WYKAZ SKRÓTÓW

AFIS	automatyczny system identyfikacji daktyloskopowej
AN	Access Network, Access Node – sieć dostępu, punkt dostępu
AON	Akademia Obrony Narodowej
BBN	Biuro Bezpieczeństwa Narodowego
BCC	Bearer Capability Channel – identyfikacja parametrów kanału
BCP	Business Continuity Planning – planowanie ciągłości biznesowej
CCTV	Closed-Circuit Television – systemy telewizji dozorowej
CEPiK	Centralna Ewidencja Pojazdów i Kierowców
CODIS	Combined DNA Index System
CM	Churn Management – zarządzanie migracją klientów
CRM	Customer Relationship Management – zarządzanie relacjami z klientami
CZS	centrum zarządzania siecią
DDoS	Distributed Denial of Service – rozproszona blokada usług
DoD	Department of Defense – Departament Obrony
DoS	Denial of Service – blokada usług
DRP	Disaster Recovery Planning – planowanie działań odtworzeniowych
DS1	Digital Subscriber Signaling No.1 – cyfrowy system sygnalizacji nr 1
ENISA	European Network and Information Security Agency – Europejska Agencja Bezpieczeństwa Sieci i Informacji (Agenda Unii Europejskiej)
EPCIP	Europejski Programem Ochrony Infrastruktury Krytycznej
FM	Fraud Management – zarządzanie nadużyciami i oszustwami
GIS	Geographical Information Systems – geograficzne systemy informatyczne
GPW	Giełda Papierów Wartościowych
GSM	Global System for Mobile Communications – globalny system telefonii komórkowej
GUS	Główny Urząd Statystyczny
HVAC	Heating, Ventilation, Air Conditioning – ogrzewanie, wentylacja, klimatyzacja

ICT	Information and Communication Technology – technologie telekomunikacji i informatyki
IDS/IPS	Intruder Detection/Prevention Systems
IK	infrastruktura krytyczna
IMS	IP Multimedia System
IP	Internet Protocol address
ISDN	Integrated Services Digital Network – sieć cyfrowa z integracją usług
ISMS	Information Security Management System – system zarządzania bezpieczeństwem informacji
ITU	International Telecommunications Union – Międzynarodowa Unia Telekomunikacyjna
ITU-T	International Telecommunication Union – Telecommunication – Międzynarodowa Unia Telekomunikacyjna – Sekcja Telekomunikacji
KIT	krytyczna infrastruktura telekomunikacyjna
KSIP	Krajowy System Informacyjny Policji
LE	Local Exchange – lokalna centrala
LOS	Loss of Signal – brak sygnału wejściowego
MAN	Metropolitan Area Network – sieć miejska
MKS	Master Key System – system klucza – matki
MPLS	Multiprotocol Label Switching – wieloprotokołowa komutacja etykiet
MS	Member State – status członka
MSWiA	Ministerstwo Spraw Wewnętrznych i Administracji
MTBF	Mean Time Between Failure – średni czas pomiędzy awariami
MTR	Mean Time to Repair – średni czas naprawy
MTTR	Mean Time To Repair – średni czas naprawy
OSI	Open Systems Interconnection – model referencyjny połączonych systemów otwartych
PABX	Private Branch Exchange – wewnętrzna centrala abonencka
PB	polityka bezpieczeństwa
POH	Path Overhead – nagłówek ścieżki
PSTN	Public Switched Telephone Network – publiczna komutowana sieć telefoniczna
RA	Revenue Assurance – zapewnienie przychodów
SDH	Synchronous Digital Hierarchy – synchroniczna hierarchia systemów cyfrowych
SLA	Service Level Agrement – gwarantowany poziom jakości

	obsługi
TCOK	telefoniczne centrum obsługi klienta
TDM	Time Domain Multiplexing – multipleksacja w dziedzinie czasu
TK	telekomunikacja
TI	teleinformatyka
TMN	Telecommunication Management Network – telekomunikacyjne sieci zarządzające
UKE	Urząd Komunikacji Elektronicznej
UPS	Unit Power System – systemy zasilania awaryjnego
VPN	Virtual Private Network – wirtualne sieci prywatne
WDM	Wave Domain Multiplexing – multipleksacja długości fali
WiMax	Wireless Max – bezprzewodowa sieć typu MAX
WLAN	Wireless Local Area Network – bezprzewodowa sieć lokalna

SŁOWNIK TERMINÓW

aktywa teleinformatyczne – struktura organizacyjna, polityki (zasady) działania, strategia, planowanie, zakres uprawnień i odpowiedzialności, normy i praktyki, procedury, procesy i zasoby (ludzkie, finansowe, sprzętowe: systemy telekomunikacyjne i informatyczne, aplikacje programowe, obiekty budowlane, tabor transportowy) w systemie informatycznym lub w działalności informatycznej

analiza podatności systemu – identyfikacja słabych punktów oraz usterek systemu

analiza ryzyka – główny proces zarządzania ryzykiem, identyfikuje ryzyko, które ma być kontrolowane lub akceptowane. Analiza ryzyka obejmuje ocenę wartości zasobów, zagrożeń, podatności i następstw w aspekcie naruszenia poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności

atrybuty bezpieczeństwa informacji – poufność, integralność, dostępność, rozliczalność(niezaprzeczalność)

bezpieczeństwo aktywów – wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, niezawodności aktywów, a także ich rozliczalności

bezpieczeństwo energetyczne – zapewnienie wielu źródeł zasilania dla niezbędnych do funkcjonowania elementów

bezpieczeństwo teleinformatyczne – zbiór zagadnień z dziedziny informatyki związany z szacowaniem i kontrolą ryzyka wynikającego z korzystania z komputerów i sieci komputerowych, rozpatrywany z perspektywy poufności, integralności i dostępności danych; jest określane jako wszelkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności

bezpieczna metodologia – odpowiedni proces planowania i określania warunków brzegowych dla infrastruktury

bezpieczny system teleinformatyczny – wyidealizowane urządzenie, które poprawnie i w całości realizuje tylko i wyłącznie cele zgodne z intencjami właściciela

biały wywiad – forma pracy wywiadowczej, polegająca na gromadzeniu informacji pochodzących z ogólnie dostępnych źródeł

cyberprzestępczość – niezgodne z prawem działania z wykorzystaniem systemów teleinformatycznych (np. kradzież własności intelektualnej), także: zorganizowana działalność przestępcza, przekraczająca granice państw, skierowana przeciwko zawartości danych oraz prawom autorskim (Traktat Rady Europy); oszustwa, fałszerstwa, nieautoryzowane wejścia do systemów komputerowych, popełniane przy użyciu komputera, sieci oraz oprogramowania. (ONZ, Symantec)

cyberterroryzm – niezgodne z prawem działania, których celem jest destrukcja infrastruktury państwowej lub poważne zagrożenie dla społeczeństwa

dostępność – gwarancja uprawnionego dostępu do informacji zawsze, gdy jest to niezbędne

infiltracja – działanie osób nieupoważnionych, które ma na celu zapewnienie sobie dostępu lub pozyskanie informacji znajdującej się w zasobach danej sieci teleinformatycznej. Infiltracja odbywa się różnymi metodami i środkami, szczególnie poprzez „przenikanie" do celowo wybranych (najbardziej wrażliwych lub słabo chronionych) elementów sieci

informacja jawna – informacja powszechnie znana lub która nie jest chroniona przed dostępem osób nieuprawnionych. Informacja jawna powinna być integralna i dostępna

informacja niejawna – ustawa o ochronie informacji niejawnych z 22.01.1999 roku, tekst jednolity z 2005 roku, DzU nr 196, poz 1631

informacja poufna – informacja chroniona przed nieuprawnionym dostępem. Informacja poufna musi być integralna, dostępna i rozliczalna

infrastruktura – środki technologiczne – elementy zapewniające funkcjonowanie organizacji, przetwarzanie i przesyłanie informacji

infrastruktura teleinformatyczna – infrastruktura składająca się z systemów i sieci teleinformatycznych. Umożliwia ona świadczenie usług on-line poprzez urządzenia telekomunikacyjne oraz serwery wraz z zainstalowanym na nich oprogramowaniem

infrastruktura krytyczna (KIT) – zespół sieci oraz struktur komunikacyjnych, które uszkodzone lub zniszczone, w sposób istotny wpłynęłyby na funkcjonowanie państwa (społeczeństwa). To część infrastruktury obejmująca materialne lub informacyjno-technologiczne urządzenia, sieci, usługi i dobra. Naruszenie jej lub zniszczenie mogłoby spowodować poważne skutki dla zdrowia, bezpieczeństwa państwa i jego obywateli, a także dla prawidłowego funkcjonowania organów władzy i administracji publicznej oraz instytucji i przedsiębiorców

integralność – ochrona przed modyfikacją lub zniekształceniem informacji przez osobę nieuprawnioną

kanał telekomunikacyjny – droga przesyłowa sygnału, zespół urządzeń umożliwiający przesyłanie sygnałów od nadajnika do odbiornika

klauzula tajności – sposób oznaczenia informacji klasyfikowanych, determinujący wymagany poziom i rodzaj ochrony tych informacji, a także (ustawa o ochronie informacji niejawnych z 22.01.1999 roku, tekst jednolity z 2005 roku, DzU nr 196, poz. 1631)

kod złośliwy – program lub fragment wykonalnego kodu, który dołącza się, nadpisuje lub zamienia inny program komputerowy, m.in. w celu reprodukcji samego siebie bez zgody użytkownika

komercyjny system teleinformatyczny (system TI) – całość środków technicznych i organizacyjnych, które służą pozyskiwaniu, przechowywaniu i przetwarzaniu informacji w celu osiągnięcia zysku ekonomicznego

kryptografia – dziedzina zajmująca się utajnianiem informacji przez jej szyfrowanie; także ogół technik szyfrowania informacji

krytyczna infrastruktura teleinformatyczna (KITI) – systemy i sieci teleinformatyczne niezbędne do prowadzenia podstawowych działań gospodarczych i funkcjonowania instytucji publicznych państwa

krytyczne aktywa teleinformatyczne – zasoby teleinformatyczne niezbędne do utrzymania bezpieczeństwa ekonomicznego państwa oraz wykorzystywane w systemie ochrony zdrowia i bezpieczeństwa publicznego

model DoD – patrz model TCP/IP

model TCP/IP – model odniesienia zwany modelem DoD wyróżnia cztery warstwy: łącza, sieciową, transportową i aplikacyjną

normy:

BS 7799 – brytyjski standard stanowiący podstawę systemów zarządzania bezpieczeństwem informacji. 20 stycznia 2005 r. została zatwierdzona do publikacji polskojęzyczna wersja normy BS 7799-2:1999, ma oznaczenie PN-I-17799-2:2005

ISO/IEC 27001 – norma, która została opracowana 14 października 2005 r. (wcześniej znana jako brytyjska norma BS 7799-2). Zawiera wymagania odnośnie do ustanowienia, wdrożenia, eksploatacji, monitorowania, prze-

glądu, utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji

ISO/IEC 17799 Technologie informacyjne – zasady postępowania w zarządzaniu bezpieczeństwem informacji

ISO/IEC 15408-1 Technologie informacyjne. Techniki bezpieczeństwa – kryteria oceny bezpieczeństwa informacji. Wprowadzenie i opis ogólny

ISO/IEC 15408-2 Technologie informacyjne. Techniki bezpieczeństwa – kryteria oceny bezpieczeństwa informacji. Wymagania bezpieczeństwa funkcjonalnego

ISO/IEC 15408-3 Technologie informacyjne. Techniki bezpieczeństwa – kryteria oceny bezpieczeństwa informacji. Wymagania zapewnienia bezpieczeństwa

PN-I-02000 Technika informatyczna. Zabezpieczenia w systemach informatycznych

ISO/IEC/TR 13335-1/PN-I-13335-1 Wytyczne do zarządzania bezpieczeństwem systemów informatycznych:
- terminologia, związki między pojęciami,
- podstawowe modele

ISO/IEC/TR 13335-2 Planowanie i zarządzanie bezpieczeństwem systemów informatycznych:
- różne podejścia do prowadzenia analizy ryzyka,
- plany zabezpieczeń,
- rola szkoleń i działań uświadamiających,
- stanowiska pracy w instytucji związane z bezpieczeństwem

ISO/IEC/TR 13335-3 Techniki zarządzania bezpieczeństwem systemów informatycznych:
- formułowanie trójpoziomowej polityki bezpieczeństwa,
- rozwinięcie problematyki analizy ryzyka,
- rozwinięcie problematyki implementacji planu zabezpieczeń,
- reagowanie na incydenty

ISO/IEC/TR 13335-4 Wybór zabezpieczeń:
- klasyfikacja i charakterystyka różnych form zabezpieczeń,
- dobór zabezpieczeń ze względu na rodzaj zagrożenia i rodzaj systemu

ISO/IEC/WD 13335-5 Zabezpieczenie dla połączeń z sieciami zewnętrznymi:
- dobór zabezpieczeń stosowanych do ochrony styku systemu z siecią zewnętrzną

oprogramowanie złośliwe – synonimy: wirus komputerowy, złośliwy program, wirus klasyczny; program lub kod zdolny do przenikania do systemów, dysków lub indywidualnych plików, zazwyczaj bez wiedzy i zgody użytkownika. Po skutecznej infekcji dalsze działanie zależy od określonego typu wirusa i obejmuje: replikację jedynie w zainfekowanym systemie, infekcję dalszych plików podczas ich uruchamiania lub tworzenia, kasowanie lub uszkadzanie danych w systemach i plikach, marnowanie zasobów systemowych bez powodowania szkód. Termin „program złośliwy" obejmuje wirusy klasyczne, robaki, konie trojańskie i inne szkodniki

organizacja – formalny podmiot sprawujący kontrolę nad daną infrastrukturą telekomunikacyjną

personel – pracownicy zarządzający daną infrastrukturą, korzystający z niej i ją utrzymujący

placówka – obiekty fizyczne należące do organizacji (budynki, obiekty techniczne)

podatność – warunek lub zbiór warunków, które mogą umożliwić zagrożeniu wpływ na zasoby

polityka bezpieczeństwa – założenia, standardy, procedury, wytyczne, normatywy bezpiecznego korzystania z infrastruktury w ramach danej organizacji; zbiór dozwolonych czynności w ramach systemu, ustalenia, dobór standardów, procedur, wytycznych i regulacji, które są realizowane za pomocą środków kontroli

polityka bezpieczeństwa informacyjnego – polityka zapewniająca ochronę istniejących systemów teleinformatycznych, jak również gwarantujących

państwu i podmiotom, które chroni, posiadanie, przetrwanie i swobodę rozwoju

poufność – ochrona przed ujawnieniem informacji nieuprawnionemu odbiorcy

Prawo telekomunikacyjne – w polskim prawie zawarte w ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (DzU nr 171, poz. 1800). Wprowadza ono szereg specyficznych określeń dotyczących telekomunikacji, wdraża podstawowe dyrektywy Wspólnot Europejskich z dziedziny telekomunikacji, tworzy również wyspecjalizowany urząd administracji rządowej, zajmujący się sprawami telekomunikacji – Urząd Komunikacji Elektronicznej. Prawo telekomunikacyjne wchodzi w skład prawa nowych technologii

redundancja – nadmiar informacji w komunikacie sformułowanym w danym kodzie

rozliczalność – możliwość określenia i weryfikacji odpowiedzialności za działania, usługi i realizowane funkcje

sabotaż – dezorganizacja pracy, zniszczenie lub uszkodzenie sieci teleinformatycznej

sieć teleinformatyczna – organizacyjne i techniczne połączenie systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi

sieć telekomunikacyjna – systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju.
Sieć telekomunikacyjna to także obiekt techniczny, będący zbiorem węzłów oraz łączy pomiędzy węzłami. Sieć telekomunikacyjna służy do przekazywania danych, informacji lub wiadomości w celu komunikacji pomiędzy dwoma lub wieloma określonymi punktami

system zarządzania bezpieczeństwem informacji MISS – część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka bizneso-

wego; odnosi się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. ISMS obejmuje strukturę organizacyjną, polityki, działania planistyczne, zakres odpowiedzialności, praktyki, procedury, procesy i zasoby.

szacowanie ryzyka – szacowanie zagrożeń i ich wpływu oraz podatności informacji i urządzeń do przetwarzania informacji, a także prawdopodobieństwa ich wystąpienia

szczególne wymagania bezpieczeństwa (SWB) – metodyka opracowania dokumentacji dla wojskowych systemów i sieci teleinfromatycznych

szyfrowanie – przekształcanie informacji do postaci nieczytelnej w celu zapewnienia jej poufności. Szyfrowanie wymaga dostarczenia klucza do odszyfrowania informacji przez odbiorcę

szyfrowanie danych – metoda zabezpieczania danych podczas ich transmisji. Polega na zmianie postaci przesyłanych danych, dzięki czemu stają się one bezużyteczne dla osoby, która nie posiada dostępu do programu rozkodowującego (klucza)

środek zaradczy – środek redukujący rozpoznane zagrożenie

uszkodzenie danych – zniekształcenie lub usunięcie danych spowodowane awarią systemu komputerowego, przypadkami losowymi bądź też atakiem na system

zagrożenie – wydarzenie, którego wystąpienie ma niepożądany wpływ na poprawny stan obiektu

zapora sieciowa – rozwiązanie sprzętowo-programowe jako mechanizm ochronno-kontrolny umieszczany na styku dwóch sieci komputerowych w celu uniemożliwienia nieuprawnionego dostępu, np. do sieci lokalnej z zewnątrz

zarządzanie bezpieczeństwem informacji (systemów informatycznych) – obejmuje zespół procesów zmierzających do osiągnięcia i utrzymywania ustalonego poziomu bezpieczeństwa, tzn. poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności

zarządzanie jakością – okresowe lub stałe sprawdzanie i zapewnianie spełnienia ustalonych wymogów, są to wszystkie działania, które odnoszą się do przygotowania i przeprowadzenia planowania, kierowania i zabezpieczania jakości

zarządzanie kryzysowe – zespół przedsięwzięć organizacyjnych, logistycznych i finansowych, których celem jest zapobieganie powstawaniu sytuacji kryzysowych, zapewnienie sprawności struktur decyzyjnych na wszystkich szczeblach zarządzania, ciągłej gotowości sił i środków do podjęcia działań, sprawnego reagowania oraz likwidacji skutków zaistniałej sytuacji

zarządzanie ryzykiem – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych, z zachowaniem akceptowalnego poziomu kosztów

zarządzanie zmianami – proces wykorzystywany do identyfikacji nowych wymagań bezpieczeństwa wówczas, gdy w systemie informatycznym występują zmiany

zasada wiedzy koniecznej – udzielanie informacji niejawnych tylko w stopniu wymaganym na danym stanowisku pracy

zespół interwencyjny – uprawniona grupa ludzi podejmująca określone działania po otrzymaniu umówionego sygnału