

Mirosław SIERGIEJCZYK¹, Adam ROSIŃSKI²

Politechnika Warszawska Wydział Transportu
Zakład Telekomunikacji w Transporcie
00-662 Warszawa, ul. Koszykowa 75
¹e-mail: msi@it.pw.edu.pl
²e-mail: adro@it.pw.edu.pl

BEZPIECZEŃSTWO DANYCH W SYSTEMACH INFORMATYCZNYCH BAZ LOGISTYCZNYCH

Streszczenie:

W referacie zaprezentowano zagadnienia związane z bezpieczeństwem danych. Przedstawiono definicje archiwizacji oraz strategię wykonywania kopii. Każda z nich posiada określone zalety i wady, które wpływają na możliwość ich zastosowania dla określonego przedsiębiorstwa. Przedstawiono również propozycję zabezpieczenia danych w systemach informatycznych baz logistycznych. Zwrócono szczególną uwagę na zapewnienie ciągłości działania przedsiębiorstwa. Wdrożenie harmonogramów wykonywania kopii danych pozwoli na zwiększenie bezpieczeństwa danych przechowywanych na serwerach firmy.

Słowa kluczowe: bezpieczeństwo danych, system informatyczny, archiwizacja, kopia zapasowa

WPROWADZENIE

Obecnie w przedsiębiorstwach informacja stała się jednym z czynników bez której trudno jest zachować ciągłość działania. Jej częściowa utrata wiąże się ze zmniejszeniem konkurencyjności na rynku a całkowita nawet z koniecznością przestojów (np. utrata kluczowych danych w przedsiębiorstwie może spowodować ryzyko braku ciągłości finansowej, tendencji do odejścia stałych kontrahentów oraz w przypadku danych finansowo-księgowych nawet odpowiedzialności karnej). Zagrożeń jest wiele. Mogą one wynikać z czynników niezależnych takich jak awarie urządzeń, ale również mogą być spowodowane przez ludzi (np. zagrożenia ze strony Internetu [2], przypadkowe lub umyślne skasowanie danych). Dlatego tak ważnego znaczenia nabiera zagadnienie bezpieczeństwa danych. Aby to uzyskać zaproponowano zastosowanie strategii kopii danych. Przedstawiono również propozycję zabezpieczenia danych w systemach informatycznych baz logistycznych, które ze względu na charakter pracy powinny mieć zapewnioną ciągłość działania.

1. BEZPIECZEŃSTWO DANYCH

Zasoby zgromadzone w bazie logistycznej mające postać informacji cyfrowej można uznać za jedno z ważniejszych aktywów biznesowych. Dlatego też niezbędne jest odpowiednie ich przechowywanie i zabezpieczanie (zarówno od strony sprzętowej jak i programowej). Bezpieczeństwo informacji można traktować jako zbiór procesów i procedur, których celem jest zabezpieczenie systemu informatycznego przed wystąpieniem awarii lub (i) niepowołanym dostępem osób nieupoważnionych. Jednym z procesów jest archiwizacja i zabezpieczenie danych [4]. Dzięki ich zastosowaniu w systemie informatycznym bazy

logistycznej zwiększa się prawdopodobieństwo zapewnienia ciągłości działań biznesowych a jednocześnie minimalizuje ryzyko niebezpieczeństwa utraty ważnych informacji.

1.1 Archiwizacja

Archiwizacja (ang. *Archiving*) jest procesem podczas którego wykonuje się kopie danych w celu zabezpieczenia ich przed utratą, która może być spowodowana czynnikami losowymi (np. zdarzenia losowe: powódź, pożar; awaria urządzeń lub oprogramowania, itp.) lub działalnością przestępczą (np. skasowanie danych, zainfekowanie wirusami, itp.). Pojęcie archiwizacji obejmuje również proces przenoszenia danych z systemów komputerowych na inne nośniki danych (najczęściej zewnętrzne), dzięki czemu następuje redukcja ilości danych będących w systemach komputerowych.

Archiwizacja może obejmować zarówno całe systemy operacyjne (np. całe dyski twarde lub ich partycje), jak i poszczególne elementy systemu (np. pliki rejestrów, konfiguracyjne) lub dane tworzone bezpośrednio przez pracowników (np. dokumenty edytorów tekstu, arkuszy kalkulacyjnych, baz danych, programów graficznych, itd.).

Archiwizację można przeprowadzać w różnych odstępach czasu, ale zazwyczaj zakłada się odstępy regularne. Zasada jest taka, że im dane są ważniejsze tym krótszy czas pomiędzy kolejną archiwizacją. Zazwyczaj stosuje się również kompresję w celu zmniejszenia objętości archiwizowanych danych. Jest to korzystne z punktu widzenia wymaganych pojemności, ale jednocześnie wydłuża czas potrzebny do odtworzenia danych w przypadku zaistnienia ich utraty. W przypadku danych, które nie muszą być natychmiastowo odtwarzane nośniki z ich kopią należy przechowywać w innym miejscu (np. banku) niż nośniki z oryginalnymi danymi (np. z powodu gwałtownych zjawisk atmosferycznych - powodzi). Należy przy tym pamiętać o konieczności zachowania zróżnicowania poziomów dostępu osób uprawnionych, które mają do nich dostęp.

1.2 Kopia zapasowa

Kopia zapasowa (zwana także kopią bezpieczeństwa) (ang. *Backup Copy*) to odpowiednio zabezpieczone i przygotowane dane. Mają one być wykorzystane do odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia.

Przykładem kopii zapasowych są kopie automatyczne, które tworzą programy podczas ich wykorzystywania (np. edytory tekstu). Dzięki temu w przypadku awarii komputera czy też układu zasilania, możliwe jest odtworzenie poprzedniej wersji pliku. Zazwyczaj kopie takie są tworzone co pewien czas (np. co 10 minut) i najczęściej następuje nadpisywanie przy wykonaniu następnej kopii.

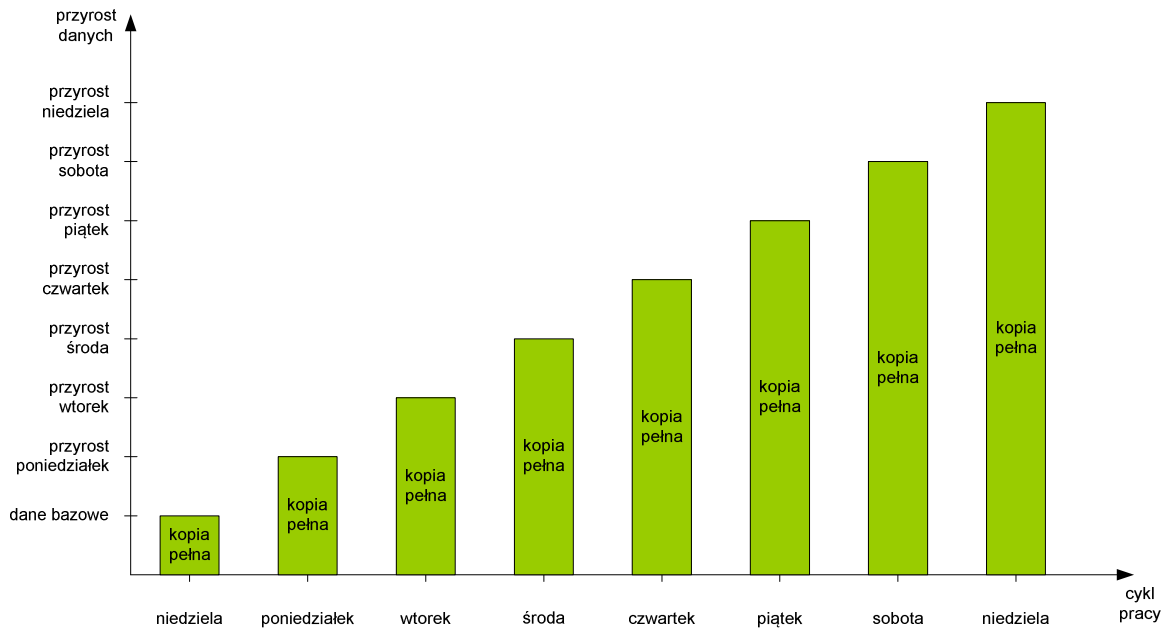
1.3 Strategia kopii danych

Podczas wykonywania kopii danych można zastosować różne strategie ich wykonywania. Jeśli przedsiębiorstwo posiada niewielką ilość danych zazwyczaj wykonuje się systematycznie kopie pełne. Jeśli jednak ich ilość jest duża to wykonywanie kopii pełnych wymaga dużych nakładów środków finansowych. Dlatego też można wówczas zastosować strategie kopii przyrostowych, różnicowych, manualnych czy dziennych [1,3].

Kopia pełna

Kopia pełna polega na skopiowaniu na nośnik archiwizujący wszystkich plików. Dzięki temu mamy kompletną kopię danych z naszego systemu informatycznego: pliki systemowe, konfiguracyjne i użytkowników. Zaletą tej strategii tworzenia kopii zapasowych jest dostępność całości danych. Do wad należy zaliczyć: długi czas tworzenia, wymagana duża

pojemność nośników, wymagany odpowiedni sprzęt, który będzie w stanie zrealizować cały proces archiwizacji w czasie pomiędzy końcem pracy a rozpoczęciem jej w dniu następnym.



Rys. 1. Strategia wykonywania kopii pełnej

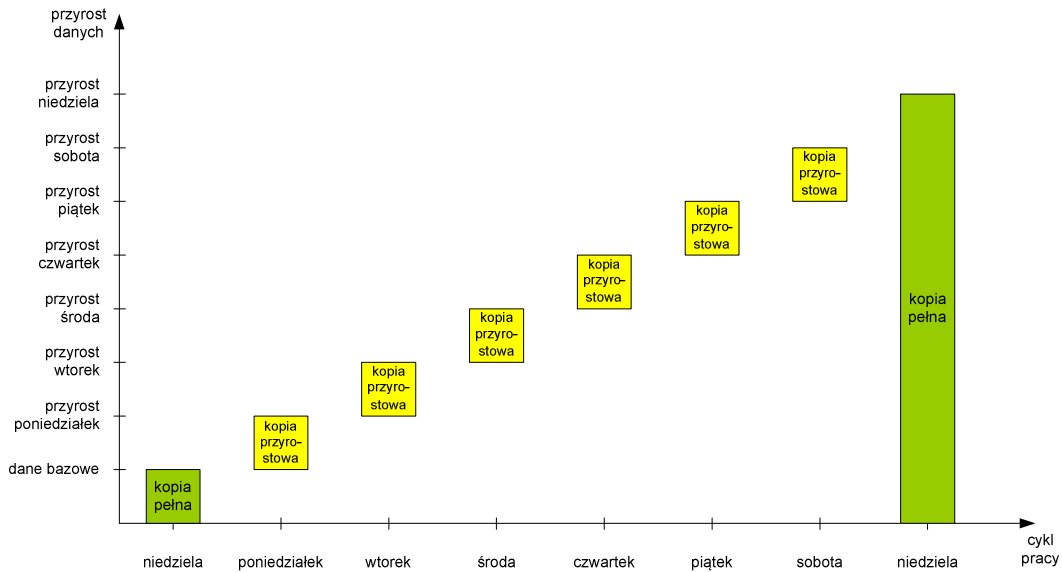
Źródło: opracowanie własne.

Na rys. 1 przedstawiono tygodniowy cykl wykonania kopii pełnej dla przedsiębiorstwa pracującego siedem dni w tygodniu. Codziennie po zakończeniu pracy, system wykonuje pełne kopie danych. Odtworzenie danych z tych kopii pełnych jest najprostsze w porównaniu z innymi typami kopii. Jest tak, ponieważ plik kopii zostaje wczytany i odtworzony tylko z ostatniego nośnika po uprzednim przygotowaniu systemu operacyjnego. Można również zastosować specjalną kopię pełną, która jest kopią krytyczną (ang. *Disaster Backup*). Charakteryzuje się ona tym, że dodatkowo oprócz kopii pełnej tworzony jest nośnik startowy, który umożliwi uruchomienie serwera i odtworzenie danych bez dodatkowych instalacji oprogramowania.

Kopia przyrostowa

Kopia przyrostowa polega na skopiowaniu na nośnik archiwizujący jedynie tych plików, które zostały utworzone lub zmodyfikowane od chwili utworzenia ostatniej kopii pełnej lub przyrostowej. Zaletą tej strategii tworzenia kopii zapasowych jest znaczne skrócenie czasu jaki jest potrzebny na utworzenie kopii, dzięki czemu można ją zastosować do największych przedsiębiorstw, gdzie wykonanie kopii pełnej nie jest możliwe ze względu na niewystarczający czas pomiędzy końcem pracy a rozpoczęciem jej w dniu następnym lub (i) zbyt dużą ilością danych. Warunkiem wykonywania kopii przyrostowych jest konieczność realizacji najpierw kopii pełnej, która będzie punktem odniesienia dla kolejnych kopii. Z tego warunku wynika wada: jeśli któraś z kolejnych kopii przyrostowych ulegnie uszkodzeniu, to może się okazać, że nie będziemy w stanie odtworzyć stanu systemu na określony dzień.

Na rys. 2 przedstawiono tygodniowy cykl wykonania kopii przyrostowej dla przedsiębiorstwa pracującego siedem dni w tygodniu. Ze względu na to że niedziela jest ostatnim dniem pracy w tygodniu, wykonywana jest wówczas pełna kopia systemu. Następnie codziennie (od poniedziałku do soboty) po pracy jest uruchamiany system wykonywania kopii przyrostowych. W następną niedzielę ponownie wykonana jest kopia pełna. Cykl ten stale się powtarza.

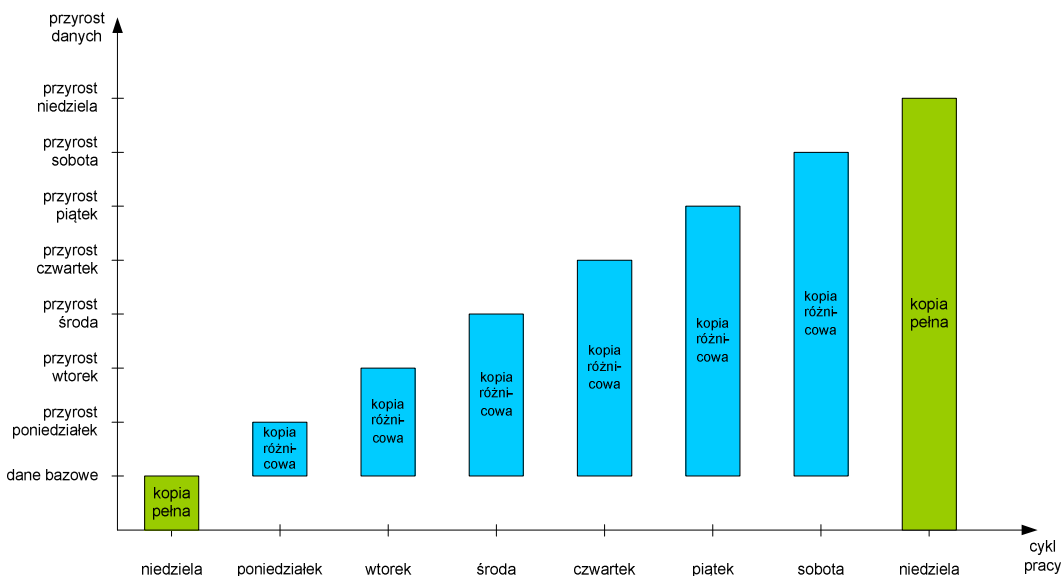


Rys. 2. Strategia wykonywania kopii przyrostowej

Źródło: opracowanie własne.

Kopia różnicowa

Kopia różnicowa polega na skopiowaniu na nośnik archiwizujący jedynie tych plików, które zostały utworzone lub zmodyfikowane od chwili utworzenia ostatniej kopii pełnej. Zaletą tej strategii tworzenia kopii zapasowych jest znaczne skrócenie czasu jaki jest potrzebny na utworzenie kopii, dzięki czemu można ją zastosować do największych przedsiębiorstw, gdzie wykonanie kopii pełnej nie jest możliwe ze względu na niewystarczający czas pomiędzy końcem pracy a rozpoczęciem jej w dniu następnym lub (i) zbyt dużą ilość danych. Warunkiem wykonywania kopii różnicowych jest konieczność realizacji najpierw kopii pełnej, która będzie punktem odniesienia dla kolejnych kopii. Zaletą jest również usunięcie wady, która istnieje przy tworzeniu kopii przyrostowych. Mianowicie, by odtworzyć stan systemu na określony dzień należy mieć tylko kopię pełną i kopie różnicową danych zarchiwizowanych dzień wcześniej. Wadą jest konieczność posiadania dość dużej pojemności nośników.



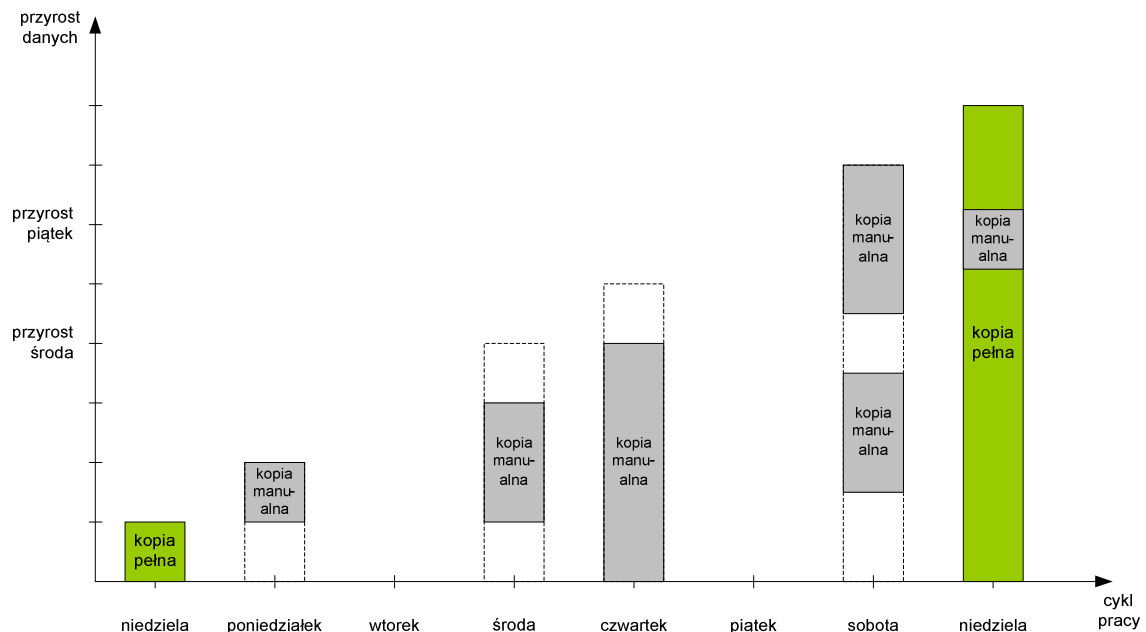
Rys. 3. Strategia wykonywania kopii różnicowej

Źródło: opracowanie własne.

Na rys. 3 przedstawiono tygodniowy cykl wykonania kopii różnicowej dla przedsiębiorstwa pracującego siedem dni w tygodniu. Ze względu na to że niedziela jest ostatnim dniem pracy w tygodniu, wykonywana jest wówczas pełna kopia systemu. Następnie codziennie (od poniedziałku do soboty) po pracy jest uruchamiany system wykonywania kopii różnicowych. W następną niedzielę ponownie wykonana jest kopia pełna. Cykl ten stale się powtarza.

Kopia manualna

Kopia manualna polega na skopiowaniu na nośnik archiwizujący jedynie tych plików, które określił administrator systemu lub operator kopii. Najczęściej są to wybrane aplikacje lub foldery, choć również może to być cały dysk twardy. Kopia manualna jest traktowana jako archiwizacja na żądanie. Nie zmienia ona ustawień atrybutu archiwizacji.



Rys. 4. Strategia wykonywania kopii manualnej

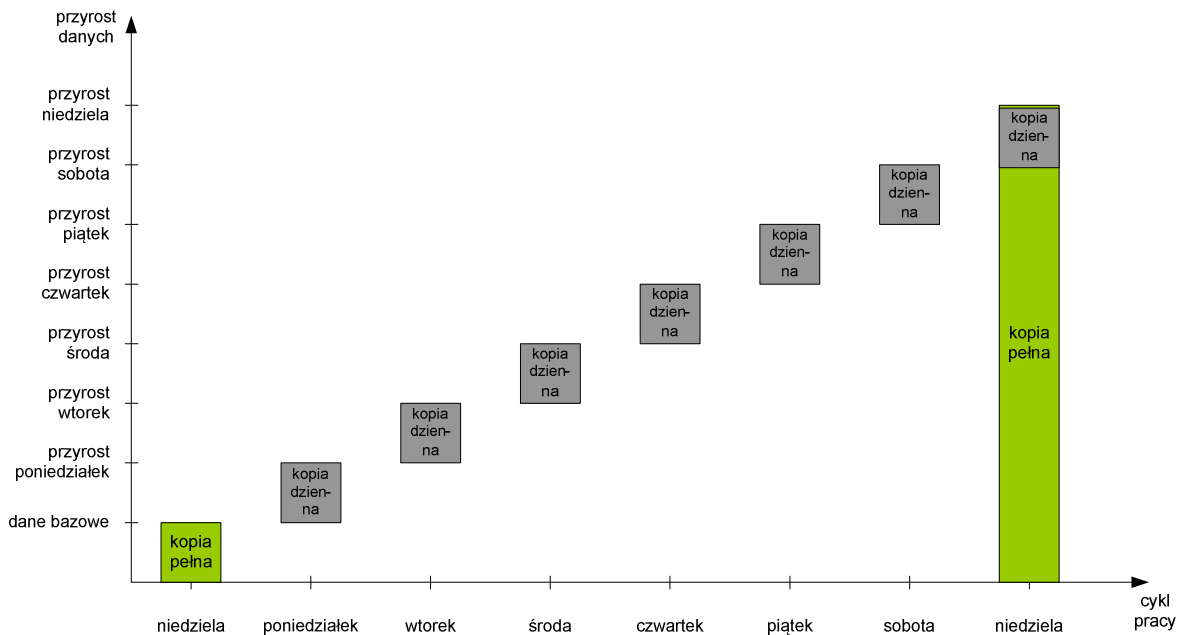
Źródło: opracowanie własne.

Na rys. 4 przedstawiono przykładowy tygodniowy cykl wykonania kopii manualnej dla przedsiębiorstwa pracującego siedem dni w tygodniu. Ich zakres określa administrator i nie wpływają one na zaplanowane kopie cykliczne (np. w niedzielę wykonana zostanie kopia pełna).

Kopia dzienna

Kopia dzienna polega na skopiowaniu na nośnik archiwizujący jedynie tych plików, które zostały zmodyfikowane określonego dnia. Proces ten rozpoczynany jest przez administratora systemu lub operatora kopii. Jest więc to mechanizm zbliżony do wykonywania kopii manualnych i przyrostowych. Jednak nie zmienia ona ustawień atrybutu archiwizacji. Zaletą jest szybkie wykonanie kopii zapasowej.

Na rys. 5 przedstawiono przykładowy tygodniowy cykl wykonania kopii dziennej dla przedsiębiorstwa pracującego siedem dni w tygodniu. Nie wpływają one na zaplanowane kopie cykliczne (np. w niedzielę wykonana zostanie kopia pełna).



Rys. 5. Strategia wykonywania kopii dziennej

Źródło: opracowanie własne.

2. KONCEPCJA ZABEZPIECZENIA DANYCH W SYSTEMACH INFORMATYCZNYCH BAZ LOGISTYCZNYCH

Wdrożony i realizowany system kopii zapasowych dla systemu informatycznego bazy logistycznej podnosi jej poziom bezpieczeństwa teleinformatycznego. Dzięki niemu możliwe jest zapewnienie ciągłości działania przedsiębiorstwa. Założono, że występują trzy serwery:

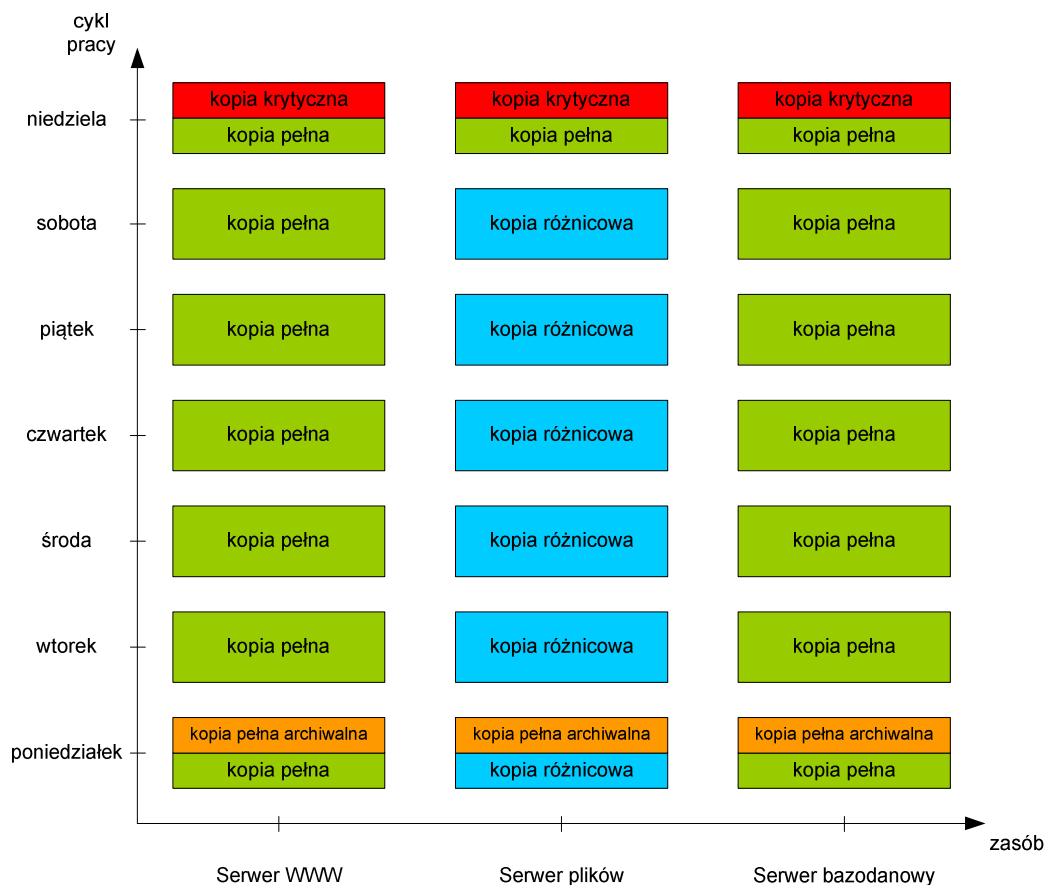
- poczty elektronicznej i strony WWW,
- plików (zawiera wszystkie strategiczne i kluczowe dane firmowe),
- bazodanowy (zawiera wszystkie aplikacje bazodanowe pracujące w firmie).

Dla danych znajdujących się na serwerze poczty i strony WWW zaproponowano strategię kopii pełnych. Powodem tego jest niewielka pojemności danych a zarazem ich dość duża zmiana w ciągu dnia (m.in. ze względu na rotację poczty email). W przypadku gdy zaistnieje potrzeba odtworzenia systemu kopia pełna gwarantuje szybki i bezproblemowy powrót danych. W niedzielę jest tworzona kopia krytyczna.

Dla danych znajdujących się na serwerze plików zaproponowano strategię kopii różnicowych. Powodem tego jest niewielki procent modyfikowania istniejących danych. W niedzielę jest tworzona kopia krytyczna. W przypadku potrzeby odtworzenia danych, odtwarzamy ostatnią kopię pełną (niedzielną) i ostatnią kopię różnicową z nocy przed awarią.

Dla danych znajdujących się na serwerze bazodanowym zaproponowano strategię kopii pełnych. Powodem tego jest dość duża zmiana w ciągu dnia danych. W niedzielę jest tworzona kopia krytyczna.

Dla wszystkich trzech serwerów w poniedziałek wykonywana jest również pełna kopia archiwalna, która przechowywana jest w banku.



Rys. 6. Harmonogram tygodniowego wykonywania kopii zapasowych i archiwizacji

Źródło: opracowanie własne.

PODSUMOWANIE

W referacie przedstawiono zagadnienia związane z bezpieczeństwem danych. Przedstawiono definicje archiwizacji oraz strategie wykonywania kopii. Każda z nich posiada określone zalety i wady, które wpływają na możliwość ich zastosowania dla określonego przedsiębiorstwa.

Przedstawiono również propozycję zabezpieczenia danych w systemach informatycznych baz logistycznych. Zwrócono przy tym szczególną uwagę na zapewnienie ciągłości działania przedsiębiorstwa. Wdrożenie harmonogramów wykonywania kopii danych pozwoli na zwiększenie bezpieczeństwa danych przechowywanych na serwerach firmy. Dodatkowo dzięki tworzeniu pełnych kopii archiwalnych (które są przechowywane w banku) zabezpieczono się przed katastroficznymi zjawiskami atmosferycznymi (np. powodzią). Tworzenie kopii pełnych gwarantuje szybkie odtworzenie systemu.

BIBLIOGRAFIA

- [1] Praca zbiorowa: Vademecum teleinformatyka 1, Wydawnictwo IDG Poland S.A., Warszawa 1999.
- [2] Praca zbiorowa: Vademecum teleinformatyka 2, Wydawnictwo IDG Poland S.A., Warszawa 2002.

- [3] Praca zbiorowa: Vademecum teleinformatyka 3, Wydawnictwo IDG Poland S.A., Warszawa 2004.
- [4] Preston W. C.: Archiwizacja i odzyskiwanie danych, Wydawnictwo Helion, Gliwice 2008.

THE SAFETY OF DATA IN COMPUTER SYSTEMS OF LOGISTIC BASES

Abstract:

In the paper are presented the problems connected with the safety of data. There are presented the definitions of the archiving and the strategies of making the copy. Each of them has specific advantages and disadvantages that affect their applicability for a particular company. Also is presented a proposal for data security in information systems of logistics bases. Special attention has been paid to ensuring the continuity of the acting of the company. Implementation of the schedules of making data copies will allow to increase the security of data stored on company servers.

Key words: safety of data, computer system, archiving, backup copy