Jerzy Stanik, Maciej Kiedrowicz, Tomasz Protasowicki

Wybrane aspekty standaryzacji w ochronie publicznych zasobów informacyjnych i świadczonych usług w kontekście społeczeństwa informacyjnego

Ekonomiczne Problemy Usług nr 113, 113-130

2014

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 809 EKONOMICZNE PROBLEMY USŁUG NR 113 2014

JERZY STANIK, MACIEJ KIEDROWICZ, TOMASZ PROTASOWICKI
Wojskowa Akademia Techniczna[1]

WYBRANE ASPEKTY STANDARYZACJI W OCHRONIE PUBLICZNYCH ZASOBÓW INFORMACYJNYCH I ŚWIADCZONYCH USŁUG W KONTEKŚCIE SPOŁECZEŃSTWA INFORMACYJNEGO

Streszczenie

W referacie przedstawiono rozważania na temat znaczenia bezpieczeństwa informacji w społeczeństwie informacyjnym pod kątem wybranych aspektów prawnych. Scharakteryzowano wybrane aspekty standaryzacji w ochronie publicznych baz danych, rejestrów i usług świadczonych przez administrację publiczną. Dla każdego wymienionego typu standardu, np. ustawa, norma czy najlepsze praktyki stowarzyszone określono minimalne wymagania i działania, jakie powinny być podejmowane i realizowane przez służby bezpieczeństwa w celu zapewnienia podstawowego poziomu bezpieczeństwa informacji przetwarzanych w instytucjach. Ponadto podkreślono, że dane, informacja i wiedza odgrywają ogromną rolę we współczesnych społeczeństwach informacyjnych, porządkach prawnych i stosunkach międzyludzkich, a także w życiu konkretnego człowieka.
Słowa kluczowe: bezpieczeństwo informacji, atrybut bezpieczeństwa, standard bezpieczeństwa, zasób informacyjny

Wprowadzenie

W dobie XXI w. o doniosłości problematyki bezpieczeństwa dla współczesnej cywilizacji decyduje przede wszystkim wszechobecność technologii i rozwiązań IT, a w szczególności platform elektronicznych, stanowiących podstawowy składnik społeczeństwa informacyjnego. Stąd też kwestia bezpieczeństwa tych platform i ich

[1] Wydział Cybernetyki.

zasobów informacyjnych w nich przetwarzanych stała się zagadnieniem priorytetowym dla wielu organizacji i instytucji życia gospodarczego, m.in. w handlu i bankowości elektronicznej, gdzie zaufanie klientów ma podstawowe znaczenie dla rozwoju usług świadczonych drogą elektroniczną.

Celem niniejszego artykułu jest określenie możliwości wykorzystania aktualnie dostępnych **standardów bezpieczeństwa** oraz stowarzyszonych z nimi **najlepszych praktyk** i zaproponowanie sposobu ich wykorzystania do zapewnienia utrzymania wymaganego bieżącego poziomu bezpieczeństwa informacji w jednostce administracji publicznej poprzez odpowiednie dobieranie i wdrażanie skutecznych mechanizmów bezpieczeństwa – zabezpieczeń technicznych i organizacyjnych. Pod pojęciem wymaganego bieżącego poziomu bezpieczeństwa rozumiany jest taki stan jednostki organizacyjnej, w którym jej podmiot działania nie odczuwa istotnego zagrożenia. Zdaniem autorów taki stan organizacji można osiągnąć poprzez właściwe ustanawianie i wdrażanie zbioru skutecznych mechanizmów bezpieczeństwa, adekwatnych do bieżących zagrożeń i do wyników zawartych w raporcie z procesu szacowania ryzyka.

Pojmując w ten sposób istotę bezpieczeństwa informacji w jednostce administracji publicznej uważa się, że:
- ma ona znaczenie fundamentalne dla społeczeństwa informacyjnego;
- rozwiązanie problemu standaryzacji bezpieczeństwa informacji jest jednym z podstawowych zadań warunkujących możliwość zbudowania sprawnie działającej administracji publicznej;
- bezpieczeństwo zasobów informacyjnych oraz świadczenie usług publicznych w dniu dzisiejszym to jeden z kluczowych czynników sukcesu lub porażki zarówno organizacji publicznej, jak i biznesu.

Do tematu zapewnienia bezpieczeństwa informacji w jednostce administracji publicznej można podejść na wiele sposobów. Mogą to być działania wyrywkowe, nieskoordynowane i intuicyjne, gdzie poziom bieżącego bezpieczeństwa zależy od poziomu wiedzy osób, którym powierzono zapewnienie bezpieczeństwa informacji. Jednostka administracji publicznej, która chce należycie zabezpieczyć swoje informacje powinna zastosować podejście systemowe oparte na standardach, w ramach których będzie zarządzać kompleksowo posiadanymi aktywami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem dotyczącym bezpieczeństwa informacji.

1. Społeczeństwo informacyjne i prawne warunki świadczenia usług informacyjnych, zasoby informacyjne, informacja bezpieczna

Nie jest przesadą stwierdzenie, że obecnie świat wkroczył w erę, gdzie najcenniejszym dobrem stała się informacja i usługi z nią związane, a w szczególności

publiczne bazy danych, rejestry i usługi. Stąd właśnie obserwuje się bardzo szybki rozwój technologii umożliwiających pozyskiwanie, przetwarzanie, przesyłanie i analizę. Wiele organizacji nie zdaje sobie sprawy z wartości oraz stopnia uzależnienia od rozwiązań informatycznych, do momentu pierwszego nadużycia lub przestępstwa związanego z bezpieczeństwem.

Brak jest jednak jasnej definicji społeczeństwa informacyjnego, co należy uznać za słabą stronę tej wizji. Intuicyjnie, przeciętny człowiek określi je, jako takie społeczeństwo, gdzie używa się powszechnie komputerów i technik z nimi związanych.

1.1. Społeczeństwo informacyjne

Spośród wielu określeń i definicji spotykanych w fachowej literaturze przedmiotu, definicja z I Kongresu Informatyki Polskiej z 1994 r. najbardziej odpowiada wymogom niniejszego artykułu. Kładzie ona duży nacisk na znaczenie informacji: „Społeczeństwo charakteryzujące się przygotowaniem i zdolnością do użytkowania systemów informatycznych, skomputeryzowane i wykorzystujące usługi telekomunikacji do przesyłania i zdalnego przetwarzania informacji".

Do podstawowych procesów związanych z tworzeniem społeczeństwa informacyjnego należy informatyzacja gospodarki i wszelkich innych dziedzin życia. W najprostszym ujęciu można ją podzielić na trzy etapy:

- powstanie „pierwotnego sektora informacyjnego", tj. przedsiębiorstw i korporacji tworzących nowe techniki informacyjno-komunikacyjne;
- „informatyzacja" podstawowych działów gospodarki i instytucji (w tym na przykład banków, oświaty, służby zdrowia, administracji państwowej itp.);
- szerokie wkroczenie nowych technik do codziennego życia mas i do gospodarstwa domowego, w tym dotarcie do nich sieci multimedialnych obejmujących: serwer, sieć transmisyjną, sieć właściwą, sieć dostępu i wyposażenie końcowego użytkownika.

1.2. Usługi publiczne

Usługi publiczne to usługi świadczone przez administrację publiczną obywatelom i obywatelkom bezpośrednio (w ramach sektora publicznego) lub poprzez finansowanie podmiotów prywatnych zapewniających daną usługę.

Prawne warunki świadczenia usług informacyjnych są wynikiem ustawowych rozwiązań prawnych oraz rezultatem polityki administracyjnej w zakresie wydawania zezwoleń, koncesji, przydziałów częstotliwości, numeracji i innych uprawnień niezbędnych do prowadzenia działalności usługowej. Podstawowe znaczenie mają przepisy prawa telekomunikacyjnego oraz prowadzona w ich ramach polityka koncesyjna. Świadczenie usług za pośrednictwem sieci informacyjnych wymaga rozwiązania kilku podstawowych problemów prawnych warunkujących odpowiednią sprawność, bezpieczeństwo tych operacji oraz odpowiednią atrakcyjność usług dla konsumentów.

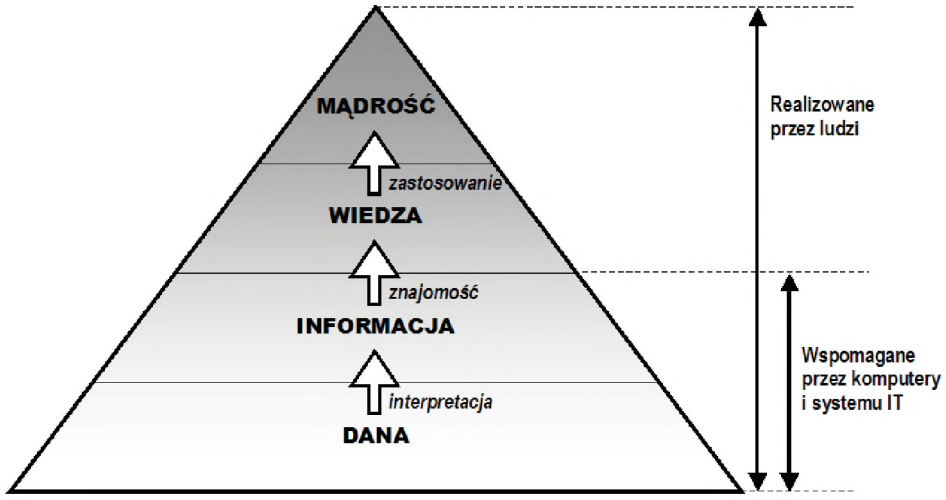
Zadania administracji w odniesieniu do bezpiecznego świadczenia usług publicznych zdefiniowane są w przepisach prawa regulujących działania poszczególnych jednostek administracji publicznej. Duża różnorodność usług komplikuje opis i ocenę organizacji, która je dostarcza – jest odpowiedzialna za dostarczanie usług, zarządza dostarczaniem usług. Skomplikowany także jest problem zdefiniowania wskaźników do oceny jakości świadczenia usług, które stanowią jedno z narzędzi podnoszenia jakości i bezpieczeństwa pracy administracji publicznej.

1.3. Zasoby informacyjne

Zasoby, zwane także aktywami, to wszystko, co dla instytucji posiada wartość i co dla jej dobra należy chronić, aby mogła ona realizować swoje zadania. Prawidłowe zarządzanie zasobami jest niezbędne do osiągnięcia celu działania instytucji i jest ono głównym obowiązkiem osób odpowiedzialnych za kierowanie instytucją na wszystkich poziomach. Zasoby instytucji można zdekomponować na następujące podzbiory (rodzaje, typy), a mianowicie:

- aktywa informacyjne: zbiory danych i pliki z danymi, dokumentacja systemu, instrukcje użytkownika, materiały szkoleniowe, procedury eksploatacyjne i wsparcia, plany utrzymania ciągłości działania, przygotowania awaryjne, informacje zarchiwizowane;
- aktywa oprogramowania: oprogramowanie aplikacyjne, oprogramowanie systemowe, programy narzędziowe i użytkowe;
- aktywa fizyczne: sprzęt komputerowy (procesory, monitory, modemy, laptopy), sprzęt komunikacyjny (rutery, centrale abonenckie, telefaksy, automatyczne sekretarki), nośniki magnetyczne (taśmy, dyski), meble, pomieszczenia;
- usługi: usługi obliczeniowe i telekomunikacyjne, inne usługi infrastruktury technicznej (ogrzewanie, oświetlenie, zasilanie, klimatyzacja itp.);
- ludzie i/lub dobra niematerialne (np. reputacja, wizerunek itp.).

Bezpieczeństwo zasobów informacyjnych odnosi się do zagadnień ochrony danych, ochrony informacji oraz wiedzy. Na rysunku 1 ukazano drogę od danych do mądrości.



Rys. 1. Wiedza a dane, informacje i mądrość

Źródło: Heracleous 1998.

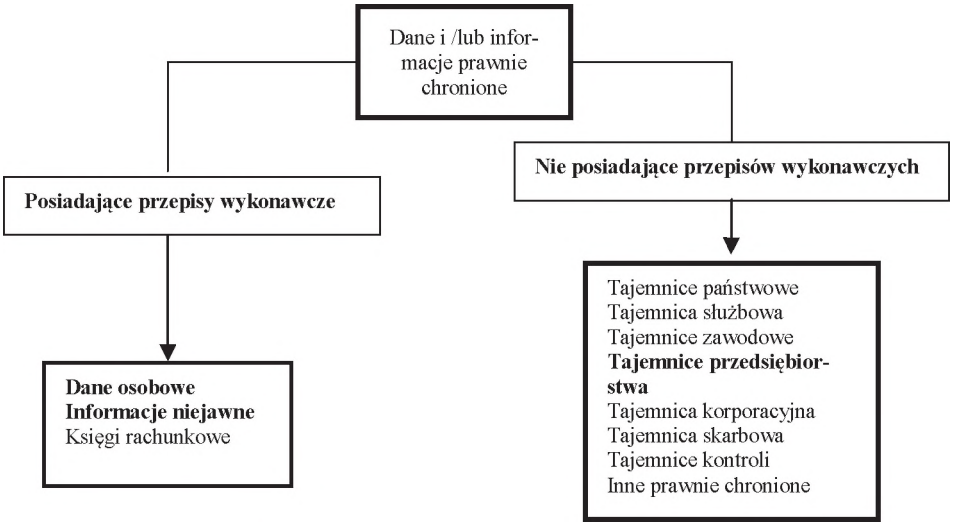
Dane definiuje się jako niepołączone ze sobą fakty. Poprzez informacje rozumiemy te dane, które zostały poddane kategoryzacji i klasyfikacji lub w inny sposób zostały uporządkowane. Natomiast wiedza oznacza uporządkowane i „oczyszczone" informacje. Powstaje ona dopiero po wyciągnięciu wniosków z dostępnych danych i informacji. Posiadanie bogatej wiedzy na dany temat prowadzi zaś do mądrości.

Zabezpieczenie publicznych baz danych i rejestrów nie powinno być traktowane tylko jako sposób zapewniający stabilne działanie systemu. Bardzo ważne w trakcie przetwarzania i przechowywania danych są wymogi prawne, które określają minimalny zakres bezpieczeństwa. Dzięki tej wiedzy możemy uniknąć przewidzianych w przepisach kar i sankcji.

W dalszej części artykułu zagadnienia standaryzacji w ochronie publicznych zasobów informacyjnych zostaną ograniczone do następujących rodzajów danych podlegających ochronie.

1. Posiadające przepisy wykonawcze dotyczące ochrony:
   - danych osobowych, rozumianych w świetle UODO,
   - danych niejawnych (tajemnica państwowa i służbowa), rozumianych w świetle UOIN.
2. Nieposiadające przepisów wykonawczych dotyczących ochrony – danych wrażliwych (tajemnica przedsiębiorstwa), rozumianych w świetle normy ISO/IEC 27001.

Przyjmujemy, że publiczne bazy danych i rejestry zawierają dane i informacje prawnie chronione: posiadające przepisy wykonawcze dotyczące ochrony i informacje, i/lub nieposiadające przepisów wykonawczych. Rysunek 2 przedstawia podział informacji na informacje prawnie chronione posiadające przepisy wykonawcze dotyczące ochrony i informacje nieposiadające przepisów wykonawczych dotyczących ochrony.



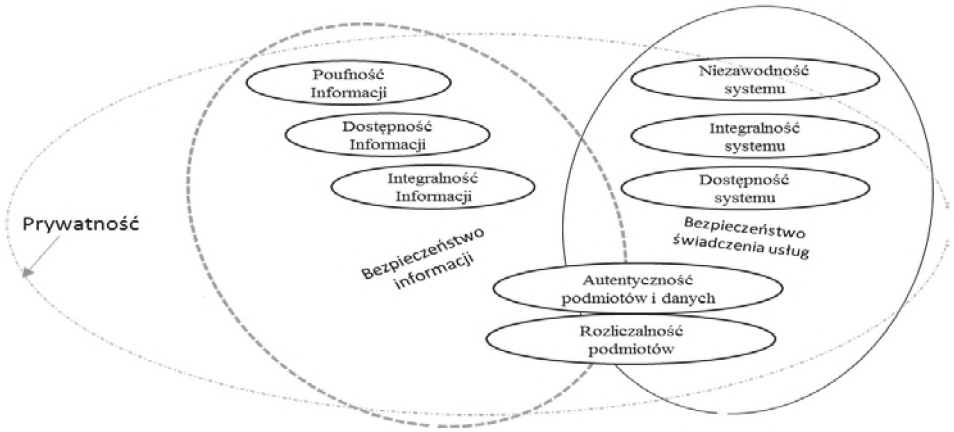
Rys. 2. Klasyfikacja ogólna tajemnic prawnie chronionych

Źródło: Białas 2006.

Kierownictwo organizacji powinno w sposób jasny i precyzyjny określić politykę bezpieczeństwa informacji przetwarzanych w swojej jednostce. Polityka ta musi być zgodna z obowiązującym prawem i zgodna z obowiązującymi aktami prawnymi.

1.4. Informacja bezpieczna

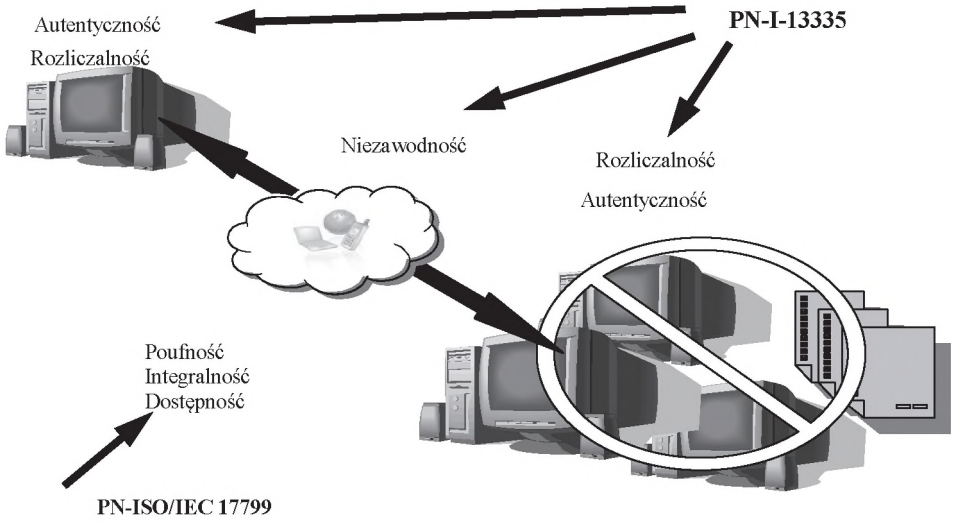
Informacja „bezpieczna" to informacja „dobrze zabezpieczona", inaczej – ma zachowane (na właściwym poziomie) atrybuty bezpieczeństwa, takie jak: poufność, dostępność, integralność, rozliczalność, autentyczność (rysunek 3).



Rys. 3. Klasyfikacja atrybutów bezpieczeństwa

Źródło: opracowanie własne.

Przypisanie poszczególnych atrybutów bezpieczeństwa do podstawowych komponentów sieci teleinformatycznej przedstawia rysunek 4.



Rys. 4. Umiejscowienie atrybutów bezpieczeństwa w sieci IT

Źródło: opracowanie własne.

Zabezpieczenie publicznych baz danych i rejestrów nie powinno być traktowane tylko jako sposób zapewniający stabilne działanie systemu informacyjnego w organizacji. Bardzo ważne w trakcie przetwarzania i przechowywania danych są

wymogi prawne, które określają minimalny zakres bezpieczeństwa. Dzięki tej wiedzy możemy uniknąć przewidzianych w przepisach kar i sankcji.

2. Standard bezpieczeństwa zgodny z Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

Dane osobowe to wszelkie informacje, dotyczące osoby fizycznej, zidentyfikowanej lub możliwej do zidentyfikowania; przy czym proces identyfikacji nie może wymagać nadmiernych kosztów i czasu. Dane osobowe podlegają ochronie zawsze, chyba że:

- istnieje przepis szczególny stanowiący, że dane osobowe są jawne lub ich przetwarzanie jest dopuszczalne,
- osoba wyraziła zgodę.

Standard w aspekcie ochrony danych osobowych to wspólnie ustalone „reguły, zasady, praktyki postępowania" w celu zwiększenia bezpieczeństwa ważnych/wrażliwych danych, dotyczących osoby fizycznej. Kwestie prawne związane z ochroną danych osobowych regulują Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz pięć rozporządzeń związanych z tą ustawą.

Ustawa określa:

- zasady przetwarzania danych osobowych osób fizycznych,
- prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych,
- organy ochrony danych osobowych,
- kompetencje generalnego inspektora ochrony danych osobowych,
- zasady zabezpieczania danych osobowych,
- zasady rejestracji zbiorów danych osobowych,
- zasady przekazywania danych osobowych do państwa trzeciego.

Minimalny zakres działań w zakresie standaryzacji ochrony danych osobowych to:

- wyznaczyć administratora bezpieczeństwa informacji – art. 36, ust. 3,
- opracować i prowadzić dokumentację przetwarzania danych osobowych art. 36, ust. 2,
- zastosować środki techniczne i organizacyjne zapewniające ochronę odpowiednią do zagrożeń – art. 36, ust. 1,
- prowadzić ewidencję osób upoważnionych do przetwarzania – art. 39,
- zapewnić kontrolę – art. 38, nad tym:
  - jakie dane osobowe zostały wprowadzone do zbioru,
  - kiedy i przez kogo,
  - komu zostały przekazane.

Prowadzenie dokumentacji ochrony danych osobowych w jednostce organizacyjnej to obowiązek wynikający z art. 36 pkt 2 ustawy z dnia 29 sierpnia 1997 r.

o ochronie danych osobowych. Sposób prowadzenia i zakres dokumentacji normującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną został sprecyzowany w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. Zgodnie z §3 pkt 1 tego rozporządzenia na dokumentację ochrony danych osobowych składają się polityka bezpieczeństwa ochrony danych osobowych i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Oba dokumenty muszą mieć formę pisemną i być prowadzone przez administratora danych osobowych. Rozporządzenie przedstawia wytyczne co do zawartości każdego z powyższych dokumentów.

Polityka bezpieczeństwa powinna zawierać:

- wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych przetwarzania tych danych,
- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
- sposób przepływu danych pomiędzy poszczególnymi systemami,
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Instrukcja powinna zawierać co najmniej:

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
- stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
- sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych,
- sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
- sposób realizacji wymogów informacyjnych co do odbiorców, daty i zakresu udostępnianych danych osobowych,
- procedury wykonywania przeglądów.

3. Standard bezpieczeństwa zgodny z Ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych

Informacja niejawna – polski termin prawniczy, który został zdefiniowany w ustawie o ochronie informacji niejawnych (UOIN) z 5 sierpnia 2010 r. Oznacza informację, która wymaga ochrony przed nieuprawnionym ujawnieniem, niezależnie od formy i sposobu jej wyrażenia, także w trakcie jej opracowania.

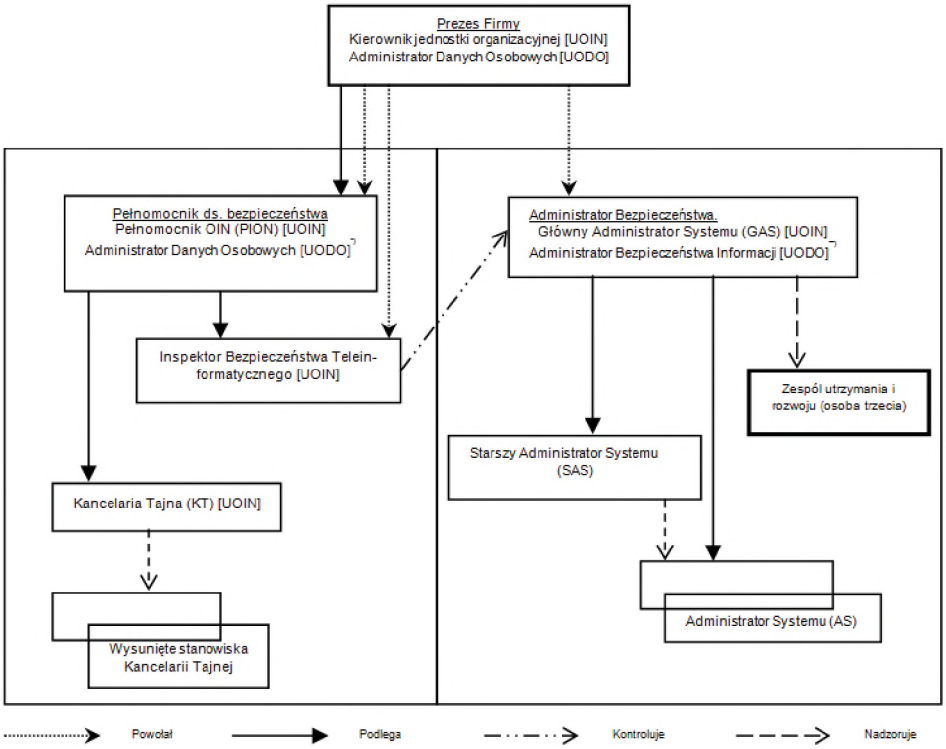
Informacje niejawne to informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania (art. 1 ust. 1 UOIN). Kontrolę ochrony informacji niejawnych prowadzą Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego w zakresie opisanym w ustawie o ochronie informacji niejawnych z 5 sierpnia 2010 r. Minimalny zakres działań w zakresie ochrony informacji niejawnych to:

- wyznaczyć służby (powołać strukturę organizacją – por. rysunek 5) zarządzania bezpieczeństwem w organizacji,
- opracować i prowadzić dokumentację przetwarzania informacji niejawnych,
- zastosować środki techniczne, proceduralne i organizacyjne zapewniające ochronę informacji niejawnych, odpowiednią do wyników zawartych w Raporcie z procesu szacowania ryzyka,
- poddać systemy i sieci TI, w których przetwarzane są informacje niejawne certyfikowaniu przez służby ochrony państwa – muszą one uzyskać akredytację w postaci certyfikatu akredytacji systemu lub sieci TI,
- zapewnić kontrolę skuteczności zaimplementowanych mechanizmów bezpieczeństwa w systemach lub sieciach TI.

W celu zapewnienia wypełniania wymogów ustawy o ochronie informacji niejawnych przez pełnomocników do spraw ochrony informacji niejawnych, a także kierowników jednostek organizacyjnych związanych z przygotowaniem dokumentacji normującej ochronę informacji niejawnych w jednostce organizacyjnej proponuje się wykonanie następujących elementów:

- analizy i oceny ryzyka ujawnienia lub utraty informacji niejawnych w jednostce organizacyjnej (art. 15 ust. 1 ppkt 3 UOIN);
- planu ochrony informacji niejawnych zawierającego plan postępowania z materiałami zawierającymi informacje niejawne w razie wprowadzenia stanu nadzwyczajnego (art. 15 ust. 1 ppkt 5 UOIN);
- dokumentu określającego sposób i tryb przetwarzania informacji niejawnych o klauzuli „poufne" w jednostce organizacyjnej (art. 43 ust. 3 UOIN);
- dokumentacji określającej poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą (art. 43 ust. 4 UOIN);

- instrukcji dotyczącej sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone" w jednostce organizacyjnej oraz określającej zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ochrony tych informacji (art. 43 ust. 5 UOIN);
- dokumentacji bezpieczeństwa teleinformatycznego (art. 48 ust. 4 UOIN);
- wykazu przedsiębiorców realizujących na rzecz jednostki organizacyjnej umowy lub zadania związane z dostępem do informacji niejawnych.



*) wypełnia obowiązki, które ustawa o ochronie danych osobowych nakłada na Administratora Danych Osobowych
**) pełni obowiązki, które ustawa o ochronie danych osobowych nakłada na Administratora Bezpieczeństwa Informacji

Rys. 5. Przykładowa struktura służb bezpieczeństwa

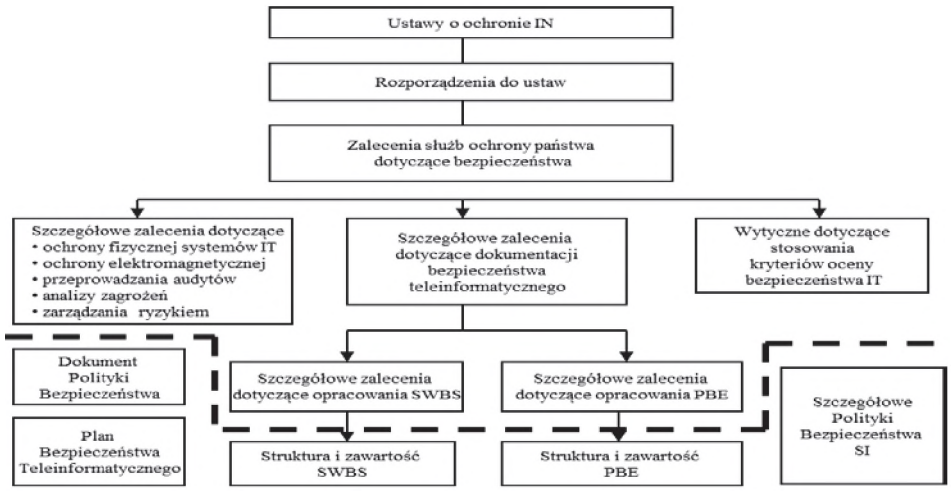
Źródło: opracowanie własne.

Ponadto w skład dokumentacji niewymaganych bezpośrednio przez ustawę o ochronie informacji niejawnych, ale branych pod uwagę przez ABW lub SKW podczas kontroli ochrony informacji niejawnych w jednostkach organizacyjnych w szczególności zalicza się:

- politykę bezpieczeństwa informacji,
- plan ochrony (zawierający m.in. instrukcję ruchu osobowo-materiałowego, instrukcję użytkowania systemu kontroli dostępu, instrukcję wykorzystywania

systemu sygnalizacji-napadu czy instrukcję użytkowania i przechowywania kluczy), instrukcje bezpieczeństwa przeciwpożarowego,
- plany zapewnienia ciągłości działania,
- plany organizacyjne funkcjonowania na czas wojny i okres pokoju.

Strukturę dokumentacji związanej z bezpieczeństwem w świetle zaleceń ABW przedstawiono na rysunku 6.



Rys. 6. Struktura dokumentacji

Źródło: opracowanie własne.

4. Standardy bezpieczeństwa zgodne z normami międzynarodowymi

Wybrane standardy zarządzania bezpieczeństwem to zbiór międzynarodowych norm serii ISO 27000, który można zdekomponować na następujące grupy:

a) opis standardu i definicje używanych terminów: ISO 27000;
b) normy specyfikujące wymagania podlegające audytowi w procesie certyfikacji:
   - ISO 27001 – wymagania stawiane SZBI,
   - ISO 27006 – wymagania wobec jednostek certyfikujących;
c) przewodniki opisujące standardy oraz praktyki ich implementowania:
   - ISO 27002 (PN-ISO/IEC 17799) – wdrażanie SZBI,
   - ISO 27003 – podejście procesowe we ustanawianiu i wdrażaniu SZBI,
   - ISO 27004 – metody pomiarowe i kontrolne dla SZBI,
   - ISO 27005 – analiza ryzyka dla potrzeb SZBI,
   - ISO 27007 – audyty SZBI.
d) standard ITIL (*Information Technology Infrastructure Library*) – jeden z najbardziej powszechnie znanych standardów zarządzania IT na świecie; ITIL

opisuje procesy potrzebne do zarządzania infrastrukturą IT tak, by były spełnione odpowiednie założenia dotyczące efektywnego świadczenia usług przez IT oraz zagwarantowana odpowiednia jakość ich świadczenia;

e) model referencyjny standardu COBIT – opracowany przez związany z ISACA IT Governance Institute standard COBIT (ang. *Control Objectives for Information and Related Technology*) definiuje referencyjny model procesów organizacyjnych związanych z funkcjonowaniem systemu informatycznego w przedsiębiorstwie;

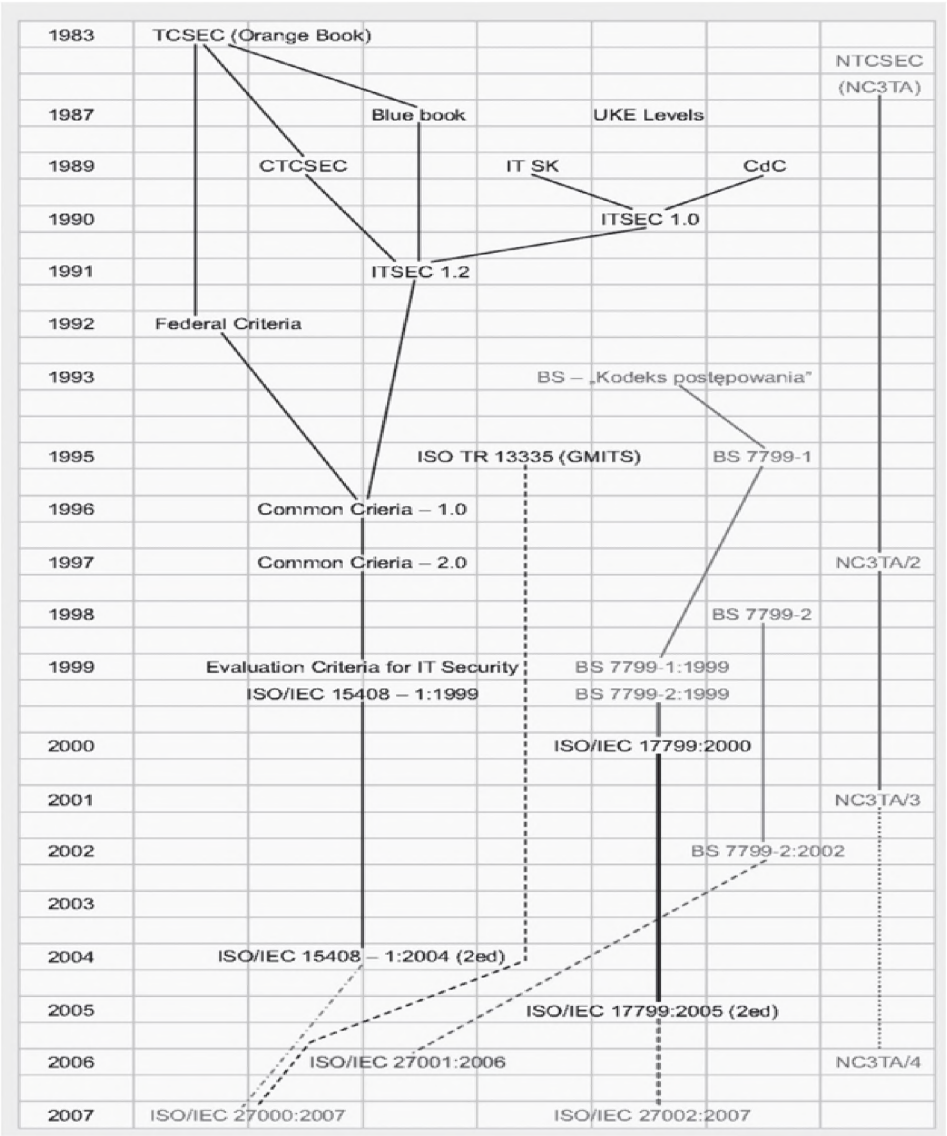
f) norma dotycząca obszaru zarządzania bezpieczeństwem samego systemu informacyjnego w organizacji (ISO 13335) oraz oprogramowania i sprzętu (ISO 15408) wsparta normami dotyczącymi projektowania systemu, jego oprogramowania i jakości (ISO/IEC 9126, ISO 12207, ISO 9000-3:2004);

g) normy stowarzyszone – sektorowe:
   - ISO 27011 – SZBI w sektorze telekomunikacyjnym,
   - ISO 27799 – implementacja Zarządzania Bezpieczeństwem Informacji dla potrzeb,
   - organizacji służby zdrowia (adaptacja ISO 27002),
   - inne normy sektorowe znajdują się w opracowywaniu.

Historyczny rozwój standardów zarzadzania bezpieczeństwem informacji odzwierciedla rysunek 7.

Minimalny zakres działań w zakresie zarzadzania bezpieczeństwem informacji to:

- wyznaczyć służby (powołać strukturę organizacją) zarządzania bezpieczeństwem informacji w organizacji,
- zdefiniować zakres i politykę bezpieczeństwa Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
- opracować **dokumentację** Systemu Zarządzania Bezpieczeństwem Informacji,
- zbudować i wdrożyć Systemu Zarządzania Bezpieczeństwem Informacji, odpowiedni do wyników zawartych w Raporcie z procesu szacowania ryzyka,
- przeprowadzić audyt certyfikacyjny,
- doskonalić SZBI.



Rys. 7. Struktura rozwoju standardów zarządzania bezpieczeństwem informacji

Źródło: http://www.zabezpieczenia.com.pl/ochrona-informacji/system-zarzadzania-bezpieczenstwem-informacji-zgodny-z-iso-iec-27001-cz-1-wprowadzenie.

Dokumentacja SZBI powinna obejmować:

- udokumentowane deklaracje polityki bezpieczeństwa oraz celów stosowania zabezpieczeń – dokument polityki bezpieczeństwa,
- plan bezpieczeństwa teleinformatycznego,

- polityki bezpieczeństwa teleinformatycznego dla poszczególnych systemów informatycznych,
- szczególne wymagania bezpieczeństwa systemów informatycznych – SWBS-y,
- procedury bezpiecznej eksploatacji – PBE,
- raport z procesu szacowania ryzyka,
- plan postępowania z ryzykiem,
- deklarację stosowania.

Wdrożenie systemu zarządzania bezpieczeństwem informacji SZBI (ang. *Information Security Management System*) tak, aby można było go certyfikować na zgodność z ISO/IEC 27001 jest procesem długotrwałym, wymagającym przeprowadzenia szeregu czynności. Wpływ na czas wdrożenia i certyfikowania SZBI ma przede wszystkim:

- wielkość środowiska bezpieczeństwa, w którym ma być docelowo eksploatowany chroniony obiekt, system czy elektroniczna platforma integracyjna oraz złożoność obiektu chronionego,
- aktualny stan bezpieczeństwa środowiska eksploatacji chronionego obiektu.

Podsumowanie

Każda technologia przechodzi okres burzliwego rozwoju, w czasie którego powstaje szereg różnych, konkurencyjnych rozwiązań. W następnym etapie niektóre rozwiązania uzyskują przewagę i mamy do czynienia z pojawianiem się standardów *de-facto*, z których część zostaje powszechnie zaakceptowana i rozpoczyna się proces normalizacyjny. Do słabych stron procesu normalizacyjnego w kraju należy fakt, że stosowanie polskich norm nie jest obowiązkowe! Nie są też obowiązkowe normy definiujące i opisujące System Zarządzania Bezpieczeństwem Informacji (rodzina ISO 27000). Do pozytywnych stron procesu standaryzacji należy zaliczyć wprowadzenie Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. W tym rozporządzeniu specyfikacje obejmują m.in.:

- minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej;
- sposoby zapewnienia bezpieczeństwa przy wymianie informacji,
- standardy techniczne zapewniające wymianę informacji z udziałem podmiotów publicznych z uwzględnieniem wymiany transgranicznej,
- minimalne wymagania dla systemów teleinformatycznych,
- Krajowe Ramy Interoperacyjności.

Pełny tekst rozporządzenia jest dostępny na stronie internetowej: http://bip.mswia.gov.pl/portal/bip/218/19586/.

Kolejnym pozytywnym krokiem w kierunku standaryzacji i procesu normalizacji było wymuszenie stosowania aktów prawnych, takich jak ustawy, rozporządzenia, zarządzenia i decyzje.

Wśród głównych korzyści stosowania standardów bezpieczeństwa wymienić można:

- zapewnienie zgodności z wymaganiami prawnymi w obszarze bezpieczeństwa informacji (na przykład dane osobowe), co jest obowiązkiem każdego przedsiębiorcy,
- kontrole zgodności z obowiązującymi przepisami prawa,
- zwiększenie poziomu bezpieczeństwa informacji przetwarzanych w organizacji, co przekłada się na jakość zarządzania w organizacji,
- zwiększenie wiarygodności oraz zaufania klientów, których dane są przetwarzane,
- identyfikacje zagrożeń i ocenienie podatności w celu zminimalizowania strat i realizacji celów biznesowych,
- zwiększenie bezpieczeństwa ważnych informacji, których utrata może spowodować duże straty finansowe, czasu i wizerunku,
- poprawę konkurencyjności i wizerunku,
- ochronę przed wyciekiem informacji,
- zwiększenie świadomości pracowników, a tym samym budowę kultury organizacyjnej i ładu,
- systemowe podejście do tematu bezpieczeństwa,
- ewentualne uzyskanie certyfikatu, który stanowi doskonały element marketingowy dla organizacji.

Dla organizacji zainteresowanych ustanowieniem i wdrożeniem SZBI najistotniejsze są normy opisujące wdrażanie systemu, a w szczególności ISO/IEC 27002, ponieważ według tych norm należy prowadzić proces wprowadzania SZBI, który może się zakończyć (lub nie) uzyskaniem certyfikatu ISO 27001.

Literatura

Białas A. (2006), *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT 2006.

Heracleous L. (1998), *Better than the Rest: Making Europe the Leader in the Next Wave of Innovation and Performance*, „Long Range Planning", February.

ISO/IEC 27000:2012 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i słownictwo.

ISO/IEC 27001:2013 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

ISO/IEC 27002:2013 Technika informatyczna – Techniki bezpieczeństwa – Kodeks postępowania w zakresie kontroli bezpieczeństwa informacji.

ISO/IEC 27004:2009 Technika informatyczna – Techniki zabezpieczeń – Zarządzanie bezpieczeństwem informacji – pomiary.

ISO/IEC 27005:2011 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie Bezpieczeństwem Informacji ryzyka.

ISO/IEC 27006:2011 Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji.

ISO/IEC 27007:2011 Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dotyczące systemów zarządzania bezpieczeństwem informacji audytu.

ISO/IEC TR 27008:2011 Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla audytorów informatycznych systemów zarządzania kontroli bezpieczeństwa.

ISO/IEC 27009 Technika informatyczna – Techniki bezpieczeństwa – Zastosowanie normy ISO/IEC 27001 – Wymagania.

ISO/IEC 27010:2008 Technika informatyczna – Techniki bezpieczeństwa – Wytyczne zarządzania bezpieczeństwem informacji dla podmiotów świadczących usługi telekomunikacyjne na podstawie normy ISO/IEC 27002.

http://bip.mswia.gov.pl/portal/bip/218/19586/.

http://wawak.pl.

http://www.abiway.pl.

http://www.immusec.com.

http://www.iso27000.pl.

http://www.piu.org.pl.

http://www.pkn.pl.

Liderman K. (2003), *Podręcznik administratora bezpieczeństwa teleinformatycznego*, Mikom.

PN ISO/IEC 15408-1:2001 Kryteria oceny zabezpieczenia systemów. Model ogólny oceny zabezpieczenia systemów.

PN ISO/IEC 15408-3:2002 Kryteria oceny zabezpieczenia systemów. Wymagania uzasadnienia pewności.

PN ISO/IEC 17799:2003 Praktyczne zasady zarządzania bezpieczeństwem informacji.

PN-I-13335-1:1998 Wytyczne do zarządzania bezpieczeństwem systemów informacyjnych – Pojęcia i modele bezpieczeństwa systemów informatycznych.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2002, Nr 1, poz. 926, ze zm.).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010, Nr 182, poz. 1228).

SOME ASPECTS OF STANDARDIZATION IN PROTECTION OF PUBLIC INFORMATION RESOURCES AND PUBLIC SERVICES IN THE AGE OF INFORMATION SOCIETY

Summary

This paper provides considerations about the meaning of selected legal aspects of the information security in the age of information society. The key role in the process of providing security of the public databases, public registers and public administration services is nowadays featured by the standards. For each presented legal act, standard or the best practice some minimal requirements and basic activities was also proposed by the authors. Those conditions should be taken by security authorities to provide basic acceptable level of security for information processed by public administration. The huge role of data, information and knowledge for the whole information society, social relations, modern legal order as well as for the individuals was also emphasized.
Keywords: information security, safety attributes, security standards, information resources

Translated by Jerzy Stanik