

## **СТВОРЕННЯ РЕЗЕРВНИХ КОПІЙ HDD. ВІДНОВЛЕННЯ З РЕЗЕРВНИХ КОПІЙ.**

Резервне копіювання, Бекап (від англ. backup) – процес створення копії даних на носії (жорсткому диску, Flash - накопичувачі, хмарі, тощо), призначеному для відновлення даних в разі їх пошкодження або видалення.

Створення резервної копії даних, дає можливість виконати відновлення інформації, у випадку втрати оригіналу з якого було створено резервну копію. При цьому під втратою треба розуміти настання будь-якої події, що призвела до зміни, завдяки якій дані втратили цінлісність або були видалені з носія. Приклад: умисне спричинення шкоди через видалення важливої для підприємства інформації.

Методи резервного копіювання:

- Повне резервне копіювання — Full Backup
- Диференціальне резервне копіювання — Differential Backup
- Додаткове резервне копіювання — Incremental Backup

**Повне резервне копіювання** — Повна копія даних.

Цей метод дозволяє забезпечити максимальну відповідність оригіналу даних та його копії.

**Диференціальне резервне копіювання** — Копіювання змін, що були зроблені після створення останньої повної копії. Створення такої копії потребує більше часу та займає більший об'єм, ніж додаткове копіювання, але дозволяє пришвидшити процес відновлення. Загалом є альтернативою між створенням повної або додаткової копії.

**Додаткове резервне копіювання** — копіювання змін, що відбулись з повного, диференційованого або додаткового копіювання. Загалом на додаткове копіювання затрачається менше часу, так як копіюється менше файлів. Однак процес відновлення даних займає більше часу, так як повинні відновлюватися дані останньої повної копії і після цього всі резервні копії, від яких залежить додаткова копія.

## **Методи передачі даних резервних копій:**

**З використанням агента.** Копіювання даних здійснюється з допомогою частини програмного забезпечення, що встановлюється з боку системи, дані якої потрібно захистити. Такий метод є обтяжливий для адміністрування, оскільки потребує контролю за встановленням та оновленням такого програмного забезпечення, але надає змогу щільно інтегруватись у програмне середовище, що використовується на клієнтській системі.

**Off-host.** Метод, що дозволяє створювати резервної копії без значного навантаження на клієнтську систему, зазвичай дані передаються безпосередньо зі сховища даних на сервер резервного копіювання. Цей метод також може потребувати встановлення агента, щоб координувати процеси всередині операційної системи.

**Serverless.** Метод що дозволяє передавати дані від клієнта у сховище резервних копій без участі сервера резервного копіювання. При цьому сервер резервного копіювання, отримує від клієнта необхідну інформацію, про об'єкти, що їх було скопійовано в сховище.

## **Методи створення копій даних:**

**Тіньова копія (Shadow Copy).** Створення миттєвої копії з дискового розділу операційної системи, при цьому використовуються властивості файлової системи.

**Snapshot дискового розділу** — створення миттєвої копії даних безпосередньо на дисковому масиві, використовуються можливості дискових масивів.

**Схеми ротації.** Для резервного копіювання дуже важливим питанням є вибір схеми ротації носіїв (наприклад, магнітних стрічок, дисків). Найчастіше використовують такі схеми:

- **Одноразове копіювання;**
- **Проста ротація;**
- **«Дід, батько, син»;**
- **«Ханойська башта»;**
- **«10 наборів».**

**Одноразове копіювання (custom)** - найпростіша схема, що не передбачає ротації носіїв. Всі операції проводяться вручну. Перед копіюванням адміністратор задає час початку резервування, перераховує файлові системи або каталоги, які необхідно скопіювати. Цю інформацію можна зберегти в базі, щоб її можна було використовувати знову. При одноразовому копіюванні найчастіше застосовується повне копіювання.

**Проста ротація** — циклічне використання носіїв для копіювання. (цикл — тиждень: певний носій на певний день тижня).

«Дід, батько, син» — ієрархічна структура використання набору з трьох комплектів носіїв. Раз на тиждень — батько (повне резервування), щоденне — син (додаткове або диференційне). Додатково проводиться повне копіювання — дід.

**Ханойська вежа** — використання комплектів носіїв даних. Кожен комплект має носії, що містять місячний, тижневий, денний резерв копій.

«10 наборів» — за кожним носієм закріплюється день, в який виконується копіювання, при цьому при повторному використанні цей індекс зміщується на одиницю.

Зберігання резервної копії:

- Стрічка стримера — запис резервних даних на магнітну стрічку стримера;
- «Хмарний» бекап — запис резервних даних за «хмарною» технологією через онлайн-служби спеціальних провайдерів;
- DVD чи CD — запис резервних даних на оптичні диски;
- HDD — запис резервних даних на жорсткий диск комп'ютера;
- LAN — запис резервних даних на будь-яку машину всередині локальної мережі;
- FTP — запис резервних даних на FTP-сервери;
- USB — запис резервних даних на будь-який USB-сумісний пристрій (флеш-карта або зовнішній жорсткий диск);
- ZIP, JAZ, MO — резервне копіювання на дискети ZIP, JAZ, MO

## **RAID — масив**

RAID (англ. redundant array of independent/inexpensive disks) — надлишковий масив незалежних/недорогих дисків для комп'ютера. Дисківий масив — це набір дисківих пристроїв, що працюють разом, щоб підвищити швидкість і надійність системи вводу/виводу. Цим набором пристроїв керує спеціальний RAID-контролер (контролер масиву), який забезпечує функції розміщення даних по масиву; а для решти всієї системи дозволяє представляти весь масив як один логічний пристрій вводу/виводу. За рахунок паралельного виконання операцій читання і запису на кількох дисках, масив забезпечує підвищену швидкість обмінів в порівнянні з одним великим диском.

Масиви також можуть забезпечувати надмірне зберігання даних, з тим, щоб дані не були втрачені у разі виходу з ладу одного з дисків. Залежно від рівня RAID, проводиться або віддзеркалювання або розподіл даних по дисках.

### **Рівні RAID**

Каліфорнійський університет в Берклі представив наступні рівні RAID, вони були прийняті як стандарт де-факто. Кожен з чотирьох основних рівнів RAID використовує унікальний метод запису даних на диски, і тому всі рівні забезпечують різні переваги. Рівні RAID 1, 3 і 5 забезпечують віддзеркалювання або зберігання бітів парності; і тому дозволяють відновити інформацію у разі збою одного з дисків.

### **RAID рівня 0**

Технологія RAID 0 також відома як розподіл даних (англ. data striping). Із застосуванням цієї технології інформація розбивається на шматки (фіксовані обсяги даних, зазвичай називаються блоками); і ці шматки записуються на диски і прочитуються з них паралельно. З погляду швидкодії це означає дві основні переваги:

- підвищується пропускна спроможність послідовного вводу/виводу за рахунок одночасного завантаження кількох інтерфейсів.

- знижується латентність випадкового доступу; декілька запитів до різних невеликих сегментів інформації можуть виконатися одночасно.

Недолік:

- рівень RAID 0 призначений виключно для підвищення швидкодії, і не забезпечує надмірності даних. Тому будь-які дискові збої вимагають відновлення інформації з резервних носіїв.

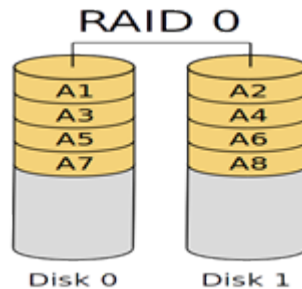


Рисунок 1 - RAID рівень 0

### RAID рівня 1

Технологія RAID 1 також відома як віддзеркалювання (англ. disk mirroring). В цьому випадку, копії кожного шматка інформації зберігаються на окремому диску; або, зазвичай кожен (використовуваний) диск має «двійника», який зберігає точну копію цього диска. Якщо відбувається збій одного з основних дисків, то він підмінюється своїм «двійником». Продуктивність довільного читання може бути покращена, якщо для читання інформації використовуватиметься той з «двійників», головка якого розташована ближче до необхідного блоку.

Час запису може бути дещо більшим, ніж для одного диска, залежно від стратегії запису: запис на два диски може проводитися або в паралель (для швидкості), або строго послідовно (для надійності).

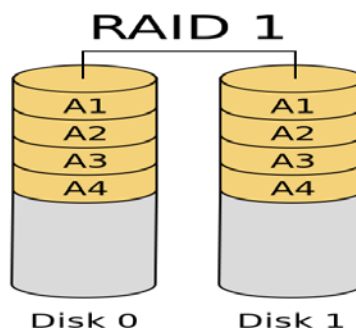


Рисунок 2 - RAID рівень 1

Рівень RAID 1 добре підходить для застосунків, які вимагають високої надійності, низької латентності при читанні, а також якщо не потрібна мінімізація вартості. RAID 1 забезпечує надмірність зберігання інформації, але у будь-якому випадку слід підтримувати резервну копію даних, оскільки це єдиний спосіб відновити випадково видалені файли або директорії.

### RAID рівнів 2 і 3

Технологія RAID рівнів 2 і 3 передбачає паралельну («в унісон») роботу всіх дисків. Ця архітектура вимагає зберігання бітів парності для кожного елементу інформації, що розподіляється по дисках. Відмінність RAID 3 від RAID 2 полягає тільки в тому, що RAID 2 використовує для зберігання бітів парності кількох дисків, тоді як RAID 3 використовує тільки один. RAID 2 використовується у край рідко.

Якщо відбувається збій одного диска з даними, то система може відновити його вміст по вмісту решти дисків з даними і диска з інформацією парності.

Продуктивність в цьому випадку дуже велика для великих обсягів інформації, але може бути вельми скромною для малих обсягів, оскільки неможливе читання декількох невеликих сегментів інформації, що перекривається.

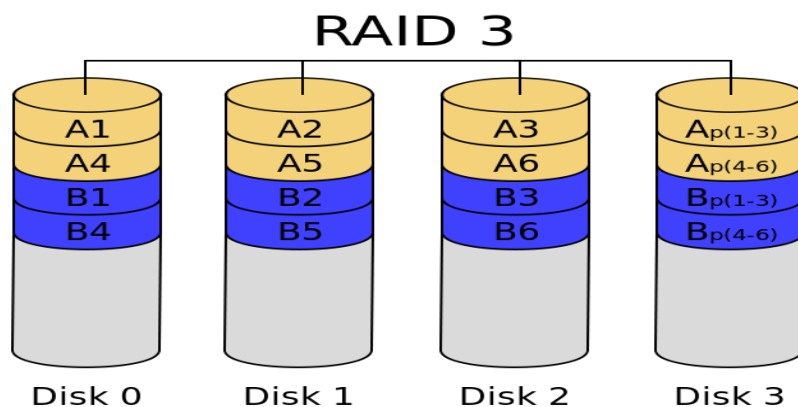


Рисунок 3 - RAID рівень 3

### RAID рівнів 4 і 5

RAID 4 виправляє деякі недоліки технології RAID 3 за рахунок використання великих сегментів інформації, що розподіляються по всіх дисках, за винятком диска з інформацією парності. При цьому для невеликих обсягів інформації

використовується тільки диск, на якому знаходиться потрібна інформація. Це означає, що можливе одночасного виконання декількох запитів на читання. Проте запити на запис породжують блокування при записі інформації парності.

RAID 4 використовується вкрай рідко.

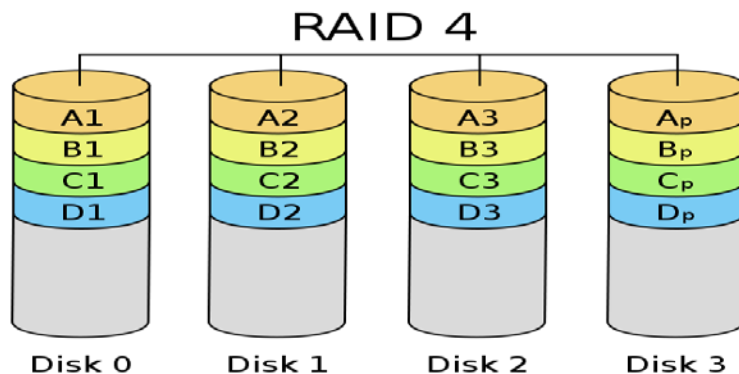


Рисунок 4 - RAID рівень 4

Технологія RAID 5 дуже схожа на RAID 4, але усуває пов'язані з нею блокування. Відмінність полягає в тому, що інформація парності розподіляється по усіх дисках масиву. В даному випадку можливі як одночасні операції читання, так і запису.

Дана технологія добре підходить для застосунків, які працюють з невеликими обсягами даних, наприклад, для систем обробки транзакцій.

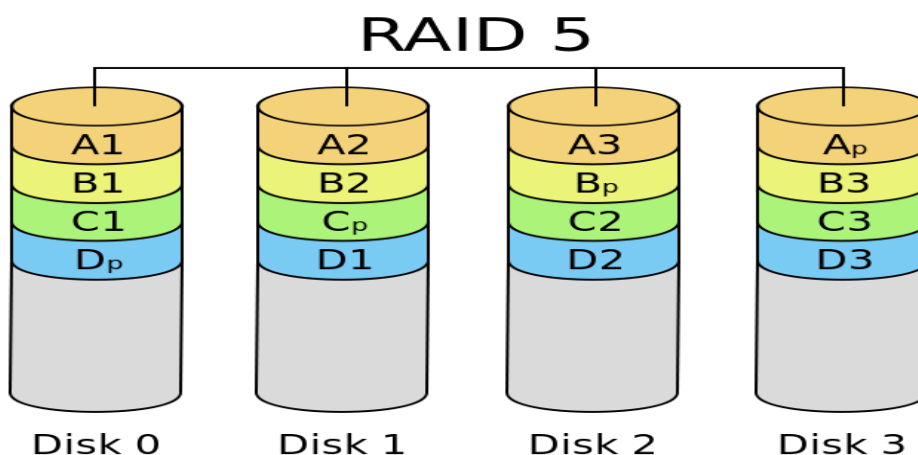


Рисунок 5 - RAID рівень 5

## Переваги і вади рівнів RAID

Рівні RAID	Механізм забезпечення надійності	Ефективна місткість масиву	Продуктивність	Область застосування
0	-	100%	Висока	Застосування без істотних вимог до надійності
1	Віддзеркалювання	50%	Висока або середня	Застосування без істотних вимог до вартості
3	Парність	80%	Середня	Застосування для роботи з великим обсягом даних (графік, CAD/CAM тощо)
5	Парність	80%	Середня	Застосунки, що працюють з великими обсягами даних(обробка транзакцій)
10	Віддзеркалювання групи RAID 0	50%	Висока або середня	Застосунки, що вимагають надійності RAID 1 з хорошою продуктивністю

### Комбіновані і додаткові рівні RAID

**RAID Levels 0+1 (Рівень 0+1):** Комбінація RAID 0 і RAID 1. Цей рівень забезпечує надмірність за рахунок віддзеркалювання.

**RAID Levels 10 (Рівень 10):** Комбінує (об'єднує) RAID 0 і RAID 1, тобто віддзеркалювання групи дисководів, об'єднаних в RAID 0 для забезпечення максимальної швидкодії. Цей рівень забезпечує надмірність за рахунок дзеркального відображення.

**RAID Levels 30 (Рівень 30):** Комбінує (об'єднує) RAID 0 і RAID 3, тобто використовується контрольна сума для групи дисководів, об'єднаних в RAID 0 для забезпечення максимальної швидкодії. Інформація про парність може використовуватися для відновлення даних.

**RAID Levels 50 (Рівень 50):** Комбінує (об'єднує) RAID 0 і RAID 5, тобто використовується переміщувана контрольна сума для групи дисководів, об'єднаних в RAID 0 для забезпечення максимальної швидкодії. Інформація про парність може використовуватися для відновлення даних.



## **ПРОГРАМИ ДЛЯ СТВОРЕННЯ БЕКАПУ**

### **AMANDA**

AMANDA (скорочено від англ. Advanced Maryland Automatic Network Disk Archiver) - ПЗ з відкритим вихідним кодом для архівування інформації, що володіє можливістю резервного копіювання даних, постійно зберігаються на безлічі комп'ютерів у комп'ютерній мережі.

Використовується клієнт-серверна модель, що включає наступні компоненти:

- сервер резервного копіювання і клієнта для нього;
- список серверів;
- індексує сервер.

Необов'язково, щоб всі три сервери були запущені на одному комп'ютері.

Amanda була розроблена в Мерілендському університеті в Коледж-Парку під ліцензією схожою на ліцензію BSD. Доступна як у безкоштовній версії розроблюваної співтовариством, так і в корпоративній версії з повною технічною підтримкою. Amanda працює майже на будь-якій UNIX-подібній системі, відключаючи Linux системі, а в Microsoft Windows і Windows NT може працювати за допомогою Samba або Cygwin.

Amanda підтримує резервне копіювання на магнітну стрічку і жорсткі диски, а також на деякі інші пристрої зберігання даних.

### **ARECA BACKUP**

Areca Backup програма для створення резервного копіювання розроблена на Java. Випущена під вільною ліцензією GNU.

Areca Backup включає в себе ядро резервного копіювання, а також графічний інтерфейс користувача і інтерфейс командного рядка.

Додатково включає в себе наступні можливості:

- стиснення ZIP/ZIP64;
- AES 128 і AES 256 шифрування;
- резервне копіювання з використанням фільтрів (з розширення, підкаталог, регулярними виразами, розміром, датою, статусу, використання);

- інкрементне резервне копіювання, диференціальне та повне резервне копіювання;

- дельта резервного копіювання (зберігатимуться тільки модифіковані частини файлів, не цілі файли);

- архіви злиття;

- стан на відновлення датою;

- Unix права доступу до файлів резервного копіювання / відновлення;

- Звіти E – Mail;

- моделювання резервного копіювання;

- FTP і HTTPS підтримка (SSL / TLS в обох явних і неявних режимах);

- Підтримка SFTP (з паролем або перевірці автентичності сертифікатів)

Agese також надає всі інструменти, необхідні для обробки архівів:

- Backup;

- Відновлення архівів (із або без віддалених файлів); цілі архіви або окремі файли можуть бути легко відновлені;

- Злиття архівів: суміжні додаткові архіви можуть бути об'єднані в єдиний архів для економії дискового простору;

- Видалення архівів;

- History Explorer: різні версії даного файлу можуть бути переглянуті і відновлені;

- Дослідник архівів: файли можуть бути знайдені серед ваших архівів.

Режим зберігання Agese може обробляти декілька режимів:

- Стандарт: Це режим за замовчуванням, який рекомендується для більшості користувачів: Якщо ви виберете цей режим зберігання, новий архів буде створений для кожної резервної копії. Всі нові або змінені файли з моменту останнього резервного копіювання, будуть зберігатися в цьому архіві.

- Дельта: Цей режим рекомендується тільки для досвідчених користувачів: Якщо ви виберете цей режим зберігання, новий архів буде створений для кожної резервної копії. Всі зміни \* частини \* файлів з моменту останнього резервного копіювання, будуть зберігатися в цьому архіві. Цей режим особливо корисний, для великих файлів.

- **Зображення:** Якщо ви виберете цей режим зберігання, унікальний архів буде створений і оновлюється при кожному резервному копіюванні.

Резервне копіювання Агеса може обробляти такі типи резервних копій:

- **Повне резервне копіювання:** Коли повне резервне копіювання виконується, всі файли зберігаються у вашому архіві (чи були вони змінені чи ні).

- **Інкрементне резервне копіювання:** При додатковому резервному копіюванню копіюються тільки файли, які були змінені з моменту останнього резервного копіювання збереженому у вашому архіві.

- **Диференціальне резервне копіювання:** При додатковому резервному копіюванню копіюються тільки файли, які були змінені з моменту останнього повного резервного копіювання збереженому у вашому архіві.

Агеса використовує розмір файлу і час останньої зміни для виявлення змінених файлів. Якщо один з цих атрибутів змінюється (незалежно від його значення), файл позначається як зміна. Це дозволяє швидко виявлення змінених файлів.

Агеса підтримує такі OS: Linux і Windows 2000/Windows XP і Windows 7. Але вона також може працювати на будь-якій іншій операційній системі, за умови, що Java Runtime Environment була встановлена (версія 1.4.2 або пізнішої версії). Підтримує такі мови: китайська (спрощена), китайська (традиційна), чеська, данська, голландська, англійська, французька, німецька, угорська, італійська, японська, російська, іспанська, шведська.

## **Déjà Dup**

Déjà Dup це простий інструмент резервного копіювання. Він приховує складність резервного копіювання Right Way (в зашифрованому вигляді, of-line копіювання, і регулярне копіювання) і використовує подвійність в бекапі.

Особливості:

- Підтримка місцевих, віддалених або хмарних сховищах архівів, таких як Amazon S3, Rackspace Cloud Files, і Ubuntu One;

- Надійно шифрує і стискає дані;

- Поетапно резервне копіювання, що дозволяє відновити з будь-якої конкретної резервної копії;
- Розклад регулярного резервного копіювання;
- Добре інтегрується робочому столі GNOME.

### **Clonezilla Live**

Clonezilla Live невелика завантажувальна програма GNU/Linux для x86/amd64 (x86 - 64). Clonezilla SE ( Server Edition ) була розроблена в 2004 році, і вона використовується для розгортання багато комп'ютерів одночасно. Це надзвичайно корисний інструмент, однак, у нього є ряд обмежень. Для того, щоб використовувати його, необхідно спочатку підготувати сервер DRBL і машини, які будуть розгорнуті для цього потрібно завантажити з мережі (наприклад PXE / iPXE ). Щоб подолати ці обмеження, об'єднали Debian Live з Clonezilla як "Clonezilla Live", яке може бути легко використане для зображення і клонування окремої машини. Основна перевага Clonezilla Live, в тому, що вона усуває необхідність створення сервера DRBL і необхідність комп'ютеру розгортається для завантаження з мережі. Clonezilla Онлайн можна використовувати для зображення або клонів окремих комп'ютерів за допомогою CD/DVD або USB флеш-диску. Хоча розмір обмежується ємністю завантажувального носія, це проблема може бути усунена за допомогою мережевої файлової системи, наприклад SSHFS або SAMBA.

### **Forensic-system**

Створення образу (dump) пам'яті комп'ютера (RAM). Створення копії RAM пам'яті у файл.

При дослідженні інформаційних інцидентів, експерти іноді стикаються з тим, що паролі та іншу інформацію, необхідну для успішної аутентифікації або ідентифікації не доступні у відкритому вигляді і зберігається в пам'яті.

При виключенні комп'ютера така інформація може бути втрачена назавжди ...  
Але все ще є шанс отримати його.

При перезавантаженні операційної системи за допомогою комбінації Ctrl-Alt-Del (так зване "м'яке перезавантаження»), комп'ютер не проводить ретельне

очищення оперативної пам'яті, а ймовірність втрати інформації прагнули значно зменшуватися, і, таким чином, збільшує шанс отримати його.

Просто, щоб створити образ (dump) оперативної пам'яті при перезавантаженні операційної системи і розподіл призначений. З його допомогою можна створити точний образ (dump) пам'яті, крім 115 МБ оперативної пам'яті, які повинні прийняти, що розподіл при завантаженні.

Отримане зображення (dump) оперативної пам'яті можна записати на зовнішній носій і подальшого аналізу його вмісту як індивідуальному порядку і в вимірній Ubuntu CyberPack (WCP).

**Судова-спеціалізована система**, призначена для фіксації і цифрових доказів у розслідуванні комп'ютерних злочинів.

Вона включає в себе інструменти для криміналістичного аналізу первинних операцій, таких як:

- Пошук, фіксування прихованих і видалених даних на носії;
- Збору доказів про використання ПК для вчинення злочинів;
- Аналіз і запис злочинів (логування всіх дій в рамках обстеження з перевіркою аналізу даних або досліджень);
- видалення цифрових копій об'єктів дослідження для подальшого детального аналізу за допомогою інструментів Ubuntu CyberPack (WCP)

Об'єктами цих дій можуть бути: засоби масової інформації даних (і їх вміст, такі як файли або розділи), веб-ресурси, мережевий трафік і так далі.

Основні властивості системи

- Система працює тільки в Live - режимі без можливості установки
- Підтримує більшість файлових систем : Ext2/3/4 , NTFS , FAT/32 , VFAT , EXFAT , XFS , Vtrfs , UFS , ReiserFS / 4 , HFS / + , ZFS і т.д.
- Виявляє і дозволяє працювати з розділами : RAID , LVM і т.д.
- Випробувальний пристрій встановлюється за умовчанням в " тільки для читання" , ви можете переключитися на запис
- Побудований на легкій графічній середі LXDE . Включені мови: російська , українська, англійська

- Дозволяє переглядати і прослуховувати контент (документи , мультимедійні файли)
- Включає зруйновані файли диска для аналізу

## **FBackup**

FBackup — це безкоштовна програма для резервного копіювання. Її особливість у тому, що її можна вільно використовувати не тільки в особистих, а й у комерційних цілях. FBackup підтримує виконання завдань резервного копіювання в ручному і автоматичному режимах. Копії можуть зберігатися на зовнішні накопичувачі USB або Firewire або на мережеві диски, з можливістю стиснення в ZIP. Перед виконанням завдання або після нього FBackup може виконувати різні дії.

Основні можливості FBackup:

- Легкий у використанні, має інтуїтивно зрозумілий інтерфейс.
- Налаштування дій до і після резервного копіювання.
- Автоматичні поновлення.
- Плагіни для резервування і відновлення налаштувань певних програм і їх спеціальних даних.
- Архівування відкритих файлів.
- Багатомовність інтерфейсу.
- Дзеркальне дублювання.
- Архівування результатів бекапу. є можливість захистити збережені копії паролем.

## **BackupPC**

BackupPC - вільне ПЗ (розповсюджується під GNU General Public License) для резервного копіювання даних з керуванням через веб-інтерфейс. Багатофункціональний програмний сервер може працювати на будь-якому сервері під управлінням GNU / Linux, Solaris або UNIX. Немає необхідності в клієнтській частині, так як сервер сам по собі є клієнтом для декількох протоколів, які підтримуються рідними службами клієнтської ОС.

Наприклад, BackupPC є SMB - клієнтом, що може використовуватися для резервного копіювання спільно використовуваних даних в мережевих папках на комп'ютерах з Microsoft Windows. Подібний сервер BackupPC може бути встановлений за міжмережевим екраном , який виконує функції мережевий трансляції адрес (NAT ), коли Windows -комп'ютер має публічний IP адресу. Так як це не рекомендується через велику кількість SMB трафіку , то більш зручним є використання веб- серверів, що підтримують SSH і можливість роботи з tar і rsync , що дозволяє серверу BackupPC перебувати в підмережі відокремленої від веб-серверів демілітаризованою зоною.

На клієнтських комп'ютерах необхідна тільки мінімальна конфігурація, коли проводиться резервне копіювання системи, що підтримує SSH спочатку. Вибір між tar і rsync диктується апаратним забезпеченням і шириною смуги пропускання каналу передачі даних на стороні клієнта. Використання rsync вимагає більшої кількості процесорного часу, в той час як використання SMB і tar вимагає більшої ширини каналу передачі даних.

Особливості:

- Немає необхідності в клієнтській частині;
- Не можна вибрати час для початку копіювання, можна тільки вказати, коли його небажано робити (параметр BlackoutPeriods).

### **DIBS (Distributed internet backup system).**

DIBS (Distributed Internet Backup System) - система резервного копіювання даних шляхом обміну ними між комп'ютерами в Інтернеті. Використовується принцип пірінгових мереж.

Метою проекту є надання простої у використанні, безпечної і надійної системи резервного копіювання. Філософія DIBS заснована на відносній дешевизні дискового простору, а гасло на сайті проекту говорить: «Резервне копіювання теж має бути дешевим».

Віддзеркалення даних шляхом додавання в комп'ютер більшої кількості запам'ятовувальних пристроїв не є абсолютно надійним, так як пожежа, повінь, стрибок напруги і інші події можуть знищити дані, що зберігаються локально на

одному комп'ютері. DIBS пересилає дані з одного комп'ютера на інший (і навпаки), так що в разі катастрофи, дані можна буде відновити, взявши їх з уцілілих комп'ютерів.

DIBS є системою резервного копіювання, а не файлообмінною системою начебто Napster або Gnutella. DIBS автоматично шифрує всі передані дані, тому комп'ютер, на якому знаходяться ваші дані, не має до них доступу.

## **ХІД РОБОТИ**

Можливості резервного копіювання та відновлення в Windows 10.

Windows 10 обладнано безліччю різних інструментів резервного копіювання. Крім того, що Microsoft повернув старий інструмент відновлення системи (Windows Backup), який свого часу прибрали з Windows 8.1, в ньому також присутній інструмент Історія файлів (File History).

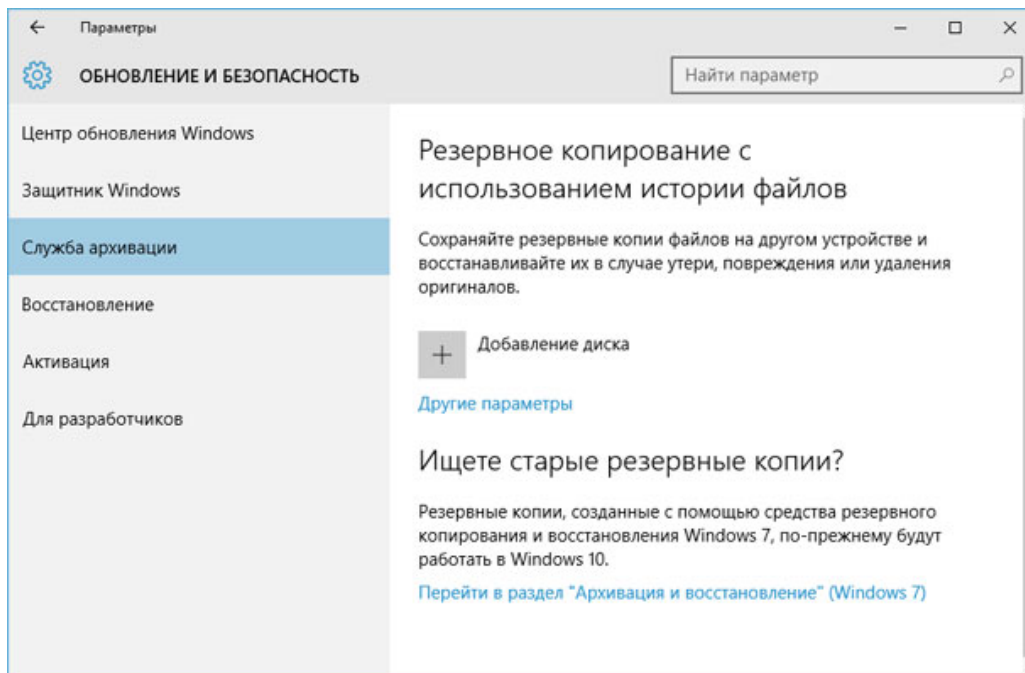
Остання версія Windows також має можливість резервного копіювання образу системи (функція «Резервна копія образу системи»), повернення комп'ютера до налаштувань за замовчуванням, збереження файлів онлайн, а також створювати диски відновлення, які можна використовувати у разі надзвичайної ситуації.

### **Історія файлів**

Історія файлів, яку було введено в Windows 8, не зникла і в Windows 10. Це ще й рекомендований спосіб відновлення. Ось чому Історія файлів інтегрована і в новий додаток «Налаштування», і в стару Панель керування. У той час як Резервне копіювання та відновлення (Windows 7) присутнє тільки в Панелі керування. Ця функція більш обмежена, і вона робить резервні копії тільки файлів з бібліотеки вашого, призначеного для користувача, акаунта. Якщо вам знадобиться відновити документи, які зберігалися в інших папках то знадобиться створити ці папки в Провіднику і додати їх до бібліотек або створити нові бібліотеки.

Після того як це буде зроблено, Windows зможе автоматично створювати резервні копії файлів. Це може бути корисним для відновлення всіх коли-небудь втрачених файлів, відновлення якогось одного файлу або відкату файлу до старої версії.



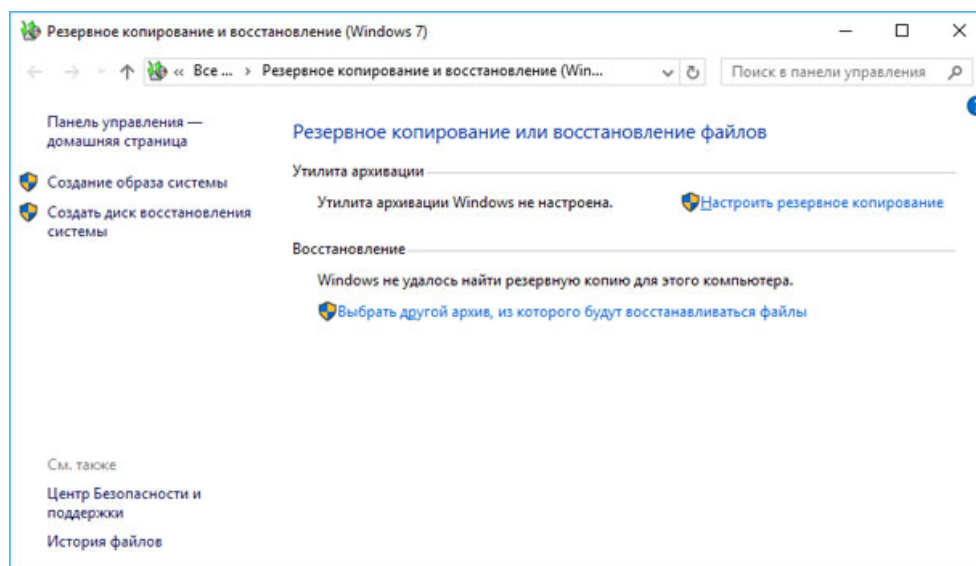


## Резервне копіювання та відновлення системи

Microsoft додав стару функцію резервних копій та відновлення з Windows 7. Вона застаріла в Windows 8, і була видалена з Windows 8.1, але тепер її знову повернули. Також вона відома як «Windows Backup».

Цей інструмент допоможе відновити будь-яку резервну копію Windows 7 на вашій Windows 10. Але також її можна використовувати для відновлення комп'ютера з Windows 10. На відміну від Історії файлів, за допомогою Windows Backup можна набагато простіше створити резервну копію практично всього на жорсткому диску.

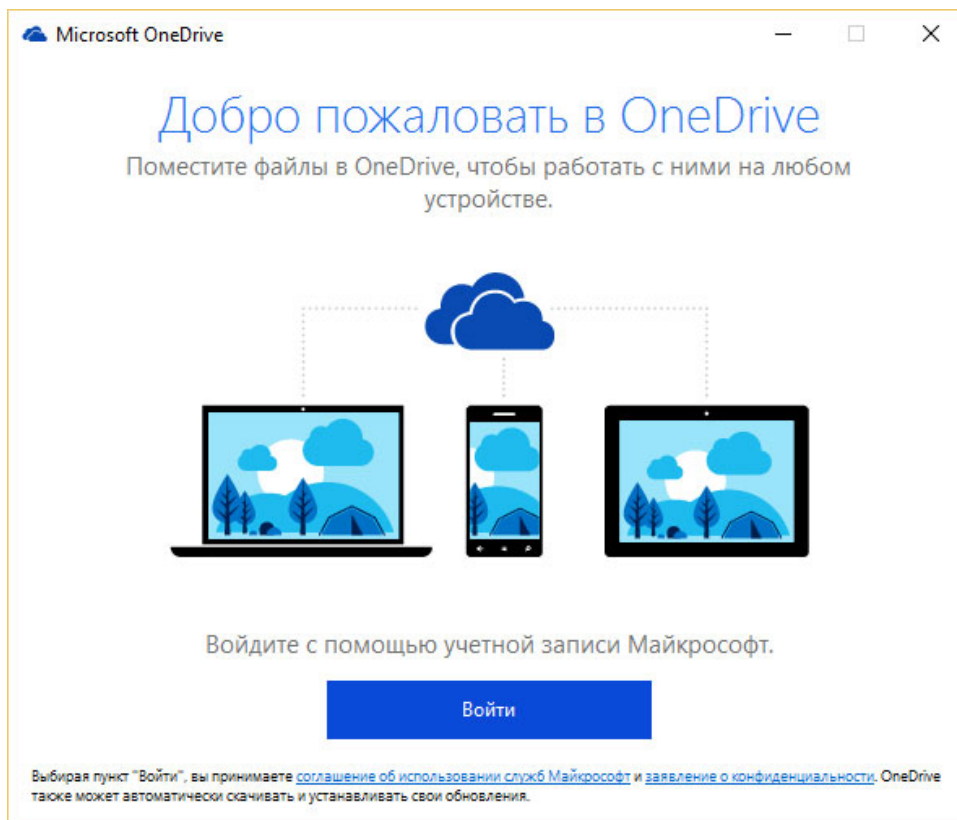
Цей інструмент можна знайти в Панелі керування, в розділі Відновлення. Однак резервне копіювання не дає 100% захисту від втрати даних.



## OneDrive

У традиційному розумінні, OneDrive не є справжнім засобом відновлення, але на даний момент він повністю інтегрований в Windows. Збережені в OneDrive файли, буде збережено в ваш акаунт користувача OneDrive, і ви зможете користуватися даними файлами з будь-якого іншого пристрою.

Навіть якщо ви перевстановите Windows або будете використовувати Windows на іншому пристрої, вам просто необхідно увійти в ваш Microsoft акаунт і всі ваші файли, які були раніше збережені в OneDrive, будуть вам доступні.

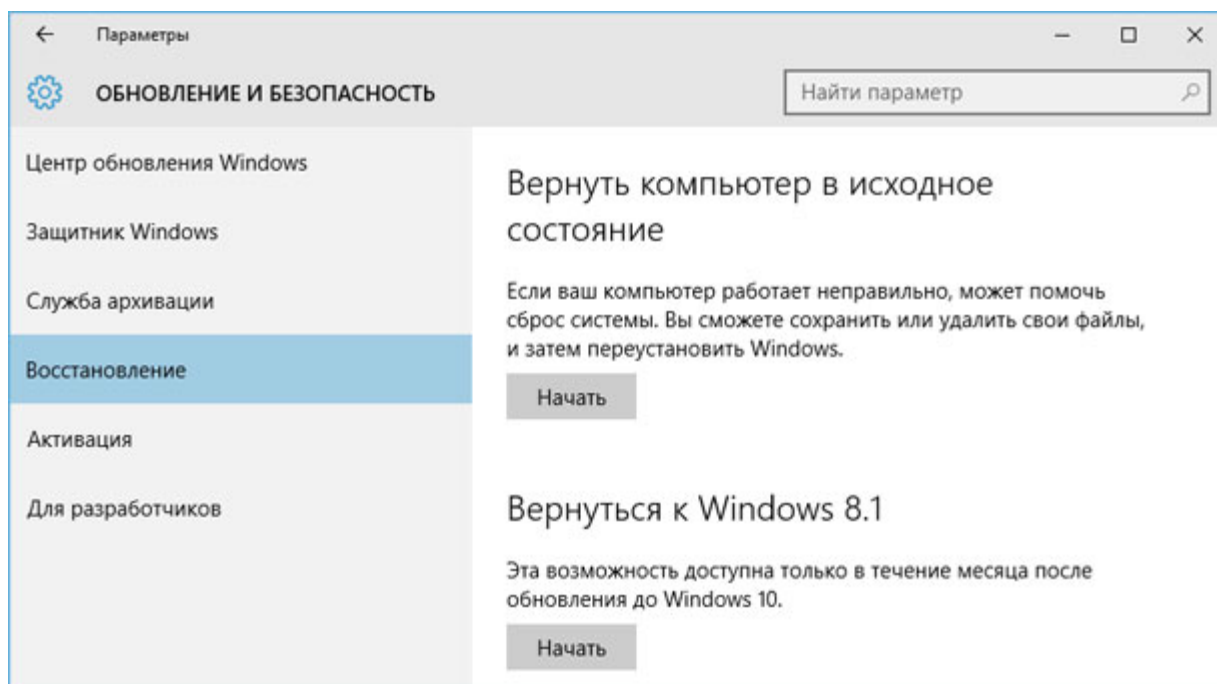


## Відновлення до початкового стану ПК

Замість того, щоб покладатися на резервну копію образу системи, більшість людей вважає за краще використовувати функцію «Відновлення до початкового стану ПК», з метою відновлення заводських налаштувань системи. Це також дає можливість забути про таке явище як перевстановлення Windows з використанням завантажувального диска або USB пристрою – просто ставимо завдання Windows повернути комп'ютер в початковий стан, і він повертається до «заводських» налаштувань.

В Windows 8 було дві опції: Оновити комп'ютер і Повернути комп'ютер в початковий стан. В Windows 10 присутня тільки опція «Відновлення до початкового стану ПК».

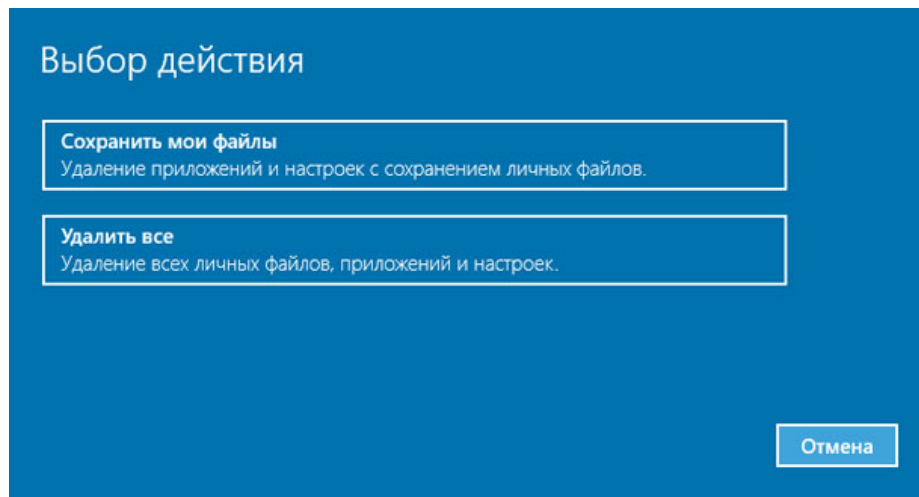
Відкриваємо інструмент Настройки, вибираємо Оновлення та захист, далі – Відновлення і натискаємо Почати, під розділом Відновлення до початкового стану ПК.



Пропонується Вибір параметра: Зберегти мої файли або Видалити все.

В даному випадку до вибору дії необхідно підійти з повною відповідальністю. Якщо вибрати функцію Видалити все, то одночасно з вашими програмами і налаштуваннями також буде видалено облікові записи користувачів і, що найголовніше – особисті файли.

Звичайно ж, це стосується тільки диска на якому встановлено Windows (як правило диск С). Але на диску С знаходяться файли з Робочого столу, а також папки Документи, Завантаження, Зображення, Відео, Музика та ін.



Повернути видалені таким чином файли, стандартними засобами Windows вже не вийде. Хоча цілком можливо за допомогою спеціалізованих програм для відновлення даних.

Однією з таких програм є Hetman Partition Recovery – це універсальний інструмент, який використовують фахівці з відновлення даних. Він аналізує жорсткий диск на предмет наявності сигнатур файлів і частин файлової системи. Такі шматочки будуть виявлені і додані в список доступних для відновлення томів.

Перше і найважливіше, вимкніть комп'ютер і вийміть диск. Вам не потрібно запускати Windows на тому ж диску, з якого необхідно відновити файли. Цей диск необхідно підключити до іншого комп'ютера як додатковий, і просканувати за допомогою програми.

### **Резервна копія образу системи**

Microsoft прибрав функцію створення резервних копій образу системи в початкових версіях Windows 8.1, але на численні прохання користувачів дану функцію повернули. В Windows 10 вона також присутня.

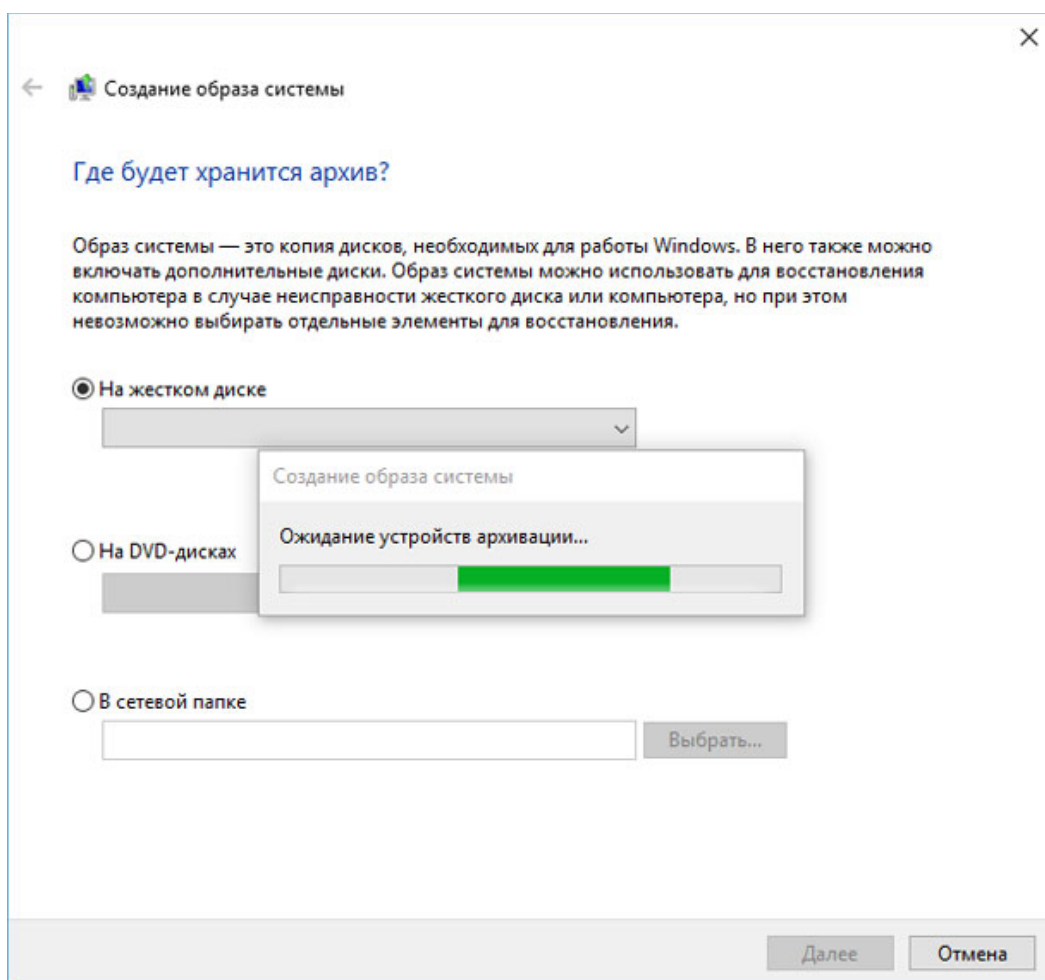
Її можна знайти в панелі Резервне копіювання та відновлення (Windows 7). Просто клікніть «Створити образ системи» в лівій частині вікна, або відкрийте панель Історія файлів і виберіть «Образ системи».

На відміну від інших рішень, ця функція дозволяє створити повний образ вашої поточної системи Windows, включаючи операційну систему, встановлені програми, настройки та файли користувача. Ця резервна копія може бути збережена

на зовнішній жорсткий диск, на декілька DVD-дисків або на мережевому ресурсі. І якщо вам коли-небудь знадобиться відновити комп'ютер, то можна буде зробити це розгорнувши збережений раніше бекап.

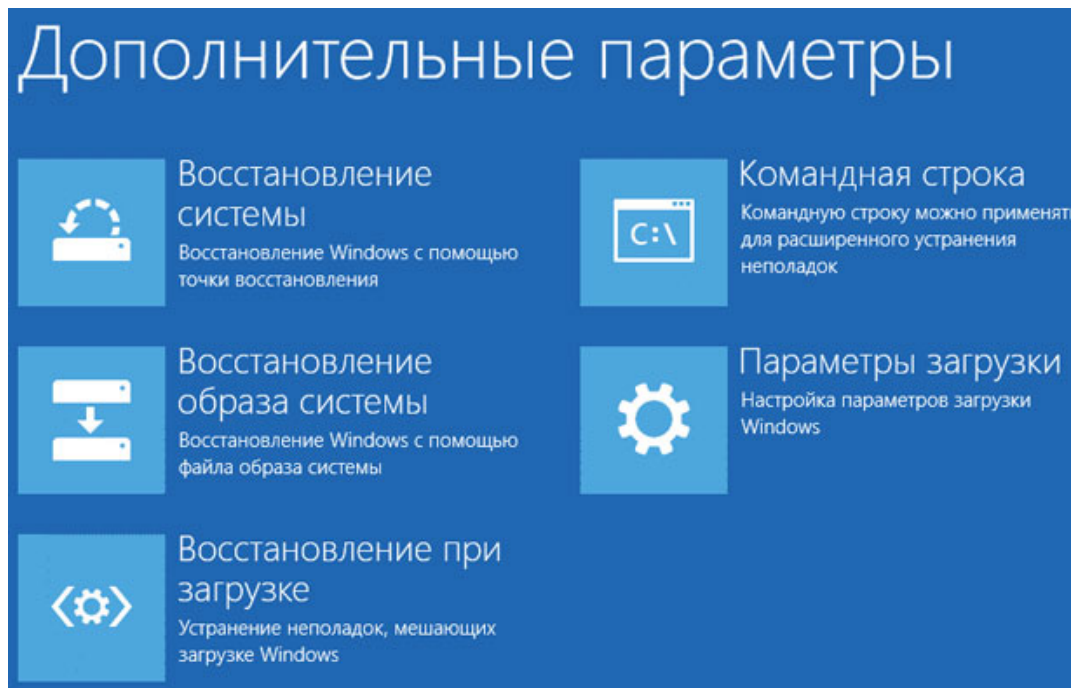
Насправді ж, більшість людей не використовує дану функцію. Можна також повернути операційну систему до початкового стану використовуючи функцію повернення комп'ютера до початкового стану та відновлення окремих файлів, перевстановити вручну всі програми. В такому випадку, резервні копії будуть набагато меншого розміру, і можна налаштувати їх регулярне автоматичне створення.

Але така функція існує і користується популярністю. І якщо необхідно створити образ системи, то не обов'язково для цього використовувати сторонні додатки.



## Додаткові варіанти запуску

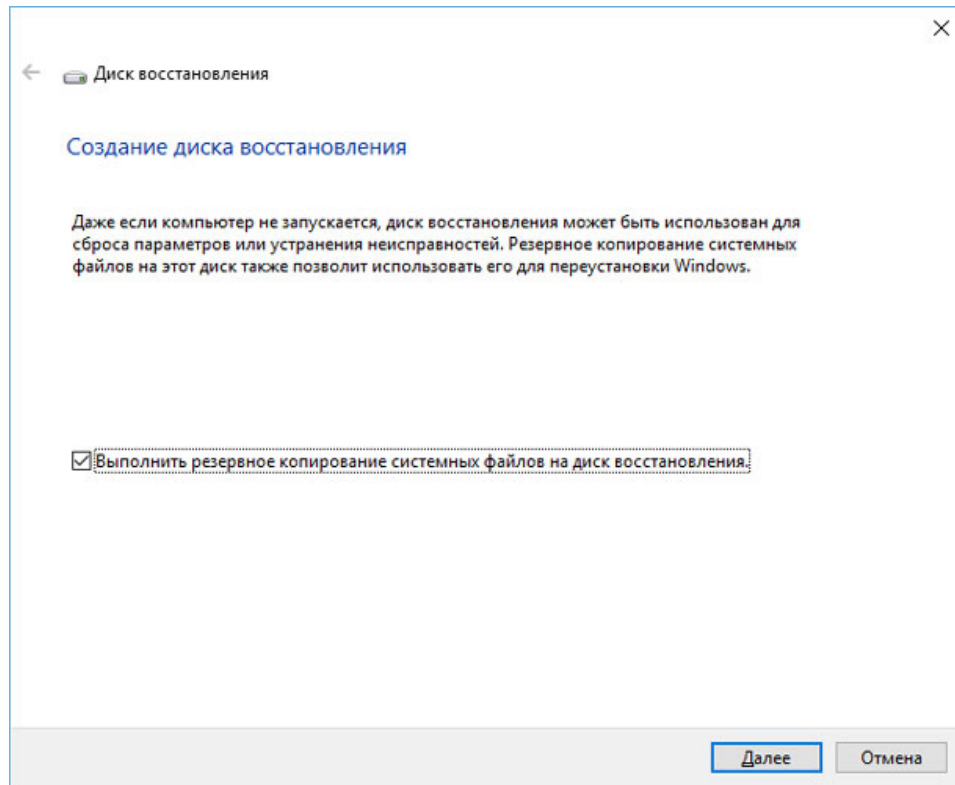
Додаткові варіанти запуску Windows 10 працюють таким же чином, як і в Windows 8. Щоб отримати до них доступ, відкрийте додаток Настройки, виберіть Оновлення та захист, далі Відновлення, і в підменю Додаткові варіанти запуску натисніть Перезавантажити зараз. Також можна скористатися цією функцією натиснувши «Перезавантажити» з утриманням клавіші Shift, в меню Пуск.



## Диск відновлення Windows

Можна створити USB-диск відновлення, який надасть доступ до Додаткових варіантів запуску, навіть якщо установку Windows 10 повністю пошкоджено і у вас немає доступу до цього меню.

Щоб створити його, відкрийте Панель керування та виберіть «Відновлення», і ви побачите список інструментів для відновлення.



Для створення USB-диска відновлення, клікніть «Створити диск відновлення». Для доступу до даного інструменту безпосередньо, можна відкрити меню Пуск та набрати RecoveryDrive.exe і натиснути Enter.

У Windows 10 більше немає окремого розділу для відновлення. Отже, цей інструмент більше не дозволить видалити розділ відновлення з комп'ютера. Він більше не потрібен, за замовчуванням користуємося вільним місцем на диску.

Windows 10 включає в себе й інші функції для усунення неполадок, які були доступні в попередніх версіях Windows. Якщо ваш комп'ютер працює нестабільно, можете використовувати функцію відновлення системи для повернення її до працездатного стану. Для тих користувачів, які не скористалися стандартними можливостями Windows буде корисна програма для відновлення видалених з жорсткого диска даних.

Передивитись відеоінструкції:

[https://hetmanrecovery.com/uk/recovery\\_news/backup-and-recovery-in-windows-10.htm](https://hetmanrecovery.com/uk/recovery_news/backup-and-recovery-in-windows-10.htm)

## **Контрольні питання:**

1. Назвіть основні програми створення резервних копій та їх переваги.
2. Які існують типи проблем, що призводять до втрати даних.
3. Назвати основні причини виникнення логічної втрати даних.
4. Назвати основні принципи створення резервних копій.
5. Розписати, які режими відновлення даних існують, в чому суть кожного з них, коли краще використовувати той чи інший.
6. Описати принцип створення та відновлення даних в ОС Windows.