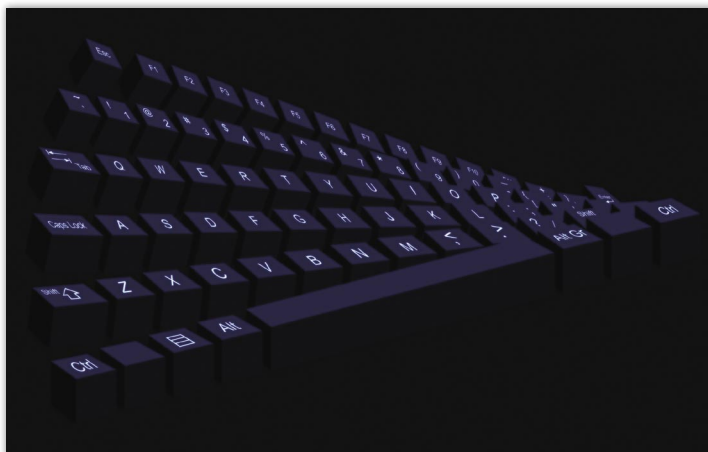


# Data Center i wszystko pod kontrolą

DCSerwis.pl

Każda współczesna organizacja, która swoje działanie opiera na usługach IT, może być schematycznie pokazana jako piramida zależności, której podstawę stanowią elementy Infrastruktury Krytycznej Serwerowni (IKS). W skład IKS wchodzi: struktura fizyczna, zasilanie, chłodzenie, okablowanie strukturalne, monitorowanie i zarządzanie, bezpieczeństwo fizyczne i ochrona przeciwpożarowa, a także dwa, często niedoceniane, filary działu IT i całej organizacji: procedury i normy oraz dokumentacja.



linux@software.com.pl

**N**ie ma tu znaczenia, czy firma lub instytucja wykorzystuje małą serwerownię z kilkoma serwerami czy też wielkie Data Center, schemat jest bardzo podobny. Podobne są też wymagania, jakie musi spełnić serwerownia w takiej organizacji – przede wszystkim musi zapewniać bezpieczną przestrzeń fizyczną, dostarczyć energię elektryczną i moc chłodniczą dla aktualnie wykorzystywanych technologii informatycznych oraz brać pod uwagę możliwy rozwój tych technologii na przestrzeni 4 – 5 lat.

Szybko rozwijające się technologie IT, m.in. takie jak: serwery blade i macierze dyskowe, wymagają coraz to większych mocy elektrycznych do ich zasilania, a potem mocy chłodniczych do odprowadzenia energii cieplnej, co przy jednoczesnym coraz większym upakowaniu urządzeń na metr kwadratowy serwerowni stawia wysokie wymagania przed projektantami wszystkich elementów IKS eksploatowanych w serwerowni.

W tym artykule postaramy się opisać wszystkie elementy IKS, ponieważ są one bardzo często niedoceniane i pomijane. Dla wielu osób, nawet tych zajmujących się zawodowo IT, elementy IKS są tak ukryte pod kolejnymi

warstwami organizacji, że zapominają lub nawet nie wiedzą o ich istnieniu. Poszczególne elementy IKS zostaną tu opisane w formie specyfikacji wybranych wymagań, jakie muszą zostać spełnione, aby serwerownia mogła być prawidłowo i bezpiecznie eksploatowana. Nie jest możliwe opisanie wszystkich wymagań w jednym artykule, dlatego wybraliśmy tylko te, które wydają się tak oczywiste, że często o nich zapominamy.

## Obszar I. Struktura fizyczna

Ten obszar jest chyba najbardziej odległy od normalnych zadań IT i bardzo rzadko zdajemy sobie sprawę, jaki wpływ na prawidłową eksploatację sprzętu IT mają decyzje podjęte w tym zakresie. Ze względu na złożoność zagadnienia, można wyróżnić tutaj kilka podobszarów tematycznych.

### Pomieszczenie serwerowni

Zazwyczaj nie mamy wpływu na lokalizację geograficzną budynku, czasami możemy jednak wybrać w ramach budynku położenie pomieszczenia, które będzie pełniło rolę serwerowni. Mając taki komfort, zwróćmy uwagę, że:



- Ze względu na nasłonecznienie i przenikanie ciepła przez ściany, pomieszczenie nie powinno się znajdować od południowej strony budynku; po stronie zacienionej będzie można także umieścić wymienniki ciepła do klimatyzatorów i tym samym skrócić drogę prowadzenia rur z czynnikiem chłodzącym od serwerowni do zewnętrznych wymienników.
- Ze względu na ryzyko zalania serwerowni nie powinna się znajdować w najniższym miejscu budynku (raczej nie w piwnicy).
- Ze względu na konieczność zapewnienia drogi transportowej dla wprowadzanego sprzętu najlepiej, aby pomieszczenie znajdowało się w okolicach parteru.

W pomieszczeniu nie powinno być żadnych rur, prze które stale lub nawet tylko okresowo płynie woda. Każda rura z wodą stanowi potencjalne źródło wycieku, nawet jeśli w samej serwerowni nie ma żadnych połączeń ani zaworów. Przeciek w dowolnym pomieszczeniu powyżej serwerowni spowoduje, że po wewnętrznej warstwie tej rury do serwerowni dostanie się woda. Jeżeli nie ma możliwości usunięcia rur z serwerowni, należy pod każdą z nich zastosować okap lub rynnę, która odprowadzi wodę poza obręb serwerowni, a wewnątrz rynny umieścić czujnik zalania.

W serwerowni powinno być jak najmniej okien. Jeśli nie można zamurować lub zasłonić ścianką kartonowo – gipsową istniejących okien, to przynajmniej należy je zasłonić żaluzjami odbijającymi ciepło. Pamiętajmy, że jedno standardowe okno w letni dzień potrafi dostarczyć do wnętrza serwerowni tyle ciepła, ile jedna szafa rack (około 5kW) i o tyle też trzeba przewymiarować system chłodzenia. Wiąże się to z koniecznością zakupienia na etapie inwestycji droższych i większych urządzeń chłodniczych, co z kolei oznacza, że w przyszłości koszty eksploatacji będą odpowiednio większe.

Częstym błędem jest pozostawienie możliwości otwarcia okien na wypadek awarii systemów chłodzenia – już przy obecnych gęstościach mocy przypadających na jeden m<sup>2</sup> powierzchni serwerowni schłodzenie pomieszczenia przez otwarcie okien nie jest możliwe, a zgodnie z tendencjami gęstość mocy cały czas rośnie, więc otwieranie okien nie schłodzi serwerowni.

Droga transportowa od wejścia do budynku aż do drzwi do serwerowni powinna mieć szerokość 120cm, wysokość minimum 2,5m i wytrzymałość na obciążenie do 1000kg/m<sup>2</sup>. Na drodze transportowej nie może być żadnych progów ani stopni, cała musi być możliwa

do pokonania przez wózek do transportu palet. Szczególną uwagę należy zwrócić na wszelkie zakręty na drodze transportowej – czy sprzęt, który planujemy wstawić, będzie mógł być przeniesiony tą drogą? Dla uzyskania pewności można wykonać model, który będzie miał podstawę o takim samym obrysie, jak planowany sprzęt i spróbować przenieść ten model drogą transportową. Sprzęt typu duże macierze dyskowe jest często dostarczany w dedykowanych szafach, które na czas transportu są umieszczane w opakowaniach transportowych o kilka centymetrów większych od wymiarów samego urządzenia i należy to uwzględnić planując drogę transportową. Urządzenia, pod groźbą utraty gwarancji, nie mogą być przechyłane w czasie transportu o więcej niż przewiduje to producent (na czas transportu na opakowanie przyklejane są elektroniczne wskaźniki przechyłu, które zapamiętują maksymalny kąt, pod jakim znalazło się opakowanie oraz czas zdarzenia), dlatego też wszelkie pochylnie na drodze transportowej nie mogą być zbyt strome.

#### Podłoga techniczna

Stosowanie podłogi technicznej w serwerowni ma swoich zwolenników i przeciwników. Z jednej strony zastosowanie podłogi technicznej pozwala utworzyć kanał do dystrybucji zimnego powietrza od maszyn chłodzących oraz łatwo rozprowadzić okablowanie zasilające i logiczne, ale z drugiej strony podłoga podniesiona zabiera sporo cennej wysokości pomieszczenia, a schowane tam kable mają tendencję do tworzenia się bałaganu i po pewnym czasie stanowią poważne przeszkody w przepływie zimnego powietrza.

Alternatywnym rozwiązaniem jest zastosowanie wylewki z masy samopoziomującej, pokrytej niepylną farbą i poprowadzenie okablowania ponad szafami. Każde z tych rozwiązań wymaga zastosowania innych rodzajów maszyn klimatyzacyjnych.

#### Kształt pomieszczenia

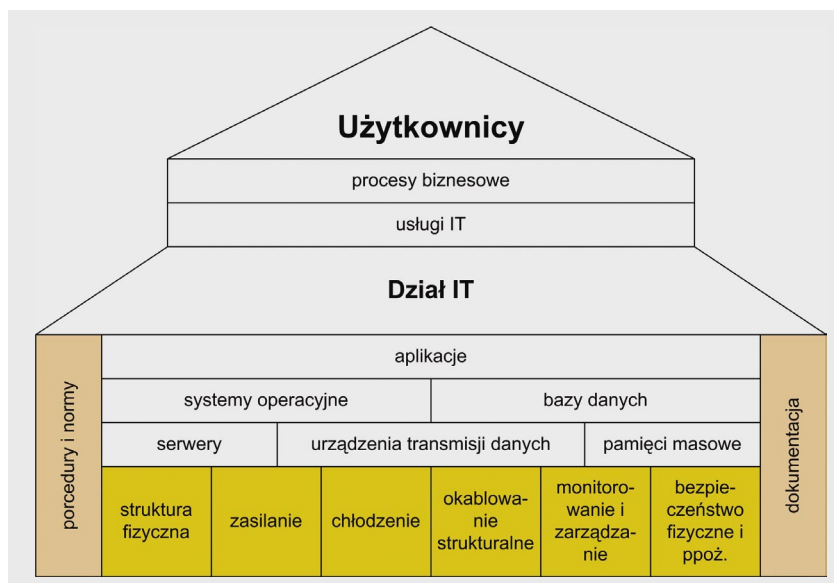
Kształt pomieszczenia serwerowni powinien być zbliżony do kwadratu. Aby w pomieszczeniu można było umieścić jeden rząd szaf rack, to jego minimalna szerokość może być obliczona po zsumowaniu następujących wymiarów:

- miejsce na pełne otwarcie tylnych drzwi szafy: 0,6 – 0,8m,
- głębokość szafy: 1,0 – 1,2m,
- miejsce na manipulowanie sprzętem przed wsunięciem go do szafy (tyle samo, co szerokość drogi transportowej): 1,2m.

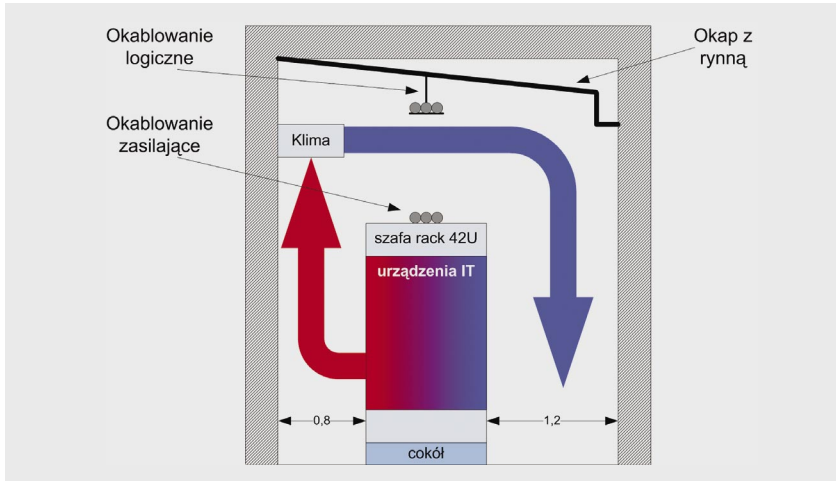
Dla wstawienia jednego rzędu najmniejszych szaf otrzymujemy minimalną szerokość pomieszczenia 2,8m, ale lepiej gdy pomieszczenie ma min. 3m szerokości.

#### Wysokość pomieszczenia

Pomieszczenie serwerowni powinno być wyższe niż 3m ze względu na konieczność zapewnienia miejsca na poprowadzenie okablowania oraz na właściwy obieg powietrza. Jeżeli wysokość pomieszczenia przeznaczonego na serwerownię będzie mniejsza niż 3m, to standardowa szafa rack 42U, która bez dolnego cokołu ma 2m wysokości, pozostawi mniej niż metr na poprowadzenie okablowania.



Rysunek 1. Proponowany model strukturalny organizacji opartej o usługi IT, inspirowany opracowaniem: Zasadnicze wymagania dotyczące zarządzania infrastrukturą NCPI (*W sieci* [2])



**Rysunek 2.** Sposób rozmieszczenia szaf w serwerowni i pozostałych elementów w pomieszczeniu o minimalnym, akceptowalnym rozmiarze. Widzimy, że ogrzane przez urządzenia IT powietrze trafia możliwie najkrótszą drogą do wlotu klimatyzatora, z kolei schłodzone powietrze jest kierowane tak, aby urządzenia IT mogły pobierać je z jednej strony szafy. Nie powinno być także problemów z montażem urządzeń i dostępem do pozostałych elementów. Na rysunku został też schematycznie zaznaczony okap z rynną, który zabezpiecza sprzęt przed zalaniem

### Sufit i to, co jest powyżej

W pomieszczeniach znajdujących się ponad pomieszczeniem serwerowni nie powinno być żadnych instalacji z bieżącą wodą. Jest to wymaganie dość trudne do spełnienia w wielu wypadkach, dlatego też, jeśli zależy nam na zabezpieczeniu sprzętu w serwerowni przed zalaniem (np. przeciekający przez kilka wolnych dni kaloryfer), to o ile pozwala na to wysokość pomieszczenia serwerowni, ochronę przed zalaniem z góry można uzyskać stosując szczelny okap z rynną wewnątrz serwerowni.

### Ściany i sąsiedzi

Współczesny sprzęt IT stosowany w serwerowniach nie należy do najcichszych, dlatego też ściany i drzwi serwerowni powinny mieć odpowiednią dźwiękochłonność, zwłaszcza, jeśli obok serwerowni znajdują się pomieszczenia biurowe do pracy. Nie wolno bagatelizować tego wymagania, ponieważ najnowsze serwery czołowych producentów produkują tak wysoki poziom hałasu, że zgodnie z instrukcją obsługi, praca przy nich jest możliwa tylko w ochronnikach słuchu.

### Sposób rozmieszczenia szaf w pomieszczeniu

Rozmieszczenie szaf (ang. *layout*) jest kluczowym elementem, który ma wpływ na obieg powietrza wewnątrz serwerowni, a tym samym na sprawność systemu chłodzenia. Aby uniknąć mieszania się powietrza zimnego z wylotów maszyn chłodzących z gorącym z wylotów wentylatorów urządzeń (serwerów, macierzy dyskowych, urządzeń łączności teleinformatycznej itp.) wskazane jest zastosowanie tzw.

*zimnych i gorących* korytarzy. W skrócie polega to na takim zaprojektowaniu ustawienia szaf, aby wszystkie maszyny pobierały zimne powietrze z jednej strony szafy i po schłodzeniu wewnętrznych elementów serwera gorące powietrze było wydmuchiwane jak najbliższej wlotów klimatyzatorów (Rysunek 2). Szczegółowe omówienie tego tematu wykracza poza ramy niniejszego artykułu.

## Obszar II. Zasilanie

System zasilania jest kolejnym krytycznym systemem serwerowni, w skład którego wchodzi:

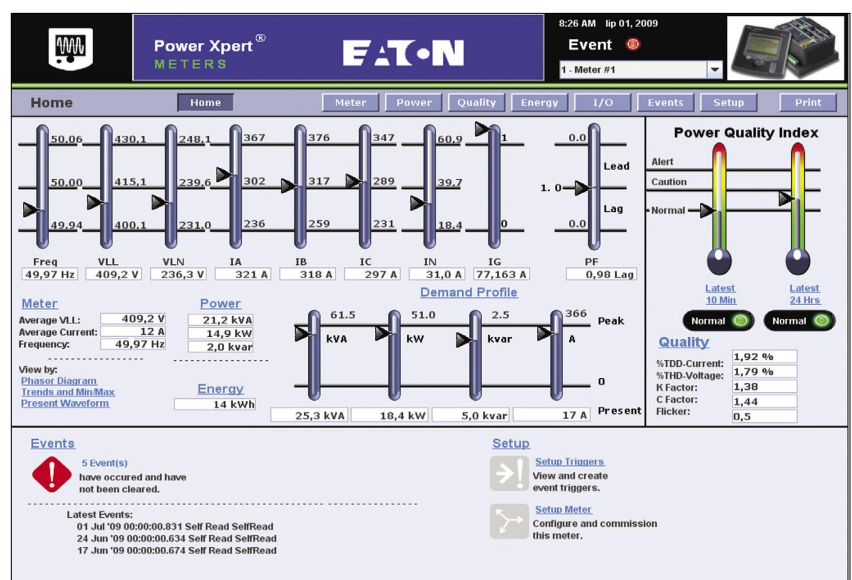
- przyłącza elektroenergetyczne,
- agregat prądowłóczy,

- układ Samoczynnego Załączania Rezerwy (SZR),
- system zasilaczy UPS,
- dedykowane rozdzielnie elektryczne,
- system dystrybucji energii dla urządzeń IT.

Przyłącza elektroenergetyczne (jeśli jest więcej niż jedno) wraz z agregatem prądowłóczym są podłączone do układu SZR, który w przypadku zaniku zasilania z jednego ze źródeł podstawowych, przełącza zasilanie na źródła rezerwowe i stanowi pierwszy stopień redundancji układu zasilania. Za układem SZR są podłączone zasilacze UPS, które w zależności od potrzeb, także mogą pracować w systemie redundantnym. Zadaniem UPS jest podtrzymanie na czas kilku minut napięcia zasilającego urządzenia IT, tak aby mogły zadziałać układy automatyki i uruchomić agregat. System zasilania musi być zaprojektowany przez uprawnionego projektanta i musi uwzględniać bilans mocy wynikający z mocy pobieranej przez:

- zainstalowany i planowany do zainstalowania sprzęt IT,
- klimatyzatory chłodzące serwerownię,
- zasilacze UPS wraz z mocą potrzebną na doładowanie akumulatorów,
- oświetlenie i inne obwody ogólne,
- planowanego wzrostu obciążenia (rezerwa).

Ważne jest takie zaprojektowanie i dobranie wszystkich elementów, aby w sytuacji awaryjnej mogły pracować jako jeden spójny system. Dotyczy to zwłaszcza odpowiedniego dobrania tandemu UPS – agregat, ponieważ w zależności od rodzaju zastosowanych zasilaczy



**Rysunek 3.** Interfejs webowy analizatora jakości mocy Eaton Power Xpert METERS – w rzeczywistości jest to wygodny w obsłudze i efektywny aplet Java



UPS wymagane jest znaczne przewymiarowanie mocy zastosowanego agregatu (w granicznych przypadkach nawet ponad dwukrotnie!).

Celem uniknięcia zakłóceń i ochrony pracujących osób w całym obiekcie serwerowni należy poprawnie zaplanować instalację połączeń wyrównawczych, która musi być dołączona do głównej szyny wyrównawczej budynku zwanej, potocznie *uziomem*. Do instalacji wyrównawczej powinny być podłączone wszystkie przewodzące części konstrukcyjne i wyposażenia serwerowni (np.: obudowy metalowych urządzeń elektrycznych, szaf serwerowych, konstrukcja wsporcza podłogi podniesionej, rury instalacji wentylacyjnej, CO, wody itp.).

### Obszar III. Chłodzenie

Dostarczanie chłodu do serwerowni jest to także obszar odległy od normalnych zadań IT, chociaż, podobnie jak w przypadku struktury fizycznej, decyzje podjęte w tym zakresie mają olbrzymi wpływ na eksploatację sprzętu IT i, co obecnie jest ważniejsze, na koszty tej eksploatacji. Urządzenia IT zainstalowane w serwerowni wymagają ciągłego dostarczania odpowiedniej ilości chłodu niezależnie od tego, czy zainstalowany system chłodzenia może je zapewnić. Jeśli w pomieszczeniu nie będzie wystarczającej ilości chłodnego powietrza, zainstalowane w szafach urządzenia będą pobierać własne gorące powietrze wylotowe (lub gorące powietrze wylotowe sąsiednich urządzeń), aż do momentu kiedy sprzęt IT ulegnie przegrzaniu. Dostarczanie chłodu dla urządzeń IT często jest nazywane *klimatyzacją precyzyjną*, ponieważ w odróżnieniu od *klimatyzacji komfortu* (tzw. biurowej lub domowej) ma na celu utrzymanie odpowiedniego klimatu, tzn. oprócz odpowiedniej temperatury w pomieszczeniu serwerowni musi także zapewnić odpowiednią wilgotność.

Dla urządzeń IT i innych urządzeń elektronicznych zbyt wysoka wilgotność to niebezpieczeństwo kondensacji pary wodnej na podzespołach, a z kolei zbyt niska wilgotność to ryzyko pojawienia się wyładowań elektrostatycznych stanowiących zagrożenie dla poprawnej pracy elektroniki. Dodatkowo, wybierając urządzenia klimatyzacji precyzyjnej należy zwrócić uwagę na następujące parametry:

- Zaawansowane systemy sterowania i automatyki:  
Układy sterowania i automatyki dla klimatyzacji precyzyjnej muszą charakteryzować się następującymi cechami:
  - Praca w układzie redundantnym z cyklicznym przełączaniem pracujących urządzeń (praca w tzw. *trybie turmowsowym*).

- Brak pojedynczego punktu awarii (ang. *Single Point Of Failure, SPOF*).
- Rozszerzone możliwości komunikacyjne – możliwości podpięcia do systemów zarządzania budynkami (ang. *Building Management System, BMS*) poprzez dedykowane protokoły komunikacyjne (np. *Modbus, canBus, LonTalk*, itp.)
- Możliwość pracy całorocznej – klimatyzacja komfortu pracuje tylko kilka godzin dziennie w okresach letnich, natomiast urządzenia klimatyzacji precyzyjnej muszą pracować w trybie 24/7/365. To powoduje, oprócz wymagań na trwałość mechaniczną, znaczne rozszerzenie wymagań co do odporności jednostek zewnętrznych na temperatury w zakresie od -25C do ponad 35C.
- Brak podgrzewacza powietrza – w instalacjach klimatyzacji precyzyjnej nie stosuje się urządzeń służących do podgrzewania powietrza, które są zwykle montowane w instalacjach klimatyzacji bytowej.

Duże ilości powietrza przepływającego przez maszyny – z powodu wysokiej gęstości mocy cieplnej (mocy przypadającej na m2 pomieszczenia) we współczesnych serwerowniach, w instalacjach klimatyzacji precyzyjnej, przepływa dużo więcej powietrza niż w klimatyzacji komfortu, co wymaga odpowiednio dużych wentylatorów w jednostkach wewnętrznych i powoduje wysoki poziom hałasu w pomieszczeniu.

Warto podkreślić, że przeznaczenie i sposób pracy urządzeń klimatyzacji precyzyjnej są całkowicie odmienne od powszechnie znanej i najczęściej widywanej klimatyzacji komfortu, ale niestety inwestorzy, bardzo często, planując serwerownię nie biorą pod uwagę tych różnic lub wręcz pomijają ten ważny aspekt działania i niezawodności nowoczesnych serwerowni.

Dodatkowym problemem jest wentylacja serwerowni dla celów bytowych, tzn. zapewniająca minimalną wymianę powietrza w po-

mieszczeniu umożliwiającą czasowe przebywanie w nim osób z obsługi IT.

### Obszar IV. Okablowanie strukturalne

Głównym problemem występującym w trakcie projektowania okablowania strukturalnego serwerowni jest konieczność upchnięcia setek, jeśli nie tysięcy, połączeń okablowania poziomego, pionowego, połączeń systemowych na zwykle dosyć ograniczonej powierzchni (a dokładniej to w ograniczonej przestrzeni) i dotyczy to zarówno rozwiązań miedzianych jak i światłowodowych. Sumaryczna długość połączeń nawet niewielkiej serwerowni często przekracza kilka kilometrów, przekroje połączonych wiązek osiągają kilkadziesiąt centymetrów, a łączna waga okablowania musi być uwzględniana w procesie obliczania całkowitego obciążenia podłogi. Przy tak skomplikowanej strukturze szczególnego znaczenia nabiera sprawa przyjęcia i konsekwentnego stosowania właściwego oznakowania okablowania, bo bez tego nie jest możliwe zapanowanie nad porządkiem w okablowaniu.

Kolejną istotną sprawą jest wybór odpowiedniego rodzaju okablowania, aby zapewnić bezawaryjną pracę przez założony, zwykle dość długi, okres eksploatacji. W miarę rozwoju rozwiązań technicznych znacznie łatwiej jest wymienić urządzenia na te nowszej generacji niż wymienić istniejące okablowanie, ponieważ zwykle jest to powiązane z praktycznym wyłączeniem z eksploatacji części serwerowni.

W przypadku okablowania miedzianego, praktycznie do wyboru jest kategoria 5e lub kategoria 6. Rozwiązania kategorii 7 nie są w zasadzie obecnie stosowane, ponieważ aby uzyskać pasmo przenoszenia tej kategorii bardziej opłaca się zastosować okablowanie światłowodowe. Kolejne decyzje dotyczą wyboru: typu okablowania (UTP lub FTP), typu powłoki zewnętrznej – niepalna, niepalna LSZH, oraz dodatkowe parametry, takie jak np. odporność

```
login as: admin
admin@i0.0.0.0:~$ ssh' password:

BusyBox v0.60.3 (2006.06.06-02:19+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

# uname -a
Linux localhost 2.4.20_mvl31-samcore #1 Mon Dec 4 10:58:58 EST 2006 ppc unknown
# ls /
bin  cf      dev    home  logs  opt    root  sram  usr
boot db    etc    lib   mnt   proc  sbin  tmp   var
# help

Built-in commands:
-----
. : alias break builtin cd chdir continue echo eval exec exit
exp export false fc hash help jobs let local read readonly return
set setvar shift times trap true type ulimit umask unalias unset
wait

#
```

**Rysunek 4.** Analizator Power Xpert METERS wykorzystuje własną wbudowaną wersję systemu operacyjnego, opartą na jądrze Linux 2.4.20 i oprogramowaniu BusyBox 0.60.3. Mamy możliwość dostępu poprzez SSH

na atak gryzoni. W przypadku wyboru rodzaju okablowania światłowodowego decyzja dotyczy: liczby włókien w kablu; wyboru rodzaju włókna: jednomodowe (9/125) lub wielomodowe (62.5/125, 50/125 lub 50/125 OM3); oraz podobnie jak dla kabli miedzianych typu powłoki zewnętrznej.

## Obszar V. Monitorowanie i zarządzanie

W przypadku IKS istotne jest ciągłe rejestrowanie parametrów pracy urządzeń, takich jak: zasilacze UPS; agregaty prądotwórcze; urządzenia systemu klimatyzacji (ang. *Humidity, Ventilation and Conditioning, HVAC*); czujki środowiskowe (ang. *Environmental Monitoring Probes, EMP*), etc. Wykorzystywane są także analizatory jakości energii elektrycznej (np. urządzenia Power XPERT Xpert METERS 4000/6000/8000 firmy Eaton Powerware – co ciekawe, oparte zresztą o własną wersję systemu GNU/Linux i zestaw narzędzi dla systemów wbudowanych BusyBox – patrz Rysunek 3 i Rysunek 4). Proces ten generuje ogromne ilości danych, które należy gromadzić w takim zakresie, aby możliwe było późniejsze ich analizowanie i wyciąganie wniosków (co stanowi nie tylko składową prac związanych z diagnozowaniem i zapobieganiem awariom, ale jest podstawą planowania działań i efektywnego zarządzania zasobami IKS).

Ponadto, monitorowanie IKS ma odmienną specyfikę niż na wyższych warstwach proponowanego modelu strukturalnego organizacji. Całkowicie nie ma tutaj sensu monitorowanie urządzeń z użyciem protokołu ICMP (PING) czy badanie dostępności usług (np. HTTPS, HTTP, Oracle SQL\*Net etc.), co ma miejsce w wyższych warstwach (serwerów, urządzeń

transmisji danych i pamięci masowych, a także systemów operacyjnych, baz danych i aplikacji – Rysunek 1). Podstawą monitorowania IKS jest protokół SNMP (ang. *Simple Network Management Protocol, SNMP*).

### Protokół SNMP w systemach monitorowania IKS

Do monitorowania IKS, podobnie jak do monitorowania urządzeń transmisji danych czy serwerów, wykorzystuje się protokół SNMP. Powstał on w roku 1988 i miał dostarczyć narzędzia pozwalającego zdalnie zarządzać zasobami infrastruktury sprzętowej sieci komputerowych (początkowy okres popularyzacji Internetu). Warto zauważyć, że protokół SNMP, choć w istocie bardzo prosty (na tym polega jego siła), bywa dość powszechnie niewłaściwie rozumiany – być może dlatego, że ma dość specyficzne zasady działania i różni się od większości powszechnie znanych, usługowych protokołów sieciowych. Ponadto, zgodnie z pierwotnym przeznaczeniem, szczególne miejsce zajął w dziedzinie zarządzania zasobami sieci teleinformatycznych, co częstokroć bywa ziarnem niezgody, jeśli chodzi o wzajemne zrozumienie potrzeb monitorowania zasobów w różnych obszarach i warstwach proponowanego modelu organizacji (Rysunek 1). Rozróżniamy 3 wersje protokołu SNMP.

SNMPv1 – wersja najstarsza, znajdująca się obecnie w powszechnym użyciu, jeśli chodzi o urządzenia IKS. Niestety, słabą stroną tej wersji są minimalne możliwości zabezpieczenia komunikacji między urządzeniami. Istnieje tu o tyle mechanizm hasła uwierzytelniających (zwykle używane są hasła podatne na ataki siłowe – ang. *brute-force attack*), ale cała komunikacja odbywa się jawnym tekstem, standardowo po

protokole UDP/IP (istnieje zagrożenie podsłuchu transmisji poprzez przechwytywanie pakietów sieciowych – ang. *packet sniffing*). Jednak producenci urządzeń IKS w dużym stopniu zdają się nie przejmować tym problemem, a szkoda (niestety, temat bezpieczeństwa SNMP wykracza poza zakres niniejszego opracowania).

SNMPv2 (w tym podwersje SNMPv2p – ang. *party-based*, SNMPv2c – ang. *community based* i SNMPv2u ang. *user-based*) – w tej wersji wprowadzono drobne rozszerzenia funkcjonalności protokołu oraz starano się podnieść poziom zabezpieczeń. Stanowczo rzadziej spotykamy urządzenia IKS wspierające SNMPv2. Zmiany spowodowały też utratę kompatybilności z wersją 1 (jej zapewnienie wymaga stosowania dedykowanych serwerów pośredniczących – ang. *proxy server* lub użycia systemów monitorowania, które obsługują obydwie protokoły, co dziś raczej nie stanowi problemu).

SNMPv3 – ta wersja ma na celu wyłącznie zniesienie problemu niskiego poziomu bezpieczeństwa poprzednich wersji. Nie wprowadza żadnych rozszerzeń funkcjonalnych i jest także rzadziej wspierana przez urządzenia IKS.

Co warto podkreślić, SNMP nie obciąża sieci w znacząco dużym stopniu, co z pewnością stanowi zaletę protokołu.

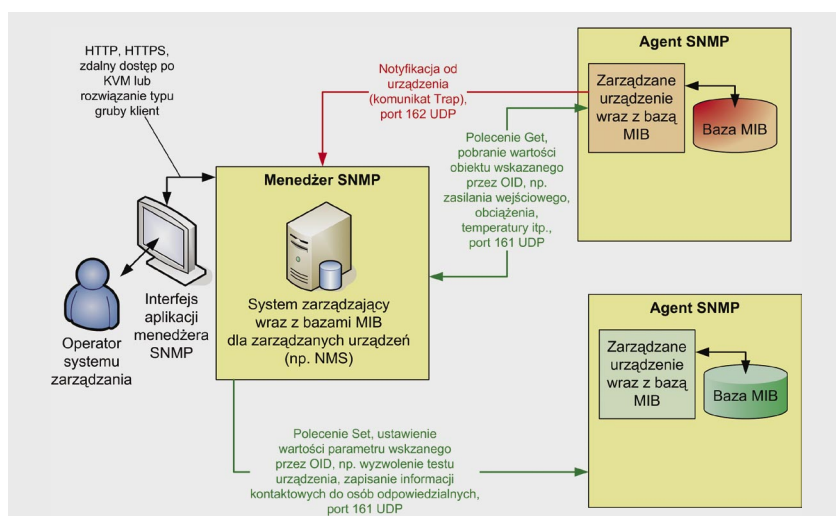
### Model komunikacji i zasada działania SNMP

Protokół SNMP wymaga, aby w sieci funkcjonowały następujące elementy: menedżerowie SNMP (aplikacje monitorujące), agenci SNMP (aplikacje działające po stronie monitorowanych urządzeń) i bazy informacji zarządzania (ang. *Management Information Base, MIB*), dostępne dla obydwu stron komunikacji. Standardowo, komunikacja między menedżerem a agentem SNMP odbywa się z użyciem protokołu UDP/IP i portów:

- 161 – służy menedżerowi do odczytu parametrów z agenta,
- 162 – jest używany podczas przesyłania notyfikacji z agenta do menedżera.

Menedżer SNMP to nic innego jak aplikacja wykorzystywana przez administratora zarządzanego systemu. Zwykle jest to aplikacja typu NMS, ale może być to aplikacja EMS, BMS lub SCADA, o ile wspiera protokół SNMP (Rysunek 5).

Obydwie strony modelu komunikacyjnego SNMP wykorzystują bazy danych MIB (Listing 1) i niewielką liczbę komend, pozwalających wymieniać informacje. Baza MIB jest bardzo charakterystycznym dla SNMP elementem – stanowi ona zorganizowany w postaci struk-



**Rysunek 5.** Schemat rozmieszczenia wymaganych elementów komunikacji dla protokołu SNMP. Widać, że zarówno menedżer, jak i agenci muszą używać właściwych dla danych urządzeń baz MIB. Menedżer SNMP pobiera parametry (tzw. pooling obiektów) oraz odbiera notyfikacje – dane są prezentowane operatorowi



**Listing 1.** Fragment pliku bazy danych MIB przedstawiający wybrane definicje obiektów w języku

```
ASN.1. Widzimy kolejno grupę obiektów odpowiadających parametrom
zarejestrowanym na wejściu zasilacza UPS, odpowiednio: xupsInput-
Voltage (napięcie wejściowe w V), xupsInputCurrent (natężenie
wejściowe w A), xupsInputWatts (moc wejściowa w W) i grupę
parametrów wyjściowych: xupsOutputLoad (obciążenie w procentach
dopuszczalnej pojemności), xupsOutputVoltage (napięcie
wyjściowe w V), xupsOutputCurrent (natężenie wyjściowe w A),
xupsOutputWatts (moc wyjściowa w W).

[...]
--
-- xupsInput group:
--
xupsInputVoltage OBJECT-TYPE
    SYNTAX INTEGER (0..2147483647) -- UNITS RMS Volts
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        „The measured input voltage from the UPS meters
        in volts.”
    ::= {xupsInputEntry 2}
xupsInputCurrent OBJECT-TYPE
    SYNTAX INTEGER (0..2147483647) -- UNITS RMS Amp
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        „The measured input current from the UPS
        meters in amps.”
    ::= {xupsInputEntry 3}
xupsInputWatts OBJECT-TYPE
    SYNTAX INTEGER (0..2147483647) -- UNITS Watts
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        „The measured input real power in watts.”

::= {xupsInputEntry 4}
--
-- xupsOutput group:
--
xupsOutputLoad OBJECT-TYPE
    SYNTAX INTEGER (0..200)
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        „The UPS output load in percent of rated capacity.”
    ::= {xupsOutput 1}
[...]
xupsOutputVoltage OBJECT-TYPE
    SYNTAX INTEGER (0..2147483647) -- UNITS RMS Volts
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        „The measured output voltage from the UPS
        metering in volts.”
    ::= {xupsOutputEntry 2}
xupsOutputCurrent OBJECT-TYPE
    SYNTAX INTEGER (0..2147483647) -- UNITS RMS Amp
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        „The measured UPS output current in amps.”
    ::= {xupsOutputEntry 3}
xupsOutputWatts OBJECT-TYPE
    SYNTAX INTEGER (0..2147483647) -- UNITS Watts
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        „The measured real output power in watts.”
    ::= {xupsOutputEntry 4}
[...]
```

tury drzewiastej zestaw informacji na temat zarządzanego urządzenia. W rzeczywistości są to pliki tekstowe, które zawierają opisy w notacji ASN.1 (ang. *Abstract Syntax Notation One*).

Menedżer SNMP, aby ustawić wartość konkretnego parametru urządzenia, odczytać ją lub zrozumieć odebraną z urządzenia notyfikację, musi się w rzeczywistości poruszać pomiędzy liśćmi drzewa, przechodząc ścieżki wytyczone po gałęziach od liścia do liścia. Te ścieżki nazywane są identyfikatorami obiektów – OID (ang. *Object Identifier*). Każdy OID wskazuje na unikalny dla danego urządzenia obiekt (możemy rozumieć go jako zmienną lub parametr) i składa się z szeregu cyfr oddzielonych kropkami. Z tego względu, identyczna baza MIB musi być dostępna zarówno dla menedżera SNMP (działającego na stacji monitorującej administratora), jak i dla monitorowanego urządzenia (Rysunek 6).

Menedżer SNMP i agent wymieniają między sobą komunikaty, które dotyczą określonej

zmiennej wskazanej za pomocą OID. Oprócz operacji odczytu i zapisu wartości parametrów, istnieje możliwość takiego skonfigurowania agenta, aby w przypadku zajścia określonego zdarzenia (zdefiniowanego w MIB), automatycznie poinformował o tym fakcie menedżera SNMP. W tym celu wykorzystywane są tzw. notyfikacje SNMP (ang. *SNMP notification*), odpowiadające komunikatom typu *Trap*.

Oto kilka numerów OID opisujących różne obiekty (parametry) dla urządzeń IKS:

- Zasilacze UPS Eaton Powerware:

- 1.3.6.1.4.1.534.1.0.0.0.6 – nazwa w MIB: *xupstbReturnFromLowBattery*, przesyła komunikat z MIB: *The battery has recovered from a low battery condition*. Jest to definicja notyfikacji, która może zostać przesłana od agenta do menedżera SNMP po tym, jak baterie zasilacza zostaną doładowane.

- 1.3.6.1.4.1.534.1.3.4.1.2 – nazwa w MIB: *xupsInputVoltage*, zawiera opis w MIB: *The measured input voltage from the UPS meters in volts*. Ten obiekt zawiera wartość napięcia wejściowego w woltach, którą menedżer może odczytać z agenta SNMP.

- Zasilacze UPS Delta-UPS:

- 1.3.6.1.4.1.2254.2.4.5.14.0 – nazwa w MIB: *dupsOutputPower3*, zawiera opis w MIB: *The Output line 3 real power of the UPS system in watts*. Ten obiekt zawiera wartość mocy wyjściowej na trzeciej fazie w watach, którą menedżer może odczytać z agenta SNMP.

- Zasilacze UPS American Power Conversion:

- 1.3.6.1.4.1.318.0.2 – nazwa w MIB *upsOverLoad*, przesyła komunikat z MIB: *SEVERE: The UPS has sensed a load greater than 100 percent of its*

*rated capacity*. Jest to definicja notyfikacji, która może zostać przesłana od agenta do menedżera SNMP po tym, jak UPS wykryje, że został przeciążony.

- Czujka środowiskowa EMP, Eaton Powerware:
  - 1.3.6.1.4.1.534.6.7.1.1.3.2.1.3 – nazwa w MIB `smDeviceTemperature`, zawiera opis w MIB: *Temperature of sensor on device RackMonitor, the unit is 0.1 degree*. Ten obiekt zawiera wartość temperatury mierzonej przez czujkę w 1/10 stopnia C. Menedżer może odczytać tą wartość z agenta.
  - 1.3.6.1.4.1.534.6.7.1.2.0.20 – nazwa w MIB `rmUmidityHighCritical`, przynosi komunikat: *CRITICAL: The humidity of sensor was higher than high critical set point*. Jest to definicja notyfikacji, która może zostać wysłana od agenta do menedżera SNMP po tym, jak czujka wykryje, że wilgotność osiągnęła wartość większą niż najwyższy dozwolony (krytyczny) próg alarmowy.

Podane powyżej ścieżki OID odpowiadają konkretnej lokalizacji w drzewie MIB. Parametry wskazywane przez numery OID mogą być (w zależności od uprawnień menedżera oraz od ich przeznaczenia): czytane lub zapisywane. Przykładem parametrów do odczytu mogą być wcześniej przywołane `xupsInputVoltage`, `dupsOutputPower3`, `smDeviceTemperature`, z kolei parametrem, którego wartość można zmieniać może być np.: dla zasilacza UPS Eaton Powerware: 1.3.6.1.4.1.534.1.8.1.0 – nazwa w MIB `xupsTestBattery`, zawiera opis w MIB: *Setting this variable to startTest initiates the battery test. All other set values are invalid*. Jeśli w tym parametrze (obiekcie) zapiszemy wartość `startTest`, zdalnie wymusimy rozpoczęcie testów baterii.

Jak wspomnieliśmy, protokół SNMP oferuje stosunkowo małą ilość poleceń. Dla wersji 1 najważniejsze to (Rysunek 7):

Odczyt:

- `Get` – pobranie wartości obiektu wskazanego przez OID,
- `GetNext` – pobranie wartości następnego obiektu.

Zapisu:

- `Set` – ustawienie wartości obiektu wskazanego przez OID,

Odpowiedź:

- `Get-Response` – wysłanie odpowiedzi na zapytanie `Get` lub `GetNext` menedżera SNMP.

Notyfikacja:

- `Trap` – asynchroniczne wysłanie notyfikacji o zaistniałym zdarzeniu.

Wersja 2 wprowadza dodatkowo polecenia: `GetBulk` (pobranie grupy wartości obiektów wskazanych OID) i `Inform` (pozwała na przesłanie przez NMS dalej do innych NMS odebranego komunikatu typu `Trap`).

Zanim jakiegokolwiek polecenie zostanie przesłane od menedżera do agenta SNMP, to – w zależności od typu operacji – menedżer SNMP łącząc się z agentem SNMP przekazuje mu jedno ze skonfigurowanych na agencie hasel:

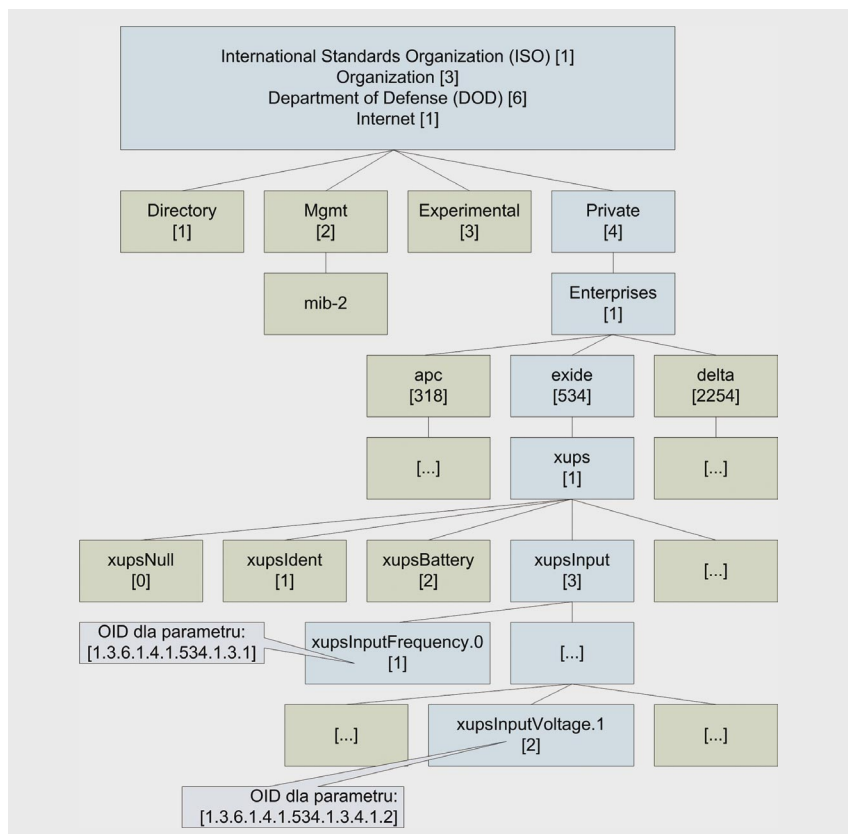
- *Public community*, czy inaczej *read community* – czyli hasło publiczne, odczytu parametrów. Dla większości urządzeń jest ono domyślnie ustawione na *public*, co oczywiście w pierwszej kolejności zaleca się zmienić.

- *Private community*, czy inaczej *write community* – czyli hasło prywatne, zapisu parametrów. Domyślnie jest ono zwykle ustawione na *private* i bezwzględnie należy je zmienić.

W rozległych IKS odbierane przez menedżerów SNMP notyfikacje mogą być przesyłane dalej, np. do nadrzędnej aplikacji menedżera SNMP lub z podstawowego systemu monitorowania na system zapasowy. Zakres tej funkcjonalności zależy od producenta aplikacji monitorującej – zwykle w połączeniu z mechanizmem filtrów daje ona spore możliwości organizowania i separowania informacji. Słabą stroną notyfikacji SNMP jest fakt, że przesyłane z użyciem protokołu UDP (na port 162) są narażone na to, że nie dotrą do celu. Na szczęście, zwykle w sytuacjach alarmowych, dostajemy większą liczbę komunikatów, a o anomaliach będzie można się zorientować także po bieżących wskazaniach monitorowanych parametrów (przekroczenie progów alarmowych).

### Monitorowanie na różne sposoby

Po pierwsze, należy wyróżnić tzw. monitorowanie aktywne (ang. *active monitoring*). – zachodzi ono wówczas, kiedy w systemie moni-



**Rysunek 6.** Drzewiasta struktura bazy MIB ze wskazaniem ścieżek prowadzących od głównego liścia (ISO [1]) do liści zawierających wartości parametrów `xupsInputFrequency.0` (częstotliwość wejściowa linii użytkowej w 1/10Hz) i `xupsInputVoltage.1` (napięcie w V dla pierwszej fazy zasilania). Widać, w jaki sposób konstruowane są numery OID dla urządzeń UPS Eaton Powerware



torującym (np. NMS), pełniącym rolę menedżera SNMP, definiujemy tzw. *pooling*. Jest to mechanizm odpytywania kolejnych urządzeń w puli o wartości ich parametrów. W menedżerze definiujemy także progi alarmowe – jeżeli odpowiedź z danego urządzenia będzie zawierała wartość parametru, która przekracza próg, generujemy zdarzenie alarmowe, np.:

- komunikat ekranowy,
- sygnał dźwiękowy,
- e-mail do administratorów,
- SMS na telefony komórkowe osób dyżurujących,
- komunikat SNMP Trap,
- wyzwolenie dowolnej operacji, na którą zezwala nasza aplikacja monitorująca – np. uruchomienie dodatkowej aplikacji, skryptu etc.

Aktywne monitorowanie pozwala na bieżąco badać parametry i generować zdarzenia alarmowe, ale jest także podstawą drugiego istotnego podejścia do monitorowania. Jest nim monitorowanie wydajności (ang. *performance monitoring*) lub inaczej (co bardziej odpowiada dziedzinie IKS) – kolekcjonowanie danych na potrzeby generowania trendów.

Parametry, które są odczytywane dzięki mechanizmowi *poolingu* z kolejnych urządzeń mogą być zapisywane w bazie danych menedżera SNMP (nie należy mylić bazy danych aplikacji z bazą danych MIB – to dwie różne rzeczy) i zbierane przez zdefiniowany okres czasu. Dzięki temu administrator ma możliwość analizowania trendów przedstawiających zmienność wartości parametrów w czasie. Taka funkcjonalność daje ogromne możliwości, jeśli chodzi o diagnozowanie przyczyn i okoliczności awarii (np. narastająca temperatura oznaczała awarię klimatyzacji), ale także pozwala z wyprzedzeniem przewidywać ewentualne incydenty, planować serwis urządzeń, planować zakupy nowych urządzeń, czy wymianę elementów podlegających zużyciu (np. baterii zasilacza UPS) – w tym sensie dane te mają bezpośrednie przełożenie na szacowane koszty operacyjne. Poza monitorowaniem aktywnym i zbieraniem trendów – czym zajmuje się menedżer SNMP – mamy do czynienia z bardzo istotną odmianą monitorowania, która stanowi w rzeczywistości podstawę efektywnego systemu monitorowania rozległych IKS. Jest to monitorowanie pasywne, oparte na wymianie notyfikacji SNMP. W tym przypadku menedżer SNMP nasłuchuje w sposób ciągły (port 162 UDP), a agenci działający na urządzeniach po zaistnieniu określonego zdarzenia wysyłają notyfikację na skonfigurowany adres zaufanej sta-

cji monitorowania (na której działa aplikacja menedżera). Notyfikacje mogą mieć różne znaczenie i występują na różnych poziomach ważności. Niestety, nie obowiązuje tutaj żaden wyraźny standard, a więc należy umiejętnie skonfigurować zarówno agentów SNMP na naszych urządzeniach, jak i wprowadzić przemyślane reguły filtrowania oraz korelowania zdarzeń w aplikacji menedżera SNMP. Notyfikacje SNMP mają różną ważność, np.:

- Minor 01/07/2009 07:46:26 UPS0001GDY upsTrapAlarmEntryRemoved [1]  
upsAlarmId.0 (Integer): 20 [2]  
upsAlarmDescr.0 (Object ID): upsAlarmCommunicationsLost [3]  
snmpTrapEnterprise.0 (Object ID): upsTraps  
– adapter SNMP utracił łączność z zasilaczem UPS. Nie jest to sytuacja bardzo krytyczna i nie musi oznaczać faktu niedostępności zasilacza UPS. Problem może leżeć po stronie adaptera SNMP lub połączenia i może być chwilowy.
- Info 30/06/2009 23:29:23 UPS0086GDN upsOnBattery [1]  
mtrapargsString.0 (DisplayString): UPS: On battery power in response to an input power problem. [2] snmpTrapEnterprise.0 (Object ID): apc  
– notyfikacja informuje, że zasilacz UPS rozpoczął podtrzymywanie zasilania z baterii w odpowiedzi na zarejestrowany zanik zasilania. Jeżeli sytuacja ta potrwa dłużej, to możemy spodziewać się zadziałania układu SZR, który załączy agregat. Jeżeli w danej lokalizacji nie ma agregatu, czas rozpocząć zatrzymywanie baz danych, aplikacji i wyłączanie sprzętu.
- Info 30/06/2009 23:29:25 UPS0921W-WA powerRestored [1] mtrapargsString.0 (DisplayString): UPS: No longer on battery power. [2] snmp-

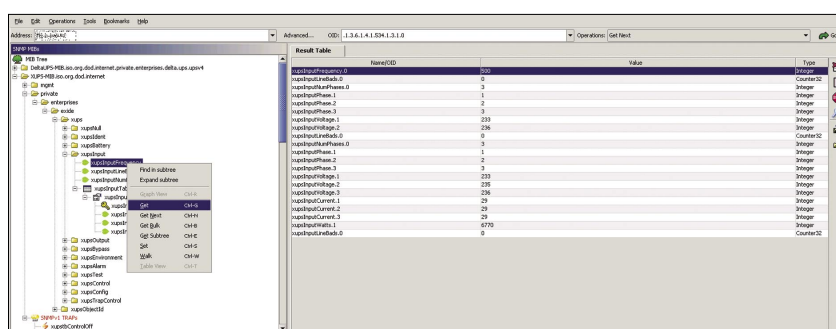
TrapEnterprise.0 (Object ID): apc – wiemy, że zasilacz UPS przestał pracować na bateriach. Oznacza to, że powróciło zasilanie z miasta lub układ SZR załączył agregat. Rozpocznie się teraz ładowanie baterii.

- Warning 30/06/2009 22:10:05 EMP00-32KRA Triggered Manual Threshold For xupsEnvRemoteTemp.0: 26>25 – czujka środowiskowa zgłasza alarm przekroczenia wartości progowej dla temperatury pomieszczenia (25 stopni C), ponieważ bieżąca temperatura wynosi 26 stopni C. To jeszcze nie jest wielki problem, ale warto sprawdzić w jaki sposób narastała temperatura i czego możemy się spodziewać w najbliższym czasie. Może ktoś wyłączył klimatyzator podczas pracy w serwerowni?

## Obszar VI. Bezpieczeństwo fizyczne i ochrona przeciwpożarowa

Ochrona fizyczna jest najstarszym, ale wciąż najpewniejszym sposobem ochrony posiadanych zasobów i stanowi pierwszą linię obrony instytucji przed zagrożeniami. Jej zadaniem, zgodnie z normą ISO 17799, jest *zapobieganie nieuprawnionemu dostępowi, uszkodzeniom i ingerencji w pomieszczenia instytucji i jej informacje*. Często organizacje kładą duży nacisk na ochronę teleinformatyczną zasobów IT i nie doceniają podstawowych mechanizmów i środków ochrony fizycznej, co faktycznie jest podstawą jakiegokolwiek bezpieczeństwa. Nawet najlepsze zainstalowane zapory ogniowe, systemy IDS, czy IPS na nic się zdadzą, jeśli można wynieść dyski z danymi przez niezabezpieczone okno lub spowodować przegrzanie serwerów i przestój serwerowni poprzez uszkodzenie zewnętrznych skraplaczy systemu klimatyzacji.

Podstawą do zaprojektowania systemu ochrony fizycznej jest przeprowadzenie analizy ryzyka i następnie dostosowanie poziomu ochrony do wymagań biznesowych (pamięta-



**Rysunek 7.** Przeglądarka plików zawierających definicje baz MIB (iReasoning MIB Browser PE). Widać dostępne z menu kontekstowego polecenia SNMP, a także odczytane, bieżące wartości dostępnych na urządzeniu parametrów itp. Silną stroną takich narzędzi jest fakt, że dzięki nim w łatwy sposób korzystamy z baz MIB – praca z notacją ASN.1 wymagałaby od człowieka ogromnego wysiłku

jąc oczywiście o wymogach prawa, zaleceniach, normach i dobrych praktykach w tym zakresie).

Poprawnie zaprojektowany system ochrony fizycznej z jednej strony ma uniemożliwić dostęp osobom nieuprawnionym, ale też nie może utrudniać lub uniemożliwiać dostępu osobom uprawnionym. Nie zawsze też trzeba się koncentrować na najnowszych rozwiązaniach technicznych typu rozwiązania biometryczne, a bardzo często funkcjonalności systemu ochrony można uzyskać poprzez odpowiednie zaimplementowanie prostych metod:

- zabezpieczenia budowlanego (odpowiednie ściany, drzwi, okna, kraty itp.),
- zabezpieczenia elektronicznego (systemy: sygnalizacji włamania i napadu, kontroli dostępu, telewizji dozorowej, itp.),
- ochrony fizycznej (recepcja, dozorca itp.),
- zabezpieczeń organizacyjnych typu proceduralne ograniczenie do minimum liczby osób mających dostęp do kluczowych pomieszczeń (często lekceważone rozwiązanie, chociaż skuteczne i najtańsze do wprowadzenia).

Elementem powiązany z system ochrony fizycznej, chociaż zgodnie z przepisami nie wchodzącym w jego skład, jest system ochrony przeciwpożarowej. Kluczowe pomieszczenia w obiekcie, a do nich należy serwerownia, powinny być wyposażone w co najmniej czujki systemu sygnalizacji pożarowej lub jeszcze lepiej w stałą instalację systemu gaszenia gazem.

## Niedocenia filary organizacji

### Procedury i normy

Procedury i normy powinny być jednym z filarów działu IT w każdej organizacji, ale bywa z tym bardzo różnie. Wszelkie procedury są uważane za przejaw biurokracji, chociaż mogą znacznie usprawnić pracę działu IT. Przykładem może być metodyka ITIL, która w zasadzie tylko opisuje, jakie procedury eksploatacyjne i kiedy warto stosować. Jedną z podstawowych pro-

cedur, jakie ITIL poleca zastosować, jest procedura zgłaszania żądań od użytkowników. Nie musi być to od razu wielki system typu Help-Desk, na początek wystarczy wprowadzić zasadę (żeby nie używać niepopularnego słowa: procedurę), że wszystkie zgłoszenia muszą być opisane i wysłane na jeden określony adres poczty. Takie proste rozwiązanie organizacyjne daje działowi IT wiele korzyści:

- powstaje ewidencja, na podstawie której można pokazać aktualne obciążenie pracą,
- automatycznie powstaje dokumentacja i historia ewentualnych zmian,
- po jakimś czasie prowadzi do zmniejszenia liczby telefonów.

Najważniejsze jest konsekwentne przestrzeganie tej zasady przez wszystkich pracowników – jeśli ktoś dzwoni, to należy poprosić o przesłanie opisu zgłoszenia e-mailem, jako podstawy do rozpoczęcia pracy.

Inną kategorią procedur są procedury awaryjne, które w prosty sposób opisują ciąg czynności do wykonania w sytuacji krytycznej. Ze swej natury procedury awaryjne są wykonywane rzadko (a najlepiej, żeby nie zaistniała potrzeba ich wykonywania) i w ich przypadku ważna jest cykliczna weryfikacja. Infrastruktura krytyczna podlega takim samym zmianom jak pozostałe elementy i chyba nikt nie chciałby się znaleźć w sytuacji, w której procedura awaryjna poleca użyć nieistniejącego narzędzia. Dobrą praktyką jest testowanie procedury przez osobę, która na co dzień nie zajmuje się danym obszarem, np. osoba odpowiedzialna za systemy monitorowania testuje procedurę awaryjnego uruchomienia agregatu. Takie podejście pozwala na szybkie zlokalizowanie nieścisłości i błędów w procedurach.

IT jest chyba jedynym obszarem techniki, w którym nie występują prawnie usankcjonowane normy, które muszą być przestrzegane i być może dlatego tak trudno jest nam zrozumieć potrzebę ich stosowania. Najwięcej do czynienia z normami mamy w trakcie procesu budowy serwerowni, a osoba prowadząca taki projekt musi się zapoznać z szeregiem norm i przepisów, m.in. takich jak:

- prawo budowlane,
- normy elektryczne,
- przepisy przeciwpożarowe,
- przepisy BHP.

Ze względu na olbrzymi zakres zagadnień, jakich dotyczą te normy, ważne jest, aby ich spełnienie było potwierdzone przez odpowiedniego specjalistę.

## Dokumentacja

Podobnie jak procedury, nie jest to obszar specjalnie lubiany przez pracowników IT. Mamy w nim do czynienia z dwoma rodzajami dokumentacji:

- Dokumentacja obiektów i urządzeń:
  - plany obiektów,
  - projekty techniczne,
  - dokumentacja konfiguracji,
  - dokumentacja producentów urządzeń.
- Dokumentacja wykonanej pracy:
  - raporty z wykonanych czynności (napraw, przeglądów),
  - wykonane zmiany,
  - obsłużone zgłoszenia.

Liczba dokumentów, z jaką mamy do czynienia w codziennej pracy, jest tak ogromna, że bez systemu porządkującego w krótkim czasie przestaniemy nad nimi panować. Nad ogromem dokumentacji można zapanować na kilka sposobów – od sprawdzonych systemów opartych na drukowanych kartkach umieszczanych w segregatorach (rozwiązanie tanie, proste i skuteczne), poprzez systemy folderów i dokumentów elektronicznych, aż do dedykowanych baz danych i aplikacji. Wybór rozwiązania zależy od liczby przetwarzanych dokumentów, ale najważniejsze jest, aby jakieś było wybrane i konsekwentnie stosowane. Nie wolno też się ludzić, że tego typu rozwiązanie uda się wdrożyć, a potem o nim zapomnieć – *dokumentacja musi żyć i być aktualizowana*, bez tego jest niepotrzebna, a w niektórych przypadkach nawet szkodliwa.

## Podsumowanie

Mamy nadzieję, że udało nam się choć trochę przybliżyć Czytelnikom tematykę ciekawego i chyba na co dzień niedoceniającego obszaru, jakim jest Infrastruktura Krytyczna Serwerowni (IKS). Zachęcamy do przesyłania pytań oraz brania udziału w dyskusjach i konkursach na naszym portalu.



### O autorach:

DCSerwis.pl to grupa specjalistów zawodowo zajmujących się problematyką budowy, utrzymania i zarządzania centrami przetwarzania danych oraz IKS. Jednym z celów działania grupy jest popularyzacja wiedzy dotyczącej IKS, centrów danych i ich znaczenia dla biznesu, także poprzez najnowsza inicjatywę, jaką jest portal społecznościowy DCSerwis.pl.  
Kontakt z autorem: [kontakt@dcservis.pl](mailto:kontakt@dcservis.pl)



### W Sieci

- Data Center Serwis – <http://DCSerwis.pl>
- Zasadnicze wymagania dotyczące zarządzania infrastrukturą NCPI: [http://www.apcmmedia.com/salestools/VAVR-626VR8\\_R0\\_PL.pdf](http://www.apcmmedia.com/salestools/VAVR-626VR8_R0_PL.pdf)
- Witryna firmy iReasoning (MIB Browser): <http://www.ireasoning.com>