Bezpieczeństwo
Sieci Komputerowych

Część 5.
Fizyczne i środowiskowe
zagrożenia bezpieczeństwa danych

Praktyczny Pedagog

Bezpieczeństwo Sieci Komputerowych

PROGRAM ZAJĘĆ cz. 5

Przyczyny oraz skutki utraty danych.
Fizyczna ochrona danych.
Systemy podtrzymywania zasilania.
System tworzenia kopii zapasowych.
Narzędzia do tworzenia kopii zapasowych.
Odzyskiwanie danych.
Narzędzia do odzyskiwania danych.
Usuwanie danych.
Narzędzia do usuwania danych.
Zestawy narzędzi na płytach „Live CD" na przykładzie Hiren's boot CD

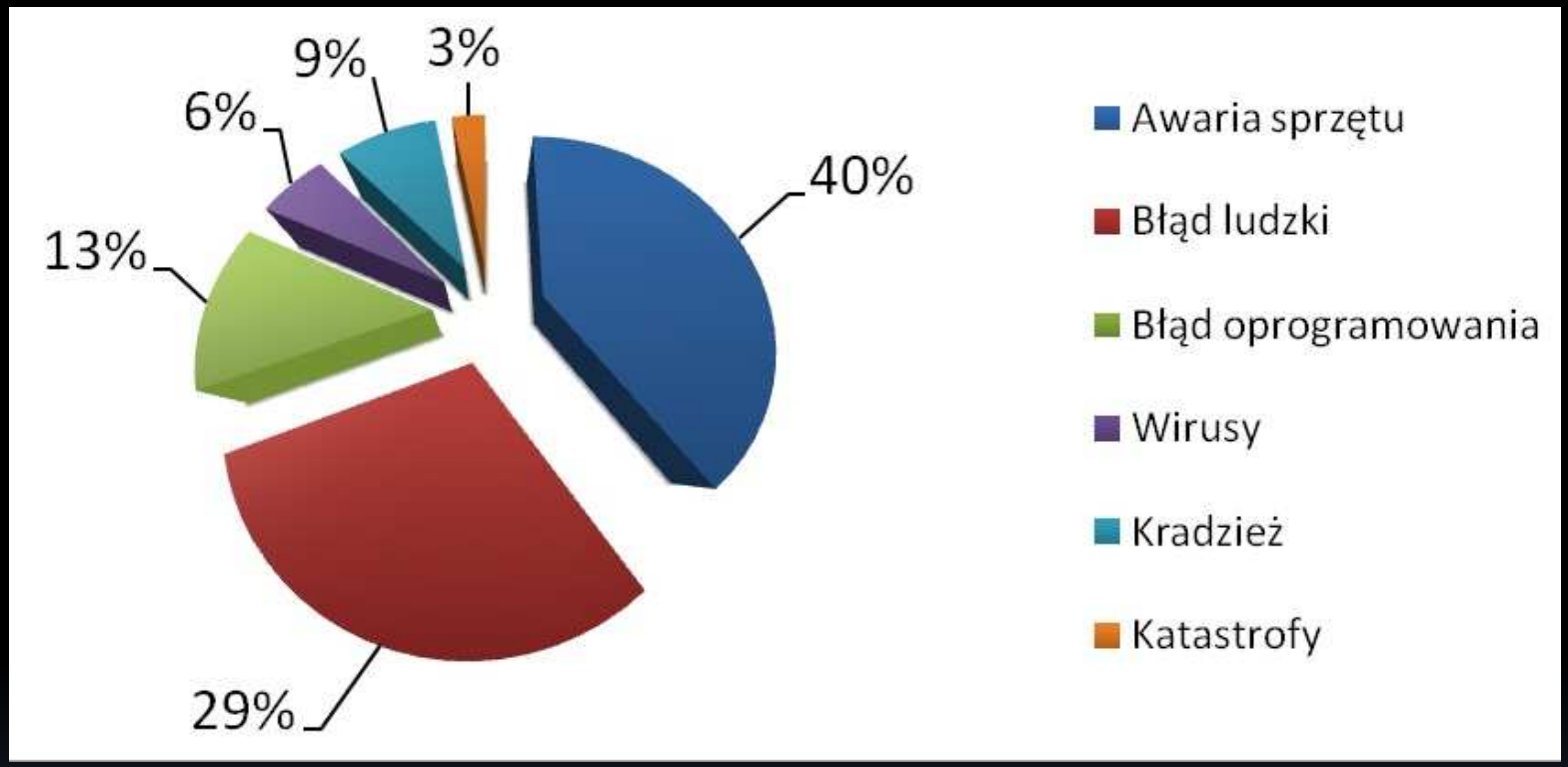
Przyczyny utraty danych

Na zgromadzone w komputerach informacje czyha wiele niebezpieczeństw. Wśród powodów prowadzących do utraty danych należy wymienić:*

- awarie sprzętu, głównie uszkodzenia dysków twardych i problemy z zasilaniem, a także błędy pamięci,
- pomyłki ludzkie, np. przypadkowe usunięcie pliku lub sformatowanie dysku,
- błędne działanie programów, systemów operacyjnych, które prowadzi do utraty niezapisanych informacji, zamazania danych lub uszkodzeń logicznych w strukturze plików,
- kradzież komputerów, laptopów, celowe niszczenie danych,
- wirusy i inne złośliwe programy,
- zniszczenia sprzętu spowodowane katastrofami naturalnymi, takimi jak pożar, powódź,
- wyładowania atmosferyczne.

*wg Michał Malinowski, „System ciagłej ochrony danych", UW 2006

Przyczyny utraty danych



David M. Smith, The Cost of Lost Data, http://gbr.pepperdine.edu/033/dataloss.html

Przyczyny utraty danych

Dane mogą zostać zniszczone poprzez niefrasobliwość administratora lub też poprzez atak wirusów lub hackera. Większość włamań do systemów komputerowych oraz spowodowanych nimi zniszczeń jest dokonywana poprzez pracownika z firmy, a nie poprzez atak osoby z zewnątrz.

Awarie zasilania i sprzętu stanowią realne zagrożenie utraty danych, ponieważ nikt nie wymyślił jeszcze absolutnie niezawodnego urządzenia. Aż 98% awarii sprzętu dotyczy uszkodzenia dysków twardych serwerów, których teoretyczna bezawaryjna praca została określona na 5-7 lat, a których okres żywotności ulega znacznemu skróceniu poprzez ich niewłaściwą eksploatację.

Przyczyny utraty danych

Krótkie podsumowanie roku 2010 w statystykach:
*6% wszystkich firm w Europie padło ofiarą kradzieży poufnych danych firmowych (poprzez działanie hackera, szkodliwe oprogramowanie oraz **kradzież dysków bądź laptopów**)*
*12% wszystkich firm w Europie doznało szkód finansowych wskutek postaci utraty danych (głównym powodem była **awaria sprzętu**)**

*Badania przeprowadzone przez instytut unijny Eurostat – http://epp.eurostat.ec.europa.eu

Przyczyny utraty danych: awarie sprzętowe

Najczęściej spotykanymi przyczynami awarii sprzętu są uszkodzenia mechaniczne oraz kłopoty z chłodzeniem. Do usterek mechanicznych należy zaliczyć na przykład zużycie obrotowych części napędów i wentylatorów.

Innym stosunkowo często pojawiającym się problemem jest wadliwy styk elementów elektrycznych. Do takiej sytuacji może dojść w wyniku zanieczyszczenia lub korozji.

Przyczyny utraty danych: awarie sprzętowe

Kurz osadzający się wewnątrz komputera, a szczególnie na wentylatorze, może również znacząco obniżyć wydajność chłodzenia. Gdy wentylator przestanie poprawnie funkcjonować, podzespoły gwałtownie się zużywają i starzeją.

Film: How To Clean Lenovo G550 Laptop Fan.mp4

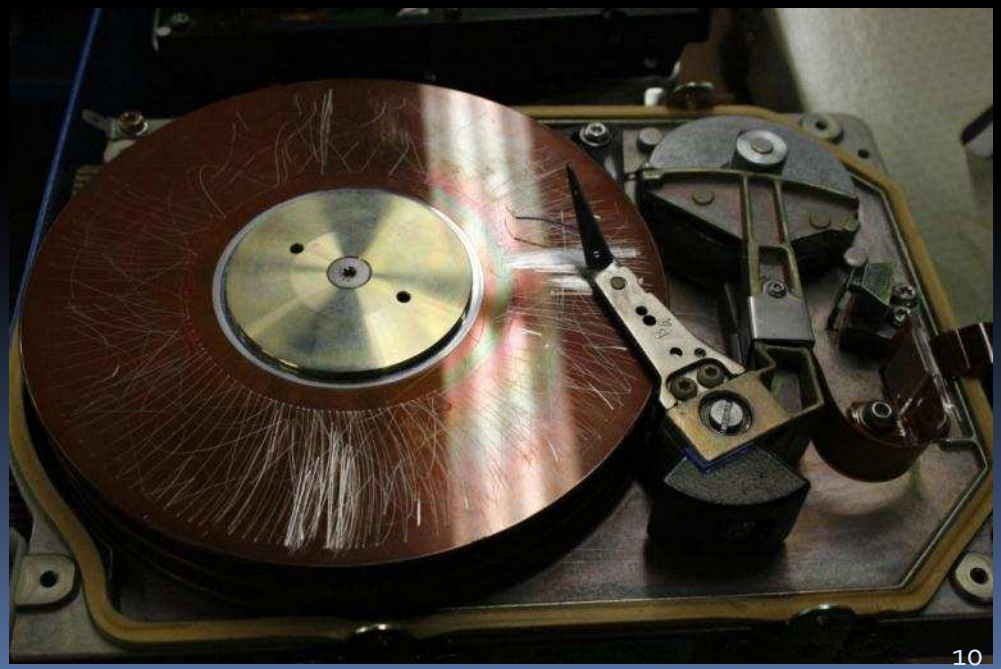
Przyczyny utraty danych: awarie sprzętowe

Dwukrotne zwiększenie temperatury otoczenia, w jakiej pracuje urządzenie, skutkuje skróceniem żywotności o połowę. Jeżeli komputery działają w nieklimatyzowanych pomieszczeniach, to pierwsze problemy z dyskami twardymi pojawią się prawdopodobnie już po dwóch latach użytkowania, a nawet szybciej.

Na zużycie podzespołów duży wpływ ma też ich rozmieszczenie w obudowie, np. ciasne ułożenie dysków twardych.

Przyczyny utraty danych: awarie sprzętowe

Dla danej serii dysków twardych na podstawie badań statystycznych można określić tzw. średni czas międzyawaryjny (ang. Mean Time Between Failure, w skrócie MTBF), mierzony w godzinach. Na podstawie tego parametru można obliczyć prawdopodobieństwo uszkodzenia nośnika w czasie roku użytkowania. Wartość MTBF podawana przez producentów nośników obecnie waha się zwykle pomiędzy 500.000 a 1.500.000, co przekłada się na dziesiątki lat. Okazuje się, że w praktyce dyski działają dużo krócej, głównie ze względu na nieodpowiednie ich użytkowanie.



Przyczyny utraty danych: awarie sprzętowe

Problemy z zasilaniem nie należą do rzadkości i są podstawową przyczyną logicznych usterek prowadzących do utraty danych. Nawet chwilowa przerwa w dostawie prądu może uniemożliwić zapisanie modyfikowanych plików na trwałym nośniku. Gdy użytkownik zleci zapis modyfikacji, zmiany nie są od razu nanoszone na dysk twardy. Najpierw trafiają do podręcznego bufora programu, potem do bufora dysku, a dopiero później są trwale zapisywane.
Awaria zasilania łatwo doprowadza do sytuacji, w której dane, pozornie zapisane, w rzeczywistości nigdy nie trafiają na dysk twardy. To wprowadza niespójność danych i powoduje ich utratę.

Przyczyny utraty danych: błędy ludzkie

Omyłkowe usunięcie pliku, czy tym bardziej sformatowanie dysku może doprowadzić do utraty cennych zasobów. Zdarza się także upuszczenie lub przypadkowe strącenie laptopa, na którym jego użytkownik przechowywał ważne informacje.

Brak doświadczenia, niewiedza oraz zaniedbanie ze strony użytkowników, w połączeniu z brakiem odpowiednich narzędzi oraz nadzoru ze strony administratorów stają się częstym powodem wystawiania systemów komputerowych na zagrożenia.

Duży wpływ na utratę dostępności danych ma część administratorów, którzy zaniedbują swe powinności, ignorując poszczególne zagrożenia oraz wykryte luki zabezpieczeń jak również nie stosując się do zasad i norm istniejących w polskich rozporządzeniach ministerialnych.

Przyczyny utraty danych: błędy oprogramowania

Nieprawidłowe wykonanie operacji przez program może doprowadzić do zamazania wcześniej zapisanych informacji lub pozostawić niespójne pliki na dysku. Zdarza się, że aplikacja nagle wykazuje brak interakcji z użytkownikiem, uniemożliwiając mu zapisanie modyfikowanego dokumentu. Błędy oprogramowania, szczególnie systemów operacyjnych, mogą prowadzić do zagubienia zawartości podręcznych buforów, wskutek czego użytkownik straci dane, których zapis zlecił chwilę wcześniej.

Skutki utraty danych

Utrata danych może poważnie utrudnić lub wręcz uniemożliwić prowadzenie działań biznesowych, powodując przestoje w pracy, ogólną dezorganizację, dotkliwe straty materialne, a w najgorszym przypadku doprowadzić nawet do bankructwa. Brak odpowiedniej polityki przywracania utraconych danych powoduje w sytuacji awaryjnej czasochłonne i kosztowne procesy powrotu działania firmy do stanu normalnego.

Skutki utraty danych

Straty ponoszone przez firmy, które nie wykonują regularnie backupu danych można oszacować. Większość przedsiębiorców utracone zasoby próbuje odzyskać, korzystając z pomocy specjalistycznych laboratoriów. Nie daje to jednak gwarancji, że uda się przywrócić wszystkie pliki, część nich może zostać zbyt mocno uszkodzona lub trwale skasowana. Diagnoza takiej sytuacji to dla firmy koszty około kilkuset złotych, zaś samo odzyskiwanie może kosztować nawet kilkanaście tysięcy złotych .

Skutki utraty danych

„Kaliber" straty jest różny w zależności od tego, kto był właścicielem utraconych danych i jakie informacje zawierały. Skutki utraty danych można podzielić na:

- bezpośrednie: koszty spowodowane koniecznością odtworzenia danych, utrata zysków w czasie przestoju przedsiębiorstwa, koszty związane z opłaceniem kar umownych dla kontrahentów w przypadku niewywiązania się z umów
- pośrednie: utrata zaufania klientów i kontrahentów, utrata zadowolenia klientów, utrata marki i prestiżu, obniżenie pozycji rynkowej firmy, spadek produktywności, spadek wartości przedsiębiorstwa np. wskutek obniżki cen akcji na giełdach

Fizyczna ochrona danych*

Ochrona fizyczna urządzeń służących do przetwarzania informacji powinna rozpocząć się od wydzielenia obszarów bezpiecznych. Należy stworzyć bariery fizyczne otaczające pomieszczenia firmy. Kolejne bariery tworzą kolejne obwody zabezpieczające, mogą to być:

- ogrodzenie dookoła budynku,
- ściana, drzwi, zamki w drzwiach,
- brama wejściowa otwierana za pomocą karty,
- recepcja obsługiwana przez człowieka
- oświetlenie chronionego obszaru,
- kamery telewizji przemysłowej (CCTV),
- systemy alarmowe,
- pracownicy ochrony.

*wg http://securityinfo.pl/publikacje/2/

Fizyczna ochrona danych

Fizyczna ochrona sprzętu powinna przeciwdziałać nie tylko zagrożeniu nieupoważnionego dostępu do informacji, ale również niebezpiecznym czynnikom środowiskowym, które mogłyby wpłynąć na działanie urządzeń.

Podstawowe kategorie zagrożeń, na które sprzęt może być narażony:

- próby nieupoważnionego dostępu,
- zagrożenia środowiskowe: pożar, powódź, trzęsienie ziemi, pył, dym,
- w środowiskach przemysłowych: pył, kurz, drgania, oddziaływania chemiczne,
- awarie zasilania, klimatyzacji, przerwa w dostawie wody,
- interferencje ze źródeł zasilania, promieniowanie elektromagnetyczne.

Fizyczna ochrona danych

Zabezpieczając linie komunikacyjne należy pamiętać nie tylko o warstwie sieciowej, ale również o ich bezpieczeństwie fizycznym. Okablowanie telekomunikacyjne powinno być chronione przed podsłuchem lub uszkodzeniem. Jeśli tylko jest to możliwe, to należy unikać wyznaczania tras kabli biegnących przez obszary publiczne. Jeśli nie ma takiej możliwości, okablowanie powinno zostać poprowadzone pod ziemią. Wszystkie punkty rozdzielcze sieci powinny znajdować się w zamykanych skrzynkach lub szafach teleinformatycznych umieszczonych w zamykanych pomieszczeniach.

Zastosowanie okablowania światłowodowego w miejsce miedzianego również poprawia bezpieczeństwo instalacji, ponieważ uniemożliwia niewykrywalne naruszenie ciągłości traktu. Oprócz tego połączenie światłowodowe jest odporne na interferencje sygnału czy uderzenie pioruna.

Fizyczna ochrona danych

Przebadano* 146 firm, z których 95% odpowiedziało, że „Większość z nas niszczy, archiwizuje lub wysyła do centrali poufne dokumenty zawierające istotne dane”. Następnie sprawdzono zawartość kilkuset worków na śmieci. Wnioski są co najmniej niepokojące:

Mimo powszechnej świadomości potrzeby stosowania jakichkolwiek procedur chronienia danych i niszczenia zbędnych dokumentów, w 38% przejrzanych worków znaleziono dokumenty, które zawierały dane personalne, faktury VAT, rachunki, oferty przetargowe, umowy.

*naukowcy Uniwersytetu Wrocławskiego na zlecenie firmy Fellowes Polska, wg http://securityinfo.pl/publikacje/2/

Fizyczna ochrona danych

Ankietowani pracownicy firm zadeklarowali, że ponad 80% zbędnej dokumentacji zostaje zabezpieczona (nie upubliczniona) — jest niszczona, archiwizowana, składowana. Mimo to 44% przeszukanych worków zawierało dokumenty, które w 52% przypadków zawierały możliwe do odczytania dane i poufne informacje.

Badania zostały przeprowadzone na stacji przeładunku śmieci, gdzie odpady są już w pewnym stopniu przetworzone. Dotarcie do śmieci znajdujących się jeszcze w śmietniku, tuż przy biurze firmy może istotnie zwiększyć prawdopodobieństwo odczytania poufnych informacji.

Fizyczna ochrona danych

Ogólne zasady polityki „czystego biurka”

- Nawet jeśli opuszcza się pokój tylko na chwilę, należy go zamknąć na klucz lub schować do zamykanej szafy wszelkie ważne dokumenty i nośniki danych (płyty CD, DVD, pendrive'y, taśmy).
- Po zakończeniu pracy dokumenty i komputerowe nośniki danych powinny być przechowywane w zamykanych, zabezpieczonych i ognioodpornych szafach.
- Na zakończenie pracy należy zamknąć aktywne sesje oraz wyrejestrować się (wylogować się) z serwerów lub też stosować oprogramowanie blokujące klawiaturę i wygaszacz ekranu zabezpieczony hasłem.
- Do faksów, kserokopiarek i drukarek nie powinny mieć dostępu osoby postronne. Jeśli jest to możliwe, urządzenia te powinny być zablokowane poza normalnymi godzinami pracy. Niezwłocznie po otrzymaniu, skopiowaniu lub wydrukowaniu dokumentów należy zabrać je z podajnika urządzenia.

Fizyczna ochrona danych

Urządzenia przenośne, praca poza siedzibą firmy

Aspekty, na które należy szczególnie zwrócić uwagę:

- Podglądanie przez nieupoważnione osoby ekranu urządzenia lub klawiatury, podsłuchanie rozmowy. Rozmowy dotyczące strategicznych spraw dla firmy mogą być prowadzone tylko w bezpiecznych, sprawdzonych miejscach. Nie powinny się odbywać w obecności osób przypadkowych, w miejscach takich jak prezentacje, targi czy restauracje.

- Utrata urządzenia przenośnego: zgubienie lub kradzież („przypadkowa" — złodziej nie kranie urządzenia dla danych, które posiada, a dla samego urządzenia lub „świadoma" — dla złodzieja istotne są dane, które znajdują się w pamięci urządzenia). Przenośne urządzenia komputerowe powinny być wyposażone w fizyczne zabezpieczenia przed kradzieżą.

Fizyczna ochrona danych

Urządzenia przenośne, praca poza siedzibą firmy

- Urządzenia przenośne oraz nośniki danych zabierane z siedziby firmy nie powinny być pozostawiane bez nadzoru w miejscach publicznych. Zaleca się przewożenie komputerów przenośnych jako bagażu podręcznego i, jeśli jest to możliwe, maskowanie ich podczas podróży (charakterystyczne torby na laptopy nie są najlepszym rozwiązaniem).

- Nie należy pozostawiać dokumentów, nośników danych i sprzętu w hotelach ani w samochodzie bez kontroli.

- Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych mogą ulec uszkodzeniu na przykład w wyniku działania silnego pola elektromagnetycznego — należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu.

- Wskazane jest, aby sprzęt wykorzystywany poza siedzibą firmy był ubezpieczony.

Fizyczna ochrona danych

Urządzenia przenośne, praca poza siedzibą firmy

- Zagrożenia nieuprawnionego dostępu do informacji lub zasobów ze strony innych osób znajdujących się w pobliżu, na przykład rodziny i przyjaciół.
- Określenie zasad i wytycznych dotyczących dostępu rodziny i gości do urządzeń i informacji.
- Określenie dozwolonych prac, godzin pracy, klasyfikacji informacji, które mogą być w posiadaniu pracownika wykonującego pracę na odległość oraz określenie wewnętrznych systemów, do których ma on uprawniony dostęp.

Systemy podtrzymywania zasilania*

Komputery, urządzenia sieciowe, systemy nadzoru wizyjnego oraz wszelka aparatura sterująca i kontrolna jest narażona na przerwy w dostawie sieci elektrycznej, zaniki i spadki napięcia oraz wszelkie inne zakłócenia.

Zaniki napięcia sieciowego - Zauważalna przerwa w dostawie energii elektrycznej. Może spowodować restart systemu operacyjnego komputera lub jego wyłączenie. Niezapisane dokumenty mogą być nie do odzyskania. Gdy trwała operacja kopiowania lub przenoszenia plików - zapis danych na dysku będzie posiadał błędy.

Spadek napięcia sieciowego - Niestabilna praca zasilacza komputera, może źle wpłynąć na pracę innych podzespołów.
Może dojść do wyłączenia lub restartu systemu operacyjnego, a niezapisane dokumenty mogą zostać utracone.

*wg. http://zasilanie-awaryjne.raport.xtech.pl/artykul.aspx?id=zasilanie_awaryjne_wiedza

Systemy podtrzymywania zasilania

Komputery, urządzenia sieciowe, systemy nadzoru wizyjnego oraz wszelka aparatura sterująca i kontrolna jest narażona na przerwy w dostawie sieci elektrycznej, zaniki i spadki napięcia oraz wszelkie inne zakłócenia.

Przepięcia - Napięcie w sieci wzrasta znacznie powyżej swojej wartości znamionowej. Może spowodować fizyczne uszkodzenie urządzeń elektronicznych oraz elementów w komputerze.

Zakłócenia w sieci energetycznej - Często objawem jest zawieszenie się systemu, blokada myszki lub klawiatury, użytkownik nawet nie zdaje sobie sprawy, że powodem awarii jest zakłócenie i zła charakterystyka prądu zasilającego.

Wyładowania atmosferyczne - Może także spowodować fizyczne uszkodzenie urządzeń elektronicznych oraz elementów w komputerze. Szczególnie gdy budynek nie posiada dostatecznej ochrony odgromowe

Systemy podtrzymywania zasilania

W zależności od szacowanego ryzyka i poziomu ciągłości działania, który należy zapewnić, możemy stosować rozwiązania:

- zasilacze awaryjne (UPS),
- generator awaryjny, jeśli przerwy w dostawie energii elektrycznej mogą być dłuższe,
- zwielokrotnione linie zasilające.

Zasilanie awaryjne powinno pozwolić na kontynuację pracy przez urządzenia służące przetwarzaniu informacji, ale również zapewnić działanie oświetlenia i łączności.

Systemy podtrzymywania zasilania

Wybór systemu zasilania awaryjnego zależy od możliwości ekonomicznych inwestora (koszt inwestycji i eksploatacji), konfiguracji obiektu, przeznaczenia obiektu, struktury instalacji elektrycznej, mocy zasilanych urządzeń i wymaganego poziomu bezpieczeństwa.

Stosownie do potrzeb obecnie stosowane są następujące typy zabezpieczeń:

- zasilacze UPS dla odbiorów indywidualnych
- zasilacze UPS centralne dla odbiorów grupowych
- agregaty prądotwórcze
- układy UPS/agregat
- układy specjalizowane

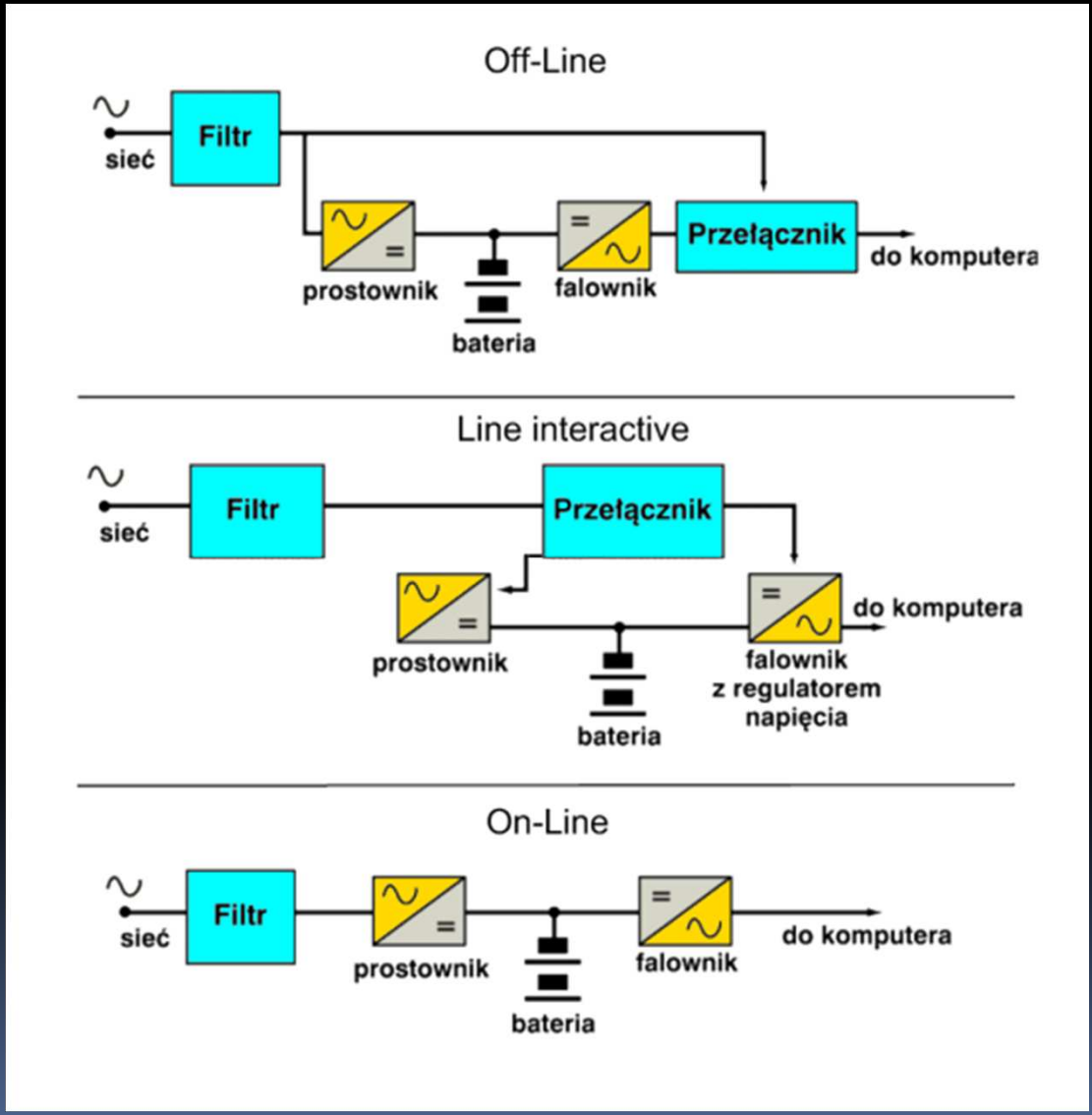
Systemy podtrzymywania zasilania: UPS

Zasilacz awaryjny UPS (Uninterruptable Power Supply) to urządzenie podtrzymujące pracę odbiornika (najczęściej komputera) przez krótki czas po ustaniu zasilania z sieci – zwykle 10-15 minut, przy czym przełączanie źródła zasilania odbywa się bezprzerwowo. Jest wtórnym źródłem energii elektrycznej – jego akumulatory ładują się w czasie, gdy napięcie w sieci zasilającej jest prawidłowe.

Systemy podtrzymywania zasilania: UPS

Typy UPS:

- off-line
- line interactive
- on-line



Systemy podtrzymywania zasilania: UPS

UPS off-line: najprostsza oraz najtańsza klasa, są bardzo rzadko obecnie spotykane, określane też nazwą *stand-by* lub UPS-ami z bierną rezerwą.

Ich możliwości zwykle ograniczają się do filtrowania i korygowania w niewielkim zakresie (±5%) parametrów napięcia zasilającego, gdyż pozbawione są modułu AVR. Przy zaniku napięcia lub przekroczeniu ustalonych progów (dolny – zwykle ok. 175 V, górny – powyżej 270 V) uruchamiane jest podtrzymywanie bateryjne. Następuje to po kilku – kilkunastu milisekundach, ale jest to czas w zupełności wystarczający, gdyż **zasilacz impulsowy komputera wytrzymuje przerwę w dostawie prądu rzędu 20–60 ms**, w zależności od użytych w nim kondensatorów.

Systemy podtrzymywania zasilania: UPS

UPS line-interactive: najliczniejsza dostępna w sklepach grupa zasilaczy awaryjnych, zwana też synchronizującymi się z siecią lub UPS-ami o działaniu wzajemnym. Dzięki zastosowaniu w nich elektronicznych modułów AVR umieją podwyższać lub obniżać napięcie zasilające bez przełączania się na zasilanie bateryjne. Mogą sobie poradzić nawet z napięciem 140–150 V. Zasilacze awaryjne line-interactive mają krótsze czasy przełączenia, poniżej 2 ms.

Systemy podtrzymywania zasilania: UPS

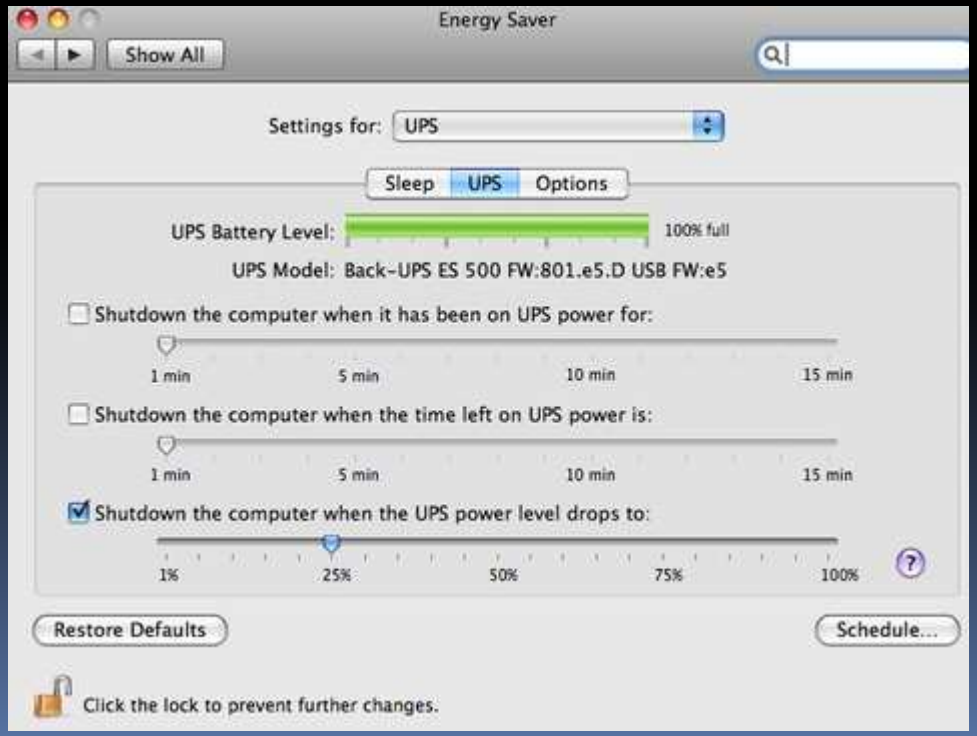
UPS on-line: nazywane też UPS-ami o działaniu ciągłym lub zasilaczami z separacją galwaniczną. W uproszczeniu można powiedzieć, że są one skonstruowane w taki sposób, że przetworniki AC/DC i DC/AC są ze sobą połączone i działają w sposób ciągły. Innymi słowy, prąd dostarczany w normalnych warunkach do komputera nie pochodzi (po przefiltrowaniu) z gniazdka, tylko z falownika zamontowanego w UPS-ie. Między prostownikiem a falownikiem jest zamontowany układ elektroniczny, który doładowuje akumulator i przełącza UPS na zasilanie bateryjne w chwili zaniku prądu. Tego typu UPS-y charakteryzują się praktycznie zerowym czasem przełączania. Jak można się domyślić, są najdroższe i zwykle wykorzystuje się je do zastosowań profesjonalnych.

Systemy podtrzymywania zasilania: UPS

Po przejęciu zasilania podłączonych do niego odbiorników czas podtrzymania napięcia zależy od pojemności akumulatorów i poboru energii. Baterie mają określoną żywotność i należy je okresowo wymieniać – takie usługi realizują wyspecjalizowane firmy. Drugą funkcją zasilacza awaryjnego jest ochrona podłączonych do niego urządzeń przed nagłym wzrostem napięcia. UPS umieszcza się pomiędzy pierwotnym źródłem zasilania, jakim jest sieć elektryczna, a chronionym odbiornikiem (**konfiguracja szeregowa**) lub grupą takich odbiorników (**konfiguracja centralna**), stosownie do mocy urządzenia. Cechą zasilacza typu UPS jest bezprzerwowe zasilanie wyznaczonych elementów sieci. Przed UPS-em może być również zainstalowany agregat prądotwórczy jako alternatywne źródło zasilania, na które przełączana jest instalacja zasilająca po awarii głównego źródła.

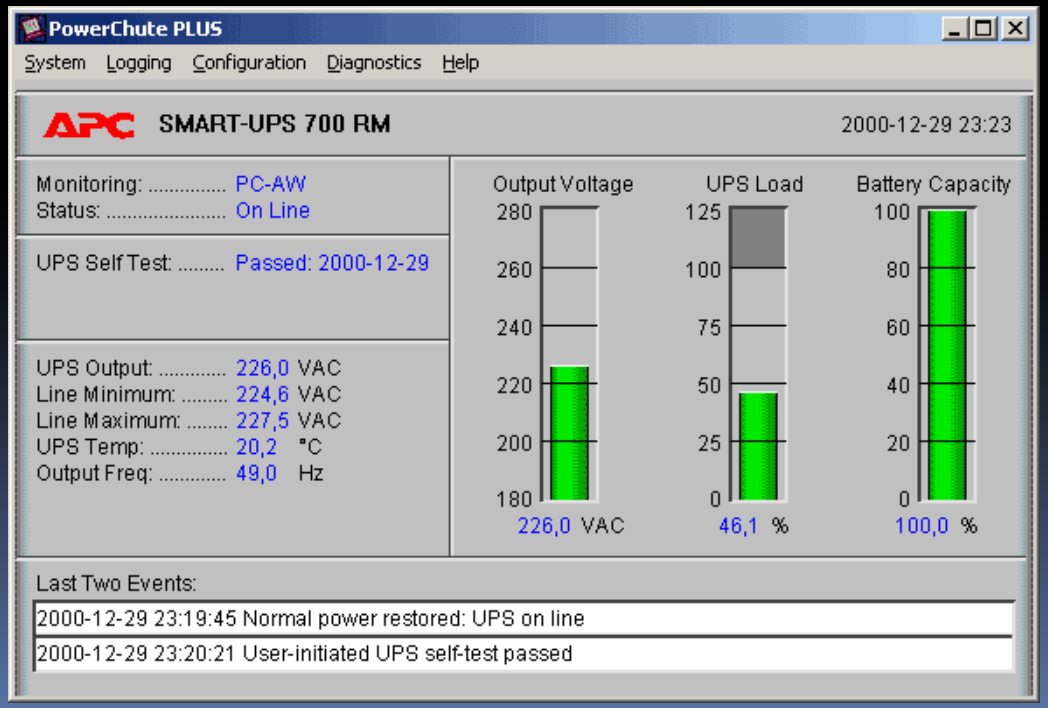
Systemy podtrzymywania zasilania: UPS

Większość domowych UPS-ów jest wyposażona w złącze USB. Służy ono do sprzęgnięcia zasilacza awaryjnego z komputerem. Po podłączeniu UPS-a do peceta z systemem Windows XP lub Windows Vista pojawia się schemat zasilania znany z notebooków wraz z ikonką bateryjki na Pasku Zadań Windows. Możliwości reakcji systemu na brak zasilania oraz informacje o stanie naładowania podczas zasilania z baterii UPS-a są dokładnie takie same jak w wypadku notebooka.



Systemy podtrzymywania zasilania: UPS

Do niektórych bardziej zaawansowanych UPS-ów producenci często dołączają oprogramowanie sterujące. Podstawowym zadaniem takiej aplikacji jest reakcja na brak zasilania i powiadomienie o tym użytkownika. Możliwe jest np. wysłanie informacji o zdarzeniu e-mailem bądź SMS-em, następnie bezpieczne zamknięcie systemu, a po przywróceniu zasilania – ponowne uruchomienie komputera. Bardziej zaawansowane oprogramowanie umożliwia również stałe monitorowanie działania UPS-a, np. pokazuje napięcie wejściowe i wyjściowe, obciążenie oraz stan baterii. Wszystkie te informacje są zapisywane w logach.



Systemy podtrzymywania zasilania: UPS

Zasilacze awaryjne dla odbiorów indywidualnych mają moc do **10 kVA**. Są one wykonywane z reguły w technologii line-interactive. Oznacza to, że zabezpieczane urządzenia są normalnie zasilane z sieci elektrycznej poprzez filtr przeciwzakłóceniowy wbudowany w zasilacz. Dopiero awaria zasilania powoduje uruchomienie wewnętrznego falownika UPS i dostarczanie energii z wewnętrznych akumulatorów zasilacza. Proces ten trwa na tyle krótko, że praca zabezpieczanych urządzeń pozostaje niezakłócona. Zaletą zasilaczy **line-interactive** jest niska cena jednostkowa za kilovoltamper – jest ona w przybliżeniu dwa do trzech razy niższa od jednostki gwarantowanej mocy zasilacza typu on-line.

System szeregowy – rozproszony

Systemy podtrzymywania zasilania: UPS

Zastosowanie rozproszonego systemu zasilania awaryjnego nie wymaga dodatkowych inwestycji w pomieszczenia i instalację elektryczną. Koszt jest wprost proporcjonalny do liczby urządzeń wymagających ochrony (jedno urządzenie – jeden zoptymalizowany pod względem mocy zasilacz awaryjny). Awaria jednego zasilacza pozbawia ochrony jedno urządzenie, nie powodując awarii całego systemu. Wadą takiego systemu zasilania awaryjnego jest słaba separacja chronionych urządzeń od sieci zasilającej podczas pracy normalnej oraz konieczność kontrolowania dużej liczby małych UPS-ów.

Systemy podtrzymywania zasilania: UPS

Dla odbiorów grupowych stosowane są urządzenia średniej mocy – od **10 kVA** do **100 kVA** i dużej mocy – ponad **100 kVA**. Wykonywane są w tzw. technologii **on-line** z podwójnym przetwarzaniem (konwersją) i ze stabilizowanym napięciem sinusoidalnym na wyjściu UPS. Centralne zasilacze awaryjne zwykle przystosowane są do pracy równoległej, co pozwala na rozbudowę gwarantowanej mocy dla chronionych odbiorników i zapewnia nadmiarowość przy zasilaniu odbiorników o zapotrzebowaniu na moc mniejszą o wielkość mocy zasilacza pracującego równolegle. Nadmiarowość (redundacja) zwiększa niezawodność systemu zasilania awaryjnego.

System równoległy – centralny

Systemy podtrzymywania zasilania: UPS

Uszkodzenie jednego z UPS-ów pracujących równolegle nie powoduje awarii w zasilaniu, ponieważ obciążenie przejmują na siebie pozostałe zasilacze. Zasilacze dużych mocy wymagają wydzielonych, klimatyzowanych pomieszczeń (m.in. ze względu na wpływ temperatury na żywotność baterii) oraz wykonania dedykowanej instalacji elektrycznej dla urządzeń wymagających bezprzerwowego zasilania.

Gniazda zasilające takiej instalacji powinny zostać zabezpieczone przed podłączeniem do nich innych urządzeń, takich jak odkurzacze, czajniki elektryczne, dystrybutory napojów itp., nie wymagających zabezpieczenia. Pełna separacja chronionego sprzętu od sieci zasilającej oraz stabilność napięcia wyjściowego UPS on-line dużej mocy wiąże się z wysokim kosztem inwestycji w takie rozwiązanie.

Systemy podtrzymywania zasilania: UPS

Pośrednim rozwiązaniem zasilania awaryjnego sieci jest **konfiguracja mieszana**: urządzenia o kluczowym znaczeniu (np. serwery czy systemy monitoringu obiektu) zabezpiecza się zasilaczem redundantnym on-line małej mocy. Taki zasilacz zbudowany jest z modułów pracujących równolegle. Uszkodzenie jednego z modułów nie powoduje przerwy w dostawie zasilania do chronionego urządzenia, pod warunkiem że obciążenie jest mniejsze o wartość mocy co najmniej jednego modułu. Zasilacze takie montuje się tuż przy odbiorniku i nie wymagają one osobnego pomieszczenia i instalacji. Do zabezpieczania urządzeń o mniejszym priorytecie można stosować tańsze zasilacze awaryjne line-interactive.

Systemy podtrzymywania zasilania: agregat prądotwórczy

Agregaty prądotwórcze stosuje się jako rezerwowe źródło energii elektrycznej w sytuacji, gdy wymagane jest podtrzymanie napięcia przez czas dłuższy, niż może to zapewnić UPS. W takim przypadku zasadny jest zakup agregatu prądotwórczego, ponieważ jego koszt jest niższy od kosztu zakupu baterii akumulatorowych do zasilaczy UPS odpowiedniej pojemności.

Agregat stanowi źródło zasilania energią elektryczną z możliwym bardzo długim czasem podtrzymania. Jednakże rozruch agregatu trwa zwykle od kilku do kilkunastu sekund. Stąd samodzielna praca agregatu jako źródła zasilania awaryjnego może mieć miejsce jedynie w przypadku zasilania odbiorców, odnośnie do których można zaakceptować taką przerwę w zasilaniu.

Systemy podtrzymywania zasilania: agregat prądotwórczy

Głównymi elementami konstrukcyjnymi każdego agregatu są: generator (najczęściej silnik wysokoprężny lub benzynowy), generator wraz z układem automatycznego wzbudzenia; opcjonalnie układ automatycznego sterowania (SZS – Samoczynne Załączanie Rezerwy), analizator sieci, system monitorujący pracę agregatu.

BUDOWA AGREGATU PRĄDOTWÓRCZEGO

1. Rama agregatu
2. Wlew paliwa
3. Uchwyt linki rewersyjnej
4. Przełącznik ssania
5. Włącznik agregatu
6. Silnik
7. Prądnica
8. Rura wydechowa
9. Wlew oleju
10. Kurek kontroli oleju

http://www.wolf-generator.pl/wolf/content2010.html?mid=mid36

Systemy podtrzymywania zasilania: agregat prądotwórczy

Automatyka sterująca pracą agregatów gwarantuje szybki i niezawodny rozruch z dostarczeniem napięcia na odbiorniki w czasie nawet od kilku do kilkunastu sekund od momentu zaniku prądu w sieci. Umożliwia także regulowanie czasu reakcji, co zapobiega niepotrzebnemu uruchamianiu urządzenia podczas chwilowych przerw w dostawie energii elektrycznej. Może zapewnić kontrolę obsługi układu sterującego przez komputer osobisty lub GSM oraz pełną kontrolę pracy silnika z opcją powiadamiania alarmowego.

Najnowszej generacji analizatory sieci monitorują parametry przepływającego prądu: napięcie, natężenie oraz częstotliwość. Pozwala to na obserwację i analizę prądu kierowanego do odbiorników, co pomaga zapobiegać nieprzewidzianym sytuacjom spowodowanym przez gwałtowne zmiany parametrów prądu w sieci.

Systemy podtrzymywania zasilania: UPS/agregat

Układy agregat prądotwórczy/UPS umożliwiają zasilanie bezprzerwowe, które charakteryzuje się zarówno dobrymi parametrami przełączeniowymi, jak i dowolnie długim czasem podtrzymania. Podczas krótkotrwałej przerwy w zasilaniu, kiedy następuje rozruch agregatu, zapotrzebowanie na prąd jest w pełni pokrywane przez energię zgromadzoną w baterii zasilacza UPS. Przejmuje on rolę źródła zasilania niezwłocznie po zaniku napięcia sieci podstawowej. Po uruchomieniu agregatu energia jest dostarczana przez UPS do odbiornika.

Układ agregat/UPS, zwany również hybrydowym lub tandemem, stanowi pewne źródło zasilania, nawet dla odbiorów o najwyższych wymaganiach. Podstawowym warunkiem jego poprawnej pracy jest umiejętne zaprojektowanie układu przełączającego oraz dobór urządzeń o odpowiednich parametrach. Konfiguracją takich systemów zajmują się specjalistyczne przedsiębiorstwa.

Systemy podtrzymywania zasilania: układy specjalizowane

Część rynku systemów zasilania awaryjnego stanowią rozwiązania tworzone dla klientów o specyficznych wymaganiach. Wynikają one ze społecznego znaczenia procesów technologicznych realizowanych w tych przedsiębiorstwach. Do grupy tej można zaliczyć m.in. wytwórców energii elektrycznej (elektrownie oraz elektrociepłownie), zakłady energetyczne, operatorów systemów przesyłowych energii elektrycznej (stacje przesyłowe WN i rozdzielcze SN).

Podobnie jak w wypadku klientów korzystających ze standardowych rozwiązań UPS, również w odniesieniu do tej części rynku awaryjne zasilanie ma na celu ograniczenie zagrożeń wynikających z zaniku napięcia. Jednak szczególne znaczenie zasilania awaryjnego w przypadku elektrowni, elektrociepłowni czy stacji elektroenergetycznej wynika z faktu, iż dotkliwe skutki ewentualnych awarii dotyczyłyby bardzo dużej grupy odbiorców.

Systemy tworzenia kopii zapasowych*

O potrzebie wykonywania regularnych kopii zapasowych wiedzą wszyscy. Nawet jeśli ktoś jeszcze nie do końca zdaje sobie z tego sprawę, to zauważy taką konieczność po pierwszej awarii dysku twardego, uszkodzeniu systemu plików czy przypadkowym usunięciu ważnego pliku. Prawa Murphy'ego sugerują, że wydarzy się to wcześniej lub później, z pewnością zaś w najmniej oczekiwanym momencie.

*wg http://securityinfo.pl/publikacje/6/

Systemy tworzenia kopii zapasowych

Statystki dotyczące polskich przedsiębiorców pokazują, że 83 proc. z nich tworzy kopie zapasowe, z czego prawie połowa wykonuje je wewnątrz firmy, a więc poprzez swoich pracowników. Wciąż 17 proc. firm w ogóle nie wykonuje backupów, zatem świadomie naraża się na ryzyko i koszty związane z utratą danych. Firmy przyznają, że nie wykonują kopii zapasowych, ponieważ wydaje im się to zbyt skomplikowane. Wina leży także po stronie pracowników, którzy albo zwyczajnie zapominają o backupie albo otwarcie przyznają, że nie mają na to czasu, bagatelizując tym samym konsekwencje i narażając pracodawcę na ogromne straty.

Systemy tworzenia kopii zapasowych

Kopia zapasowa a archiwizacja

Wykonywanie kopii zapasowej danych (ang. backup copy) i archiwizacja danych (ang. archiving) to pojęcia oznaczające dwa procesy, których częścią wspólną są dane, a które różnią się celem, przebiegiem i wykorzystywanymi środkami.

Kopia zapasowa powinna umożliwiać szybkie przywrócenie systemu do działania w przypadku awarii (ang. *disaster recovery*). Najczęściej zawiera więc nie tylko kopię plików, ale również aplikacji i całego systemu operacyjnego.

Archiwizowane są dane (bez aplikacji czy plików systemowych), które nie muszą być już modyfikowane. Przy archiwizacji danych istotne znaczenie ma czas życia nośników danych i właściwy sposób ich przechowywania.

Systemy tworzenia kopii zapasowych

Kopie zapasowe mogą być tworzone przede wszystkim w celu umożliwienia:

- odzyskania pojedynczych plików utraconych w wyniku skasowania lub nadpisania zawartości,
- wykonania operacji przywrócenia do działania całego systemu, nawet bez konieczności reinstalacji systemu operacyjnego (ang. *bare-metal restore*).

Systemy tworzenia kopii zapasowych

Podział ze względu na strategię dodawania plików do tworzonej kopii:

kopia pełna — kopiowane są wszystkie pliki, niezależnie od daty ich ostatniej modyfikacji, najczęściej stanowi podstawę dla kopii różnicowych i przyrostowych; wykonanie kopii może być czasochłonne; odzyskiwanie danych jest szybkie, wymagany jest tylko jeden nośnik.

kopia przyrostowa — kopiowane są pliki, które zostały zmodyfikowane (lub utworzone) od czasu wykonania ostatniej pełnej lub przyrostowej kopii; czas wykonywania kopii może być dość krótki; odtworzenie danych wymaga odtworzenia najpierw ostatniego pełnego backupu, a następnie wszystkich następujących przyrostowych.

kopia różnicowa — kopiowane są pliki, które zostały zmodyfikowane (lub utworzone) od czasu wykonania ostatniej pełnej kopii; czas wykonywania kopii różnicowej jest stosunkowo krótki, ale rośnie wraz z każdą kolejną kopią; odtworzenie danych wymaga odtworzenia najpierw ostatniego pełnego backupu, a następnie ostatniej kopii różnicowej.

Systemy tworzenia kopii zapasowych

Strategia

Rozpoczęcie wykonywania kopii bezpieczeństwa należy zacząć od przemyślenia jakimi środkami dysponujemy, jak duże poniesiemy straty w przypadku utraty danych i jaką część tej kwoty jesteśmy w stanie wydać by uniknąć przykrych konsekwencji awarii.

Ciągłe wykonywanie pełnej kopii danych na tych samych nośnikach jest jednym z podstawowych błędów. Przede wszystkim — nie pozwala na zachowanie historii wykonywanych zmian. Nie chroni więc przed sytuacją, kiedy fakt uszkodzenia plików jest odnotowywany w kilka dni po awarii. Zastosowanie wielu nośników i właściwego harmonogramu rotacji nośników rozwiązuje ten problem.

Systemy tworzenia kopii zapasowych

Strategia

Pierwszym i najważniejszym przykazaniem wykonywania kopii bezpieczeństwa jest **systematyczność**.

Dopilnowanie ustalonego harmonogramu najlepiej powierzyć bezdusznej maszynie i samemu ograniczyć się do wymiany nośników danych oraz okresowego sprawdzania czy cały system w ogóle jeszcze działa.

Systemy tworzenia kopii zapasowych

Popularną strategią wykonywania kopii jest Wieża Hanoi.

Nośniki oznaczane są kolejnymi literami alfabetu: A, B, itd. (w poniższym przykładzie mamy 5 nośników). Proces rozpoczynamy od nośnika A i używamy go cyklicznie co drugi dzień. Na nośniku B zapisujemy kopię w pierwszy dzień, w którym nie został użyty nośnik A. Nośnik B będzie teraz wykorzystywany co czwarty dzień cyklu. Kolejny nośnik (C) zostaje użyty po raz pierwszy, kiedy nie był wykorzystywany nośnik A ani nośnik B i będzie wykorzystywany cyklicznie co 8 dni. W łatwy sposób można dodawać kolejne nośniki.

Tabela: Ilustracja działania algorytmu rotacji Wieża Hanoi

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
A		A		A		A		A		A		A		A	
	B				B				B				B		
			C								C				
							D								
															E

Systemy tworzenia kopii zapasowych

Rozwiązania techniczne*

1. Kopia na płytki CD i DVD - metoda najtańsza, ale nośniki te oferują małe pojemności. Z tego powodu jej wygoda pozostawia wiele do życzenia.

*wg http://www.storagestandard.pl/news/145125_2/Backup.od.podstaw.html

Systemy tworzenia kopii zapasowych

Rozwiązania techniczne

2. Kopia na kartę pamięci USB - metoda najprostsza do zabezpieczania niewielkich zbiorów danych ze względu na małe pojemności i relatywnie wysokie ceny.

Systemy tworzenia kopii zapasowych

Rozwiązania techniczne

3. **Kopia na zewnętrzny dysk** - możliwość zabezpieczenia setek GB danych za kilkaset zł, a jeśli dysponujemy starszym, niepotrzebnym dyskiem, to obudowę USB do niego można kupić już za kilkadziesiąt zł.

Systemy tworzenia kopii zapasowych

Rozwiązania techniczne

4. **Kopia na dysk dołączony do sieci lokalnej** - dysk podłączony do sieci w modelu Network Attached Storage (NAS) można wykorzystać do backupu z kilku serwerów i stacji roboczych pracujących w sieci. Jako że taki dysk jest włączony cały czas, czynność ta może być wykonywana automatycznie (za pomocą specjalnego oprogramowania do backupu, czasem dostarczanego wraz z urządzeniem). Wadą tego rozwiązania jest duże obciążenie sieci podczas wykonywania backupu (sama czynność też trwa dość długo) oraz wciąż nie najniższa cena sieciowych dysków. Niektóre modele takich urządzeń mieszczą wewnątrz dwa dyski połączone w RAID 1. Dobrze jest, jeśli do dysku sieciowego przez porty USB można dołączyć jeszcze jeden dysk zewnętrzny, na który codziennie wykonywana byłaby kopia danych z dysku sieciowego.

Systemy tworzenia kopii zapasowych

Rozwiązania techniczne

5. **Kopia na taśmę** - systemy rejestracji na taśmach magnetycznych wciąż są najbardziej pojemnym nośnikiem, a plany ich rozwoju wskazują, że jeszcze długo będą królowały w systemach backupu. Ich sprzymierzeńcem jest wykładniczo rosnąca ilość przetwarzanych danych. Dziś najbardziej pojemne napędy taśmowe gromadzą setki gigabajtów danych na jednym nośniku. Transfer danych sięga dziesiątek gigabajtów na godzinę. Wartości te na dodatek systematycznie rosną.

Rozwiązanie korzystne tam, gdzie backup obejmuje bardzo duże ilości danych, gdzie trzeba mieć ich kilka kopii z różnych momentów w historii, a kopię danych trzeba wywieźć od czasu do czasu do innej siedziby.

Systemy tworzenia kopii zapasowych

Rozwiązania techniczne

6. **Kopia przez Internet** - usługi backupu online, czasem określanego jako Storage 2.0 lub backup w chmurze, stają się coraz popularniejsze. To usługa tych, dla których inwestycja w napęd taśmowy jest zbyt dużym wydatkiem, a danych do zabezpieczenia mają niewiele. Po wykupieniu konta u operatora takich usług otrzymujemy aplikację, którą należy odpowiednio skonfigurować, wskazując które dane i z jaką częstotliwością mają być kopiowane do centrum danych operatora. Opłata za usługę z reguły jest naliczana ze względu na wykupioną objętość i miesięczny transfer danych. Ale usługi przechowywania danych online nie zapewniają wystarczającej wydajności dla aplikacji transakcyjnych czy baz danych - transfer przez Internet jest po prostu zbyt wolny (zresztą do backupu dokumentów czy zdjęć też warto mieć dość szybkie łącze). Można też mieć obawy odnośnie zachowania poufności danych.

Systemy tworzenia kopii zapasowych

Trwałość nośników

Trwałość zapisu na **dyskach twardych HDD** wynosi ok. 10 lat. Zamontowanie takiego dysku pionowo skraca jego żywotność o 30%. Jeśli dysk twardy jest wykorzystywany wyłącznie do przechowywania danych poza komputerem, należy podłączyć go raz na pół roku – gdy nośnik jest zbyt długo nieużywany, tężeje substancja w jego łożyskach. Warto dodać, że dyski 3,5-calowe są dodatkowo mniej zawodne od modeli 2,5-calowych.

Systemy tworzenia kopii zapasowych

Trwałość nośników

Nośniki optyczne. Znaczenie ma prędkość obrotowa nagrywarki i wypalania płyt (im szybciej, tym więcej błędów zapisu). Dyski optyczne zawierają warstwę barwnika, która zmienia właściwości optyczne pod wpływem wiązki laserowej – jednak z czasem traci swoje właściwości. Dlatego też nie należy nagrywac na płyty, które przeleżały ponad 3 lata – na tyle określono żywotność niewypalonego organicznego barwnika. Generalnie trwałość optycznych nośników określa się na 5-10 lat. Bardziej wytrzymałe są dyski wykonane w technologii DVD-DTD (*Data Tresor Disc*), których trwałość szacowana jest na co najmniej 160 lat. Nie dość, że tego typu dysk jest całkowicie odporny na wpływ środowiska, to dodatkowo nieorganiczne materiały, z których jest wykonany, nie podlegają naturalnemu starzeniu się (w odróżnieniu od standardowego nośnika DVD). Oryginalne (tłoczone) płyty kompaktowe z muzyką oraz filmy na DVD są znacznie trwalsze niż te nagrywane domowymi sposobami, ale i one w końcu się zestarzeją. Ich trwałość szacuje się na 20-30 lat.

Systemy tworzenia kopii zapasowych

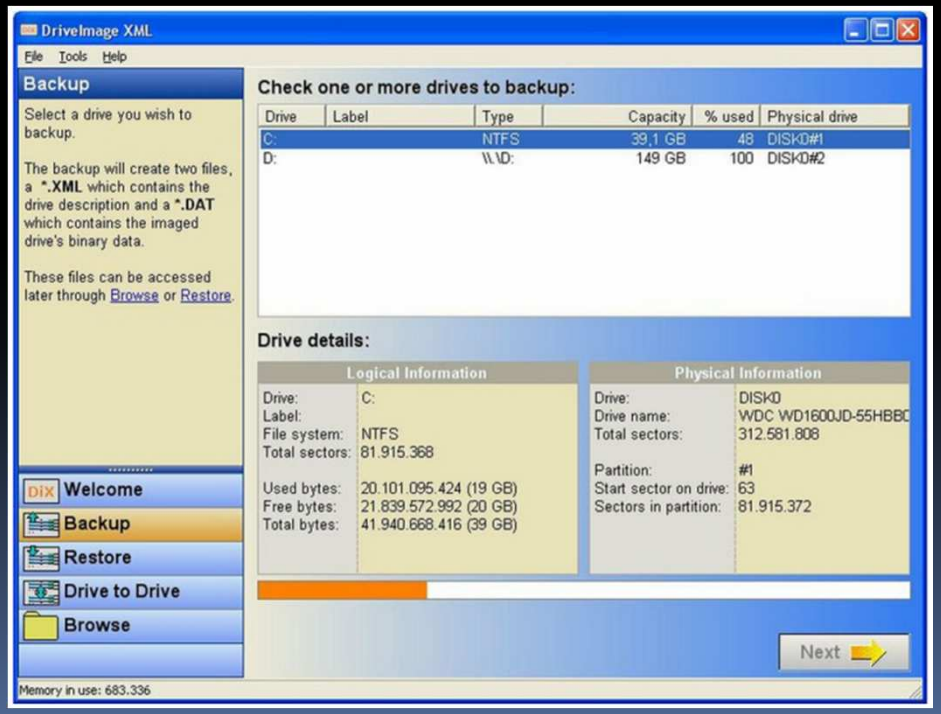
Trwałość nośników

Pamięci flash – trwałość tych nośników zależy w dużej mierze od jakości wykonania – w przypadku solidniejszych producentów można się spodziewać, że dane na pamięciach Flash będą możliwe do odczytania przez okres do 10 lat, w przypadku najmniej dbających o jakość – jedynie 2 lata. Częste korzystanie z nośnika skraca jego żywotność. Zazwyczaj liczba odczytów pamięci jest nieograniczona, ale inaczej jest w przypadku zapisów i kasowań – tutaj, w zależności od typu i producenta pamięci, żywotność nośnika szacowana jest od 10 do 100 tysięcy cykli kasowania i programowania.

Systemy tworzenia kopii zapasowych

Oprogramowanie*

DriveImage XML oferuje w pełni funkcjonalny mechanizm tworzenia kopii zapasowych. Ta darmowa aplikacja umożliwia tworzenie obrazów dysków twardych. Obsługiwane systemy to FAT12, FAT16, FAT32 oraz NTFS. Program używa usługi Microsoft Volume Shadow Services. Gotowe obrazy mogą być przeszukiwane, a także wgrywane bez konieczności restartu komputera.



*wg chip.pl

Systemy tworzenia kopii zapasowych

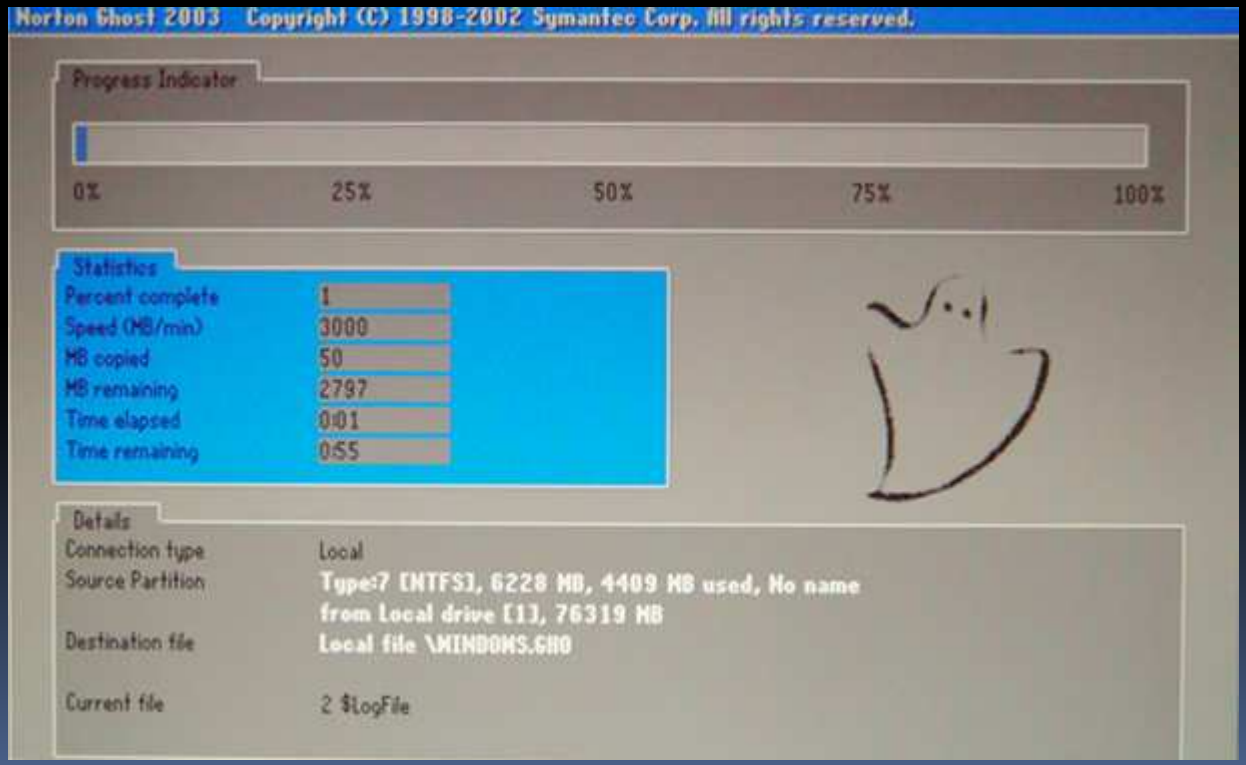
Oprogramowanie

Back2ZIP. Niewielki program tworzący kopie zapasowe wybranych folderów w formacie ZIP i aktualizuje je regularnie. Dzięki temu programowi możesz tworzyć i kontrolować kopie zapasowe. Sam zdecyduj kiedy i jak często kopia powinna być tworzona. Zapobiegaj utracie danych na swoim komputerze dzięki ciągłej aktualizacji swoich backupów. Twoje kopie zapasowe będą przechowywane w wybranej przez ciebie lokalizacji.

Systemy tworzenia kopii zapasowych

Oprogramowanie

Norton Ghost umożliwia zapisywanie obrazu dysku twardego na innym dysku twardym (także zewnętrznym) oraz na popularnych nagrywarkach CD i DVD, co ułatwia tworzenie kopii zapasowych istotnych danych.



Systemy tworzenia kopii zapasowych

RAID - zmniejszanie ryzyka utraty danych

RAID1 polega na replikacji pracy dwóch lub więcej dysków fizycznych. Powstała przestrzeń ma rozmiar najmniejszego nośnika. RAID 1 jest zwany również lustrzanym (ang. mirroring).

Korzyści:
odporność na awarię N – 1 dysków przy N-dyskowej macierzy
możliwe zwiększenie szybkości odczytu
możliwe zmniejszenie czasu dostępu

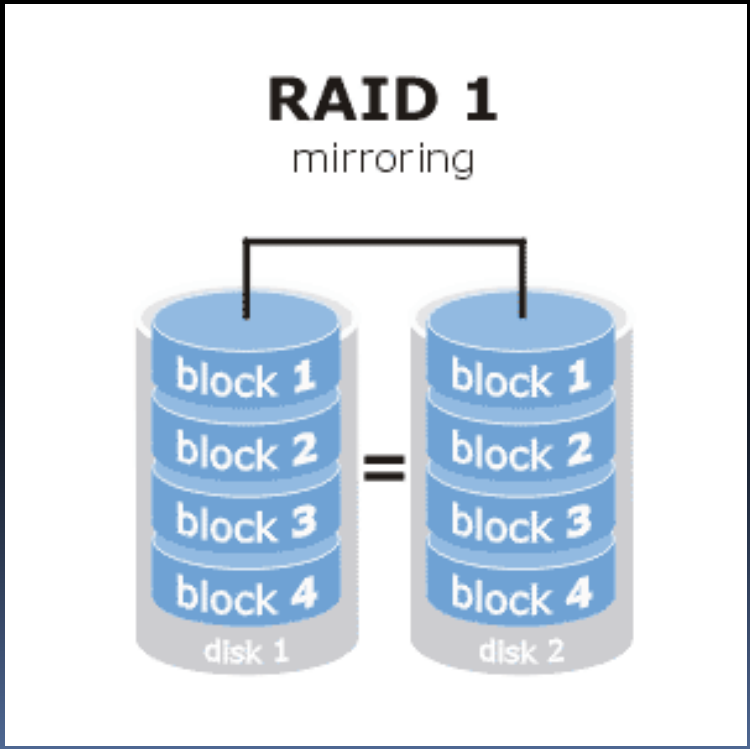
Wady:
możliwa zmniejszona szybkość zapisu
utrata pojemności (całkowita pojemność jest taka jak pojemność najmniejszego dysku)

RAID to nie backup, jednak dzięki niemu można zmniejszyć ryzyko utraty danych.

Systemy tworzenia kopii zapasowych

RAID - zmniejszanie ryzyka utraty danych

Przykład
Dwa dyski po 250GB zostały połączone w RAID 1. Powstała w ten sposób przestrzeń ma rozmiar 250 GB. Jeden dysk w pewnym momencie ulega uszkodzeniu, system nadal działa.

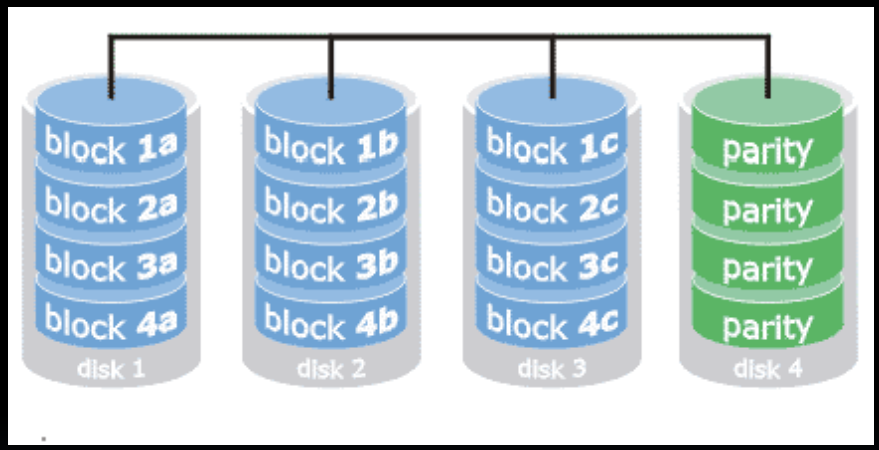


Systemy tworzenia kopii zapasowych

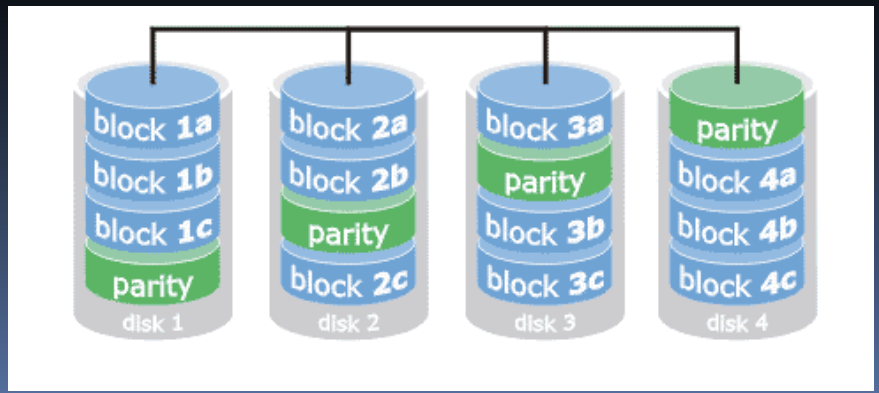
RAID - zmniejszanie ryzyka utraty danych

Inne technologie RAID zwiększające odporność na awarię to RAID3, RAID4, RAID5, RAID6.

RAID 3, RAID 4
(czwarty dysk zapisuje sumy kontrolne; przy macierzy liczącej N dysków jej objętość wynosi N – 1 dysków)



RAID 5, RAID 6
(sumy kontrolne zapisywane na wszystkich dyskach, przy macierzy liczącej N dysków jej objętość wynosi N – 1 dysków, N zajmują sumy kontr.)



Systemy tworzenia kopii zapasowych

Wskazówki

- Wykonuj backup maksymalnie często.
- Kontroluj systematycznie poprawność wykonania backupu.
- Backup powinien zawierać dane zarówno najnowsze, jak i starsze.
- Nie oszczędzaj na nośnikach.
- Po wykonaniu archiwizacji, dobrze ją opisz.
- Przechowuj nośniki w bezpiecznym miejscu (sejf to dobry pomysł).
- Dbaj o warunki, w jakich pracują stacje robocze i serwery (film: How To Clean Lenovo G550 Laptop Fan.mp4)
- Używaj sprzętu wysokiej jakości (dyski, zasilacze, płyty główne dedykowane do zastosowań serwerowych), czytaj testy wytrzymałości sprzętu (film: Lenovo ThinkPad Torture Test_ The Water Spill.flv).

Odzyskiwanie danych

Koszmar administratora

- Nastąpiła poważna awaria dysku, danych nie można odczytać
- Backupu brak, jest uszkodzony lub nieaktualny
- Ponowne wprowadzenie danych jest niemożliwe lub zajęłoby zbyt wiele czasu

Odzyskiwanie danych

Jak samemu zdiagnozować przyczynę uszkodzenia dysku?*

uszkodzenie logiczne - dysk jest widoczny w BIOS, nie słychać żadnych stuków, ale nie ma na nim żadnych danych

uszkodzenie głowic zapisująco/odczytujących - wszelkiego typu zgrzyty, ostre piski, odgłosy mechanicznego tarcia, stuki

uszkodzenie elektroniki zewnętrznej dysku - dysk nie wydaje żadnych odgłosów, nie słychać charakterystycznego dźwięku wirujących talerzy

Dysk twardy jest jednak skomplikowanym urządzeniem i niejednokrotnie podobne objawy są spowodowane zupełnie różnymi uszkodzeniami.

*wg http://infojama.pl/129,artykul.aspx

Odzyskiwanie danych

Jak się zachować po wykryciu utraty danych?

- Wyłączyć komputer
- Wykonać kopię dysku 1 do 1 na innym systemie (jeśli dysk nie jest uszkodzony mechanicznie) i spróbować użyć programów do odzyskiwania danych
- W przypadku uszkodzeń mechanicznych zwrócić się do specjalistycznej firmy
- W przypadku zalania lub spalenia nośnika należy uczynić to jak najszybciej, gdyż dochodzi do tzw. kontaminacji nośnika (powoduje to np. jego utlenianie) i im bardziej zwlekamy, tym uszkodzenia będą większe.

Odzyskiwanie danych

Usługi i koszty odzyskiwania danych w specjalistycznej firmie*

Dyski twarde

Lp.	Typ usługi	Opis	Szacowany czas wykonania	Warunek usługi lub szacowany koszt (netto PLN)
1.	Tryb standardowy	Analiza dysku twardego ATA, S-ATA, SCSI, 1.8", 2.5", 3.5"	4-7 dni roboczych	Warunkowo bezpłatnie*
2.	Tryb przyspieszony	Analiza dysku twardego ATA, S-ATA, SCSI, 1.8", 2.5", 3.5"	2-5 dni roboczych	300
3.	Tryb ekspresowy	Analiza dysku twardego ATA, S-ATA, SCSI, 1.8", 2.5", 3.5"	W trybie 24h/dobę	1000

Odzyskiwanie danych z dysków twardych w trybie standardowym

Lp.	Typ usługi	Opis	Szacowany koszt (netto PLN)
1.	Uszkodzenia logiczne	Usuniecie danych, skasowanie partycji, formatowanie dysku	200-1500
2.	Uszkodzenia techniczne	Uszkodzenia nie wymagające wymiany podzespołów - Bad sektory, uszkodzony translator, zerowa pojemność dysku	800-1800
3.	Uszkodzenia fizyczne	Uszkodzenia wymagające wymiany podzespołów - uszkodzenia elektroniki, elementów wewnętrznych dysku, uszkodzenia powierzchni dysku	1500-4000

*na przykładzie http://www.datalab.pl/dzialy/cennik.html

Odzyskiwanie danych

Usługi i koszty odzyskiwania danych w specjalistycznej firmie*

Odzyskiwanie danych z pendrive'ów			
Lp.	Pojemność pendrive'a	Typ uszkodzenia	
		Logiczne (pendrive sprawny, np. skasowanie, sformatowanie danych)	Techniczne (pendrive niesprawny, np. brak dostępu do urządzenia, nierozpoznane urządzenie w systemie, zerowa pojemność)
		Szacowany koszt (netto PLN)	Szacowany koszt (netto PLN)
1.	do 512 MB	50-150	300
2.	do 1 GB	50-250	450
3.	do 2 GB	50-350	600
4.	do 4 GB	50-450	750
5.	do 8 GB	50-550	900
6.	do 16 GB	50-650	1050
7.	do 32 GB	50-750	1200
8.	do 64 GB	50-850	1350
9.	powyżej 64 GB	50 - telefon	telefon

*na przykładzie http://www.datalab.pl/dzialy/cennik.html

Odzyskiwanie danych

Usługi i koszty odzyskiwania danych w specjalistycznej firmie*

Odzyskiwanie danych z kart pamięci			
Lp.	Pojemność karty	Typ uszkodzenia	
		Logiczne (karta sprawna, brak danych np. skasowanie, sformatowanie)	Techniczne (karta niesprawna np. error memory card, zerowa pojemność, zawieszanie czytnika)
		Szacowany koszt (netto PLN)	Szacowany koszt (netto PLN)
1.	do 512	50-100	200
2.	do 1 GB	50-150	300
3.	do 2 GB	50-200	400
4.	do 4 GB	50-250	500
5.	do 8 GB	50-300	600
6.	do 16 GB	50-350	700
7.	do 32 GB	50-400	800
8.	do 64 GB	50-500	900
9.	powyżej 64 GB	50 - telefon	telefon

*na przykładzie http://www.datalab.pl/dzialy/cennik.html

Odzyskiwanie danych

Usługi i koszty odzyskiwania danych w specjalistycznej firmie*

Odzyskiwanie danych z dyskietek, płyt CD, DVD, HD, BlueRay w trybie standardowym

Lp.	Typ usługi	Szacowany koszt (netto PLN)
1.	Dyskietka	50
2.	Nośnik CD	50-250
3.	Nośnik DVD	50-450
4.	Nośniki HD, BlueRay	50-1000

*na przykładzie http://www.datalab.pl/dzialy/cennik.html

Odzyskiwanie danych

Usługi i koszty odzyskiwania danych w specjalistycznej firmie*

Odzyskiwanie plików (przykłady) w trybie standardowym

Lp.	Opis usługi	Szacowany koszt (netto PLN)
1.	Odzyskiwanie hasła w programie Płatnik	50
2.	Odzyskiwanie zawartości pliku Word	50-250
3.	Odzyskiwanie zawartości pliku Excel	50-450
4.	Odzyskiwanie zawartości pliku Access	50-1000
5.	Odzyskiwanie zawartości skrzynki Outlook Express (cena za jeden dbx) - bez segregowania i analizy wiadomości	300
6.	Odzyskiwanie zawartości skrzynki MS Outlook - bez segregowania i analizy wiadomości	450

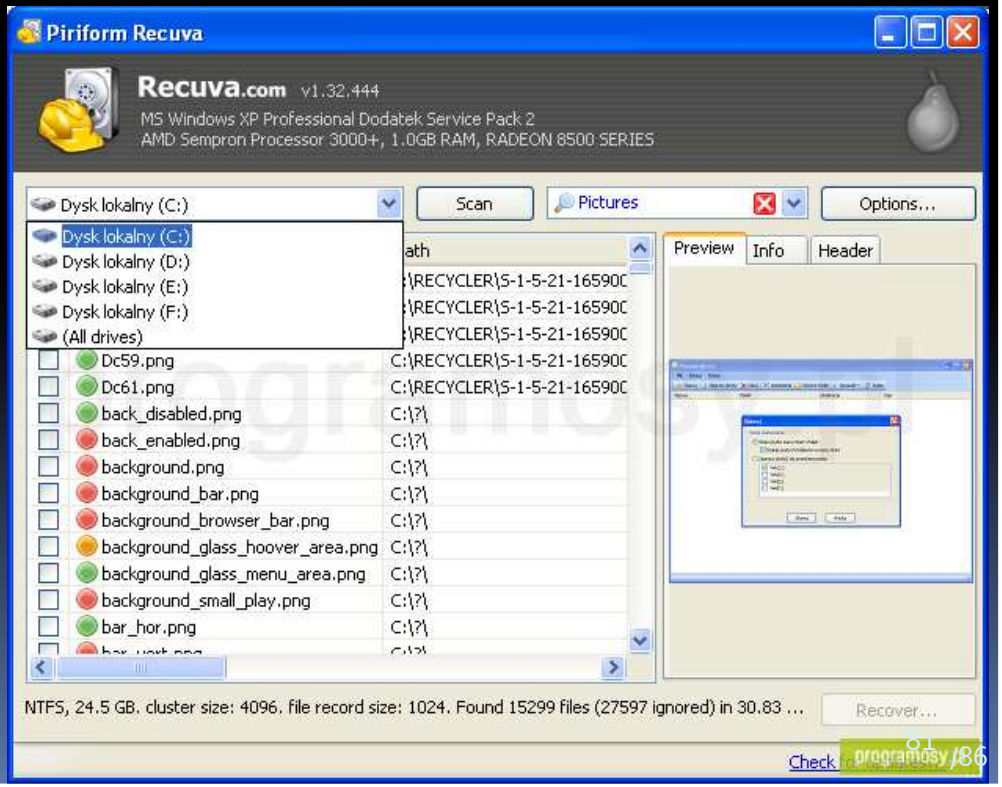
*na przykładzie http://www.datalab.pl/dzialy/cennik.html

Odzyskiwanie danych

W sytuacji, gdy nie nastąpiła awaria dysku, a jedynie zostały usunięte pliki, należy niezwłocznie wyłączyć komputer, aby w ich miejsce nie zostały zapisane inne dane. Następnie należy podpiąć dysk do innego komputera lub uruchomić w komputerze system Live CD i użyć programu do odzyskiwania skasowanych plików.

Odzyskiwanie danych

Jednym z nich jest Recuva* - darmowy program do odzyskiwania przypadkowo usuniętych plików. Radzi sobie z plikami usuniętymi z kosza, z kamery cyfrowej, odtwarzacza mp3, oraz plikami usuniętymi przez robaki i wirusy. Przejrzysty interfejs oraz ojczysty język sprawiają że program jest łatwy w obsłudze i nie powinien sprawiać trudności nawet początkującym użytkownikom.



*http://www.programosy.pl/program,recuva.html

Usuwanie danych

Przenosząc pliki do systemowego "kosza" a następnie opróżniając go jesteśmy pewni, że dane zawarte w nich uległy ostatecznej zagładzie i my oraz nikt inny nie jest w stanie ich odzyskać. Tak się jednak nie dzieje. Dane te w większości przypadków można z powodzeniem odzyskać za pomocą odpowiedniego oprogramowania.

Tak naprawdę stuprocentową pewność destrukcji danych uzyskamy tylko w przypadku fizycznego zniszczenia nośnika. Można tego dokonać nagrzewając dysk twardy do dość wysokiej temperatury. Traci on wtedy swoje właściwości magnetyczne. Innym sposobem jest poddanie naszego "twardziela" działaniu pola magnetycznego (*film: Demagnetyzer Garner HD3.mp4*).

Usuwanie danych

Istnieją dwa sposoby kasowania danych przy użyciu oprogramowania.
Poziom "0" - polega na jednokrotnym zapisaniu całego dysku bitami o wartości o lub 1. Jednak ta metoda nie jest w pełni skuteczna. Dane można częściowo odzyskać w laboratorium za pomocą specjalistycznego sprzętu i oprogramowania.

Poziom "2" - polega na wykorzystaniu skomplikowanego algorytmu niszczenia danych w której określa się liczbę przebiegów jak i rodzaj zapisanych bitów.

Wybierając sposób kasowania należy wziąć pod uwagę rodzaj danych oraz stopień ich tajności. Trzeba jednak pamiętać o tym, że im bardziej skomplikowany algorytm zostanie zastosowany tym więcej czasu zajmie zamazywanie.

Usuwanie danych

Jednym z takich programów jest Eraser*.

Eraser to darmowe narzędzie do całkowitego usuwania plików i folderów z dysku twardego tak aby nie było możliwe ich odzyskanie (jak ma to miejsce przy normalnym kasowaniu plików).

Umożliwia kasowanie plików ze wszystkich dysków pracujących w standardach IDE i SCSI (także pracujących w trybie RAID), z systemami plików FAT16, FAT32 lub NTFS. Obsługuje ponadto dyskietki, dyski sieciowe, płyty CD-RW i DVD-RW. Oprócz trybu "na życzenie" (On-Demand), zaawansowanym użytkownikom program daje możliwość tworzenia cyklicznych zadań (Sheduler), które można wykorzystać np. do całkowitego kasowania niepotrzebnych plików po codziennej pracy.

*http://www.dobreprogramy.pl/Eraser,Program,Windows,12852.html

Gotowe zestawy narzędzi

Hiren's Boot CD

Jest to kolejna wersja "zestawu pierwszej pomocy" na wypadek jakichś awarii w naszych PC. Paczka zawiera obraz bootowalnej płyty, z której możemy uruchomić zestaw narzędzi, a nawet mini system i przeprowadzić niezbędną diagnostykę, naprawy, a także wiele innych zaawansowanych rzeczy.

http://www.hiren.info/pages/bootcd

Hirens boot