ZATWIERDZAM:

KOMENDANT GŁÓWNY
PAŃSTWOWEJ STRAŻY POŻARNEJ

gen. brygadier Ryszard LEŚNIAKIEWICZ

17. XI. 2012

KOMENDA GŁÓWNA PAŃSTWOWEJ STRAŻY POŻARNEJ

Biuro Informatyki i Łączności

Zasady organizacji i funkcjonowania systemów teleinformatycznych, w tym na potrzeby kierującego działaniem ratowniczym.

Warszawa 2012

Opracował: Bogusław Rychlik KG PSP Warszawa
Tomasz Kalyta KG PSP Warszawa
Bartłomiej Ziemiński KW PSP Wrocław
Krzysztof Pietrucki KW PSP Gorzów Wlkp.
Wiktor Bauer KW PSP Opole
Tomasz Szymaniuk KW PSP Białystok
Przemysław Szulakowski KW PSP Katowice

Sprawdził: nadbryg. J Skulich

ZASTĘPCA KOMENDANTA GŁÓWNEGO
PAŃSTWOWEJ STRAŻY POŻARNEJ
nadbryg. Janusz Skulich

bryg. Z Góral

DYREKTOR
BIURA INFORMATYKI I ŁĄCZNOŚCI
bryg. mgr inż. Zbigniew GÓRAL

Spis treści.

Dokument ten, zwany dalej Zasadami, jest wypełnieniem wymogów zapisu § 4 ust. 3 pkt 6 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r., w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego (Dz. U. Nr 46, poz. 239 z 2011 r.).

1. Wstęp

Zasoby teleinformatyczne są w obecnych czasach zaliczane do wrażliwej infrastruktury, zarówno przedsiębiorstwa jak i państwa. Oznacza to, że bez sprawnego funkcjonowania zasobów teleinformatycznych nie będzie sprawnego funkcjonowania organizacji, co w konsekwencji może doprowadzić do złego funkcjonowania gospodarki i państwa.

Coraz więcej aplikacji, wewnętrznych systemów teleinformatycznych (system wspomagania decyzji, systemy do zarządzania zasobami, finansami, kadrami), sieci teleinformatyczne, serwerownie (centra przetwarzania danych) i infrastruktura wirtualna wymagają kompetencji i wysokich standardów pracy. Dlatego też, wymagają one obsługi przez kadrę posiadającą wiedzę nt. technologii w celu skutecznej realizacji przedsięwzięć z zakresu teleinformatyki. Wraz ze wzrostem ilościowym i jakościowym usług i technologii teleinformatycznych wzrastać powinno znaczenie zasobów kadrowych i organizacyjnych odpowiedzialnych za zasoby teleinformatyczne.

Każda jednostka organizacyjna PSP, w okresie 3 miesięcy od wejścia w życie niniejszego dokumentu, opracuje własny harmonogram przystosowania wymienionych w niniejszym dokumencie obszarów organizacji i funkcjonowania systemów teleinformatycznych.

2. Cele dokumentu

- Ułatwienie identyfikacji zagadnień zarządzania obszarem technologii teleinformatycznych w jednostkach organizacyjnych PSP w ramach KSRG.
- Wskazanie kierunków standaryzacji i integracji rozwiązań technologicznych i organizacyjnych.
- Zwiększenie efektywności i sprawności wykorzystania zasobów kadrowych i technologicznych w obszarze teleinformatyki.

3. Zakres dokumentu

Niniejszy dokument obejmuje swym zakresem rekomendacje w zakresie organizacji i funkcjonowania systemów teleinformatycznych na wszystkich szczeblach organizacyjnych PSP.

4. Podstawy prawne i normatywne oraz dokumenty powiązane

4.1 Wymagania prawne

Zapisy zawarte w niniejszym dokumencie są zgodne z przepisami prawa. W szczególności są zgodnie z:

- Ustawa o *ochronie przeciwpożarowej* z dnia z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. z 2009 r. Nr 178, poz. 1380, z późn. zmianami),
- Ustawa o *informatyzacji działalności podmiotów realizujących zadania publiczne* z dnia 17 lutego 2005 r. (Dz. U. Nr 64 poz. 564 i 565 z późn. zmianami),
- Ustawa *Kodeks Cywilny* z dnia 23 kwietnia 1964 r. (Dz. U. Nr 16 poz.93 z późn. zmianami),
- Ustawa *Kodeks Karny* z dnia 6 czerwca 1997 r. (Dz. U. Nr 88 poz. 553 z późn. zmianami),
- Ustawa *Kodeks Pracy* z dnia 26 czerwca 1974 r. (Dz. U. Nr 21 poz.94 z późn. zmianami),
- Ustawa *o ochronie informacji niejawnych* z dnia 5 sierpnia 2010 r. (Dz. U. Nr 182, poz. 1228 z późn. zmianami).
- Ustawa *o ochronie danych osobowych* z dnia 29 sierpnia 1997r. (Dz. Nr 133, poz. 883 z późn. zmianami).
- Ustawa *o zwalczaniu nieuczciwej konkurencji* z dnia 16 kwietnia 1993 r. (Dz. U. Nr 153 poz. 1503 z późniejszymi zmianami),
- Ustawa z dnia 27 lipca 2001r. *o ochronie baz danych* (Dz. U. Nr 128, poz. 1402).
- Ustawa z dnia 18 lipca 2002r. *o świadczeniu usług drogą elektroniczną* (Dz. U. Nr 144, poz.1204).
- Ustawa z dnia 29 września 1994 r. *o rachunkowości* (Dz. U. nr 121 poz. 591 z późn. zmianami).
- Ustawa z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych* (Dz. U. Nr 24 poz. 83 z późn. zmianami).
- Ustawa z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne* (Dz. U. Nr 171 poz. 1800 z późn. zmianami).
- Ustawa a dnia 6 września 2001 r. *o dostępie do informacji publicznej* (Dz. U. Nr 112 poz. 1198).
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie *Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (Dz. U. 2012, poz. 526),

- Rozporządzenie Ministra Spraw Wewnętrznych z dnia 18 lutego 2011 r. *w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo – gaśniczego* (Dz. U. Nr 46 poz. 239).

4.2. Wymagania własne

Zasady tworzone są w oparciu o obowiązujące przepisy prawa, ale także z uwzględnieniem specyfiki działalności PSP, oraz tzw. „dobrych praktyk" w zakresie organizacji, funkcjonowania i ochrony systemów teleinformatycznych. W szczególności znaczenie ma tu spójność z dokumentami wewnętrznymi jednostek organizacyjnych PSP, takimi jak: regulaminy organizacyjne, polityki jakości, polityki ochrony informacji. Duże znaczenie mają także normy bezpieczeństwa, z których najważniejsze są to:

- *PN-ISO/IEC 17799:2007 Technika informatyczna - Praktyczne zasady zarządzania bezpieczeństwem informacji.*
- *PN-ISO/IEC 27001:2007 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania.*
- *ISO/IEC 20000-1:2007 Technika informatyczna – zarządzanie usługami-- Część 1: Specyfikacja.*
- *PN-ISO/IEC 20000-2:2007 Technika informatyczna -- Zarządzanie usługami -- Część 2: Reguły postępowania.*
- *ISO/IEC 27001 Zarządzanie bezpieczeństwem informacji.*

5. Zasady organizacji i funkcjonowania

Opisane zasady określają zalecenia oraz tzw. „dobre praktyki" do stosowania przez jednostki organizacyjne PSP, w celu prawidłowego funkcjonowania, zarówno w sferze administracyjnej jak i operacyjnej.

5.1. Organizacja obszaru IT w jednostkach organizacyjnych PSP

5.1.1 Regulaminy organizacyjne jednostek oraz komórek organizacyjnych PSP

Jednostki organizacyjne PSP (KGPSP, KW PSP, KP/KMPSP, szkoły PSP) swoją strukturę zarządzania budują w oparciu o obowiązujące Regulaminy organizacyjne. Kierownik jednostki organizacyjnej zapewnia planowanie, funkcjonowanie i rozwój systemów teleinformatycznych swojej jednostki. Kierownik jednostki organizacyjnej odpowiedzialny jest także za nadzór i kontrolę nad funkcjonowaniem systemów teleinformatycznych jednostki. Regulamin organizacyjny jednostki powinien zawierać

wskazanie, kto i w jakim zakresie zajmuje się utrzymaniem systemów teleinformatycznych w jednostce. Rekomenduje się, aby Kierownik tworzył komórki organizacyjne odpowiedzialne za utrzymanie systemów teleinformatycznych.

5.1.2 Główne cele i zadania IT

Celem wszystkich działań IT jest osiągnięcie takiego poziomu organizacyjnego i technicznego, który:

- zapewni sprawność i ciągłość działania jednostek organizacyjnych,
- zagwarantuje odpowiedni poziom bezpieczeństwa przetwarzanych informacji w systemach teleinformatycznych,
- zapewni zgodność podejmowanych działań z prawem,
- ochroni wizerunek jednostki organizacyjnej PSP oraz jednostek współpracujących w ramach KSRG,
- maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji,
- zapewni poprawne i bezpieczne funkcjonowanie systemów teleinformatycznych jednostki organizacyjnej,
- zapewni gotowość podjęcia działań w sytuacjach kryzysowych,
- usprawni wyminę informacji, zarówno w strukturach KSRG jak i z innymi instytucjami,
- podniesie kulturę informatyczną i stworzy warunki do rozwijania społeczeństwa informacyjnego.

5.1.3 Zasoby kadrowe i usługi zapewniające realizację zadań IT

Kierownik jednostki organizacyjnej wyznaczy wydzielone zasoby organizacyjne odpowiedzialne za utrzymanie i rozwój systemów teleinformatycznych swojej jednostki. Odpowiada również za:

- pozyskanie i utrzymanie usług związanych z wymianą informacji,
- budową i utrzymaniem infrastruktury IT w swojej jednostce,
- zapewnienie ciągłości działania systemów teleinformatycznych, niezbędnych do prawidłowego funkcjonowania Stanowiska Kierowania.

Komórka odpowiedzialna za teleinformatykę skupia osoby pełniące role administratorów systemów teleinformatycznych. Zapewnia ciągłość działania systemów, poprawia ich wydajność. Każdy wyodrębniony system posiada swojego administratora. Jeden administrator może nadzorować kilka systemów. Ze względu na znaczą ilość zadań związanych z utrzymaniem systemu nie należy przydzielać więcej niż czterech systemów jednemu administratorowi. Zaleca się, aby wszystkie systemy zarządzane przez jednego administratora należały do tej samej grupy logicznej (systemy operacyjne, bazy danych, systemy backupowe itp.) Administrator

odpowiada za bezpieczeństwo systemu. Realizuje zadania określone w Polityce Bezpieczeństwa Informacji.

5.1.4 Finansowanie teleinformatyki w jednostkach organizacyjnych

Jednostka organizacyjna planuje w każdym roku budżetowym środki przeznaczone na utrzymanie ciągłości działania oraz rozwój systemów teleinformatycznych. Zaleca się, aby planowanie i wydatkowanie środków finansowych odbywało się przy udziale struktur odpowiedzialnych za teleinformatykę w jednostce organizacyjnej.

5.1.5 Polityka bezpieczeństwa IT

Kierownik jednostki organizacyjnej odpowiada za bezpieczeństwo systemów i sieci teleinformatycznych w swojej jednostce. Rekomenduje się, aby w każdej jednostce organizacyjnej stworzono i wprowadzono do użytkowania politykę ochrony informacji w postaci sformalizowanego dokumentu oraz wyznaczono osoby odpowiedzialne za:

- zarządzanie bezpieczeństwem informacji (Administrator Bezpieczeństwa Informacji (ABI) – zgodnie z Ustawą o ochronie danych osobowych),

- realizację zaleceń zawartych w polityce ochrony informacji jednostki (administratorzy systemów).

W przypadku braku wyznaczonego administratora bezpieczeństwa informacji (ABI) funkcję tę pełni Kierownik jednostki organizacyjnej (Administrator danych).

Ze względu na konflikt interesów nie należy łączyć funkcji Administratora bezpieczeństwa informacji oraz Administratora systemów teleinformatycznych.

Zaleca się, aby polityka ochrony informacji została tworzona w oparciu o tzw. „dobre praktyki" oraz normy (PN-ISO/IEC 17799, PN 07799-2, ISO/IEC 27001, ISO/IEC 20000).

5.2 Obszar funkcjonowania IT w jednostkach organizacyjnych PSP

5.2.1 Infrastruktura

a) Sieć WAN oraz połączenia do operatorów telekomunikacyjnych

Dla zapewnienia prawidłowego funkcjonowania jednostek organizacyjnych PSP konieczne jest posiadanie połączenia z siecią Internet. Połączenie to powinno być szerokopasmowe na łączu symetrycznym. Zalecana jest redundancja łącza od co najmniej dwóch operatorów telekomunikacyjnych, którzy nie posiadają wspólnego styku z siecią Internet.

Zaleca się, aby integralną częścią punktu styku było zintegrowane urządzenie do zarządzania zagrożeniami (UTM), lub rozwiązanie sprzętowo-programowe zapewniające co najmniej :

- standardowe usługi zapór ogniowych, jak np. translacja adresów (NAT).
- ochronę antyspamową,
- ochronę antywirusową,
- wykrywanie intruzów,
- zapobieganie wtargnięciu intruzów.

Szczegóły konfiguracji oraz ochrony są elementem Polityki bezpieczeństwa informacji.

Należy dążyć do tego, aby stosowane rozwiązania były dedykowane do tego typu zadań oraz były jednolite w skali województwa.

W związku z ciągłym rozwojem infrastruktury teleinformatycznej przy planowaniu zakupu należy przewidzieć w w/w urządzeniach nadmiarowe interfejsy sieciowe na potrzeby przyszłych połączeń np. OST 112, radiolinie itp.

b) Węzły teleinformatyczne i serwerownie.

Pomieszczenie techniczne serwerowni to główny punkt dystrybucyjny okablowania strukturalnego, w którym zbiega się okablowanie poziome i pionowe obiektu, kable światłowodowe, jak również doprowadzenia traktów sieci rozległej we/wy od głowicy telekomunikacyjnej budynku. 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 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.

Zaleca się, aby serwerownie były zabezpieczone przed dostępem osób trzecich oraz spełniać wymagania Ustawy o ochronie danych osobowych (jeżeli w serwerownia jest strefą przetwarzania danych).

Pomieszczenie(a) przeznaczone dla administratorów oraz operatorów powinno być oddzielone fizycznie od pomieszczenia technicznego serwerowni. Pomieszczenie to powinno być wyposażone w szafę 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.
Z punktu widzenia poprawności działania zaleca się, aby w miarę możliwości pomieszczenie serwerowni spełniało następujące wytyczne:
- zapewnienie redundancji urządzeń klimatyzacyjnych,
- dostarczenie odpowiedniej ilości chłodnego powietrza do każdego urządzenia technicznego,
- odprowadzenia takiej samej ilości gorącego powietrza, zapobiegania recyrkulacji gorącego powietrza,
- zrealizowania powyższych wytycznych w sposób ciągły, nadmiarowy i energooszczędny.

Dodatkowo poza wymaganiami czysto technicznymi, układ chłodzenia serwerowni musi spełniać następujące wymagania:
- skalowalność systemu i możliwość adaptacji,
- niezawodność działania,
- niskie koszty eksploatacyjne,
- łatwość serwisowania.

Zaleca się, aby urządzenia aktywne, pasywne były umieszczone w szafach teletechnicznych typu „rack" w standardzie 19". Liczba elementów aktywnych zależy od zwymiarowania sieci.

O ile w infrastrukturze nie ma centralnego systemu UPS szafa powinna uwzględniać miejsce na zamontowanie lokalnego UPS'a, podtrzymującego działanie urządzeń zamontowanych w szafie.

Elementy związane z zasilaniem energetycznym, chłodzeniem, ochroną przeciwpożarową, systemy kontroli dostępu i alarmowania oraz monitoringiem warunków pracy powinny być uwzględnione w projektach bądź innego rodzaju koncepcjach, czy dokumentach dotyczących nowych zadań bądź też modernizacji istniejącej infrastruktury teleinformatycznej.

Zaleca się budowę sieci wg. normy PN-EN 50173 *Systemy okablowania strukturalnego.*

c) Zasilanie elektryczne.

System energetyczny zasilania obiektu, powinien być zbudowany tak, aby istniała możliwość zasilania z dwóch, niezależnych, przełączanych automatycznie źródeł zasilania w energię elektryczną.

Zaleca się, aby sieć zasilająca infrastrukturę techniczną systemu informatycznego była wykonana w postaci wydzielonej instalacji elektrycznej z możliwością podtrzymywania napięcia w sytuacjach awaryjnych.

Czas podtrzymania zasilania pracy urządzeń aktywnych powinien być obliczony w taki sposób, by było możliwe co najmniej bezpieczne wyłączenie zasilanych urządzeń aktywnych w przypadku zaniku zasilania w sieci, lub włączenia agregatu prądotwórczego. 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.

Projektując system zasilania awaryjnego (UPS) należy wziąć pod uwagę następujące kryteria w momencie rozpoczęcia projektu:

- łączną wydajność energetyczną wyrażaną dostarczaną mocą średnią w założonym czasie podtrzymania,
- niezbędny czas podtrzymania wyrażany w minimalnej wymaganej liczbie minut pracy na zasilaniu awaryjnym,
- lokalizację położenia systemu, np. UPS-y z uwagi na ciężar baterii są umieszczane zwykle w piwnicy lub na parterze, a agregaty na zewnątrz z uwagi na zagrożenie pożarowe i emisje spalin,
- ilość odbiorników energii oraz ich lokalizacji geograficznej (piętra, budynki),
- przewidywane profile odbiorników energii (zapotrzebowanie na moc średnią oraz moc szczytową),
- moc bierną odbiorników i charakter obciążenia, które wnoszą do sieci zasilającej (indukcyjne, pojemnościowe, reaktancyjne, czysta rezystancja),
- charakter pracy odbiorników – praca ciągła czy urządzenie włączane okresowo,
- szacowaną docelową liczbę odbiorników i ich profile energetyczne,
- w zależności od powyższych parametrów ważnym czynnikiem doboru architektury sieci zasilającej jest jej skalowalność czyli zdolność do łatwej i taniej rozbudowy o kolejne odbiorniki. Dla niektórych systemów skalowalność może być osiągnięta poprzez instalację równoległą kolejnego UPS do już pracującego,
- niezawodność sieci zasilania. Z uwagi na wspomniane wcześniej wymagania wpływają one zarówno na topologię sieci zewnętrznej, część odbiorników ma podwójne lub potrójne zasilacze pozyskujące prąd z różnych źródeł,
- odporność na zakłócenia od przełączania wysokich prądów w sieci zewnętrznej.
- sposób zarządzania. Systemy zasilania awaryjnego umożliwiają zdalne zarządzanie (IP) zgodnie z protokołami SNMP i zdalny monitoring oraz konfiguracją systemu, sprawdzanie stanu naładowania baterii, wysyłanie ostrzeżeń do administratora mailem lub SMS-em itp.

d) Serwery, macierze.

Decyzję o stosowaniu serwerów, macierzy należy podejmować na podstawie analizy funkcjonalnej i ekonomicznej.
Przy wyborze rozwiązań technicznych należy stosować urządzenia i oprogramowanie dedykowane w ramach koncepcji, projektów oraz innych działań organizacyjno-zarządczych.

e) Systemy archiwizacji danych.

Archiwizacja danych ma na celu zabezpieczenie danych na wypadek konieczności odtworzenia w razie ich utraty (awaria systemu, umyślne bądź nieświadome wykasowanie, uszkodzenie fizyczne dysków/serwerów, katastrofy itp.). Rekomenduje się, aby system do archiwizacji danych teleinformatycznych zapewniał automatyzację i centralizację całego procesu oraz umożliwiał odtworzenie utraconych danych lub systemów w jak najkrótszym czasie.

Archiwizację danych należy wykonywać w regularnych odstępach czasu, które uzależnione są od potrzeb zgłaszanych przez administratorów aplikacji. Zaleca się, aby systemy do archiwizowania danych posiadały możliwość tworzenia kopii przyrostowych lub różnicowych oraz deduplikacji danych.

Zaleca się, aby archiwizować dane przynajmniej raz dziennie. Szczegóły dotyczące archiwizacji powinna zawierać Polityka bezpieczeństwa.

f) Systemy bezpieczeństwa.

Bezpieczeństwo systemów teleinformatycznych oraz informacji przetwarzanych w tych systemach jest kluczowym aspektem dla każdej jednostki organizacyjnej. Wszystkie aspekty związane z bezpieczeństwem zapisane są w Polityce ochrony informacji jednostki organizacyjnej. Polityka stanowi sformalizowany dokument, podpisany przez kierownika jednostki organizacyjnej oraz wdrożony do stosowania w danej jednostce. Wszystkie działania w obszarze teleinformatyki skorelowane są z Polityką bezpieczeństwa informacji oraz stanowią pochodną zapisów zawartych w Polityce.

Wszelkie systemy i urządzenia teleinformatyczne użytkowane w jednostce muszą być chronione przed skutkami działania szkodliwego oprogramowania oraz dostępem osób trzecich. W celu zabezpieczenia przed powyższymi zagrożeniami zaleca się zastosowanie następujących rozwiązań:

- Firewall,

- Systemy wykrywania i prewencji włamań – IPS,
- Sieci VPN,
- Systemy kontroli treści,
- Systemy ochrony stacji roboczych (w tym systemy antywirusowe),
- Zabezpieczenie poczty elektronicznej,
- Autoryzacja i uwierzytelnianie,
- Systemy zarządzania bezpieczeństwem,
- Systemy ochrony danych,
- Systemy monitoringu IP.
-

g) <u>Wymagania przeciwpożarowe dla pomieszczeń serwerowni</u>

Urządzenia przeciwpożarowe w pomieszczeniach serwerowni powinny być wykonane zgodnie z projektem uzgodnionym przez rzeczoznawcę do spraw zabezpieczeń przeciwpożarowych, a warunkiem dopuszczenia do ich użytkowania jest przeprowadzenie odpowiednich dla danego urządzenia prób i badań, potwierdzających prawidłowość ich działania. **<u>Wymagania przeciwpożarowe dla pomieszczenia serwerowni przetwarzającej dane o znaczeniu krajowym.</u>**

1. Pomieszczenie serwerowni powinno być wydzielone przeciwpożarowo przegrodami o klasie odporności ogniowej co najmniej EI 60 i zamknięte drzwiami o klasie odporności ogniowej co najmniej EI 60.
2. Przepusty instalacyjne w przegrodach wydzielenia przeciwpożarowego pomieszczenia serwerowni powinny mieć klasę odporności ogniowej co najmniej EI 60.
3. Przewody wentylacyjne lub klimatyzacyjne w miejscu ich przejścia przez przegrody wydzielenia przeciwpożarowego pomieszczenia serwerowni powinny być wyposażone w przeciwpożarowe klapy odcinające o klasie odporności ogniowej co najmniej EIS 60. W przypadku zapewniania poza pomieszczeniem serwerowni klasy odporności ogniowej EIS 60 przez przewody lub ich obudowę dopuszcza się nie wykonywanie przeciwpożarowych klap odcinających w miejscu przejścia tych przewodów przez przegrody pomieszczenia serwerowni.
4. Podest technologiczny, na którym sytuuje się szafy serwerów oraz jego konstrukcja nośna powinny być wykonane z materiałów niepalnych (klasy reakcji na ogień odpowiednio co najmniej $A2_{fl}$ lub A2,d0).
5. Okładziny sufitów lub sufity podwieszone powinny być wykonane z materiałów niepalnych lub niezapalnych, niekapiących i nieodpadających pod wpływem ognia (o klasie reakcji na ogień co najmniej B,d0).
6. Pomieszczenie serwerowni należy wyposażyć w stałe urządzenia gaśnicze (na gazy obojętne i mieszaniny gazów gaśniczych, chlorowcopochodne węglowodorów lub dwutlenek węgla) uruchamiane samoczynnie we wczesnej fazie rozwoju pożaru.
7. Pomieszczenie serwerowni należy wyposażyć w system sygnalizacji pożarowej, obejmujący urządzenia sygnalizacyjno-alarmowe, służące do samoczynnego wykrywania i przekazywania informacji o pożarze.

8. System sygnalizacji pożarowej serwerowni powinien być podłączony do systemu monitoringu pożarowego Państwowej Straży Pożarnej.
9. Pomieszczenie serwerowni należy wyposażyć w gaśnice zalecane do gaszenia sprzętu elektronicznego.

Wymagania przeciwpożarowe dla pomieszczenia serwerowni przetwarzającej dane o znaczeniu wojewódzkim.

1. Pomieszczenie serwerowni powinno być wydzielone przeciwpożarowo przegrodami o klasie odporności ogniowej co najmniej EI 60 i zamknięte drzwiami o klasie odporności ogniowej co najmniej EI 60.
2. Przepusty instalacyjne w przegrodach wydzielenia przeciwpożarowego pomieszczenia serwerowni powinny mieć klasę odporności ogniowej co najmniej EI 60.
3. Przewody wentylacyjne lub klimatyzacyjne w miejscu ich przejścia przez przegrody wydzielenia przeciwpożarowego pomieszczenia serwerowni powinny być wyposażone w przeciwpożarowe klapy odcinające o klasie odporności ogniowej co najmniej EIS 60. W przypadku zapewniania poza pomieszczeniem serwerowni klasy odporności ogniowej EIS 60 przez przewody lub ich obudowę dopuszcza się nie wykonywanie przeciwpożarowych klap odcinających w miejscu przejścia tych przewodów przez przegrody pomieszczenia serwerowni.
4. Podest technologiczny, na którym sytuuje się szafy serwerów oraz jego konstrukcja nośna powinny być wykonane z materiałów niepalnych (klasy reakcji na ogień odpowiednio co najmniej $A2_{fl}$ lub A2,d0).
5. Okładziny sufitów lub sufity podwieszone powinny być wykonane z materiałów niepalnych lub niezapalnych, niekapiących i nieodpadających pod wpływem ognia (o klasie reakcji na ogień co najmniej B,d0).
6. Pomieszczenie serwerowni należy wyposażyć w system sygnalizacji pożarowej, obejmujący urządzenia sygnalizacyjno-alarmowe, służące do samoczynnego wykrywania i przekazywania informacji o pożarze.
7. System sygnalizacji pożarowej serwerowni powinien być podłączony do systemu monitoringu pożarowego Państwowej Straży Pożarnej.
8. Pomieszczenie serwerowni należy wyposażyć w gaśnice zalecane do gaszenia sprzętu elektronicznego.

Wymagania przeciwpożarowe dla pomieszczenia serwerowni przetwarzającej dane o znaczeniu powiatowym, w tym szkoły PSP

1. Pomieszczenie serwerowni powinno być wydzielone przeciwpożarowo przegrodami o klasie odporności ogniowej co najmniej EI 60 i zamknięte drzwiami o klasie odporności ogniowej co najmniej EI 60.
2. Przepusty instalacyjne w przegrodach wydzielenia przeciwpożarowego pomieszczenia serwerowni powinny mieć klasę odporności ogniowej co najmniej EI 60.
3. Przewody wentylacyjne lub klimatyzacyjne w miejscu ich przejścia przez przegrody wydzielenia przeciwpożarowego pomieszczenia serwerowni powinny być wyposażone w przeciwpożarowe klapy odcinające o klasie odporności ogniowej co najmniej EIS

60. W przypadku zapewniania poza pomieszczeniem serwerowni klasy odporności ogniowej EIS 60 przez przewody lub ich obudowę dopuszcza się nie wykonywanie przeciwpożarowych klap odcinających w miejscu przejścia tych przewodów przez przegrody pomieszczenia serwerowni.
4. Podest technologiczny, na którym sytuuje się szafy serwerów oraz jego konstrukcja nośna powinny być wykonane z materiałów niepalnych (klasy reakcji na ogień odpowiednio co najmniej A_{2fl} lub A2,d0).
5. Okładziny sufitów lub sufity podwieszone powinny być wykonane z materiałów niepalnych lub niezapalnych, niekapiących i nieodpadających pod wpływem ognia (o klasie reakcji na ogień co najmniej B,d0).
6. Pomieszczenie serwerowni należy wyposażyć w gaśnice zalecane do gaszenia sprzętu elektronicznego.

5.2.2 Aplikacje i usługi

a) System Wspomagania Decyzji dla Stanowisk Kierowania.

Podstawowym systemem służącym do wspomagania decyzji kierującego akcją ratowniczą jest oprogramowanie SWD. System funkcjonuje na wszystkich trzech poziomach organizacyjnych PSP tj. w KG, KW i KM/KP, będąc podstawowym narzędziem pracy stanowisk kierowania. Dane w systemie są migrowane w czasie rzeczywistym w układzie pionowym i poziomym, przy czym proces wprowadzania informacji następuje na poziomie KM/KP, natomiast struktura i słowniki są tworzone centralnie. System zawiera moduły odpowiadające za bieżącą informację o stanie sił i środków na terenie obszaru działania jednostki organizacyjnej, umożliwia ewidencjonowanie przeprowadzonych zdarzeń (zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego) oraz analizę statystyczną.

Funkcjonalność systemu dopełniają moduł mapowy oraz moduł lokalizacji ruchu pojazdów. W systemie zostały zaimplementowane role dedykowane poszczególnym komórkom organizacyjnym odpowiedzialnym za wprowadzanie i bieżącą kontrolę merytorycznej zawartości danych.

W tak rozbudowanym systemie rekomenduje się utrzymywanie na każdym poziomie systemu, osób odpowiedzialnych za zarządzanie danymi (administratorzy aplikacji) oraz zapewnienie ciągłości funkcjonowania pod względem technicznym (administratorzy systemu teleinformatycznego). Administratorem aplikacji jest pracownik merytoryczny komórki odpowiedzialnej za obszar informacyjny (dziedzinowy) systemu, np. operacyjny, kadrowy, techniczny, itd. Administratorem systemu

teleinformatycznego jest pracownik komórki odpowiedzialnej za teleinformatykę.

b) **Dostęp do sieci LAN.**

Dostęp do sieci LAN, ze względu na lokalizację stacji klienckiej możemy podzielić na dostęp z sieci wewnętrznej (przewodowy i bezprzewodowy) oraz dostęp spoza sieci wewnętrznej. Rekomendowany jest dostęp z sieci wewnętrznej przy użyciu mechanizmu katalogowego (zarówno w zakresie sieci przewodowej, jak i bezprzewodowej). Bezpośrednia realizacja dostępu odbywa się poprzez uwierzytelnienie użytkownika unikalnym identyfikatorem oraz hasłem o złożoności i okresie ważności zgodnym z przyjętą polityką ochrony informacji.

Uzupełnieniem systemu bezpieczeństwa dostępu może być zastosowanie mechanizmów blokady portów przed nieautoryzowanym dostępem oraz zastosowanie urządzeń typu firewall, sondy treści (IDS, IPS). W przypadku dostępu bezprzewodowego zaleca się stosowanie najwyższego możliwego mechanizmu zabezpieczenia dostępu do sieci.

Dostęp do sieci LAN spoza lokalizacji jednostki należy realizować z wykorzystaniem szyfrowania oraz tuneli VPN pomiędzy stacją kliencką a urządzeniami styku sieci jednostki organizacyjnej. Po zestawieniu tunelu dalsza autoryzacja i dostęp odbywa się na zasadach analogicznych, jak w sieci wewnętrznej.

c) **Dostęp do sieci Internet – serwisy produkcyjne i klienckie, informacyjne, bankowe, usługowe, aplikacyjne, itp.**

Podstawowym łączem dostępowym do Internetu powinno być szerokopasmowe łącze symetryczne. Na poziomie KG i KW wskazane jest utrzymywanie symetrycznego łącza redundantnego od niezależnych dostawców. Dopuszcza się wykorzystanie sieci OST112 jako łącza zapasowego dla dostępu do Internetu, w przypadku udostępnienia takiej funkcjonalności.

Dostęp do sieci zewnętrznej powinien być realizowany za pośrednictwem urządzeń do tego celu dedykowanych (routery, firewalle), wyposażonych w mechanizmy ochrony przed niepowołanym ich wykorzystaniem. Możliwe jest stosowanie rozwiązań programowych. Sposób i zakres dostępu do zasobów zewnętrznych określa polityka bezpieczeństwa informacji.

Serwisy własne udostępniane na zewnątrz (WWW, BIP, e-mail itp.) muszą stanowić odrębną strefę urządzeń zabezpieczających (tzw. DMZ). Sposób i zakres dostępu do zasobów określa polityka bezpieczeństwa informacji.

d) **Systemy informacji przestrzennej (GIS) – pozyskiwanie, przetwarzanie i udostępnianie danych GIS.**

1) Do lokalizacji, prezentacji i modyfikacji obiektów w przestrzeni geograficznej oraz dokonywania analiz przestrzennych wykorzystuje się dane pochodzące przede wszystkim z Państwowego Zasobu Geodezyjnego i Kartograficznego (PZGiK) oraz innych danych przestrzennych wytwarzanych, gromadzonych i modyfikowanych przez organy państwa i udostępniane nieodpłatnie w ramach ustawy o infrastrukturze informacji przestrzennej, ustawy prawo geodezyjne i kartograficzne oraz ustawy o podmiotach realizujących zadania publiczne w postaci usług sieciowych tj. WMS, WFS, a także w postaci wektorowej i rastrowej. Dopuszcza się pozyskiwane danych przestrzennych od dostawców komercyjnych, o ile pozyskanie tych danych wynika z potrzeb operacyjnych i nie ma możliwości ich pozyskania z zasobów prowadzonych przez organy państwa. Na potrzeby operacyjne oraz dla działań prowadzonych w trybach planowania, zapobiegania i odbudowy istnieje możliwość nieodpłatnego pozyskiwania zobrazowań satelitarnych i warstw wektorowych w ramach usług operacyjnych GMES – Global Monitoring for Environment and Security (Globalny Monitoring na potrzeby Środowiska i Bezpieczeństwa). KG PSP posiada status tzw. użytkownika autoryzowanego dla International Charter for Space and Major Disasters oraz jest tzw. National Focal Point (Krajowy Punkt Kontaktowy) dla usług operacyjnych GMES.

Do zarządzania zbiorem danych przestrzennych wykorzystuje się narzędzia klasy GIS pozyskiwane komercyjnie lub open source. Dedykowanym narzędziem w pracy operacyjnej jest system klasy wspomagania decyzji zintegrowany z modułem mapowym.

e) **Systemy wymiany informacji – systemy elektronicznego zarządzania dokumentami, poczta elektroniczne, wymiana plików, wideokonferencja, telefonia IP.**

Rekomenduje się wdrażanie w jednostkach organizacyjnych systemu elektronicznego zarządzania dokumentami. Wprowadzenie systemu zapewnia rozliczalność pracy, kontrolę przepływu i terminowość prowadzonych spraw.

W zakresie poczty elektronicznej wskazane jest centralizowanie usług pocztowych, w oparciu o dedykowaną dla potrzeb organizacji domenę internetową oraz ujednolicenie adresacji i dostępu określonego przez przyjętą spójną politykę bezpieczeństwa informacji. Do realizacji zadań służbowych należy wykorzystywać wyłącznie służbowe konta poczty elektronicznej.

Dla potrzeb wymiany plików (serwisy typu ftp, sftp) wskazane jest wykorzystywanie sieci OST 112. Dopuszcza się realizację usług poprzez sieć Internet z zastosowaniem mechanizmów zabezpieczeń, jak dla dostępu zdalnego.

Usługi związane transmisją głosu i wideo (wideokonferencje, telefonia IP, itp.) należy w miarę możliwości projektować i wdrażać w oparciu o infrastrukturę sieci OST 112.

f) **Systemy zarządzania organizacją – kadry, płace, magazyny, finanse, logistyka.**

Dopuszcza się stosowanie dowolnych systemów dziedzinowych w jednostkach organizacyjnych, we wszystkich obszarach przetwarzania danych, jednakże muszą one zapewniać komunikację z wykorzystaniem otwartego protokołu wymiany danych z centralnym systemem SPD.

6. Podsumowanie.

Dokument ten stanowi zbiór zasad oparty o tzw. „dobre praktyki" oraz stosowane dotychczas wzorce w jednostkach organizacyjnych PSP. Zasady te maja stanowić pomoc dla Kierowników jednostek organizacyjnych w dążeniu do uzyskania wysokiego poziomu zarządzania zasobami teleinformatycznymi oraz podniesienia sprawności i funkcjonowania swoich jednostek.

7. Załączniki.

1. Słownik terminologii.

Słownik terminów używanych w Zasadach.

1) **AI – Administrator Informacji** – (właściciel informacji) - osoba (lub osoby) odpowiedzialna za daną, wyodrębnioną grupę informacji podlegającej ochronie. Ustala zakres grupy informacji i zasady przetwarzania grupy informacji. Ustala jakie osoby i na jakich prawach mają mieć dostęp do informacji z danej grupy. Każda grupa informacji ma swojego AI. Jeden AI może nadzorować kilka grup informacji. AI jest nadzorowany przez ABI.
2) **ABI – Administrator Bezpieczeństwa Informacji** - osoba (lub osoby) odpowiedzialna za zarządzanie bezpieczeństwem informacji. Nadzoruje i kontroluje AS (Administratora Systemu) w sferze realizacji zasad określonych w Polityce Bezpieczeństwa Informacji. Kontroluje przyznawanie określonych praw dostępu do zasobów informacji.
3) **Administrator Systemu** - osoba odpowiedzialna za poprawne działanie systemu, w którym przetwarzane są informacje.
4) **Bezpieczeństwo informacji** – wszelkie przedsięwzięcia w sferze technicznej, organizacyjnej, prawnej mające na celu ochronę:
   - **integralności** - właściwości zapewniającej dokładność i kompletność informacji oraz, że informacje nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   - **poufności** – właściwości zapewniającej, że informacja nie jest udostępniana i ujawniana nieautoryzowanym podmiotom lub procesom,
   - **dostępności** - właściwości bycia dostępnym i możliwym do wykonania na żądanie osób uprawnionych do informacji wtedy, gdy zachodzi taka potrzeba,
5) **DMZ** - *(ang. Demilitary Zone)* – strefa zdemilitaryzowana – określenie obszaru lokalizującego urządzenia sieciowe (serwery) między bezpośrednim polaczeniem z siecią Internet, a siecią LAN. Z reguły umieszcza się tam zasoby, które mają za zadanie udostępnianie usług lub (zasobów) na zewnątrz (do Internetu). W tej strefę ustala się inny – z reguły mniejszy – stopień bezpieczeństwa dla tych zasobów. Stanowi ona strefę buforową dla zasobów w sieci LAN i pierwszą linie obrony przez niebezpieczeństwami związanymi z siecią Internet.
6) **E-mail** - (ang. *electronic mail*) – usługa pozwalająca na przesyłanie informacji za pomocą Internetu. Każdy użytkownik posiada swój unikalny adres skrzynki pocztowej, pozwalający jednoznacznie określić konkretny serwer oraz korzystającą z poczty osobę (identyfikator@adres_serwera)
7) **Firewall** - z ang. zapora ogniowa - termin określający złożony system zabezpieczeń sieci przed włamaniami. Z reguł składa się z zaawansowanego oprogramowania zainstalowanego na komputerze (firewall programowy) lub

stanowiący urządzenie instalowane w sieci (firewall sprzętowy), pośredniczący w komunikacji między siecią lokalną i Internetem. Umożliwia kontrolę połączeń.

8) **FTP** - (ang. *File Transfer Protocol*), protokół służący do przesyłania plików w sieci Internetowej. Jedna z usług dostępnych w Internecie (serwery FTP). Podobnie **SFTP** (Secure FTP – bezpieczny FTP) protokół z dodatkowo włączonym systemem kryptograficznym.
9) **Gateway** - urządzenie podłączone do sieci komputerowej (komputer pełniący funkcję routera lub router sprzętowy) na styku z siecią zewnętrzną, za pośrednictwem którego komputery z sieci lokalnej komunikują się z komputerami w innych sieciach.
10) **GDLP** – Generalna Dyrekcja Lasów Państwowych.
11) **Grupa Informacji** – zbiór informacji podlegających ochronie, opisujących podobne zagadnienia lub dotyczących jednego tematu (np. informacje kadrowe, finansowe, operacyjne).
12) **GIS** – *(ang. Geografic Information System)* – system informacji przestrzennej umożliwiający przedtsawianie danych w środowisku mapowym, wykorzystujący różne rodzaje i formaty map.
13) IMAP - (ang. *Internet Message Access Protocol*) to internetowy protokół pocztowy zaprojektowany jako następca POP3. W przeciwieństwie do POP3, który umożliwia jedynie pobieranie i kasowanie poczty, IMAP pozwala na zarządzanie wieloma folderami pocztowymi oraz pobieranie i operowanie na listach znajdujących się na zdalnym serwerze.
14) **Informacja** - jest to treść wszelkiego rodzaju dokumentów przechowywana na dowolnym nośniku informacji. Może być wyrażona za pomocą pisma, mowy, obrazu, dźwięku, znaku, kodu lub w jakikolwiek inny sposób. Jest podstawą funkcjonowania każdej organizacji.
15) **Informacje chronione** – informacje stanowiące w PSP tajemnicę przedsiębiorstwa oraz informacje prawnie chronione.
16) **Informacje prawnie chronione** – informacje, których ochronę nakazują obowiązujące przepisy prawa.
17) **Informacje jawne** – informacje nie należące do informacji chronionych.
18) **Internet** – globalna sieć komputerowa, łącząca ze sobą miliony hostów zasobów), wykorzystująca połączenia za pomocą protokołu TCP/IP. Udostępnia usługi i serwisy takie jak www,
19) **IT** – (ang. *Information Technology)* – pojęcie określające szeroko rozumianą technologię informacyjną. Obejmuje swym zasięgiem zarówno zarządzanie informację jak i technologię (rozwiązania techniczne) służącą do zarządzania informacją.
20) **KSRG** – Krajowy System Ratowniczo – Gaśniczy.

21) **LAN** – (ang. *Local Area Network*) – sieć teleinformatyczna ograniczona do jednej fizycznej lokalizacji, z reguły w obrębie jednostki organizacyjnej (jeden lub kilka budynków na danym terenie).
22) **LP** – Lasy Państwowe.
23) **Macierz** – sieciowe urządzenie serwerowe służące do udostępniania plików. Macierze wyposażone są w dużą ilość dysków połączonych za pomocą specjalizowanych kontrolerów, zapewniających im duży stopień niezawodności oraz system operacyjny służący do zarządzania zasobami macierzy.
24) **NAT** – (ang. *Network Adres Translation)* – translacja adresów internetowych – mechanizm ukrywania adresów sieciowych stosowany w przypadku np. udostępniania zasobów do sieci Internet.
25) **Nośnik informacji** – medium, na którym zapisuje się i przechowuje informację.
26) **OST112 – O**gólnopolska Sieć Teleinformatyczna na potrzeby obsługi numeru 112 – sieć rozległa na potrzeby służb.
27) **Polityka Bezpieczeństwa Informacyjnego** – opisany zestaw reguł związany z zarządzaniem informacją w jednostce organizacyjnej, stanowiący sformalizowany dokument, podpisany przez Kierownika jednostki i wdrożony do stosowania i przestrzegania. Wg PN jest to *zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wewnątrz określonego systemu.* Polityka opisuje zarówno sferę zarządzania informacja jak i sferę techniczną (informatyczną), czyli systemy w których przetwarzane są informacje.
28) **POP3 - (ang. *Post Office Protocol version 3*) to protokół internetowy z warstwy aplikacji pozwalający na odbiór poczty elektronicznej ze zdalnego serwera do lokalnego komputera poprzez połączenie TCP/IP.**
29) **Przetwarzanie informacji** – procesy związane z tworzeniem, zbieraniem, utrwalaniem, odczytem, modyfikacją, przechowywaniem, kopiowaniem, udostępnianiem lub usuwaniem informacji.
30) **PSP** – Państwowa Straż Pożarna.
31) **PZGiK** - Państwowy Zasób Geodezyjny i Kartograficzny.
32) **Router** – (ang. *router*) – urządzenie służące do kierowania pakietów informacji w sieci. Decyduje którędy mają płynąć pakiety danych. Za zwyczaj znajduje się na styku kilku sieci (np. lokalnej i Internetu).
33) **Serwer** – najczęściej komputer lub inne urządzenie służące do udostępniania swoich zasobów do użycia w sieci. Serwery mogą udostępniać pliki, aplikacje, miejsce na dysku, dane, drukarki itp.

34) SMTP - (ang. *Simple Mail Transfer Protocol*) – protokół komunikacyjny opisujący sposób przekazywania (wysyłania) poczty elektronicznej w Internecie.
35) **Społeczeństwo Informacyjne** – jest to takie społeczeństwo, które:
    - produktywnie wykorzystuje zasób jakim jest informacja, oraz w którym intensywna pod względem wiedzy produkcja odgrywa dominującą rolę,
    - nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz środki te są podstawą tworzenia dochodu narodowego i dostarczają źródła utrzymania większości społeczeństwa,
    - charakteryzuje się przygotowaniem i zdolnością do użytkowania systemów informatycznych, jest skomputeryzowane i wykorzystujące usługi telekomunikacji do przekazywania i zdalnego przetwarzania informacji.
36) SNMP - Simple Network Management Protocol — rodzina protokołów sieciowych wykorzystywanych do zarządzania urządzeniami sieciowymi, takimi jak routery, przełączniki, komputery czy centrale telefoniczne. Do transmisji wiadomości SNMP wykorzystywany jest głównie protokół UDP: standardowo port 161 wykorzystywany jest do wysyłania i odbierania żądań, natomiast port 162 wykorzystywany jest do przechwytywania sygnałów trap od urządzeń. Możliwe jest także wykorzystanie innych protokołów do przekazywania żądań, na przykład TCP.
37) SSH - (ang. *Secure SHell* - bezpieczna powłoka) jest to protokół (czyli język, za pomocą którego porozumiewają się komputer) umożliwiający zdalne sterowanie innym komputerem lub urządzeniem sieciowym np. router, swich, access point. Połączenie poprzez protokół SSH jest szyfrowane. Protokoły z rodziny SSH korzystają zwykle z portu 22 protokołu TCP.
38) **SSL** - (ang. *Secure Sockets Layer*) warstwa bezpiecznych gniazdek - protokół opracowany przez *Netscape Comunicatnions* dla potrzeb Internetu. Zabezpiecza strony WWW, umożliwiając szyfrowanie i uwierzytelnianie przekazywanych informacji.
39) **SWD_ST** – System Wspomagasnia Decyzji Systemy Teleinformatyczne wdrożony w PSP jako podstawowy system dla Stanowisk Kierowania.
40) **Switch** – przełącznik, urządzenie sieciowe służące do łączenia w sieci komputerów oraz innych urządzeń sieciowych.
41) **System Informacyjny** – zespół określonych powiązanych ze sobą elementów, (działających według określonych reguł) którymi są: źródła danych, metody ich gromadzenia i przetwarzania, kanały przepływu informacji, środki techniczne i ludzie realizujący to przetwarzanie oraz miejsca przeznaczenia informacji.

42) **System informatyczny** – część systemu informacyjnego, wspomagająca przetwarzanie informacji, składająca się z urządzeń komputerowych, oprogramowania oraz zewnętrznych nośników informacji.
43) **Sytuacja Kryzysowa** – podejrzenie lub stwierdzenie faktu naruszenia przyjętej Polityki Bezpieczeństwa Informacyjnego.
44) **Szerokopasmowe łącze symetryczne – łącze o dużej przepustowości (Mbit), zapewniające szybki dostęp do zasobów Internetu, o takich samych parametrach transmisji w obydwu kierunkach, tzn takiej samej prędkości wysyłania i odbierania danych.**
45) **TCP/IP** - (ang. *Transport Control Protocol / Internet Protocol*) rodzina protokołów transmisyjnych wykorzystywanych w sieci Internet.
46) TELENET - standard protokołu komunikacyjnego używanego w sieciach komputerowych do obsługi odległego terminala w architekturze klient-serwer. Podobnie jak SSH Telenet umożliwia zdalne sterowanie innym komputerem lub urządzeniem sieciowym np. router, swich, access point. Połączenie poprzez protokół SSH jest nie jest szyfrowane. Protokół telnet korzystają zwykle z portu 23 protokołu TCP. Ze względu na łatwość podsłuchania coraz rzadziej stosowany.
47) **UPS** - (ang. *Uninterruptable Power Supply*) - zasilacz awaryjny; stabilizuje napięcie, usuwa zakłócenia sieci energetycznej i umożliwia pracę podłączonych do niego urządzeń w przypadku nagłego zaniku napięcia
48) **UTM** – (ang. *Unified Threat Management*) – zintegrowane urządzenie do zarządzania zagrożeniami – rodzaj robudowanoeo firewall, zawierającego oprócz standardowych usług firewall–a i rouetra zawiera również ochronę antyspamową, antywirusową, wyrywanie intruzów, filtrację treści.
49) **WAN** – (ang. *Wide Area Network*) – sieć teleinformatyczna o zasięgu rozległym, obejmująca wiele lokalizacji geograficznie oddalonych. Z reguły łączy ze sobą obszar kilku miast lub całego kraju.
50) VLAN - (ang. *Virtual Local Area Network)* – sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej.
51) **VPN** – (ang. *Virtual Private Network)* – sieć wirtualna – technologia umożliwiająca bezpieczny (szyfrowany) dostęp do zasobów innej sieci, z reguły sieci LAN, w której medium transportowym jest Internet.