Standaryzacja wykonania infrastruktury sieciowej.

Przedstawione poniżej wskazówki dotyczą sposobów wykorzystania standardów projektowania i wdrażania sieci LAN w jednostkach Poczty Polskiej S.A.. Materiał ma za zadanie wspomagać podejmowanie decyzji w zakresie technologii budowy sieci lokalnych w jednostkach pocztowych, nie zawiera jednak obligatoryjnych wymagań i parametrów technicznych urządzeń dedykowanych do budowy, rozbudowy czy modernizacji sieci lokalnych. Zakres opisanych zagadnień obejmuje istotne elementy niezbędne przy opracowywaniu projektów, specyfikacje techniczne oraz szczegółowe wymagania w zakresie budowy sieci lokalnych.

Prawidłowo wykonana infrastruktura sieciowa w budynku charakteryzuje się łatwością modyfikacji lub rozbudowy, do czego konieczne jest uwzględnienie wytycznych zawartych w szczegółowym opisie projektu sieci. Podstawą założeń projektu są polskie normy budowlane, przepisy branżowe dotyczące prac kablowych, wytyczne producentów elementów systemu oraz międzynarodowe standardy dla sieci komputerowych (ISO, IDEE, TSB). Urządzenia, sprzęt i akcesoria wykorzystywane do budowy sieci muszą spełniać parametry techniczne określone w odpowiednich standardach i normach. Projekt sieci logicznej musi umożliwiać etapową budowę sieci i punktów logicznych oraz proponować konkretne rozwiązania i użycie odpowiednich materiałów (elementy, urządzenia, sprzęt i akcesoria).

OKABLOWANIE STRUKTURALNE

Najbardziej optymalnym rozwiązaniem dla całego budynku jest okablowanie strukturalne kategorii 5e z podziałem na okablowanie pionowe i poziome, które integruje wszystkie systemy teletechniczne instalowane w budynku z siecią telefoniczną włącznie. Budynek powinien też posiadać sieć energetyczną do zasilania lokalnej sieci komputerowej.

Projekt rozkładu PEL (punkt elektryczno–logiczny) w budynku powinien uwzględniać strukturę całej jednostki oraz dopuszczać możliwość przemieszczania się pracowników. Z tego powodu należy szacować liczbę PEL z pewnym nadmiarem, co ułatwi ewentualną rekonfigurację sieci. Aby uniknąć trudności w trakcie użytkowania sieci oraz przy rozbudowie okablowania strukturalnego opis i numerację szaf krosowniczych i PELi należy

wykonać w sposób jednoznaczny. Dla każdego piętra w budynku (lub segmentu sieci, lub piętra i segmentu sieci) należy przewidzieć wydzieloną szafę krosowniczą. Zarządzanie siecią bardzo ułatwia zastosowanie kabli łączących serwery i urządzenia z szafą krosowniczą w innym kolorze niż pozostałe. W pomieszczeniach użytkowników systemów specjalizowanych oraz w pomieszczeniach biurowych należy zainstalować punkty elektryczno–logiczne składające się z dwóch gniazd logicznych i czterech gniazd elektrycznych, wg następującej zasady: pokój jednoosobowy - 2 PEL, pokój dwuosobowy - 3 PEL, pokój trzyosobowy – 4 PEL. W pomieszczeniach technicznych serwerowi, obsługi technicznej, monitoringu i zarządzania oraz w pomieszczeniach administratorów sieci lokalnej LAN i salach uruchomień i testów sprzętu i oprogramowania ilość PEL powinna być projektowana zgodnie z realnymi potrzebami. W projekcie należy uwzględnić budowę okablowania w oparciu o kabel UTP kategorii 5e z możliwością transmisji danych z szybkością do 1000 Mbps oraz połączenie punktów dystrybucyjnych kablami optycznymi. Gniazda abonenckie powinny być wykonane w standardzie 45x45, gdzie w jednym module 45 x 45 mogą być zainstalowane 2 pojedyncze gniazda RJ45. Systemy kanałów kablowych, które powinny umożliwiać zwiększenie pojemności, do co najmniej 30%, oraz gniazda natynkowe powinny pochodzić od jednego producenta. Do wykonania systemu należy zastosować materiały PCV oznakowane symbolem CE, których jakość gwarantuje norma EN 50085 1. Miejsca poprowadzenia przewodów transmisyjnych okablowania poziomego oraz kabli okablowania pionowego należy skoordynować z istniejącymi i wykonywanymi instalacjami w budynku m.in. instalacją elektryczną, instalacją elektryczną ogólną, instalacją centralnego ogrzewania, wody, gazu, itp. Instalację elektryczną, przeznaczoną dla okablowania strukturalnego, należy wykonać zgodnie z obowiązującymi normami i przepisami. Minimalne wymagania elementów okablowania strukturalnego to kategoria 5e oraz RJ45 jako interfejs końcowy dla połączeń na skrętce miedzianej 4 parowej. Sieć logiczna powinna zostać wykonana zgodnie z najnowszymi standardami okablowania strukturalnego - normą ISO/IEC 11801 wydanie drugie (wrzesień 2002) lub EN 50173 wydanie drugie (październik 2002).
Dla połączeń światłowodowych zaleca się włókno wielodomowe 50/125mm oraz nowy standard dla sieci LAN - MT-RJ.

W projekcie należy przewidzieć budowę okablowania poziomego w wersji ekranowanej ze względu na bezpieczeństwo transmisji oraz w celu zminimalizowania oddziaływania zakłóceń w miejscach o dużej ilości kabli transmisyjnych i nakładania się różnych instalacji prądowych. Większe bezpieczeństwo transmisji danych zapewnia dopilnowanie

kompatybilności elektromagnetycznej, czyli zwiększenie odporności systemu informatycznego na zakłócenia elektromagnetyczne i ograniczenie emisji zakłóceń do środowiska zewnętrznego. Wydajność okablowania powinna być zgodna z najnowszymi normami, tj. draftem specyfikacji JTC 1/25N 981.

W budynkach zabytkowych i o starszej konstrukcji należy wcześniej rozpoznać, jakie rozwiązania będą najwłaściwsze w konkretnych przypadkach i w zależności od oceny zaproponować trasę okablowania. Najczęściej przeprowadza się je w rynnach PCV lub w podwieszkach sufitowych wraz z pozostałym okablowaniem. Dla budynków zabytkowych trzeba uzyskać stosowne zezwolenia na wykonywane prace. Jedno okablowanie strukturalne, czyli zintegrowanie sieci komputerowej, alarmowej, telewizyjnej, przeciwpożarowej i telefonicznej znacznie obniża koszty, ułatwia zarządzanie, konfigurację i rekonfigurację sieci. Odległość od głównego punktu dystrybucyjnego nie powinna przekraczać 90 m. Jeżeli ten warunek nie może być spełniony, sieć należy podzielić na mniejsze fragmenty połączone przez światłowód albo Gigabit Ethernet, lub zastosować 'reapet'ery' (wzmacniacze). Wybór najkorzystniejszego rozwiązania zależy od istniejących uwarunkowań lokalnych.

Oprócz powyżej wymienionych system okablowania musi bezwzględnie spełniać następujące warunki:

- wszystkie elementy okablowania strukturalnego muszą pochodzić od jednego producenta, o co należy zadbać również przy rozbudowie systemu (o ile to możliwe); takie działanie zapewnia jednolite zarządzanie i uprości instalację,
- zakończenie kabli transmisyjnych powinno być trwałe na 8-pozycyjnym złączu modularnym, tak aby w trakcie pracy systemu nie dopuszczać do rekonfiguracji rozszycia,
- do typowego punktu przyłączeniowego należy doprowadzić dwa kable logiczne zakończone na dwóch gniazdach z dwoma wkładkami 1xRJ45 Kat.5e, inne niż typowe rozwiązania należy uzgadniać z użytkownikiem,
- kable sygnałowe należy oznaczać numerem od strony gniazda i szafy montażowej w sposób trwały; te same oznaczenia umieszcza się na gniazdach sygnałowych w punktach przyłączeniowych użytkowników oraz na panelach w piętrowych punktach dystrybucyjnych.

- w dokumentacji powykonawczej instalacji kablowej, którą sporządza się po zrealizowaniu projektu, uruchomieniu i wykonaniu pomiarów instalacji, uwzględnia się wszystkie zmiany w trasach kablowych i rzeczywiste rozmieszczenie punktów przyłączeniowych w pomieszczeniach.

- w celu zapewnienia możliwości przyszłej rekonfiguracji przez użytkownika projekt powinien uwzględniać odpowiednią ilość zapasowych elementów wymiennych (wkładek wielokrotnych).

Poprawność wykonania instalacji sieci sygnałowej potwierdza się poprzez przeprowadzenie pomiarów statycznych i dynamicznych właściwości poszczególnych torów, które wykonuje się specjalistycznymi testerami okablowania (np. OmniScanner, DSP 4300). Testy kablowania powinny objąć wszystkie punkty przyłączeniowe. Dla łączy światłowodowych należy przeprowadzić pomiary tłumienności zgodnie z wymaganiami odpowiednich standardów (dwukierunkowe pomiary sygnałem w dwóch oknach transmisyjnych).

Do dokumentacji powykonawczej dołącza się wszystkie raporty z pomiarów.

ZASILANIE ENERGETYCZNE, DEDYKOWANA SIEĆ ELEKTRYCZNA

Konstrukcja systemu energetycznego zasilania obiektu musi dopuszczać możliwość zasilania z dwóch zewnętrznych, niezależnych, przełączanych automatycznie linii energetycznych.
Sieć zasilająca infrastrukturę techniczną systemu informatycznego powinna być wydzieloną instalacją elektryczną z możliwością podtrzymywania napięcia w sytuacjach awaryjnych, tak aby bezpieczne wyłączyć urządzenia. Aby spełnić ten warunek można zastosować kilka UPSów obsługujących poszczególne strefy:

- kablownię (przy traktach transmisyjnych, klimatyzatorze centralnym i przyłączach telefonicznych),
- siłownię (UPS powinien mieć moc sumaryczną stanowisk komputerowych i innych urządzeń pracujących w sieci LAN),
- serwerownię (UPS powinien mieć moc sumaryczną serwerów i urządzeń obsługujących użytkowników poszczególnych aplikacji lub jednego centralnego UPS o mocy pozwalającej na podtrzymanie wszystkich urządzeń aktywnych komputerowej sieci lokalnej).

Bezpieczne wyłączenie zasilanych urządzeń aktywnych w przypadku zaniku zasilania w sieci jest gwarantowane poprzez prawidłowe obliczenia czasu podtrzymania zasilania pracy urządzeń aktywnych. Należy oszacować maksymalną i nominalną moc [kVA] urządzenia podtrzymującego zasilanie w oparciu o sumaryczny pobór mocy zasilanych urządzeń, co pozwoli na dobranie typu i producenta UPS. Moc pojedynczego standardowego gniazda zasilania PC powinna wynosić ok. 200÷300 [W], dla drukarki laserowej ok. 1 [kW], w jeden obwód prądowy można grupować ok. 10 gniazd. Zaleca się w serwerowi instalację, co najmniej 4 gniazd po 2,5 [kW] oraz kilku-kilkunastu po 500 [W]. Przy projektowaniu sieci i montażu PEL trzeba uwzględniać zasady ergonomii w zakresie ich rozmieszczenia np. odległości od podłogi (30÷50 [cm] lub większej). Długość sznurów zasilających dla komputera i monitora wynosi ok. 1,2÷1,5 m. Do wydzielonych obwodów zasilania sieci komputerowej nie można podłączać innych urządzeń elektrycznych, np. czajników, grzejników itp. Pomieszczenia, w których znajdują się aktywne urządzenia sieciowe (serwery, routery, UPS i inne) powinny być klimatyzowane, należy w nich zapewnić odpowiednią wentylację i temperaturę oraz przeprowadzać okresowe kontrole i monitoring. Możliwość zdalnego monitorowania i zarządzania pracą UPS z pomieszczenia administratora zapewni doprowadzone do pomieszczeń z UPS okablowanie logiczne. Serwerownie i inne pomieszczenia techniczne powinny być zabezpieczone przed dostępem do nich osób niepowołanych. Wszystkie elementy związane z systemem zasilania dedykowanego, główne bezpieczniki, przełączniki, 'bypass', doprowadzenia w głównej szafie zbiorczej zasilania jak i poszczególne podziały na obwody prądowe, kolejność faz w głównym przyłączu powinny być starannie oznakowane zgodnie z dokumentacją.

SERWEROWNIA I POMIESZCZENIA TECHNICZNE

Okablowanie poziome i pionowe obiektu, kable światłowodowe, doprowadzenia traktów sieci rozległej we/wy od głowicy telekomunikacyjnej budynku zbiegają się w pomieszczeniach technicznych serwerowi – głównym punkcie dystrybucyjnym okablowania strukturalnego. Jako urządzenia aktywne można zastosować przełączniki zarządzane warstwy 2/3 z gwarancją Lifetime producenta. Do połączenia okablowania szkieletowego sieci może być wykorzystany przełącznik światłowodowy w standardzie 1000Base-SX. Zaleca się położenie w serwerowni antystatycznej i niepalnej podłogi technologicznej, ponieważ w trakcie eksploatacji sieci ułatwi to prowadzenie i rekonfigurację okablowania strukturalnego oraz zwiększy bezpieczeństwo. Liczba gniazd (punktów PEL) powinna być o 20% większa od wstępnie oszacowanej w serwerowni i pomieszczeniu administratorów. Należy zabezpieczyć pomieszczenia serwerowi przed możliwością dostępu osób trzecich, jak i zadbać o ochronę przeciwpożarową. Administratorzy i operatorzy sieci nie powinni pracować w tym samym pomieszczeniu, w którym znajdują się serwery. Jeśli jest to możliwe, należy techniczne pomieszczenia serwerowi projektować jako osobne, fizycznie oddzielone, wyposażone w szafę pancerną z zabezpieczeniami przeciwpożarowymi, gdzie przechowywane będą kopie danych oraz użytkowane systemy i aplikacje, pakiety oprogramowań oraz inne informacje i dane wymagające szczególnej ochrony. Dobrym rozwiązaniem jest łączenie pomieszczeń technicznych serwerowi. Klimatyzacja w tych pomieszczeniach powinna być dostosowana do warunków i mocy cieplnej wydzielanej przez zainstalowane urządzenia. Urządzenia aktywne, pasywne, modemy i serwery należy umieszczać w szafach dystrybucyjnych typu „rack”, szafy krosownicze i teletechniczne powinny być montowane w standardzie 19" oraz powinny umożliwiać zainstalowanie odpowiedniej liczby urządzeń aktywnych, która to zależy od ilości punktów sieci. Przyjmuje się, że na każde 48 punktów logicznych należy przewidzieć miejsce w szafie o wysokości 2U. W szafie należy zarezerwować przestrzeń dla urządzeń teletransmisyjnych o wysokości 15 cm, miejsce na zamontowanie lokalnego UPS'a podtrzymującego działanie urządzeń aktywnych zamontowanych w szafie oraz listw zasilających zamontowanych tam urządzeń. Koncentratory (HUB'y) i przełączniki (SWITCH'e) oraz urządzenia transmisji danych (ROUTER'y, MODEM'y) powinny zabezpieczać dodatkowo około 5÷10 % wolnych gniazd logicznych dla łatwej rekonfiguracji połączeń w ramach sieci lokalnej i powinny pochodzić od renomowanych producentów. Zaleca się zastosowanie zapasowego (redundantnego) łącza teletransmisyjnego. Z uwagi na bezpieczeństwo planowanej do wdrożenia korporacyjnej sieci WAN w szafach

teletechnicznych serwerowni trzeba przewidzieć miejsce do włączenia i uruchomienia dodatkowego routera i urządzenia bezpieczeństwa operatora telekomunikacyjnego. Szafy krosownicze powinny być umieszczane na poszczególnych piętrach budynku w osobnych pomieszczeniach, chronionych przed dostępem osób niepowołanych, z odpowiednią wentylacją. Jeżeli warunek ten nie jest spełniony należy pomieszczenie wyposażyć w dodatkowe wentylatory lub obudowę szafy w dodatkowe otwory wentylacyjne.

Załącznik Nr 1

NORMY I WYMAGANIA

Normy ISO/IEC 11801:2002 wydanie drugie lub EN 50173-1:2002 wydanie drugie, dotyczące okablowania strukturalnego budynków nakładają szereg warunków, które muszą zostać spełnione przy budowie systemu okablowania strukturalnego. Wyceniając prace należy wziąć pod uwagę obowiązek dostarczenia przez wykonawcę wyników pomiarów powykonawczych i testów okablowania (statycznych i dynamicznych), potwierdzonych protokołami. Ponadto należy dołączyć odpowiednie certyfikaty 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

Długi czas eksploatacji okablowania strukturalnego a także niezmienność parametrów transmisyjnych sieci w trakcie użytkowania systemu zaręcza końcowemu użytkownikowi gwarancja systemowa uznanego producenta okablowania, a nie gwarancji firmy instalacyjnej, która w przyszłości może zakończyć działalność gospodarczą.
Wymagania na rynkach światowych w zakresie wydajności systemów okablowania stale rosną, na co zwracają uwagę międzynarodowe komitety normalizacyjne (ISO/IEC 11801 i EN 50173). Pierwszą aplikację prowadzącą poprzez dodatkowe parametry (Power Sum Next, Elfext, PowerSum Elfext i Delay Skew) do systemu powszechnie nazywanego kategorią 5 podwyższoną był gigabitowy Ethernet. Wymagania te zostały ujęte w edycji standardu ISO/IEC 11801 z roku 2000 na Kategorią 5/Klasę D. Systemy okablowania 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. Dla nowszych systemów i aplikacji, które wymagają szerszego pasma przenoszenia, opracowywany jest protokół Gigabitowego Ethernetu pracujący na dwóch parach (podobnie jak to było w przeszłości z protokołami Ethernet i Fast Ethernet). W czerwcu 2002 r. w USA i we wrześniu tego roku w Europie zaakceptowano i wprowadzono standard Kategorii 6 (Klasy), zgodnie z którym systemy okablowania muszą posiadać wydajność do 200/250 MHz (praca/test). Obecnie powszechnie znanym i stosowanym interfejsem dla systemów okablowania kategorii 5 i 6 jest RJ45, jednak, ze względu na swoją konstrukcję, RJ45 nie jest w stanie poprawnie pracować na czterech parach zgodnie z wymaganiami dla kategorii 7.

Pojawia się Komisja normalizacyjna IEC SC48B: IEC 60603-7-x aktualnie opracowuje nowy interfejs o bardzo wysokiej wydajności. Nowe propozycje interfejsów dla okablowania kategorii 7 to zazwyczaj tzw. Interfejsy czterokanałowe, które są najbardziej odpowiednie dla kabli o konstrukcji PiMF, wymaganych dla bardzo szybkich systemów i aplikacji. Nowe aplikacje, w szczególności multimedialne, wymagają szerokich pasm przenoszenia, co nakłada na systemy okablowania strukturalnego dodatkowe wymagania. 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. Jednocześnie trwają prace nad nowym standardem kategorii 8. W ciągu najbliższych dwóch-trzech lat ponad 90% wszystkich nowych instalacji okablowania strukturalnego wykonanych z kabli miedzianych będzie pracowało w oparciu o standard okablowania strukturalnego kategorii 6.

Załącznik Nr 2

ELEMENTY POLITYKI BEZPIECZEŃSTWA

Eksploatacja systemów informatycznych oraz użytkowanie pomieszczeń, gdzie zlokalizowane są serwerownie i infrastruktura techniczna sieci lokalnej (serwery, urządzenia aktywne, modemy i urządzenia dystrybucyjne) wymaga wdrożenia stosowania zasad polityki bezpieczeństwa. Informacje korporacyjne (biznesowe) nie są kwalifikowane jako informacje niejawne stanowiące tajemnicę państwową czy służbową, jednocześnie mają zasadnicze znaczenie dla funkcjonowania instytucji, dlatego ich przetwarzanie, wymiana i archiwizacja powinna odbywać się w sposób kontrolowany a dostęp do nich powinien być ograniczony. Utrata lub zniszczenie takich danych może spowodować duże straty dla instytucji. Ochroną powinny zostać objęte wszystkie atrybuty bezpieczeństwa: dostępność (zasoby informacyjne są dostępne użytkownikowi w wymaganym miejscu, czasie i w wymaganej formie), poufność (dostęp do zasobów informacyjnych jest ograniczony tylko do kręgu osób uprawnionych) i integralność (oryginalna forma lub stan zasobów może być zmieniony tylko przez osoby do tego uprawnione). Oceną poziomu wrażliwości zasobów, w tym zasobów informacyjnych, które nie są klasyfikowane jako informacje stanowiące tajemnicę państwową lub służbową przeprowadza się wykorzystując następujące dokumenty:

- 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.

Ze względu na stopień zagrożenia i wartość szkód wyróżnia się 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.
Dla mienia średniej wartości, które można wymienić lub zastąpić oraz dla dokumentów, również elektronicznych, których uszkodzenie, zniszczenie, ujawnienie lub kradzież spowoduje straty w instytucji przewiduje się kategorię zagrożonej wartości Z2 - KO (II –V). Natomiast dla mienia o dużej wartości oraz dokumentów i innych zasobów o dużej wartości, których uszkodzenie, zniszczenie lub kradzież jak również dostęp do informacji w nich zawartych przez osoby nieuprawnione może prowadzić do dużych szkód stosuje się kategorię Z3 – KO (VI-VIII), gdzie KO to klasa odporności pomieszczeń i urządzeń na włamanie [RWP]. Klasyfikacją danych i przypisanie ich do odpowiedniej grupy kategorii zagrożonych wartości przeprowadza się po analizie danych, zamieszczonych w dokumentacji projektowej poszczególnych systemów informatycznych eksploatowanych w resorcie sprawiedliwości i charakterystyki przetwarzanych informacji. Systemy alarmowe przeciwwłamaniowe i przeciwnapadowe muszą spełniać wymagania trzeciego poziomu tzn. kategorii SA3 według PN-93/E-08390/14, jak również zabezpieczenia ochrony fizycznej – budowlane i mechaniczne - powinny spełniać wymagania trzeciego poziomu.

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 nieuprawnione (spoza instytucji lub spośród nieuprawnionych pracowników), nieposiadające dostępu do danego rodzaju zasobów i/lub bez uzasadnionej potrzeby mogą celowo lub przypadkowo zostać dopuszczone do zasobów informacyjnych, w tym także do danych, sprzętu lub oprogramowania oraz do informacji 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:

- instalacja teletechniczna kontroli we/wy z identyfikacji osób oraz instalacja alarmową klasy SA3 w pomieszczeniach technicznych serwerowi, włączenie w system zabezpieczenia obiektu instalacji technicznych i zabezpieczających;
- co najmniej 8-minutowy czas wytrzymałości na włamanie zewnętrznych ścian i okien pomieszczeń;
- instalacja alarmowa pożaru, włączona w ogólny system alarmowy obiektu, wyposażona w czujki wczesnego ostrzegania (czujki wykrywania tlenku węgla, dymu itp.);
- klasa odporności na przestrzelenie szyb okiennych zastosowanych w pomieszczeniu powinna mieć wartość co najmniej S3 według norm EN 356 i DIN 52 290 (zwykle stosuje się je w budynkach o podwyższonym zagrożeniu terroryzmem, napadami rabunkowymi itp.); · zamontowanie drzwi wejściowe klasy „B" według PN-90/B92270, oraz zamków kluczowych klasy „B" lub „C" wg PN-88/B-94399;
- pisemne upoważnienia dostępu do przetwarzanych zasobów informacyjnych dla wszystkich administratorów, upoważnionych pracowników i osób kontrolujących;
- stosowanie kart identyfikacyjnych i kodu identyfikacyjnego dla pracowników, operatorów i administratorów, wydawanych i regulowanych zgodnie z procedurami nadawania i cofania uprawnień wstępu do pomieszczeń technicznych serwerowni;
- stosowanie odpowiednich procedur wstępu osób (interesanci, naprawa lub konserwacja urządzeń, sprzątanie pomieszczeń itp.) nie posiadających odpowiednich uprawnień;
- nie dłuższy niż 8 min czas reakcji służby ochrony na sygnały alarmu.

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, można zastosować autoryzacją 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 – 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:

- zastosowanie zasady „dwóch par oczu" w systemie ochrony zasobów informacyjnych serwerowni;
- system autoryzacji i identyfikacji administratorów i użytkowników systemów zorganizowany w oparciu o dostępne środowisko systemowe i system zarządzania bazami danych;
- oznaczanie (etykiety) wszystkich nośników informacji kategorii zagrożonej wartości Z3 – np. oznaczenie MS/Z3 ;
- procedura niezwłocznego, trwałego (niszczarki) niszczenia zbędnych materiałów roboczych na nośnikach papierowych ;
- rejestr osób upoważnionych, pracujących w pomieszczeniach technicznych serwerowni zarówno w godzinach pracy jak również po godzinach pracy regulaminowej;
- nadzór i rejestracja ruchu przed wejściem do pomieszczenia chronionego umożliwiające przeglądy (kontrole) tych działań ;
- kontrole przestrzegania zasad bezpieczeństwa użytkowania serwerów i innych urządzeń w pomieszczeniach technicznych serwerowi, 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.

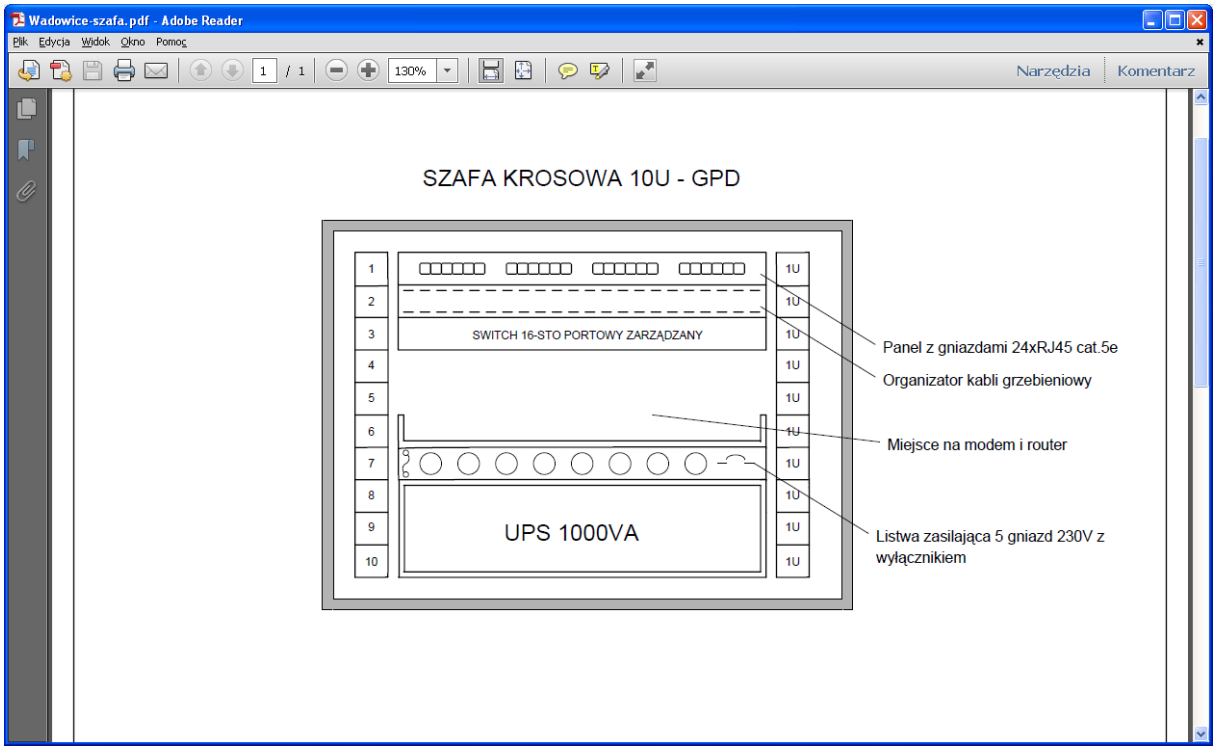
Załącznik Nr 3

Przykładowe zestawienie materiałów

lp	Nazwa	miara	ilość	Cena netto	Wartość netto
	Materiały				
1	Organizator grzebieniowy	szt.	1	30	30
2	Półka 1U 450mm	szt.	1	75	75
3	Panel zasilający 5-gniazdowy	szt.	1	60	60
4	Patchpanel kat 5e UTP 24xRJ45 certyfikowany	szt.	1	90	90
5	Szafa krosowa 19" 10U 600mm	szt.	1	450	450
8	Koryta z przegrodą 60x40	m	60	10	600
9	Puszka typu OBUK 2M	szt.	5	10	50
10	Puszka typu OBUK 6M	szt.	4	15	60
11	Adapter jednomodułowy	szt.	8	4	32
12	Gniazda Keyston kat 5e UTP certyfikowane	szt.	8	12	96
13	Gniazda elektryczne z kluczem czerwone potrójne	szt.	4	35	140
14	Gniazda elektryczne z kluczem czerwone pojedyncze	szt.	1	12	12
15	Patchcord kat 5e UTP 0,5 m	szt.	8	11	88
16	Patchcord kat 5e UTP 3 m	szt.	8	16	128
17	Zakręty, zakończenia, łączniki koryt	szt.	10	100	1000
18	Kabel UTP kat 5e certyfikowany	m	305	1	305
19	Kabel elektryczny 3x2,5	m	50	2,2	110
20	Rozdzielnica natynkowa 8 MOD	szt.	1	45	45
21	Wyłącznik główny FR63A	szt.	1	37	37
22	Wyłącznik nadprądowy typu C16A	szt.	2	16	32

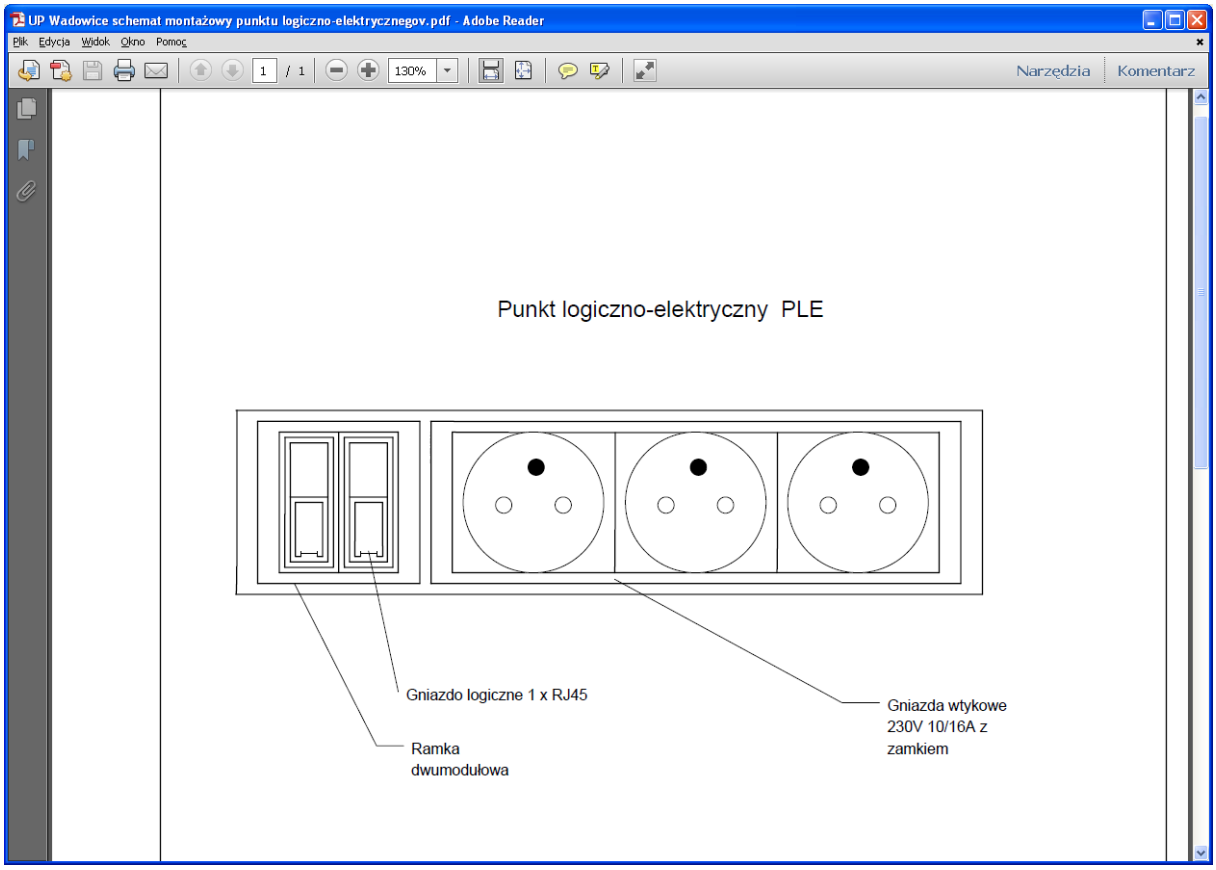
Załącznik Nr 4

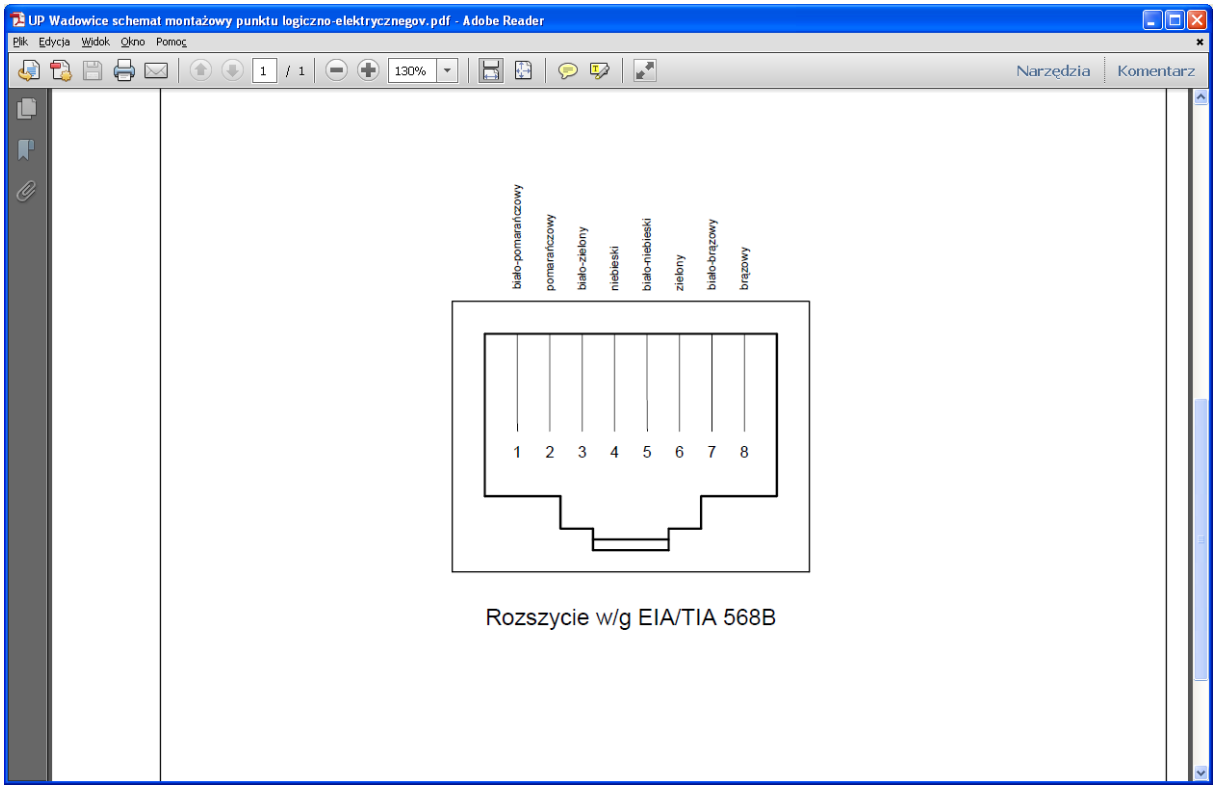
Przykład rysunku zastosowanej w projekcie szafy krosowej

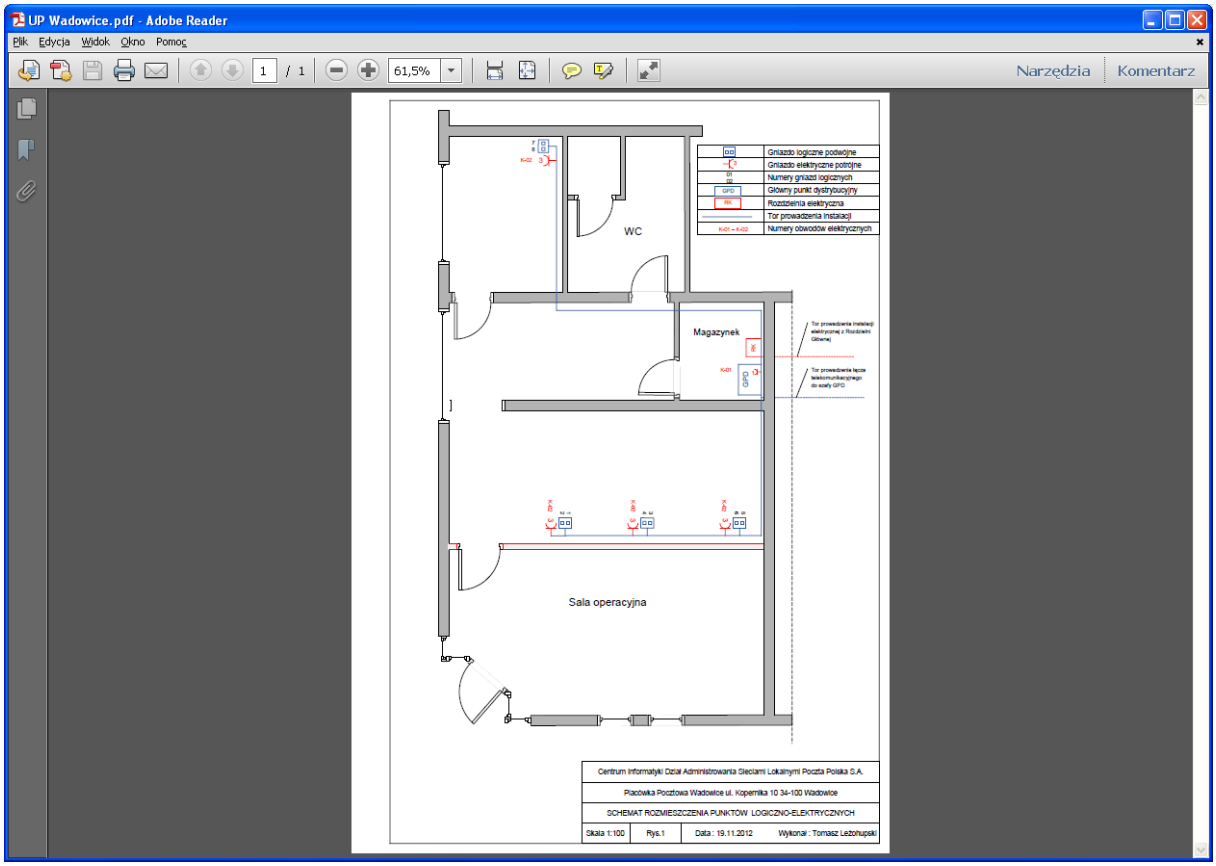


Załącznik Nr 5

Przykład punktu logiczno-elektrycznego PEL





Załącznik Nr 6

Przykład rysunku technicznego z rozmieszczeniem punktów logiczno-elektrycznych PEL.