живлення. Зокрема, недостатньо оцінити лише споживання системного блока, якщо до того самого ДБЖ підключаються монітор та інші пристрої. Вибір за одним показником потужності без урахування сукупного навантаження й потрібної автономності може призвести до невідповідності захисту фактичним умовам використання [4; 5]. Для навчальної лабораторії доцільно складати перелік обладнання для кожного ДБЖ та переглядати його після зміни конфігурації робочих місць. Такий облік дає змогу встановити, які пристрої отримують резервне живлення та для виконання яких завдань воно передбачене.

Іншою помилкою є оцінювання захищеності лабораторії лише за кількістю комп’ютерів, підключених до ДБЖ. Якщо навчальні завдання передбачають запис результатів на мережевий ресурс, потрібно враховувати весь шлях передавання інформації. У такому сценарії пропонується окремо визначати потребу в резервному живленні комутатора та пристрою, на якому розміщено спільні файли. Захист робочої станції без підтримання необхідних мережевих вузлів може виявитися недостатнім для завершення збереження. Тому одиницею планування доцільно вважати сукупність пристроїв, потрібних для виконання конкретної навчальної операції.

За обмежених ресурсів доцільно встановити пріоритетність захисту обладнання. Пропонується насамперед визначати вузли, від яких залежить збереження спільних даних, керування лабораторією та доступ до навчальних матеріалів. Далі оцінюється можливість забезпечення резервним живленням студентських робочих місць. При цьому пріоритет має визначатися наслідками втрати даних і переривання завдання. Такий підхід дозволяє обґрунтувати розподіл доступних ДБЖ без припущення, що всі комп'ютери лабораторії мають однакові потреби.

Організаційною помилкою є відсутність визначених місць збереження студентських робіт. За використання спільних комп'ютерів результати можуть залишатися в різних локальних папках, що ускладнює включення їх до резервного копіювання та подальший пошук. Тому пропонується встановити єдину структуру каталогів за групами, дисциплінами й користувачами, а також визначити, які папки підлягають резервуванню. Для File History потрібно перевірити включення відповідних каталогів до захищених бібліотек, оскільки довільне розташування файлу не означає автоматичного створення його резервної копії [8].

Особливістю лабораторій комп'ютерної інженерії є виконання завдань, під час яких студенти змінюють параметри операційної системи або працюють із віртуальними машинами. У цьому випадку необхідно розмежувати відновлення початкового навчального середовища та збереження індивідуальних результатів. Перед поверненням системи чи віртуальної машини до вихідного стану слід передбачити винесення звітів, програм і конфігураційних файлів до визначеного сховища. Відсутність такого порядку створює ризик втрати виконаної роботи вже під час відновлення середовища після збою.

Окремим недоліком є невизначеність відповідальності за дії під час припинення електропостачання. Для лабораторії пропонується встановити короткий порядок: студенти припиняють запуск нових завдань і зберігають результати, викладач координує завершення заняття, а відповідальна технічна особа контролює стан спільних ресурсів. Налаштування автоматичного завершення роботи мають забезпечувати виконання процедури й за відсутності користувача [6]. Під час перевірки готовності лабораторії доцільно оцінювати не лише працездатність обладнання, а й зрозумілість цього порядку для всіх учасників освітнього процесу.

Таким чином, забезпечення стійкості персонального комп'ютера до раптового припинення електроживлення потребує багаторівневого підходу. Резервне живлення створює часовий ресурс для завершення роботи, програмна взаємодія з ДБЖ забезпечує автоматизацію цієї процедури, механізми збереження документів зменшують ризик втрати поточних змін, а резервні копії підтримують відновлення інформації. Практичне значення запропонованого підходу полягає в узгодженні цих засобів у єдиний алгоритм, придатний для адаптації до домашніх, офісних і навчальних комп'ютерів.

СПИСОК ДЖЕРЕЛ

1. Microsoft. File Caching. URL: https://learn.microsoft.com/en-us/windows/win32/fileio/file-caching (дата звернення: 05.11.2026).

2. Microsoft. NTFS overview. URL: https://learn.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview (дата звернення: 05.11.2026).

3. Kingston Technology. SSD Power Loss Protection: How Hardware & Firmware PLP Prevent Data Loss. URL: https://www.kingston.com/en/blog/servers-and-data-centers/ssd-power-loss-protection (дата звернення: 05.11.2026).

4. Eaton. UPS and Power Management Fundamentals Handbook. URL: https://www.eaton.com/content/dam/eaton/products/backup-power-ups-surge-it-power-distribution/backup-power-ups/eaton-ups-fundamentals-handbook-en-us-2025.pdf (дата звернення: 05.11.2026).

5. Eaton. UPS sizing guide. URL: https://www.eaton.com/us/en-us/products/backup-power-ups-surge-it-power-distribution/backup-power-ups/ups-sizing-guide.html (дата звернення: 05.11.2026).

6. Eaton. Intelligent Power Protector. URL: https://www.eaton.com/gb/en-gb/catalog/backup-power-ups-surge-it-power-distribution/eaton-intelligent-power-protector-.html (дата звернення: 05.11.2026).

7. Microsoft. Help protect your files in case of a crash. URL: https://support.microsoft.com/en-us/office/collab-files/help-protect-your-files-in-case-of-a-crash (дата звернення: 05.11.2026).

8. Microsoft. Backup and restore with File History. URL: https://support.microsoft.com/en-us/windows/experience/backup-recovery/backup-and-restore-with-file-history (дата звернення: 05.11.2026).

9. Microsoft. Advanced troubleshooting for Event ID 41: The system has rebooted without cleanly shutting down first. URL: https://learn.microsoft.com/en-us/troubleshoot/windows-client/performance/event-id-41-restart (дата звернення: 05.11.2026).