Bezpieczna Firma

Bezpieczeństwo teleinformatyczne danych osobowych

Andrzej Guzik

stopień trudności

System informatyczny, w którym przetwarza się dane osobowe, powinien – oprócz wymagań wynikających z przepisów prawa – uwzględniać wymagania Generalnego Inspektora Ochrony Danych Osobowych w zakresie struktur baz danych osobowych oraz funkcjonalności zarządzających nimi aplikacji.

Zagadnienie bezpieczeństwa systemów informatycznych, w których przetwarza się dane osobowe, nabiera coraz większego znaczenia, ponieważ zakres takiego przetwarzania staje się coraz szerszy. Pod pojęciem bezpieczeństwa teleinformatycznego danych osobowych należy rozumieć ochronę poufności, rozliczalności i integralności danych osobowych, które przetwarza się w systemie informatycznym.

Za bezpieczeństwo przetwarzania danych osobowych w systemie informatycznym odpowiada administrator danych. *Administratorem danych* jest organ, jednostka organizacyjna, podmiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych. Bezpieczeństwo teleinformatyczne danych osobowych należy zapewnić przed rozpoczęciem oraz w trakcie przetwarzania danych osobowych. Podstawowe zasady zabezpieczenia danych osobowych określa *Rozdział 5 – Zabezpieczenie danych osobowych* ustawy o ochronie danych osobowych. Szczegółowe wymagania techniczne i organizacyjne związane z przetwarzaniem danych osobowych w systemach informatycznych oraz zakres dokumentacji przetwarzania danych osobowych określa *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*.

Przepisy prawa nakładają na administratora danych szereg obowiązków. Podstawowym obowiązkiem administratora danych jest zastosowanie środków technicznych i organizacyjnych zapewniających ochronę danych osobowych. Zastosowane środki ochrony, zgodnie z zasadą adekwatno-

Z artykułu dowiesz się

- jak zapewnić bezpieczeństwo danym osobowym, które przetwarza się w systemie informatycznym.

Co powinieneś wiedzieć

- znać podstawowe zasady ochrony danych osobowych.

ści, powinny zapewniać ochronę danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną (dane zwykłe bądź dane *wrażliwe*). Ustawa określa następujące zagrożenia związane z przetwarzaniem danych osobowych: udostępnienie osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, przetwarzanie z naruszeniem ustawy oraz przypadkową zmianę, utratę, uszkodzenie lub zniszczenie danych osobowych. Wśród środków technicznych służących do ochrony danych osobowych można wymienić środki: sprzętowe, programowe (oprogramowanie systemowe, użytkowe, narzędziowe) oraz telekomunikacyjne (oprogramowanie urządzeń teletransmisji). W celu nadzorowania przestrzegania zasad ochrony danych osobowych w organizacji wyznacza się administratora bezpieczeństwa informacji (ABI). ABI odpowiada między innymi za: nadzór nad zakresem dostępu osób upoważnionych do przetwarzania danych osobowych, nadzór nad sposobem przetwarzania danych osobowych w systemach informatycznych, kontrolę zgodności systemu informatycznego z wymaganiami określonymi w przepisach prawa oraz za reakcję na incydenty naruszenia bezpieczeństwa danych osobowych.

Rysunek 1. *Operacje przetwarzania danych osobowych*

Administrator bezpieczeństwa informacji powinien nadzorować, aby do przetwarzania danych osobowych były dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez administratora danych. Osoby, które zostały upoważnione do przetwarzania danych osobowych, zobowiązane są do zachowania w tajemnicy tych danych oraz sposobów ich zabezpieczenia. W jednostce organizacyjnej powinna być prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych. Ewidencja ta powinna zawierać między innymi: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych (upoważnienie do zbierania, utrwalania, przechowywania, opracowywania, zmieniania, udostępniania lub usuwania danych osobowych) oraz identyfikator osoby. Dodatkowo administrator danych zobowiązany jest

Podstawy prawne

- Rozdział 5 – Zabezpieczenie danych osobowych – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 100, poz. 1025).
- Zalecenia Generalnego Inspektora Ochrony Danych Osobowych:
- Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa,
- Wskazówki dotyczące sposobu opracowania instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji,
- Wymagania dotyczące struktur baz danych osobowych oraz funkcjonalności zarządzających nimi aplikacji.

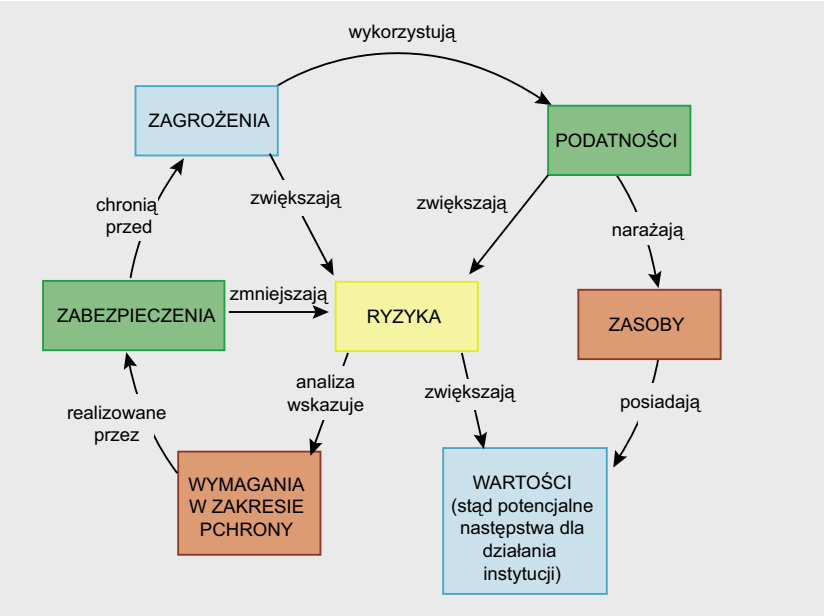
Przykłady nieprawidłowości przetwarzania danych osobowych w systemach informatycznych

- nie wyznaczono administratora bezpieczeństwa informacji,
- nie dostosowano systemów informatycznych do wymagań wynikających z przepisów prawa,
- nie opracowano instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- nie zastosowano środków technicznych i organizacyjnych zapewniających ochronę danych osobowych,
- nie określono poziomów bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych,
- nie wydano upoważnień do przetwarzania danych osobowych osobom przetwarzającym dane osobowe w systemie informatycznym,
- nie nadano odrębnych identyfikatorów osobom przetwarzającym dane osobowe w systemie informatycznym,
- nie zawarto umowy powierzenia przetwarzania danych osobowych,
- nie prowadzono ewidencji osób upoważnionych do przetwarzania danych osobowych,
- nie zgłoszono zbiorów danych osobowych do rejestracji do GIODO,
- nie sporządzano kopii zapasowych,
- nie zapewniono kontroli dostępu do danych osobowych.

zapewnić kontrolę nad tym, jakie dane osobowe i przez kogo zostały do zbioru danych wprowadzone oraz komu zostały przekazane.

Dokumentacja przetwarzania danych

Na administratorze danych ciąży obowiązek opracowania dokumentacji opisującej sposób przetwarzania danych osobowych oraz wdrożonych środków technicznych i organizacyjnych. Na dokumentację przetwarzania danych osobowych składa się *polityka bezpieczeństwa danych osobowych* oraz *instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.* Dokumentację opracowuje się po przeprowadzeniu analizy ryzyka z uwzględnieniem warunków charakterystycznych dla jednostki organizacyjnej, w której mają być przetwarzane dane osobowe. Analizy ryzyka można dokonać stosując na przykład metody opisane w raporcie technicznym *ISO/IEC TR 13335-3 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych Część 3: Techniki zarządzania bezpieczeństwem systemów informatycznych.* Raport ten przedstawia cztery warianty podejścia do analizy ryzyka: *podejście podstawowego poziomu bezpieczeństwa, podejście nieformalne, szczegółową analizę ryzyka* i *podejście mieszane.* Podstawowa różnica pomiędzy nimi dotyczy stopnia szczegółowości analizy ryzyka. W oparciu o wyniki analizy ryzyka dobiera się zabezpieczenia. Zastosowane zabezpieczenia powinny być efektywne kosztowo i uwzględniać wymagania wynikające z przepisów prawa, wymagania biznesowe i wymagania z analizy ryzyka. Ryzyko, jakie powstaje po wprowadzeniu zabezpieczeń, nazywamy *ryzykiem szczątkowym.*



Rysunek 2. *Zarządzanie ryzykiem*

Polityka bezpieczeństwa danych osobowych powinna zawierać w szczególności dane określone w Tabeli 1. Przy konstruowaniu polityki bezpieczeństwa danych osobowych należy uwzględnić zalecenia Generalnego Inspektora Ochrony danych Osobowych (GIODO) – *Wytycznych w zakresie opracowania i wdrożenia polityki bezpieczeństwa* oraz opcjonalnie zapisy rozdziału 7.2 - *Polityka bezpieczeństwa instytucji w zakresie systemów informatycznych* i Załącznika A – *Przykładowy spis treści polityki bezpieczeństwa instytucji w zakresie systemów informatycznych* raportu technicznego ISO/IEC TR 13335-3.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych powinna zawierać w szczególności dane określone w Tabeli 2. Przy konstruowaniu instrukcji należy uwzględnić zalecenia GIODO - *Wskazówki dotyczące sposobu opracowania instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.*

Tabela 1. *Zawartość dokumentu Polityka bezpieczeństwa danych osobowych*

Lp.	Zawartość dokumentu Polityka bezpieczeństwa danych osobowych
1	Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe
2	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych
3	Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi
4	Sposób przepływu danych pomiędzy poszczególnymi systemami
5	Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Wymagania systemu informatycznego

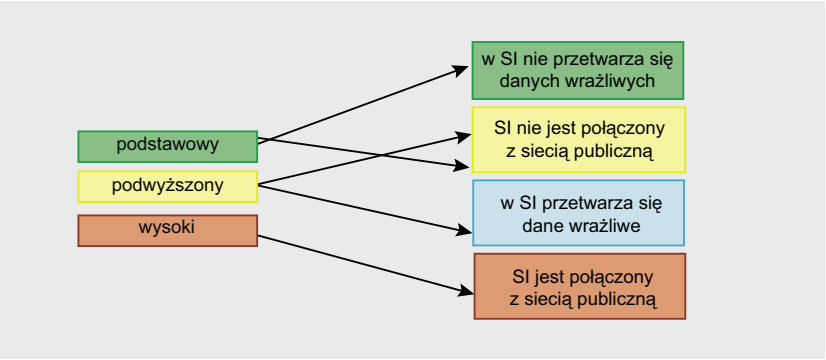
System informatyczny służący do przetwarzania danych osobowych powinien charakteryzować się określoną funkcjonalnością oraz

umożliwiać sporządzenie i wydruk raportu dla każdej osoby, której dane osobowe są przetwarzane w systemie. System powinien zapewniać odnotowanie: daty pierwszego wprowadzenia, identyfikatora użytkownika, źródła danych, informacji o odbiorcach oraz sprzeciwu osoby wobec przetwarzania jej danych w przypadkach określonych w ustawie.

Przy projektowaniu systemów informatycznych należy uwzględnić zalecenia GIODO – *Wymagania dotyczące struktur baz danych osobowych oraz funkcjonalności zarządzających nimi aplikacji*.

Poziomy bezpieczeństwa

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych wprowadza trzy poziomy bezpieczeństwa przetwarzania danych osobowych: podstawowy, podwyższony i wysoki.



Rysunek 3. *Poziomy bezpieczeństwa przetwarzania danych osobowych*

Poziom podstawowy

Poziom podstawowy stosuje się, gdy w systemie informatycznym nie przetwarza się danych *wrażliwych* (danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, dane o stanie zdrowia, kodzie genetycznym, nałogach, życiu seksualnym, danych dotyczących skazań, orzeczeń o ukaraniu, o mandatach karnych, orzeczeń wydanych w postępowaniu sądowym lub administracyjnym) oraz żadne z urządzeń systemu informatycznego nie jest połączone z siecią publiczną. Środki bezpieczeństwa na poziomie podstawowym określa część A załącznika do rozporządzenia MSWiA.

Na poziomie podstawowym stosuje się następujące środki ochrony: administrator danych powinien zapewnić fizyczną kontrolę dostępu do obszaru przetwarzania danych osobowych określonego w polityce bezpieczeństwa danych osobowych oraz logiczną kontrolę dostępu do danych przetwarzanych w systemie informatycznym, stosując mechanizm w postaci odrębnego identyfikatora i hasła do uwierzytelniania użytkowników systemu. Hasła stosowane do uwierzytelniania użytkowników powinny składać się z co najmniej 6 znaków i być zmieniane nie rzadziej niż co 30 dni. System informatyczny powinien być zabezpieczony przed oprogramowaniem szkodliwym oraz utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej. Dane przetwarzane w systemie należy zabezpieczyć wykonując kopie zapasowe – zarówno zbiorów danych, jak i programów. Kopie należy przechowywać w miejscach zabezpieczonych przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem (jak najdalej w poziomie

Tabela 2. *Zawartość dokumentu Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*

Lp	Zawartość dokumentu Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
1	Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności
2	Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem
3	Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu
4	Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania
5	Sposób, miejsce i okres przechowywania: elektronicznych nośników informacji zawierających dane osobowe, kopii zapasowych zbiorów danych
6	Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego
7	Sposób realizacji odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych w zbiorach jawnych

i w pionie od miejsca ich wytworzenia). W przypadku stosowania komputerów przenośnych do przetwarzania danych osobowych, należy zapewnić ochronę kryptograficzną danych osobowych przetwarzanych poza obszarem przetwarzania.

Urządzenia, dyski, elektroniczne nośniki informacji przeznaczone do likwidacji lub przekazania podmiotowi nieuprawnionemu należy pozbawić zapisu danych w sposób trwały, a w przypadku ich naprawy – naprawiać je pod nadzorem.

Na administratorze danych spoczywa obowiązek monitorowania wdrożonych zabezpieczeń systemu informatycznego.

Poziom podwyższony

Poziom podwyższony stosuje się, gdy w systemie informatycznym przetwarza się dane *wrażliwe* oraz żadne z urządzeń systemu informatycznego nie jest połączone z siecią publiczną. Środki bezpieczeństwa na poziomie podwyższonym określa część B załącznika do rozporządzenia MSWiA.

Na poziomie podwyższonym stosuje się – zgodnie z zasadą kaskadowości – środki ochrony właściwe dla poziomu podstawowego. Dodatkowo administrator danych ma obowiązek wdrożyć niżej wymienione środki ochrony. W przypadku, gdy do uwierzytelniania użytkowników systemu używa się hasła, hasło powinno zawierać małe i duże litery oraz cyfry lub znaki specjalne i składać się z co najmniej 8 znaków. W przypadku, gdy urządzenia i elektroniczne nośniki informacji zawierające dane osobowe tzw. *wrażliwe* przekazywane są poza obszar przetwarzania, należy zabezpieczyć je w sposób zapewniający ochronę poufności i integralność danych. Opis zastosowanych środków powinna określać *instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*.

Tabela 3. *Poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym*

Lp.	Poziomy bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych
1	podstawowy
2	podwyższony
3	wysoki

Poziom wysoki

Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego połączone jest z siecią publiczną. Środki bezpieczeństwa na poziomie wysokim określa część C załącznika do rozporządzenia MSWiA.

Na poziomie wysokim stosuje się – zgodnie z zasadą kaskadowości – środki ochrony właściwe dla poziomu podwyższonego i poziomu podstawowego. Dodatko-

Podstawowe pojęcia związane z bezpieczeństwem teleinformatycznym

- dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
- administrator danych – organ, jednostka organizacyjna, podmiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych,
- administrator bezpieczeństwa informacji – osoba nadzorująca przestrzeganie zasad ochrony danych osobowych,
- zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
- przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
- system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
- zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
- hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
- identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym
- uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
- poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
- rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
- integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- usuwanie danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
- raport – przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,
- teletransmisja – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
- sieć publiczna – publiczna sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych.

O autorze

Audytor systemów zarządzania jakością i zarządzania bezpieczeństwem informacji, specjalista w zakresie ochrony informacji prawnie chronionych, redaktor portalu *www.ochrona-informacji.pl*

Kontakt z autorem: *a.guzik@ochronainformacji.pl*

wo administrator danych ma obowiązek wdrożyć niżej wymienione środki ochrony. System informatyczny należy chronić przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

W przypadku zastosowania logicznych zabezpieczeń należy zapewnić kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych (np. poprzez zastosowanie zapory ogniowej). W przypadku, gdy dane do uwierzytelniania użytkowników systemu przesyłane są w sieci publicznej, należy zastosować środki ochrony kryptograficznej.

Szczegółowe informacje na temat środków ochrony na poszczególnych poziomach bezpieczeństwa określa załącznik do rozporządzenia MSWiA.

Należy zauważyć, że wyżej wymienione rozporządzenie określa minimalne wymagania w zakresie bezpieczeństwa teleinformatycznego danych osobowych.

Administrator danych może dodatkowo zastosować inne środki ochrony w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych, niż to wynika z wymagań określonych w ustawie i rozporządzeniu MSWiA.

Podsumowanie

Przepisy prawa określają minimalne wymagania związane z bezpieczeństwem teleinformatycznym danych osobowych.

Oprócz nich należy uwzględnić zalecenia Generalnego Inspektora Ochrony Danych Osobowych dotyczące problematyki bezpieczeństwa teleinformatycznego danych osobowych oraz polskie normy dotyczące bezpieczeństwa informacji, które stanowią źródło tzw. dobrych praktyk, a w szczególności: *PN-ISO/IEC 17799: 2007 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji* i *PN-ISO/IEC 27001: 2007 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.* ●