ZAŁACZNIK NR 3 DO OPZ

Ministerstwo Sprawiedliwości RP

IUSTITIA EST CONSTANS ET PERPETUA VOLUNTAS IUS SUUM CUIQUE TRIBUENDI

WYTYCZNE
DOTYCZĄCE STANDARDÓW PROJEKTOWANIA, BUDOWY I WDRAŻANIA SIECI LAN W JEDNOSTKACH RESORTU.

Przedstawiony materiał nie zawiera obligatoryjnych wymagań i parametrów technicznych urządzeń dedykowanych do budowy, rozbudowy czy modernizacji sieci lokalnych. Przedmiotowy zarys wytycznych dotyczy propozycji wykorzystania standardów projektowania i wdrażania sieci LAN w jednostkach resortu i ma za zadanie ułatwić podejmowanie optymalnych decyzji w zakresie technologii budowy sieci lokalnych w jednostkach resortu. Zakres tematyczny zagadnień kompleksowo ujmuje większość istotnych elementów niezbędnych do uwzględnienia przy opracowywaniu projektów, specyfikacji technicznych czy też ustaleń szczegółowych wymagań w zakresie budowy sieci lokalnych.

Istotą projektu jest stworzenie podstaw do właściwego wykonania infrastruktury w budynku, charakteryzującej się możliwością łatwej modyfikacji lub rozbudowy, z koniecznym uwzględnieniem wytycznych zawartych w opisie szczegółowym. Projekt sieci powinien być oparty na założeniach wynikających z polskich norm budowlanych, przepisów branżowych, dotyczących wykonania prac kablowych, wytycznych producentów elementów systemu, międzynarodowych standardów dla sieci komputerowych (ISO, IDEE, TSB). Projekt sieci logicznej musi umożliwiać etapową budowę sieci i punktów logicznych. Użyte w projekcie elementy, urządzenia, sprzęt i akcesoria, muszą odpowiadać parametrom technicznym zgodnie z przyjętymi standardami i normami w tym zakresie. Projekt musi zawierać propozycję konkretnych rozwiązań (elementy, urządzenia, sprzęt i akcesoria).

OKABLOWANIE STRUKTURALNE

Całość budynku powinna posiadać okablowanie strukturalne co najmniej kategorii 6 z podziałem na okablowanie pionowe i poziome integrujące wszystkie systemy teletechniczne włącznie z siecią telefoniczną instalowane w budynku oraz dedykowaną sieć energetyczną do zasilania lokalnej sieci komputerowej.

- projekt rozkładu PEL (punkt elektryczno – logiczny) w budynku powinien uwzględniać strukturę danej jednostki.
- oszacowanie liczby PEL w poszczególnych pomieszczeniach powinno być projektowane z określonym nadmiarem. Ułatwia to rekonfigurację oraz dopuszcza mobilność pracowników.
- opis i numeracja gniazd w szafach krosowniczych i PEL'i powinna być wykonana w sposób jednoznaczny i nie nastręczać trudności w interpretacji zarówno w bieżącym użytkowaniu sieci jak i przy rozbudowie okablowania strukturalnego.
- dla każdego piętra w budynku (lub segmentu sieci, lub piętra i segmentu sieci) powinna być przewidziana wydzielona szafa krosownicza.
- kable łączące serwery i urządzenia z szafą krosownicą lub też inne o istotnym znaczeniu powinny być w innym kolorze niż pozostałe – ułatwia to zarządzanie.
- w każdym pomieszczeniu użytkowników systemów specjalizowanych, jak również w pomieszczeniach biurowych powinny zostać zainstalowane punkty elektryczno – logiczne składające się z dwóch gniazd logicznych i 4 gniazd elektrycznych wg następującej zasady:
- pokój jednoosobowy 2 PEL
- pokój dwuosobowy 3 PEL
- pokój 3 osobowy 4 PEL

Wyjątek stanowią pomieszczenia techniczne serwerowni, pomieszczenie obsługi technicznej centrum monitoringu i zarządzania , pomieszczenie administratorów sieci lokalnej LAN oraz sale uruchomień i testów sprzętu i oprogramowania, gdzie ilość PEL powinna być określana w zależności od potrzeb.

· projekt powinien uwzględniać budowę okablowania w oparciu o kabel UTP kategorii 6 z możliwością transmisji danych z szybkością do 1000 Mbps, a także połączenie punktów dystrybucyjnych kablami optycznymi.

· projekt winien przewidywać instalowanie gniazd abonenckich wykonanych w standardzie 45 x 45. W jednym module 45 x 45 mogą być zainstalowane 2 pojedyncze gniazda RJ45.

· systemy kanałów kablowych, gniazda natynkowe , powinny pochodzić od jednego producenta. Kanały kablowe muszą umożliwiać zwiększenie pojemności minimum 30% zapasu pojemności. Gwarancją jakości materiału PCV użytego do wykonania systemu jest znak CE w oparciu o normę EN 50085 1.

· trasy prowadzenia przewodów transmisyjnych okablowania poziomego oraz kabli okablowania pionowego należy skoordynować z istniejącymi i wykonywanymi instalacjami w budynku m.in. dedykowaną instalacją elektryczną, instalacją elektryczną ogólną, instalacją centralnego ogrzewania, wody, gazu, itp.

· dedykowaną dla okablowania instalację elektryczną należy wykonać zgodnie z obowiązującymi normami i przepisami (minimalne wymagania elementów okablowania strukturalnego to kategoria 6 / klasa E oraz RJ45 jako interfejs końcowy dla połączeń na skrętce miedzianej 4 parowej). Aby w momencie uruchamiania sieć logiczna nie stała się przestarzałą, powinna zostać wykonana zgodnie z najnowszymi standardami okablowania strukturalnego - normą ISO/IEC 11801 wydanie drugie (wrzesień 2002) lub EN 50173 wydanie drugie (październik 2002).

Ze względu na wciąż rosnące wymagania prędkościowe komputerów i aplikacji, coraz mocniej zaznaczające swą obecność i przydatność usługi multimedialne, minimalne wymagania elementów okablowania strukturalnego to kategoria 6 / klasa E oraz RJ45 jako interfejs końcowy dla połączeń na skrętce miedzianej 4 parowej, a dla połączeń światłowodowych włókno wielodomowe 50/125mm oraz nowy standard dla sieci LAN - MT-RJ. Kategoria 6 jest najnowszym dodatkiem do standardów okablowania strukturalnego i posiada dwukrotnie szersze pasmo przenoszenia niż okablowanie Kategorii 5e. To poszerzone pasmo przenoszenia, razem ze znacznie powiększoną odpornością na zewnętrzne zakłócenia, zabezpiecza potencjał Kategorii 6, który pozwoli obsługiwać wielo-gigabitowe aplikacje. Określone w nowym standardzie specyfikacje narzucają producentom konieczność opracowania takich komponentów Kategorii 6, które będzie można dowolnie mieszać i łączyć (ang. Mix&Match) nawet z produktami konkurencji. Taka sytuacja gwarantuje użytkownikom sieci swobodę wyboru technologii lub zmianę dostawcy. Norma eliminuje również możliwość wyboru komponentów, które są tylko oznaczone symbolem "Cat.6", a w rzeczywistości nie spełniają wymagań założonych przez zatwierdzony nowy standard. Dlatego inwestor, przyszły użytkownik czy instalator okablowania powinien wiedzieć, jak odróżnić systemy RZECZYWISTEJ kategorii 6 od systemów, które tylko mają napis "Cat.6". Oprócz oznaczenia produktu istotne jest również dołączenie do niego odpowiednich certyfikatów testowania nową metodą "De-Embedded Testing" określoną dokładnie w standardzie ANSI/TIA/EIA 568-B.2 Cat.6 (załącznik E i F). Tylko komponenty, które są przetestowane tą metodą gwarantują uzyskanie RZECZYWISTEJ Kategorii 6/Klasy E. Poprzednie metody testowania nie spełniają aktualnych potrzeb i okazały się zawodne (ze względu na brak powtarzalności wyników) szczególnie przy częstotliwościach powyżej 100MHz. Dlatego by zagwarantować użytkownikowi rzeczywiste i powtarzalne parametry Kategorii 6 wymaganym jest, by na etapie składania oferty na realizację projektu wykonawca przedstawił odpowiednie certyfikaty wydane przez niezależne laboratoria uwzględniające najnowszą metodę kwalifikacji komponentów sieciowych (tj. de-embedded testing).

· ze względu na bezpieczeństwo transmisji oraz w celu zminimalizowania oddziaływania zakłóceń, szczególnie w miejscach o dużej ilości kabli transmisyjnych i nakładania się różnych instalacji prądowych, w projekcie należy przewidzieć budowę okablowania poziomego w wersji ekranowanej. Spełnienie postulatów kompatybilności elektromagnetycznej, a więc zwiększenie odporności systemu informatycznego na zakłócenia elektromagnetyczne oraz ograniczenie emisji zakłóceń do środowiska zewnętrznego znacząco zwiększa bezpieczeństwo transmisji danych.

· wydajność okablowania powinna być zgodna z najnowszymi wytycznymi komitetów normalizacyjnych, tj. draftem specyfikacji JTC 1/25N 981 określającym pasmo przenoszenia dla systemów Klasy E/Kategorii 6 na 625MHz, a pasmo przenoszenia dla systemów Klasy F/Kategorii 7 na 1GHz.

W przypadku budowy sieci LAN w nowych budynkach (często są one projektowane i wykonywane zgodnie z zaleceniami 'inteligentny budynek') wymagane są jedynie prace dostosowawcze konfiguracyjne zależnie od potrzeb. W przypadku budynków o starszej konstrukcji, czy też zabytkowych wymagane jest wcześniejsze rozpoznanie najdogodniejszych rozwiązań – trasowania okablowania lub też uzyskania stosownych zezwoleń dla budynków o charakterze zabytkowym. W przypadku starszych budynków okablowanie powinno być prowadzone w rynnach PCV lub w podwieszkach sufitowych wraz z pozostałym okablowaniem. Zalecana jest integracja sieci komputerowej, alarmowej, telewizyjnej, przeciwpożarowej, telefonicznej w postaci jednego okablowania strukturalnego (znaczne obniżenie kosztów – ułatwione zarządzanie, konfiguracja i rekonfiguracja sieci itp.).

· zaleca się nie przekraczanie odległości 90 [m] od głównego punktu dystrybucyjnego. W przypadku braku możliwość spełnienia niniejszego warunku sieć należy podzielić na segmenty (połączone np. poprzez światłowód w przypadku znacznego oddalenia lub Gigabit Ethernet), lub stosować 'reapet'ery' (wzmacniacze). Wybór najkorzystniejszego rozwiązania zależy od istniejących uwarunkowań lokalnych.

Ponadto projektowany system okablowania strukturalnego powinien bezwzględnie spełniać następujące warunki:

· wszystkie elementy przeznaczone do budowy okablowania strukturalnego muszą pochodzić od jednego producenta. W przypadku rozbudowy systemu okablowania strukturalnego należy go kontynuować o ile to możliwe w tym samym systemie w celu zapewnienia jednolitego zarządzania i instalacji,

· należy zastosować ekranowane kable logiczne o paśmie przenoszenia od co najmniej 600 MHz (kategoria 6) do 1200 MHz (kategoria 7) w celu zapewnienia przyszłej rozbudowy i możliwości integracji usług multimedialnych w ramach okablowania.

· kable transmisyjne muszą być zakończone w sposób trwały na 8-pozycyjnym złączu modularnym; nie są dopuszczalne zmiany i rekonfiguracje rozszycia w trakcie pracy systemu.

· system powinien pozwalać na zmianę typu interfejsu dowolnego punktu przyłączeniowego bez zmiany rozszycia kabla, tj. poprzez wymianę wkładki na odpowiednią w panelu krosowym lub zestawie instalacyjnym (gnieździe) użytkownika.

· montaż / wymiana wkładki nie może wymagać ponownej terminacji kabla na złączu.

· do typowego punktu przyłączeniowego należy doprowadzić dwa kable logiczne zakończone na dwóch gniazdach z dwoma wkładkami 1xRJ45 Kat.6. Wyjątek stanowić będą niektóre miejsca wskazane po uzgodnieniach z użytkownikiem.

· system powinien pozwalać na wykorzystanie w przyszłości transmisji wielokanałowej (rozdział par pod wspólną osłoną kabla) bez zmian w rozszyciu kabla, wyłącznie poprzez wymianę wkładki.

· system powinien dopuszczać możliwość wykorzystania wkładek z nowymi interfejsami (min. na klasę F) po wprowadzeniu ich do specyfikacji przez komitety normalizacyjne.

· system powinien pozwalać na transmisję sygnału TV w pełnym paśmie oraz integrację transmisji CATV w ramach istniejącej infrastruktury kablowej przez zamontowanie / wymianę wkładki na odpowiednią (z interfejsem typu F) bez konieczności ingerencji w zakończenie kabla.

· wszystkie kable sygnałowe powinny być oznaczone numerycznie, w sposób trwały, tak od strony gniazda, jak i od strony szafy montażowej. Te same oznaczenia należy umieścić w sposób trwały na gniazdach sygnałowych w punktach przyłączeniowych użytkowników oraz na panelach w piętrowych punktach dystrybucyjnych. Po zrealizowaniu projektu, uruchomieniu i wykonaniu pomiarów instalacji, wykonawca powinien sporządzić dokumentację powykonawczą instalacji kablowej uwzględniającej wszelkie, ewentualne zmiany w trasach kablowych i rzeczywiste rozmieszczenie punktów przyłączeniowych w pomieszczeniach.

· wykonawca powinien udzielić jednolitej 15 lub 25-letniej bezpłatnej gwarancji na system od producenta oferowanego systemu okablowania strukturalnego (powinien być dostarczony certyfikat po wykonaniu pomiarów kontrolnych okablowania) zawierająca również gwarancję na komponenty (min. kable, gniazda, panele krosowe, wkładki, kable krosowe i przyłączeniowe, szafę kablową i elementy zarządzające, system połączeń telefonicznych, zabezpieczenia linii telefonicznych, itp).

· na etapie projektu należy uwzględnić odpowiednią ilość zapasowych elementów wymiennych (wkładek wielokrotnych) w celu zapewnienia możliwości przyszłej rekonfiguracji przez użytkownika.

Poprawność wykonania instalacji sieci sygnałowej powinna być potwierdzona pomiarami statycznymi i dynamicznymi właściwości poszczególnych torów. Pomiary takie wykonuje się specjalistycznymi testerami okablowania (np. OmniScanner, DSP 4300). Należy przeprowadzić testy okablowania dla wszystkich punktów przyłączeniowych. Dla łączy światłowodowych należy przeprowadzić pomiary tłumienności zgodnie z wymaganiami odpowiednich standardów (dwukierunkowe pomiary sygnałem w

dwóch oknach transmisyjnych). Wszystkie raporty z pomiarów powinny zostać dołączone do dokumentacji powykonawczej i przekazane zamawiającemu.

ZASILANIE ENERGETYCZNE, DEDYKOWANA SIEĆ ELEKTRYCZNA

System energetyczny zasilania obiektu, powinien być zbudowany tak , by istniała możliwość zasilania z dwóch zewnętrznych, niezależnych, przełączanych automatycznie linii energetycznych. Sieć zasilająca infrastrukturę techniczną systemu informatycznego musi być wykonana w postaci wydzielonej instalacji elektrycznej oraz mieć możliwość podtrzymywania napięcia w sytuacjach awaryjnych pozwalających na bezpieczne wyłączenie urządzeń.
Jednym z rozwiązań jest zastosowanie kilku UPS-ów obsługujących poszczególne strefy:
1. Kablownia - wprowadzenia i wyprowadzenia traktów transmisyjnych, klimatyzatora centralnego oraz przyłączy telefonicznych,
2. Siłownia –UPS o co najmniej mocy sumarycznej stanowisk komputerowych i urządzeń aktywnych pracujących w sieci LAN,
3. Serwerownia - UPS o co najmniej mocy sumarycznej serwerów i urządzeń aktywnych obsługujących użytkowników poszczególnych aplikacji lub jednego centralnego UPS o mocy pozwalającej na podtrzymanie wszystkich urządzeń aktywnych komputerowej sieci lokalnej.
Czas podtrzymania zasilania pracy urządzeń aktywnych powinien być obliczony w taki sposób, by było możliwe bezpieczne wyłączenie zasilanych urządzeń aktywnych w przypadku zaniku zasilania w sieci. Na potrzeby doboru typu i producenta UPS, należy wstępnie oszacować maksymalną i nominalną moc [kVA] urządzenia podtrzymującego zasilanie w oparciu o sumaryczny pobór mocy zasilanych urządzeń.
Moc przewidziana na standardowe pojedyncze gniazdo zasilania PC powinna wynosić ok. 200÷300 [W], dla drukarki laserowej ok. 1 [kW]. Standardowo w jeden obwód prądowy zaleca się grupować ok. 10 gniazd. W serwerowi zaleca się instalację, co najmniej 4 gniazd po 2,5 [kW] oraz kilku-kilkunastu po 500 [W].
Najczęściej długość sznurów zasilających (dla komputera oraz dla monitora) wynosi ok. 1,2÷1,5 [m]. Przy projektowaniu sieci i montażu PEL należy uwzględnić zasady ergonomii w zakresie ich rozmieszczenia np. odległości od podłogi (30÷50 [cm] lub większej). W czasie eksploatacji, należy zadbać aby do wydzielonych obwodów zasilania sieci komputerowej nie były podłączone inne urządzenia np. czajniki, grzejniki itp.
Należy zapewnić również odpowiednią wentylację i klimatyzację pomieszczeń, w których zainstalowano aktywne urządzenia sieciowe (serwery, routery, UPS i inne). W pomieszczeniach tych należy sprawdzać poprawność instalacji systemu wentylacji jak też zapewnić okresowe kontrole i monitoring temperatury. Do pomieszczenia (pomieszczeń) UPS powinno być doprowadzone okablowanie logiczne, tak by istniała możliwość zdalnego monitorowania i zarządzania pracą UPS z pomieszczenia administratora. Pomieszczenia techniczne, w tym serwerownie powinny być zabezpieczone przed dostępem osób trzecich.
Wszystkie elementy związane z systemem zasilania dedykowanego powinny być starannie oznakowane. Główne bezpieczniki, przełączniki, 'bypass', doprowadzenia w głównej szafie zbiorczej zasilania jak i poszczególne podziały na obwody prądowe, kolejność faz w głównym przyłączu powinny być jasno i prosto oznakowane zgodnie z dokumentacją.

SERWEROWNIA I POMIESZCZENIA TECHNICZNE

Pomieszczenie techniczne serwerowni to główny punkt dystrybucyjny okablowania strukturalnego, w którym zbiegać się będzie okablowanie poziome i pionowe obiektu, kable światłowodowe, jak również doprowadzenia traktów sieci rozległej we/wy od głowicy telekomunikacyjnej budynku. Jako urządzenia aktywne można zastosować przełączniki zarządzalne warstwy 3, które powinny posiadać dożywotnią gwarancję producenta. Do połączenia okablowania szkieletowego sieci może być wykorzystany przełącznik światłowodowy w standardzie 1000Base-SX.
O ile jest to możliwe w serwerowni zalecane jest stosowanie podłogi technologicznej co w trakcie eksploatacji sieci ułatwi prowadzenie i rekonfigurację okablowania strukturalnego. Podłoga powinna być antystatyczna i niepalna ze względu na koncentrację w pomieszczeniu urządzeń pracujących w sposób ciągły.
Liczba gniazd (punktów PEL) powinna być o 20% większa od wstępnie oszacowanej w serwerowni i pomieszczeniu administratorów.

Serwerownia powinna być zabezpieczona przed dostępem osób trzecich z dodatkowymi zabezpieczeniami w zakresie ochrony przeciwpożarowej.
Pomieszczenie(a) przeznaczone dla administratorów oraz operatorów powinno być (o ile to możliwe) oddzielone fizycznie od pomieszczenia technicznego serwerowni. Pomieszczenie to powinno być wyposażone w szafę pancerną, zabezpieczoną ppoż. przeznaczoną do przechowywania zapasowych kopii danych oraz użytkowanych systemów i aplikacji, pakietów oprogramowania oraz innych informacji i danych podlegających szczególnej ochronie.
Korzystnym jest, aby wszystkie pomieszczenia techniczne serwerowni były pomieszczeniami przyległymi i były ze sobą połączone.
Klimatyzacja w pomieszczeniu serwerowni powinna być dostosowana do warunków pomieszczenia i mocy cieplnej wydzielanej przez zainstalowane urządzenia.
Wszystkie urządzenia aktywne, pasywne, modemy i serwery powinny być umieszczone w szafach dystrybucyjnych typu „rack". Szafy krosownicze i teletechniczne powinny być montowane w standardzie 19" i umożliwiać zainstalowanie odpowiedniej liczby urządzeń aktywnych. Liczba elementów aktywnych zależy od ilości punktów sieci. Należy przyjąć, że na każde 48 punktów logicznych należy przewidzieć miejsce w szafie o wysokości 2U. W szafach powinno być zarezerwowana przestrzeń umożliwiająca ewentualne ustawienie urządzeń teletransmisyjnych o wysokości 15 [cm]. Szafa powinna uwzględniać miejsce na zamontowanie lokalnego UPS'a podtrzymującego działanie urządzeń aktywnych zamontowanych w szafie. W szafie powinna być zainstalowana listwa zasilająca (lub listwy, w zależności od potrzeb) umożliwiająca zasilanie zamontowanych tam urządzeń.
Montowane w szafach koncentratory (HUB'y) i przełączniki (SWITCH'e) i urządzenia transmisji danych (ROUTER'y, MODEM'y), powinny pochodzić od renomowanych producentów i tak dobrane, by zabezpieczały około 5÷10 % wolnych gniazd dla łatwej rekonfiguracji połączeń w ramach sieci lokalnej. Zalecane jest zaimplementowanie zapasowego (redundantnego) łącza teletransmisyjnego.
Dla zabezpieczenia planowanej do wdrożenia korporacyjnej sieci WAN w szafach teletechnicznych serwerowni należy przewidzieć miejsce do włączenią i uruchomienia dodatkowego routera i urządzenia bezpieczeństwa dostarczanych przez operatora telekomunikacyjnego.
Zaleca się instalowanie szaf krosowniczych na poszczególnych piętrach budynku w wydzielonych pomieszczeniach. Pomieszczenia powinny być zabezpieczone przed dostępem osób nieupoważnionych i mieć zapewniony odpowiedni poziom wentylacji umożliwiający poprawną eksploatację zamontowanego tam sprzętu. W przypadku niewystarczającej samoistnej wentylacji i zbyt wolnej wymiany powietrza w pomieszczeniu należy stosować dodatkowe wentylatory lub wyposażyć obudowę szafy w dodatkowe otwory wentylacyjne.

Załącznik Nr 1

NORMY I WYMAGANIA.

System okablowania strukturalnego musi spełniać wymagania aktualnie obowiązujących norm: ISO/IEC 11801:2002 wydanie drugie lub EN 50173-1:2002 wydanie drugie, dotyczących okablowania strukturalnego budynków.
Przy wykonywaniu wyceny prac należy uwzględnić wymóg dostarczenia przez wykonawcę wyników pomiarów powykonawczych i testów okablowania (statycznych i dynamicznych), potwierdzonych protokołami.
Wymagane jest również dołączenie do dokumentacji odpowiednich certyfikatów zgodności komponentów i systemu okablowania z jednym z obowiązujących standardów:
· ISO/IEC 11801:2002 wydanie drugie
· EN50173-1:2002 wydanie drugie
· ANSI/TIA/EIA 568-B.2 Cat.6
· draft specyfikacji JTC 1/25N 981

Aby zapewnić długi czas eksploatacji okablowania strukturalnego a także niezmienność parametrów transmisyjnych sieci w trakcie użytkowania systemu wymagane jest udzielenie użytkownikowi końcowemu możliwie najdłuższej gwarancji systemowej uznanego producenta okablowania (a nie gwarancji firmy instalacyjnej, która w przyszłości może zniknąć z rynku).

Międzynarodowe komitety normalizacyjne (ISO/IEC 11801 i EN 50173) zwracają uwagę na stały wzrost wymagań na rynkach światowych w zakresie wydajności systemów okablowania. Gigabitowy Ethernet był pierwszą aplikacją prowadzącą poprzez dodatkowe parametry (Power Sum Next, Elfext, PowerSum Elfext i Delay Skew) do systemu powszechnie nazywanego kategorią 5 podwyższoną. Wymagania te ujęte zostały w najnowszej edycji standardu ISO/IEC 11801 (rok 2000) na Kategorię 5/Klasę D. Systemy okablowania zbudowane zgodne z wymaganiami tego standardu są wystarczające dla wszystkich aplikacji potrzebujących pasma przenoszenia do 100 MHz włącznie z Gigabitowym Ethernetem pracującym na czterech parach okablowania strukturalnego.
Aktualnie opracowywane są nowe systemy użytkowe i aplikacje, które wymagają szerszego pasma przenoszenia. Odpowiedzią na powyższe jest aktualnie opracowywany protokół Gigabitowego Ethernetu pracujący na dwóch parach (podobnie jak to było w przeszłości z protokołami Ethernet i Fast Ethernet). Z tego powodu w czerwcu 2002 roku zaaprobowano standard Kategorii 6 (Klasy E) w USA, a w Europie został on wprowadzony w życie we wrześniu 2002 r. Zgodnie z jego wymaganiami, systemy okablowania kategorii 6 muszą posiadać wydajność do 200/250 MHz (praca/test).
Obecnie powszechnie znanym i standardowym interfejsem dla systemów okablowania kategorii 5 i 6 jest RJ45. Interfejs ten pozostanie standardowym interfejsem dla obecnie eksploatowanych i projektowanych systemów kategorii 5 i 6. Jednak, ze względu na swoją konstrukcję, RJ 45 nie jest w stanie poprawnie pracować na czterech parach zgodnie z wymaganiami dla kategorii 7 i z tego powodu aktualnie pojawiły się nowe propozycje interfejsów dla okablowania kategorii 7.
Komisja normalizacyjna IEC SC48B: IEC 60603-7-x aktualnie opracowuje nowy interfejs o bardzo wysokiej wydajności. Większość nowoopracowywanych interfejsów dla kategorii 7 to tzw. interfejsy czterokanałowe. Są one najbardziej odpowiednie dla kabli o konstrukcji PiMF, które będą wymagane w niedalekiej perspektywie dla bardzo szybkich systemów i aplikacji. Nowe aplikacje (szczególnie multimedialne) nakładają na systemy okablowania strukturalnego dodatkowe wymagania – aplikacje te potrzebują gwarancji znacznie szerszego pasma przenoszenia. Z tego też powodu komitet normalizacyjny ISO/IEC opracował kolejny standard - kategorię 7 (Klasę F) przeznaczony do obsługi aplikacji o paśmie do 600 MHz w oparciu o kabel PiMF 1.2 GHz. Trwają również prace nad nowym standardem kategorii 8.
Nie stanowi zatem zaskoczenia fakt, że najnowsze badania rynku przewidują, że w ciągu najbliższych dwóch - trzech lat ponad 90 procent wszystkich nowych instalacji okablowania strukturalnego opartych na kablach miedzianych będzie pracowało w oparciu o standard okablowania strukturalnego kategorii 6.

Załącznik Nr 2

ELEMENTY POLITYKI BEZPIECZEŃSTWA

dla pomieszczeń, gdzie zlokalizowane będą serwerownie i infrastruktura techniczna sieci lokalnej (serwery, urządzenia aktywne, modemy i urządzenia dystrybucyjne) oraz w zakresie eksploatacji systemów informatycznych.

Przetwarzanie, wymiana i archiwizacja informacji korporacyjnych (biznesowych) mających zasadnicze znaczenie dla funkcjonowania instytucji z wykorzystaniem technicznych środków teleinformatycznych powinno odbywać się w sposób kontrolowany i dostęp do nich powinien być ograniczony pomimo iż nie są one kwalifikowane jako informacje niejawne stanowiące tajemnicę państwową czy służbową . Są to jednak informacje bardzo ważne (wrażliwe) dla instytucji i ich utrata lub zniszczenie może spowodować duże straty. Jednakowej ochronie powinny podlegać wszystkie atrybuty bezpieczeństwa tych informacji takie jak: dostępność, poufność i integralność .
Dostępność – cecha zapewniająca, że zasoby informacyjne są dostępne użytkownikowi w wymaganym miejscu, czasie i w wymaganej formie;
Poufność – cecha zapewniająca, że dostęp do zasobów informacyjnych jest ograniczony tylko do kręgu osób uprawnionych.
Integralność – cecha zapewniająca, że oryginalna forma lub stan zasobów może być zmieniony tylko przez osoby do tego uprawnione.
Do oceny poziomu wrażliwości zasobów, w tym zasobów informacyjnych, które nie są klasyfikowane jako informacje stanowiące tajemnicę państwową lub służbową można wykorzystać:

· wymagania normy PN-ISO/IEC 17799/2003 Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji,
· wymagania normy PN-93/E-08390/14 Systemy alarmowe. Wymagania ogólne. Zasady stosowania.
Na podstawie tych dokumentów wyróżnia się (ze względu na stopień zagrożenia i wartość szkód) cztery kategorie zagrożonych wartości i jedenaście klas odporności (KO), odpowiadające różnym poziomom ryzyka utraty danych. Dla pomieszczeń , gdzie są zlokalizowane serwerownie mają zastosowanie kategorie Z2 i Z3.
Kategoria zagrożonej wartości Z2 - KO (II –V) - mienie średniej wartości, które można wymienić lub zastąpić oraz dokumenty (w tym w formie elektronicznej), których uszkodzenie, zniszczenie, ujawnienie lub kradzież spowoduje straty w instytucji.
Kategoria zagrożonej wartości Z3 – KO (VI-VIII) - mienie dużej wartości oraz dokumenty (inne zasoby) o dużej wartości, których uszkodzenie, zniszczenie lub kradzież jak również dostęp do informacji w nich zawartych przez osoby nieuprawnione może prowadzić do dużych szkód.
gdzie:
· KO - klasa odporności pomieszczeń i urządzeń na włamanie [RWP].

Z analizy danych, zamieszczonych w dokumentacji projektowej poszczególnych systemów informatycznych eksploatowanych w resorcie sprawiedliwości i charakterystyki przetwarzanych informacji należy przyjąć, że informacje te kwalifikują się do drugiej i trzeciej grupy kategorii zagrożonych wartości (Z2, Z3). Oznacza to, że systemy alarmowe przeciw włamaniowe i przeciw napadowe powinny spełniać wymagania trzeciego poziomu tzn. kategorii SA3 według PN-93/E-08390/14. Również zabezpieczenia ochrony fizycznej – budowlane i mechaniczne - powinny spełniać wymagania trzeciego poziomu. Czas ich pokonania z użyciem specjalistycznych narzędzi nie powinien być krótszy niż 8 min.

Ogólne wymagania dla systemów teleinformatycznych

Dostęp / kontrola dostępu
Dostęp:– rodzaj oddziaływania pomiędzy podmiotem (użytkownikiem) i obiektem (zasobami informacyjnymi jednostki), którego rezultatem jest zmiana stanu (przetwarzanie), przepływ informacji itp.

Zagrożenia: osoby nie uprawnione (spoza instytucji lub spośród nieuprawnionych pracowników) do dostępu do danego rodzaju zasobów i/lub bez uzasadnionej potrzeby wiedzy mogą celowo lub przypadkowo uzyskać dostęp do zasobów informacyjnych, w tym także do danych, sprzętu lub oprogramowania oraz do danych o metodach ochrony.
Polityka bezpieczeństwa: dostęp do informacji wrażliwych (Z3) powinien być ograniczony zgodnie z pełnioną funkcją w instytucji oraz z zasadą wiedzy niezbędnej.
Zabezpieczenia:
· pomieszczenia, w których planuje się zorganizowanie serwerowni powinny być wyposażone w instalację teletechniczną kontroli we/wy z identyfikacją osób i instalację alarmową klasy SA3. Wszystkie instalacje techniczne i zabezpieczające powinny być włączone w system zabezpieczenia obiektu;
· zewnętrzne ściany i okna pomieszczeń powinny charakteryzować się czasem wytrzymałości na włamanie co najmniej 8 min;
· instalacja alarmowa pożaru powinna być wyposażona w czujki wczesnego ostrzegania (czujki wykrywania tlenku węgla, dymu itp.) i powinna być włączona w ogólny system alarmowy obiektu;
· szyby okienne w pomieszczeniach powinny posiadać klasę odporności na przestrzelenie co najmniej S3 według norm EN 356 i DIN 52 290 (zwykle stosuje się je w budynkach o podwyższonym zagrożeniu terroryzmem, napadami rabunkowymi itp.);
· drzwi wejściowe powinny spełniać wymagania klasy „B" według PN-90/B92270, a zamki kluczowe – wymagania klasy „B" lub „C" wg PN-88/B-94399;
· wszyscy administratorzy, upoważnieni pracownicy i osoby kontrolujące powinny posiadać odpowiednie upoważnienia dostępu do przetwarzanych zasobów informacyjnych;
· czas reakcji służby ochrony na sygnały alarmu nie powinien być dłuższy niż 8 min.
· wstęp pracowników, operatorów i administratorów do pomieszczeń technicznych serwerowni powinien odbywać się na podstawie kart identyfikacyjnych i kodu identyfikacyjnego, zgodnie z procedurami nadawania i cofania uprawnień;

· wstęp osób (interesanci, naprawa lub konserwacja urządzeń, sprzątanie pomieszczeń itp.) nie posiadających odpowiednich uprawnień powinien odbywać się według ustalonych procedur.
Uwierzytelnianie

Uwierzytelnianie – proces ustalania wiarygodności podmiotu w strefie ochrony i uwierzytelnianie na etapie uruchamiania i pracy z systemem (systemami).
Zagrożenie: osoby mogą się podawać za inne, w celu uzyskania nieuprawnionego dostępu do informacji, programów lub zasobów materiałowych.
Polityka bezpieczeństwa: wszystkie osoby podejmujące próbę dostępu do zasobów informacyjnych, powinny być zidentyfikowane i opcjonalnie, powinna nastąpić ich autoryzacja w systemie informatycznym.

Zabezpieczenia:
· proces ustalania wiarygodności osób jest prowadzony na podstawie rozpoznania wizualnego, dowodów tożsamości, haseł, kart identyfikacyjnych. Identyfikacja osób jest dwustopniowa: przez służbę ochrony oraz przez administratora, system kontroli wejścia/wyjścia do pomieszczenia chronionego oraz system autoryzacji w systemie informatycznym.
Rozliczalność

Rozliczalność – rejestrowanie faktów wytwarzania, przesyłania, modyfikowania lub kasowania (wybrakowania) zasobów.
Zagrożenie: osoby , które posiadają uprawniony dostęp do zasobów informacyjnych instytucji mogą nadużywać tych uprawnień.
Polityka bezpieczeństwa: zastosowane mechanizmy zabezpieczeń (organizacyjne i programistyczne) powinny w sposób jednoznaczny przypisywać konkretne działania prowadzone w systemie (backup, instalacja, zmiana zawartości okien dialogowych itp.) konkretnemu podmiotowi (użytkownikowi). W ten sposób mechanizmy powinny zabezpieczać przed działaniami niedozwolonymi.

Zabezpieczenia:
· system ochrony zasobów informacyjnych serwerowni z założenia powinien być oparty wg. zasady „dwóch par oczu";
· zorganizowany , w oparciu o dostępne środowisko systemowe i system zarządzania bazami danych system autoryzacji i autentyfikacji administratorów i użytkowników systemów;
· zaleca się, aby wszystkie nośniki informacji posiadały etykiety (oznaczenia): nośniki informacji kategorii zagrożonej wartości Z3 – np. oznaczenie MS/Z3;
· zbędne materiały robocze na nośnikach papierowych powinny być niezwłocznie niszczone w niszczarkach,
· służba ochrony powinna prowadzić rejestr osób upoważnionych, pracujących w pomieszczeniach technicznych serwerowni zarówno w godzinach pracy jak również po godzinach pracy regulaminowej;
· system ochrony powinien nadzorować i rejestrować, z wykorzystaniem kamer ruch przed wejściem do pomieszczenia chronionego umożliwiając przeglądy (kontrole) tych działań;
· powinny być prowadzone kontrole przez przełożonych przestrzegania zasad bezpieczeństwa użytkowania serwerów i innych urządzeń w pomieszczeniach technicznych serwerowni jak też użytkowników systemów i aplikacji i w ramach sieci lokalnej jednostki.
Niezawodność

Niezawodność – cecha systemu oznaczająca spójne i zamierzone działanie.
Zagrożenie: niska niezawodność sprzętu i/lub oprogramowania, niski poziom wyszkolenia administratorów i operatorów systemu może zakłócić ciągłość działania instytucji lub jej części.
Polityka bezpieczeństwa: w systemach gromadzenia, przechowywania, przetwarzania i/lub dystrybucji zasobów powinny być wykorzystywane urządzenia, zapewniające dostępność tych zasobów w określonym miejscu, czasie i w określonej formie.

Zabezpieczenia:
· systemy gromadzenia, przechowywania, przetwarzania i/lub dystrybucji zasobów powinny być budowane w oparciu o certyfikowany (licencjonowany) sprzęt i oprogramowanie;
· w systemach powinny być wykorzystywane bezprzerwowe dedykowane systemy zasilania

energetycznego,
· wdrożone procedury wykonywania i przechowywania zapasowych kopii danych;
· wdrożone procedury postępowania w sytuacjach kryzysowych zintegrowane z ogólnym planem kryzysowym jednostki organizacyjnej resortu.

Bezpieczeństwo transmisji i bezpieczeństwo danych
Ochrona antywirusowa

Ochrona antywirusowa – zespół przedsięwzięć programowych i organizacyjno - technicznych, przeciwdziałających przenikaniu i skutkom aktywności złośliwego oprogramowania w systemach teleinformatycznych.
Zagrożenie: wniknięcie złośliwego oprogramowania do sieci teleinformatycznej może doprowadzić do naruszenia poufności, integralności i/lub dostępności informacji (danych).

Zabezpieczenia:
1. stosowanie oprogramowania antywirusowego i aktualizacja baz danych wirusów
2. unikanie korzystania z wymiennych nośników danych
3. w przypadku wystąpienia na serwerach i/lub stacjach roboczych wirusa lub innego szkodliwego oprogramowania należy natychmiast powiadomić Administratora Systemu Informatycznego, który musi podjąć odpowiednie kroki, w szczególności:
· zidentyfikować wirus i określić obszar występowania,
· odseparować część systemu objętą wirusem od całości,
· dokonać wpisu w Dzienniku Pracy Systemu i powiadomić przełożonych o zaistniałej sytuacji,
· przystąpić do usuwania wirusa, zgodnie z wymaganiami zastosowanego programu antywirusowego,
· w razie konieczności, należy ponownie zainstalować oprogramowanie systemu i skopiować dane systemu z ostatnich aktualnych kopii, przetestować poprawność systemu i ponownie wykonać wszystkie operacje z okresu zagrożonego utratą danych.
Ochrona transmisji
Ochrona transmisji – zespół przedsięwzięć programowych, organizacyjnych i technicznych, zapobiegających przejęciu przez osoby nieuprawnione adresów IP, identyfikacji użytkowników i topologii sieci teleinformatycznej.

Zagrożenia: dane o zmianach intensywności ruchu w sieci, adresy IP i identyfikacja użytkowników mogą być wykorzystane przez osoby nieuprawnione do ataku na zasoby (informacje, sprzęt komputerowy itp.) lub na sieć teleinformatyczną w celu np. pozyskania danych, skutecznej blokady sieci.
Zabezpieczenia:
· Wykorzystywanie dedykowanych łączy transmisji danych np. VPN
· Separowanie łączy transmisji danych korporacyjnych i łączy dostępu do sieci INTERNET
· Wykorzystywanie sprzętowego i programowego systemu zabezpieczeń typu firewal, IPS, IDS itp.
Audyt

Audyt – monitorowanie stanu bezpieczeństwa w celu wykrycia i ostrzegania przed potencjalnymi zagrożeniami. Audyt jest elementem zarządzania ryzykiem w instytucji.
Polityka bezpieczeństwa: potencjalne lub istniejące luki w systemie bezpieczeństwa firmy powinny być możliwie szybko wykryte.
Ryzyko: mogą powstać celowo wytworzone lub przypadkowe luki w systemie bezpieczeństwa.
Zabezpieczenia:
· wykryte przez użytkowników systemu potencjalne lub istniejące luki w systemie bezpieczeństwa powinny być niezwłocznie zgłaszane administratorowi (inspektorowi bezpieczeństwa);
· prowadzenie okresowych przeglądów, testów i treningów w celu oceny skuteczności zabezpieczeń sieciowych i aplikacyjnych.

Plany kryzysowe
Plany kryzysowe – element zarządzania bezpieczeństwem - procedury postępowania w krytycznym stanie bezpieczeństwa, tzn. w sytuacji zagrożeń, ciągłości funkcjonowania instytucji lub jej ważnej części (sytuacja kryzysowa). W sytuacji takiej może znaleźć się instytucja w wyniku oddziaływania

zagrożeń w postaci klęsk żywiołowych (pożar, powódź, gwałtowne burze itp.), katastrof (wybuch lub wyciek substancji chemicznych, uaktywnienie się złośliwych programów w sieci teleinformatycznej, przetwarzającej bardzo ważne dla firmy informacje), działań terrorystycznych lub sabotażowych. Plany kryzysowe powinny uwzględniać ocenę i analizę ryzyka spowodowanego zaistniałą sytuacją nadzwyczajną.
Analizę ryzyka prowadzi się w oparciu o usystematyzowane zestawienie w postaci podziału na kategorie i skalę zagrożeń wraz ze środkami im przeciwdziałającymi. W oparciu o takie zestawienie opracowuje się plan działania określający ukierunkowanie działań na najbardziej prawdopodobne zagrożenia. Realizacja planu powinna skutkować dokumentacją techniczną w postaci formularza analizy ryzyka. Formularz analizy ryzyka powinien zawierać następujące informacje:
· opis możliwego do zdefiniowania ryzyka
· potencjalne skutki zagrożeń bezpieczeństwa informacji
· szacunkowe koszty finansowe, logistyczne, techniczne i osobowe zagrożeń
· prawdopodobieństwo wystąpienia zagrożeń
· priorytety realizacji przedsięwzięć profilaktycznych
· opis działań zapobiegawczych
· koszty zabezpieczeń i prowadzenia działań zapobiegawczych

Zagrożenia: utrzymywanie się sytuacji kryzysowej (długi czas zahamowania, rozwoju i wychodzenia z sytuacji kryzysowej) może doprowadzić do poważnego ograniczenia możliwości funkcjonowania instytucji i utraty zaufania publicznego.
W rozpatrywanym obiekcie - serwerowni nie można wykluczyć prawdopodobieństwa powstania:
· pożaru;
· awarii instalacji wodnej i CO;
· działań terrorystycznych lub sabotażowych na terenie obiektu.

Polityka bezpieczeństwa: plany kryzysowe powinny być obowiązkowym elementem systemu bezpieczeństwa jednostki organizacyjnej resortu i obejmować możliwie wszystkie aspekty funkcjonowania instytucji w tym serwerowni i infrastruktury technicznej sieci LAN.

Zabezpieczenia:
• wyspecyfikowanie funkcji, które bezwzględnie muszą być utrzymane;
• wdrożenie systemu zapobiegania i wczesnego wykrywania sytuacji kryzysowej;
• wdrożenie procedur odtwarzania pełnej zdolności funkcjonowania np. odzyskiwanie danych i uruchomienie systemów z kopii zapasowych.

Szkolenia
Szkolenia administratorów i użytkowników systemów w zakresie bezpieczeństwa – proces podnoszenia poziomu świadomości użytkowników oraz doskonalenia umiejętności bezpiecznej eksploatacji systemu, w tym postępowania w przypadku wystąpienia incydentów (naruszenia zasad) bezpieczeństwa lub sytuacji kryzysowych.

Zagrożenie: użytkownicy o niskim poziomie świadomości z zakresu bezpieczeństwa, poprzez nonszalanckie, lekkomyślne obchodzenie się z zasobami lub chaotycznie działający w sytuacji kryzysowej mogą znacznie obniżyć skuteczność systemu bezpieczeństwa użytkowanych aplikacji.
Polityka bezpieczeństwa: szkolenie powinno być elementem decydującym o stanie bezpieczeństwa aplikacji i funkcjonowania systemu informatycznego jednostki. Szkolenia powinny dotyczyć wszystkich użytkowników i administratorów sieci i systemu a także służb ochrony. Zakres i formy szkoleń powinny być dostosowane do zakresu obowiązków i odpowiedzialności poszczególnych pracowników i osób funkcyjnych.
Zabezpieczenia:
Pełnomocnik ochrony i administrator bezpieczeństwa powinni organizować systematyczne wewnętrzne szkolenia, testy i ćwiczenia dotyczące postępowania administratorów i użytkowników systemu informatycznego z zasobami informacyjnymi oraz postępowania w przypadku wystąpienia incydentów bezpieczeństwa lub sytuacji kryzysowych.
Wybrane właściwości systemu zabezpieczeń sieciowych typu firewall/AV:
System zabezpieczeń powinien realizować zadania firewall, wykonując kontrolę na poziomie sieci oraz

aplikacji. Może to być rozwiązanie programowe lub sprzętowo - programowe. System zabezpieczeń musi umożliwiać wykrywanie i blokowanie ataków intruzów IDP (Intrusion Detection and Prevention), zarządzanie pasmem sieci (QoS) oraz posiadać możliwość zestawiania zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site.
System zabezpieczeń powinien posiadać wbudowany moduł kontroli antywirusowej umożliwiający kontrolę poczty elektronicznej (SMTP, POP3) oraz HTTP. Włączenie kontroli antywirusowej nie wymaga dodatkowego serwera. Aktualizacja bazy wirusów oraz sygnatur ataków in-line IDS (Deep Packet Inspection) powinna odbywać się na żądanie, bądź automatycznie zgodnie z zaplanowanym harmonogramem.

System zabezpieczeń powinien być oparty o dedykowane urządzenie sieciowe nie posiadające wrażliwych na awarie elementów sprzętowych (np. twardego dysku). zabezpieczeń nie powinien posiadać ograniczeń na liczbę chronionych komputerów w sieci wewnętrznej.
System zabezpieczeń firewall zgodnie z ustaloną polityką bezpieczeństwa powinien umożliwiać prowadzenie kontroli ruchu sieciowego pomiędzy dwoma obszarami sieci (strefami). Polityki bezpieczeństwa powinny być definiowane pomiędzy dowolnymi strefami. Urządzenia bezpieczeństwa powinny być sterowane opracowywanym przez producenta zabezpieczeń, dedykowanym systemem operacyjnym. (tzn. nie powinien to być zmodyfikowany system operacyjny ogólnego przeznaczenia jak Linux, WINDOWS czy FreeBSD).
Urządzenia zabezpieczeń powinny posiadać możliwość podłączenia modemu i automatycznego zestawiania łącza zapasowego Dialup w razie wystąpienia awarii łącza podstawowego.
Polityka bezpieczeństwa systemu zabezpieczeń powinna uwzględniać strefy bezpieczeństwa, adresów IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasma gwarantowane i maksymalne, priorytety, oznaczenia DiffServ). System zabezpieczeń powinien umożliwiać administratorom wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan), blokowanie URL i niebezpiecznych komponentów (m.in. Java/ActiveX/zip/exe), ochronę sieci przed atakami powtórzeniowymi (Replay Attack) oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP.
Zarządzanie zabezpieczeniami w pełnym zakresie powinno odbywać się z linii poleceń (CLI) oraz graficznej konsoli GUI. W systemie musi istnieć możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy powinni być uwierzytelniani za pomocą haseł statycznych, haseł dynamicznych (RADIUS, RSA SecureID) oraz certyfikatów SSL.

Ostatnia aktualizacja: **18 września 2007r.**
WebAdmin: **Jacek Kołkowski**