ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1995

Seria: INFORMATYKA z. 28 Nr kol. 1270

Naceur FRIH

BEZPIECZEŃSTWO SIECI KOMPUTEROWYCH

Streszczenie. Artykuł omawia problematykę bezpieczeństwa pracy sieci komputerowych. Przedstawiono zagadnienia identyfikacji użytkownika, zabezpieczenia dostępu do zasobów, zabezpieczenia trasy (identyfikacje węzłów), szyfrowanie i bezpieczeństwo sprzętu.

THE NETWORK SECURITY

Summary. This article deals with the problems of the security in network, many possibilities (technical) and methods was discussed to resolve this problem. In this articule was presented technics such as identification process of users, the data base access, the mechanism of cryptography and finally electrical breakdowns.

LA SECURITE DES RESEAUX D'ORDINATEURS

Resume. L'article suivant évoque le probleme qui se pose pour la sécurité des réseaux d'ordinateurs, ainsi que les moyens et les différentes méthodes utilisées afin de le résoudre. Dans cet article il a été présenté la méthode d'identification des utilisateurs de réseau, l'acces aux différentes bases de données, le codage et le décodage des informations. Il a été également évoqué la sécurité des réseaux d'ordinateurs contre les pannes électriques.

1. Wprowadzenie

Teoria sieci komputerowych stwarza możliwości uzyskiwania coraz bardziej różnorodnych rozwiązań architektury sieci, dzięki czemu powstają nowe typy sieci, doskonali się metodologię przetwarzania, przechowywania i przesyłania informacji.

Sieć komputerowa jest to zbiór wzajemnie połączonych autonomicznych komputerów. Mówimy, że dwa komputery są połączone, wtedy, kiedy są zdolne do wymiany informacji.

Wprowadzenie do eksploatacji sieci komputerowych wiąże się również z zagrożeniami. Brak kontroli legalności przypływu milionów bitów informacji krążących codziennie między komputerami w sieci powoduje, że użytkownik nie ma pewności, czy jego dane nie są rejestrowane w czasie ich transmisji. Powoduje to potrzebę zabezpieczania sieci komputerowych. Niezależnie od tego awaria sieci to również problem, który może być bardzo poważny z punktu widzenia użytkowników sieci.

System, którego działanie oparte jest na pracy sieci komputerowej, wymaga rozwiązania problemu bezpieczeństwa pracy. Na bezpieczeństwo sieci komputerowych składają się następujące zagadnienia:

- identyfikacji użytkownika,
- zabezpieczenia dostępu do zasobów,
- zabezpieczenia trasy (identyfikacje węzłów),
- szyfrowanie,
- bezpieczeństwo sprzętu.

2. Bezpieczeństwo sieci związane z problemami identyfikacji użytkowników i dostępu do zasobów

Użytkownicy, którzy chcą dokonać transmisji informacji, muszą się nawzajem zidentyfikować i być pewnymi, że "rozmawiają" właśnie ze sobą. Można rozróżnić identyfikacje konkretnego użytkownika i identyfikacje węzłów sieci. Użytkowników identyfikuje się na różne sposoby:

- Za pomocą podawania hasła.

  Hasło jest to ciąg znaków wprowadzanych przez użytkownika i sprawdzanych przez komputer. Jeżeli hasło podane przez użytkownika jest takie samo, jak pamiętane przez komputer hasło związane z tym użytkowniem, to zostaje udzielone zezwolenie na

dostęp do wszystkich informacji, do których użytkownik jest upoważniony (hasła mogą być wykorzystane niezależnie od użytkownika do ochrony zbiorów, rekordów, pól w rekordach itp.).

- Za pomocą urządzeń hardwarowych jak "karta magnetyczna".

Dodatkowo można wprowadzić tzw. PIN (Personel Identification Number), który wraz z kartą magnetyczną jednoznacznie określa użytkownika. Ostatnio wprowadza się karty inteligentne, wyposażone w programowalny mikroprocesor.

Inną metodą sprawdzania tożsamości użytkownika jest sprawdzanie tak zwanego upoważnienia, które determinuje rodzaj zezwolenia na dostęp do chronionych zasobów. Identyfikator to niepowtarzalna nazwa lub numer nadany obiektowi. Uwierzytelnianie to sprawdzanie, czy osoba lub obiekt jest tym, za kogo się podaje. Procedura upoważnienia bada, czy osoba ta lub ten obiekt ma prawo do chronionego zasobu.

3. Bezpieczeństwo ustawiania trasy

Dane, które są zgromadzone w komputerach i przesyłane pomiędzy węzłami sieci komputerowej, są narażone na zagrożenia, więc trzeba je w skuteczny sposób chronić, aby zapewnić ich bezpieczeństwo.

Bezpieczeństwo systemów rozproszonych to bezpieczna eksploatacja różnego rodzaju sieci komputerowych zintegrowanych ze sobą. Systemy rozproszone tworzą połączone ze sobą węzły, które są systemami komputerowymi z własnymi monitorami odniesienia chroniącymi swoje własne zasoby.

Monitorem odniesienia może być jednostka centralna, system operacyjny i tak zwany program zaufania.

Węzłowy monitor odniesienia jest odpowiedzialny wyłącznie za "bezpieczeństwo" węzła i realizuje tak zwaną węzłową strategię bezpieczeństwa.

Najważniejszą różnicą pomiędzy bezpieczeństwem systemu rozproszonego a systemu wolnostojącego stanowi mechanizm, którego używa monitor odniesienia, aby zapewnić odwzorowanie pomiędzy lokalnymi a odległymi nazwami procesów.

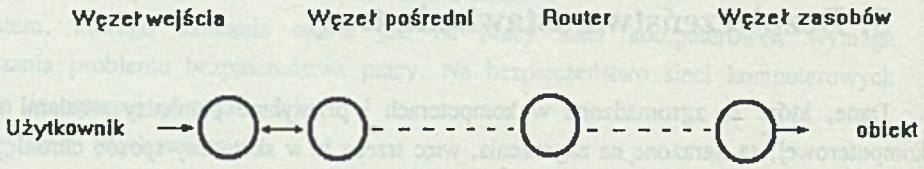
W systemie rozproszonym trzeba założyć, że tak zwany "master", którym jest każda jednostka aktywna, może generować żądanie dostępu do innej jednostki. Każdy "master" ma zdefiniowane swoje własne prawa.

W systemie rozproszonym można wyróżnić tak zwane "węzły przyjazne". Węzłami przyjaznymi nazywamy węzły realizujące tę samą strategię bezpieczeństwa. Węzły przyjazne udostępniają sobie na żądanie pliki. Węzły tego samego typu tworzą region

zaufania. W sieci może być oczywiście wiele różnych regionów zaufania, co wiąże się z różnymi strategiami bezpieczeństwa.

W celu zdefiniowania bezpieczeństwa sieci przyjmuje się, że informacja, którą transmitują węzły, może "wędrować" po całej sieci (system w pełni połączony). Jeżeli informacja ta nie jest zaszyfrowana, to każdy może ją w sieci "przeczytać". Każdy węzeł może odebrać każdą informację z innego węzła i żaden czynnik zewnętrzny nie może temu zapobiec. Jeżeli odległy węzeł otrzyma informację, to nie ma on innej możliwości, jak zaufać tej informacji. Z tego powodu węzeł, który przesyła informację, musi zwrotnie otrzymać z węzła odległego potwierdzenie, że jest on węzłem zaufania. Wynika stąd wymaganie, by żądania dostępu były sprawdzane przez węzeł. Zaufanie do innych węzłów musi być oparte na zrozumiałym modelu zaufania.

System rozproszony można przedstawić jako różnego typu węzły łączące użytkownika z obiektami (rys.1).



Rys.1. Rozproszony system obliczeń
Fig.1. Distributed Computing Model

Każdy węzeł posiada swój własny monitor odniesienia. Węzły tworzą tak zwaną kaskadę działania. Dla dowolnej kaskady działania można przyjąć następujące założenia:

- użytkownik współpracuje tylko z jednym węzłem,
- węzeł wejścia współpracuje z węzłem pośrednim,
- węzeł zasobów współpracuje z jednym węzłem pośrednim,
- węzeł zasobów odbiera żądania dostępu do zasobów węzła pośredniego,
- węzły, które nie współdziałają ze sobą, są tak zwanymi węzłami nieosiągalnymi.

Dla przyjętych założeń można zdefiniować zależności zaufania między elementami systemu rozproszonego:

1. Węzeł wejścia sprawdza autentyczność użytkownika,
2. Użytkownik sprawdza autentyczność węzła,
3. Węzeł wejścia sprawdza autentyczność węzeła pośredniego,
4. Węzeł zasobów sprawdza prawo dostępu do zasobów.

4. Szyfrowanie

W celu podniesienia bezpieczeństwa pracy sieci komputerowych przy transmisji informacji i zapewnienia prywatności i tajności danych stosuje się kryptografię.

Kryptografia (ukryte pismo) jest to nauka zajmująca się tworzeniem kryptogramów - wiadomości lub napisów niezrozumiałych (tajnych). Proces tworzenia kryptogramu nazywa się **szyfrowaniem.**

Tekst źródłowy (jawny) uzyskuje się wskutek deszyfrowania kryptogramu, więc istotnymi elementami, od których zależy skuteczność szyfrowania, są klucze: szyfrujący i deszyfrujący. Systemy kryptograficzne powinny spełniać następujące warunki:

1. Bezpieczeństwo systemu powinno zależeć od zagwarantowania poufności kluczy, a nie od poufności algorytmów szyfrowania i deszyfrowania.
2. Przekształcenia szyfrujące i deszyfrujące muszą być efektywne dla wszystkich kluczy.
3. Użytkowanie systemu musi być łatwe.

Mówimy, że system kryptograficzny zapewnia poufność informacji, jeżeli przy zastosowaniu metod obliczeniowych nie jest możliwe systematyczne określanie przekształcenia deszyfrującego na podstawie zaszyfrowanej wiadomości, jeżeli znana jest odpowiadająca jej informacja jawna.

Ponadto nie powinno być możliwe systematyczne określanie jawnej treści na podstawie przechwyconego kryptogramu. Powyższe zasady powinny być niezależne od długości i liczby przechwyconych zaszyfrowanych informacji.

Mówimy, że system kryptograficzny zapewnia autentyczność informacji, jeżeli przy zastosowaniu metod obliczeniowych niemożliwe jest systematyczne określenie przekształcenia szyfrującego, jeżeli jest znana informacja jawna oraz odpowiadająca jej informacja zaszyfrowana. Także nie powinno być obliczeniowo możliwe systematyczne generowanie zaszyfrowanej informacji należącej do przestrzeni wiadomości zaszyfrowanych systemu kryptograficznego. Spełnienie powyższych warunków może być zależne od ilości tekstu przechwyconego w postaci zaszyfrowanej. Autentyczność danych oznacza, że każda próba zastąpienia oryginalnej zaszyfrowanej informacji wiadomością fałszywą powinna być wykrywalna.

Algorytmy szyfrowania i deszyfrowania są powszechnie znane - utajniony jest tak zwany klucz. Znane i stosowane są dwa typy algorytmów kryptograficznych:

- algorytmy symetrycznego klucza,
- algorytmy asymetrycznego klucza.

W algorytmie symetrycznego klucza ten sam klucz (k) używany jest do szyfrowania (E) i deszyfrowania (D). Oznaczając informację pierwotną przez (M), a informację

zaszyfrowaną przez M', można zapisać:

$$M' = E \bullet k (M)$$

$$M' = D \bullet k (M)$$

Dobry algorytm szyfrowania musi mieć tę cechę, że znajomość M', D i E nie może doprowadzić do klucza k i informacji pierwotnej M. Bezpieczeństwo algorytmu szyfrowania jest funkcją liczby możliwych do zastosowania kluczy.

Algorytmy symetrycznego klucza są stosowane do transmisji plików. Jednym z najlepszych i powszechnie stosowanych algorytmów szyfrowania jest tak zwany algorytm oparty na standardzie DES (Data Encryption Standard).

Szyfr DES szyfruje 64-bitowe bloki danych przy użyciu klucza o długości 56 bitów. Zapewnia to wysoki stopień bezpieczeństwa.

Dla algorytmów asymetrycznych każdy użytkownik posiada klucz ogólny (pk) oraz klucz prywatny (sk). Istnieje ścisła relacja pomiędzy (pk) a (sk):

$$M' = Epk(M)$$

$$M = Dsk(M)$$

Relacja ta oznacza, że wiadomość zaszyfrowana za pomocą (pk) może być rozszyfrowana przy użyciu klucza (sk).

W sieciach komputerowych stosuje się:

- szyfrowanie periodyczne (serial encryption),
- szyfrowanie pakietowe (packet encryption).

Szyfrowanie periodyczne ogranicza się do warstwy danych, gdzie informacja jest "przenoszona" jako strumień bitów. Przy transmisji pakietów lub datagramów szyfrowania szyfrowanie dotyczy określonej jednostki "wiadomości". Istnieje wówczas niezależność logiczna jednego pakietu od drugiego, co umożliwia stosowanie efektywniejszych metod szyfrowania. Przy szyfrowaniu pakietowym część nagłówka jest nieszyfrowana. Wynika to z faktu, że węzły sieci muszą identyfikować np. adresy do realizacji połączeń.

Zasady szyfrowania są ujęte w tak zwanych protokołach szyfrujących, które są dołączane do istniejących architektur logicznych sieci. Z szyfrowaniem jest związana tzw. ochrona wtórna (replay protection). Ochrona ta ma zapewnić niemożliwość powtórnej transmisji przy wymianie przez hackera zaszyfrowanej informacji. W celu "zwalczania" powtórzeń nadawca wysyła między pakietami kolejne liczby (tzw. wybielanie pakietów). Ten typ ochrony jest implementowany zwykle w łączach danych.

W celu identyfikacji nadawcy stosuje się protokoły oparte na zasadzie "znajomości" klucza (konwersacja potwierdzająca znajomość tajnego klucza).

Dystrybucja i zarządzanie kluczem stanowi istotny element bezpieczeństwa i poufności transmisji oraz skuteczności szyfrowania. To przecież klucz jest jedynym tajnym

elementem algorytmu szyfrowania. Gdy klucz przestanie być tajny, całe szyfrowanie mija się z celem.

Istnieje kilka możliwości rozprowadzania klucza:

- "ręczne" rozprowadzanie klucza,
- automatyczne (sieć służy do rozprowadzania klucza),
- dystrybucja klucz "on line".

Pierwsze dwie metody niosą ze sobą poważne zagrożenie łatwego dostania się klucza w niepowołane ręce. Dlatego obecnie stosowana jest metoda trzecia dystrybucji klucza przez ośrodek dystrybucji klucza. Ten system rozprowadzania klucza umożliwa równocześnie identyfikowanie użytkownika sieci oraz wprowadzenie czasowej zmiany klucza. System ten wymaga jednak zaufanego odwzorowania nazw użytkowników sieci i ich ogólnego klucza.

Szyfrowanie warto stosować szczególnie w systemach komputerowych o słabo zabezpieczonych liniach komunikacyjnych.

5. Bezpieczeństwo sprzętu

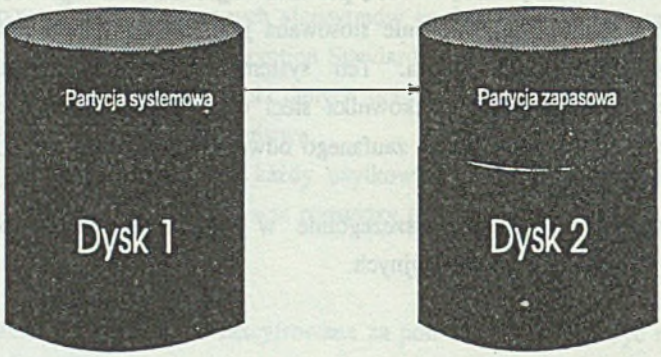
W celu podniesienia niezawodności pracy sieci i zapewnienia bezpieczeństwa danych przechowywanych w pamięci masowej stosuje się zamiast pojedynczych dysków macierze dyskowe.

Dysk twardy - jak wszystko - jest urządzeniem zawodnym. Zawsze starano się temu zaradzić, np. zalecając częste tworzenie kopii zapasowych. Technika taka jest wystarczająca w przypadku komputerów indywidualnych.

W systemach sieciowych ważna jest jednak nie tylko ochrona danych, ale również zapewnienie ciągłości działania systemu mimo uszkodzenia któregoś z elementów składowych. Chronić można i chroni się wiele składników, stosując np. nadmiarowe systemy dyskowe, wielokrotne zasilanie, komputery z dwoma równolegle pracującymi procesorami, a w skrajnym przypadku nawet dwa identyczne serwery, wykonujące te same operacje.

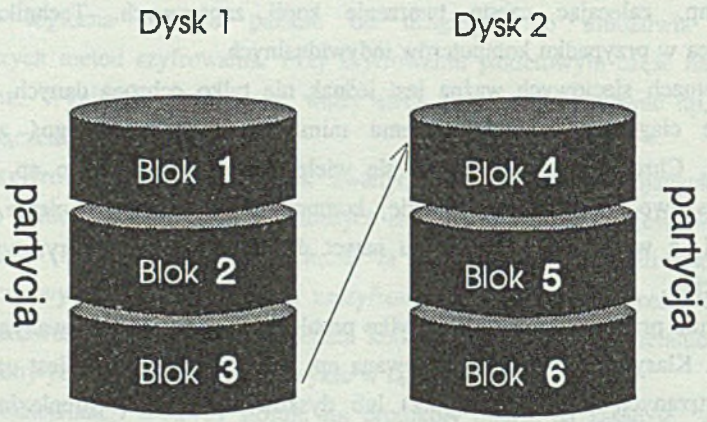
W artykule przedstawione zostaną tylko problemy związane z tak zwanymi systemami dyskowymi. Klasyczną techniką - stosowaną np. w Novell Netware - jest używanie tzw. dysków lustrzanych (mirroring - rys.2) lub dysków zdwojonych (duplexing). Idea ta, bardzo podobna w obu przypadkach, polega na tym, że wszystkie operacje wykonywane są równocześnie na dwóch identycznych dyskach i w przypadku uszkodzenia jednego z nich, np. z powodu lokalnego uszkodzenia nośnika albo nawet awarii całego dysku -

serwer może nadal pracować, wykorzystując dysk lustrzany (zapasowy dysk). Duplexing działa niemal identycznie, z tym że oprócz dwóch dysków stosuje się również dwa kontrolery, co z jednej strony zwiększa szybkość działania systemu (operacje na dyskach mogą być wykonywane równocześnie), z drugiej zaś dodatkowo zabezpiecza przed uszkodzeniem jednego z kontrolerów. Obie metody mogą być realizowane sprzętowo lub - tak to standardowo wykonuje firma Novell - programowo.



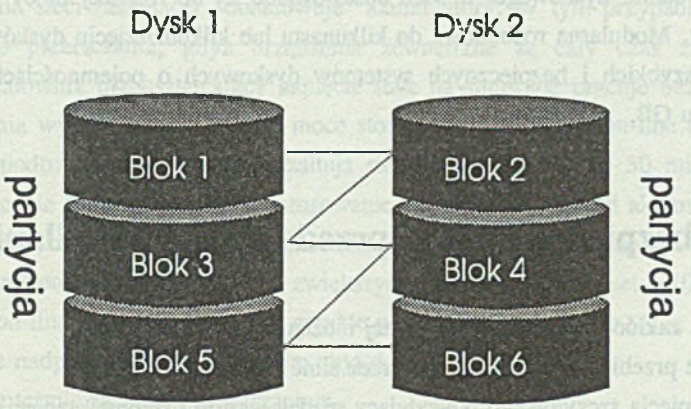
Rys.2. Mirroring
Fig.2. Mirroring

Kolejną metodą jest spanning, który polega na utworzeniu jednego dużego dysku logicznego poprzez połączenie razem kilku małych dysków. Logicznie do końca pierwszego dysku dołączony jest drugi, do końca drugiego początek trzeciego, itd., lecz służy to jedynie do dynamicznego powiększenia pojemności dyskowej (rys.3).



Rys.3. Spanning
Fig.3. Spanning

Następną metodą jest striping, który polega na naprzemiennym zapisywaniu porcji danych to na jednym, to na drugim dysku. Uzyskujemy w ten sposób równoległą pracę wszystkich dysków. Im ich jest więcej, tym większa będzie szybkość (rys.4).



Rys.4. Striping
Fig.4. Striping

Nowszą metodą poprawienia bezpieczeństwa systemu przechowującego informacje jest macierz dyskowa typu RAID (Redundant Array of Inexpensive Disk), pozwalająca na zapewnienie niemal identycznego poziomu zaufania jak w przypadku dysków lustrzanych.

System RAID, łączący razem wiele dysków, zapewnia bezpieczeństwo i wielokrotne przyspieszenie dostępu do danych. Dzięki specjalnej konstrukcji, pozwalającej wymieniać uszkodzone dyski bez przerywania pracy systemu komputerowego, systemy RAID przybliżają nas do bezpiecznych i bezawaryjnych systemów komputerowych. Obecnie istnieje 6 poziomów RAID. Z punktu widzenia ochrony danych najbardziej interesujące są: RAID 1, RAID 3 i RAID 5.

RAID 1 - mirroring lub duplexing. Poziom RAID 1 jest więc pierwszym, który zapewniał bezpieczeństwo poprzez nadmiarowość pamiętanej informacji.

RAID 3 - dane rozproszone są na wszystkich dyskach. Istnieje jeden wyróżniony dysk, przechowujący informację nadmiarową: parzystość. Parzystość nie jest więc rozproszona, zatem prędkość całego systemu jest prędkością dysku parzystości.

RAID 5 - dane i parzystość są rozproszone na wszystkich dyskach w systemie. Nie ma wyróżnionego dysku parzystości.

Systemy dysków macierzowych powinny być stosowane wszędzie tam, gdzie komputer musi pracować niezawodnie, a utrata danych jest ogromną stratą dla banku, firmy ubezpieczeniowej czy zakładu pracy. Zasada pracy "Disk Array" gwarantuje zwiększenie szybkości systemu dyskowego, a więc dostosowanie jej do rosnącej mocy obliczeniowej komputerów. Modularna rozbudowa do kilkunastu lub kilkudziesięciu dysków pozwala na stworzenie szybkich i bezpiecznych systemów dyskowych o pojemnościach od kilkuset MB do wielu GB.

6. Zabezpieczenia sieci przed awariami zasilania

Awarie i zakłócenia sieci energetycznej można podzielić na:

- zakłócenie przebiegu sinusoidalnego przez silne impulsy,
- spadek napięcia szczytowego powodujący spadek wartości średniej napięcia i przenoszonej mocy,
- krótkotrwały zanik napięcia,
- zanik napięcia.

Zabezpieczenie sieci komputerowej może w różnym stopniu eliminować wymienione rodzaje niesprawności zasilania. W zależności od poniesionych kosztów możemy zdecydować się na ochronę serwera plików, wszystkich serwerów lub wszystkich komputerów w sieci przed zakłóceniami lub poważniejszymi awariami zasilania.

Do zabezpieczenia jednego lub kilku blisko położonych stanowisk może służyć tak zwany **ACAR** (jest to aktywny filtr elektroniczny poprawiający jakość napięcia zasilającego). Lepszym rozwiązaniem jest stosowanie urządzeń typu **UPS** (Unterruptable Power Suply - Bezprzerwowe Źródło Zasilania). Ze względu na budowę i działanie można mówić o UPS'ach off-line oraz on-line.

UPS off-line działa w oparciu o szybki przekaźnik przełączający zasilanie podłączanego urządzenia na zasilanie z sieci energetycznej lub na własne, gdy sieć nie działa. Zasilanie własne czerpie energię z wewnętrznych akumulatorów. Akumulatory są automatycznie ładowane podczas "aktywności" sieci zasilającej, a ich pojemność jest parametrem ograniczającym czas podtrzymywania zasilania.

Jedną z wad UPS'ów off-line jest przełączanie zasilania związane z pewnym opóźnieniem. W czasie przełączania następuje bardzo krótka przerwa w zasilaniu, która najczęściej jest niezauważalna dla komputerów. Typową wartością czasu przełączania jest ok. 5ms, a stosowane moce to 300 do 1000 W. Najczęściej za pomocą UPS'a off-line podtrzymuje się pracę pojedynczych stacji roboczych, czy wolnostojących komputerów

przez czas ok. 10 minut do 1 godziny (w zależności od akumulatorów i pobieranej mocy).

Lepszym rozwiązaniem w rodzinie UPS'ów są UPS'y on-line. Ten typ zasilaczy przez cały czas przekazuje energię zgromadzoną w akumulatorach podłączonym urządzeniom, a w czasie działania sieci zasilającej "doładowuje" akumulatory. W tym przypadku trudno mówić o czasie przełączania, gdyż urządzenia zewnętrzne są cały czas zasilane z akumulatorów, falownik przekształcający napięcie stałe na sinusoidę pracuje bez przerwy i czas przełączania wynosi 0 sek. Typowe moce stosowane w UPS'ach on-line to 500 do 1500 W, czasy podtrzymania zasilania kształtują się w granicach 10 do 30 minut, choć mogą być drastycznie zwiększone przez zastosowanie zewnętrznych baterii akumulatorów.

Niektóre modele zasilaczy mogą posiadać tzw. TURBO MODE, czyli tryb pracy, w którym przez określony (krótki) czas mogą zwiększyć wydawaną moc nawet o 100%.

UPS'y serii on-line mają wbudowanych zwykle wiele zabezpieczeń, np.:

- zabezpieczenie nadprądowe przed poborem zbyt dużego prądu,
- zabezpieczenie termiczne przed przegrzaniem,
- zabezpieczenie zwarciowe (zwarcie wyjść powoduje wyłączenie urządzenia).

Zasilacze on-line mogą być wykorzystywane do podtrzymania pracy serwerów sieci wraz z podłączonymi drukarkami. UPS współpracując z serwerem sieci jest w stanie wysłać do użytkowników systemu informację o:

- wyłączeniu sieci energetycznej,
- mającym nastąpić wyłączeniu UPS'a,
- powrocie napięcia.

Oprogramowanie reagując na informacje z zasilacza awaryjnego powinno:

- "poprosić" działających jeszcze użytkowników o zamknięcie zadań, gdyż prawdopodobnie nastąpi wyłączenie serwera (power shut-down),
- zakończyć pracę serwera (szczególnie wszelkie operacje dyskowe) i wyłączyć serwer w odpowiedzi na informację o wyłączeniu zasilacza (z powodu wyczerpania akumulatorów)

7. Wnioski

Zabezpieczenie sieci komputerowych staje się obecnie bardzo aktualnym problemem naukowym i technicznym. Bezpieczeństwo pracy sieci komputerowych wymaga bez wątpienia właściwego doboru metod i sposobów realizacji pozwalających na uzyskanie żądanej niezawodności sieci komputerowych.

Bezpieczeństwo sieci komputerowych musi uwzględniać wszystkie omawiane w

artykule czynniki. Wszystkie wymienione problemy wymagają również pewnych prac standaryzacyjnych, które umożliwią bezpieczną pracę sieci komputerowych w różnych aplikacjach.

LITERATURA

[1] Praca zbiorowa: Systemy komputerowe. Wydawnictwo PRO-NET, 1994.

[2] Grzywak A.: Bezpieczeństwo w systemach rozproszonych. Zeszyty Naukowe Politechniki Śląskiej, Seria Informatyka z. 24, Gliwice 1993.

[3] Hoffman L.: Modern Methods for Computer Security and Privacy., Printice-Hall, Inc New Jersy 7632, USA 1977.

[4] Stokłosa J.: Kryptograficzne metody ochrony danych. Wydawnictwo Politechniki Poznańskiej, Poznań 1992.

Recenzent: Dr inż. Włodzimierz Boroń

Wpłynęło do Redakcji 1 października 1994 r.

Abstract

Network security is now as important as operating system security for just about any computer facility. So, the primary naming problem in network is interpreting his security. In this paper are presented the problems of the security in Network, several possibility (technical) are also described to resolve this problem. Throughout this article was demonstrated technics such as identification process of users, the data base access, the mechanism of cryptography and finally electrical breakdowns.