Polityka bezpieczeństwa informacji instytucji na przykładzie Instytutu Łączności – Państwowego Instytutu Badawczego

Marian Kowalewski

Anna Ołtarzewska

Zwrócono uwagę na potrzebę opracowania oraz stosowania w instytucjach polityki bezpieczeństwa informacji (PBI), koniecznej do ochrony gromadzonej, przetwarzanej i przesyłanej informacji. Wyjaśniono pojęcia i zakres polityki bezpieczeństwa informacji w instytucji. Określono podstawy prawne jej tworzenia. Na przykładzie Instytutu Łączności – Państwowego Instytutu Badawczego zaprezentowano układ dokumentu PBI, uwzględniający dokumenty normatywne i praktykę badawczą wraz z jej głównym składnikiem – strategią.

ochrona informacji, polityka bezpieczeństwa instytucji

Wprowadzenie

O skuteczności działania i rozwoju instytucji (organizacji) świadczy stopień osiągania zamierzonego celu. W procesie tym jest bardzo ważne stosowanie współczesnych technik i technologii, narzędzi i systemów informatycznych oraz przetwarzania i zarządzania informacją[①].

Informacja jest jednym z ważniejszych zasobów instytucji, na ogół decydującym o jej sukcesach. Dlatego powinna być chroniona zarówno przez kierownictwo, jak i pozostałych pracowników. Instytucje rygorystycznie przestrzegające tego nakazu na ogół bezkolizyjnie funkcjonują w swoim środowisku i dynamicznie się rozwijają.

Ważne jest, aby zapewnić ochronę informacji na pożądanym poziomie, a tym samym spełnić wymagany poziom bezpieczeństwa systemów informacyjnych. W tym celu należy odpowiednio zorganizować zasoby instytucji i skutecznie nimi zarządzać, czyli mieć właściwie opracowaną i bezwzględnie przestrzeganą politykę bezpieczeństwa informacji (PBI) instytucji. Jest to jeden z warunków osiągania sukcesów.

Istota polityki bezpieczeństwa informacji instytucji

W każdej instytucji (organizacji) znajdują się różnorodne informacje, które z reguły powinny być chronione; część ze względu na interes instytucji (np. szczegółowe informacje związane ze strategicznymi planami, informacje finansowe i inwestycyjne, patenty itp.), część zaś z mocy prawa (np. zbiory danych osobowych, informacje niejawne). Zasadniczy zbiór informacji instytucji jest jawny i dotyczy całości problemów związanych z jej funkcjonowaniem. Nie oznacza to, że nie powinien być chroniony, wręcz przeciwnie, każda bowiem informacja jest podatna na zagrożenia (np. zniszczenie czy zafałszowanie) lub – szerzej mówiąc – niepożądane modyfikowanie.

① *Przez informację rozumie się treści wszelkiego rodzaju, przechowywane na dowolnym nośniku informacji, wyrażone za pomocą mowy, pisma, obrazu, rysunku, znaku, kodu, dźwięku lub w jakikolwiek inny sposób.*

Celem działań w zakresie ochrony i zapewnienia bezpieczeństwa informacji w instytucji jest osiągnięcie takiego poziomu organizacyjnego i technicznego, który:

- zagwarantuje zachowanie poufności informacji chronionych;
- zapewni integralność informacji chronionych i jawnych oraz dostępność do nich;
- zagwarantuje wymagany poziom bezpieczeństwa przetwarzanych informacji;
- maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji;
- zapewni poprawne i bezpieczne funkcjonowanie systemów przetwarzania informacji;
- zapewni gotowość do podejmowania działań w sytuacjach kryzysowych.

Najogólniej ujmując, PBI jest zbiorem dokumentów, określających metody i zasady ochrony oraz zapewnienia bezpieczeństwa informacji w instytucji. Mówiąc szerzej, PBI jest zbiorem spójnych, precyzyjnych i zgodnych z obowiązującym prawem przepisów, reguł i procedur, według których dana instytucja (organizacja) buduje, zarządza i udostępnia zasoby oraz systemy informacyjne i informatyczne. W szczególności w PBI zdefiniowano zasoby, które powinny być chronione i sposoby (metody) tej ochrony.

W PBI określono zasady ochrony grup informacji, dotyczące sposobów ich przetwarzania i przechowywania, z uwzględnieniem nie tylko zagadnień bezpieczeństwa i komunikacji przetwarzanych informacji, sprzętu i oprogramowania, za pomocą których są przetwarzane informacje, lecz również ludzi, którzy te informacje przetwarzają. Punktem wyjścia do tworzenia PBI jest wyznaczenie grup informacji, które powinny podlegać ochronie.

Polityka bezpieczeństwa informacji stanowi podłoże do tworzenia dokumentów, zawierających specyficzne wymagania dla konkretnych grup informacji, a także określających warunki, jakie muszą spełniać systemy informatyczne i papierowe je przetwarzające, z uwzględnieniem aspektów prawnych ochrony informacji i systemów informatycznych.

W praktyce są różne metody tworzenia PBI instytucji. Jednak, bez względu na to, jakiego są to typu rozwiązania, jest ważne, aby opracowana PBI odpowiadała potrzebom danej instytucji, w zakresie skutecznej ochrony gromadzonych i przetwarzanych w niej informacji. Dla przykładu, jeśli PBI tworzy się wg metodyki TISM (*Total Information Security Management*) [20], wówczas ma ona strukturę modułową, zawiera odrębne zasady bezpieczeństwa dla poszczególnych grup informacji i systemów ich przetwarzania oraz zestawy instrukcji, regulaminów i procedur.

Podstawy opracowania polityki bezpieczeństwa instytucji

Przy opracowywaniu PBI jest niezwykle ważne zdefiniowanie pojęcia bezpieczeństwa informacji. Znawcy tego tematu uważają, że bezpieczeństwo informacji jest to zachowanie poufności, integralności i dostępności informacji. Przy czym przez poufność informacji należy rozumieć zapewnienie, że dostęp do informacji mają tylko osoby upoważnione, a przez dostępność informacji, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy istnieje taka potrzeba, natomiast przez integralność informacji należy rozumieć zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania [15].

Jak już wspomniano, PBI instytucji powinna ujmować ogólne zasady wytwarzania, przetwarzania, przesyłania i przechowywania informacji w aspekcie zapewnienia jej bezpieczeństwa oraz organizację i zasady sprawnego zarządzania tym procesem. Wymóg ten jest niezwykle istotny, ponieważ zawiera

podstawowe treści związane z budową PBI instytucji, szczególnie jej strategii w tym zakresie. PBI powinna uwzględniać też normy oraz zalecenia międzynarodowe i krajowe [5, 10, 11, 12, 15].

Podstawą prawną opracowania PBI w instytucji są obowiązujące ustawy oraz rozporządzenia (dokumenty wyższego rzędu) dotyczące m.in. ochrony informacji niejawnych, podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych, ochrony danych osobowych i ochrony praw autorskich[①].

Opracowanie PBI instytucji wymaga uwzględnienia wielu czynników, funkcjonujących w danej organizacji, np. takich jak: charakter, specyfika funkcjonowania, struktura organizacyjna oraz procesy zachodzące w tej instytucji.

Polityka bezpieczeństwa informacji instytucji powinna stanowić podstawę działań dotyczących jej wdrożenia oraz obejmować wszystkich pracowników i współpracowników danej instytucji, czy też organizacji. Jest oczywiste, że nie może być dokumentem zamkniętym, powinna być bowiem ciągle uaktualniana, modyfikowana i dostosowywana do potrzeb danej instytucji.

Struktura dokumentu PBI

W dokumentach normatywnych związanych z zagadnieniem polityki bezpieczeństwa informacji nie wskazano konkretnego układu, czy też treści PBI organizacji. W obowiązującej normie krajowej [15] przedstawiono jedynie **minimum zawartości dokumentu PBI**; podano, że PBI musi zawierać:

– definicję bezpieczeństwa informacji, jego cele i zakres oraz znaczenie bezpieczeństwa informacji jako mechanizmu współużytkowania informacji;
– oświadczenie o intencji kierownictwa instytucji, potwierdzające cele i zasady bezpieczeństwa informacji w instytucji;
– krótkie wyjaśnieni PBI, zasad, standardów i wymagań dotyczących zgodności, mających szczególne znaczenie dla instytucji;
– definicje ogólnych i szczegółowych obowiązków w zakresie zarządzania bezpieczeństwem informacji, w tym zgłaszania przypadków naruszenia bezpieczeństwa;
– odsyłacze do dokumentacji, stanowiące uzupełnienie PBI.

Ponadto podkreślono, że PBI powinna zostać udostępniona użytkownikom w całej instytucji, **w formie właściwej, dostępnej i zrozumiałej dla czytelników, do których jest adresowana**.

W praktyce spotyka się różne układy i zróżnicowane co do stopnia szczegółowości treści w opracowywanych PBI organizacji. Jedną z metod jest TISM [20], interesująca, szczególnie w zakresie układu i zawartości merytorycznej, rzeczowego i kompleksowego ujęcia problemów bezpieczeństwa informacji. Jest ona oraz możliwa do zastosowania w różnego rodzaju instytucjach i organizacjach, w tym w środowisku naukowym.

Autorzy tej metody uważają, że w każdej opracowanej PBI instytucji, niezależnie od przyjętego jej układu, ważne powinno być to, aby powyżej wskazane minimalne treści polityki, jakie wynikają z przytaczanej i obowiązującej normy [15], były uwzględnione i nie kolidowały z obowiązującymi w kraju dokumentami prawnymi. Ponadto powinny zostać wzięte pod uwagę potrzeby danej instytucji, jej zasoby i specyfika funkcjonowania.

① *Ze względu na znaczny zbiór tego typu dokumentów prawnych w niniejszym artykule jest on tylko zasygnalizowany.*

Prowadzone prace w obszarze polityk bezpieczeństwa informacji oraz bezpieczeństwa systemów informatycznych, a także analiza obowiązujących przepisów i norm dotyczących tej istotnej problematyki świadczą, że PBI instytucji, dla przykładu polityka bezpieczeństwa informacji Instytutu Łączności – Państwowego Instytutu Badawczego (IŁ – PIB), może mieć następującą strukturę organizacyjną[①].

POZIOM I

1. Polityka bezpieczeństwa informacji:
   - część I: zwarte ujęcie PBI instytucji (podstawy prawne opracowanego dokumentu, podstawowe definicje bezpieczeństwa informacji, ogólne zasady i strategia bezpieczeństwa informacji, podstawowe wymagania w zakresie zapewnienia bezpieczeństwa informacji, identyfikacja informacji wytwarzanej, przetwarzanej i przechowywanej w instytucji);
   - część II: zasady zarządzania bezpieczeństwem informacji w instytucji (cel, zakres i ogólne zasady zarządzania bezpieczeństwem informacji; podział, obieg i dostęp do informacji podlegającej ochronie; wymagania i specyfikacja systemów przetwarzania informacji oraz metody ochrony informacji; zasady reagowania w sytuacjach kryzysowych, organizacja i zasoby osobowe zarządzania bezpieczeństwem informacji).
2. Polityka bezpieczeństwa systemu informatycznego – regulamin sieci komputerowej (sposoby korzystania z sieci komputerowej, tryb dostępu do sieci, zasady pracy w sieci, zasady i sposoby tworzenia kopii zapasowych, zasady działania w sytuacjach kryzysowych, osoba (osoby) odpowiedzialna za administrowanie sieci).

POZIOM II

Polityki bezpieczeństwa grup informacji chronionych (cel i zakres polityki bezpieczeństwa danej grupy informacji, dostęp do informacji i zasady zarządzania nią, wykaz systemów przetwarzania wraz z wymaganiami, zasady archiwizacji informacji i postępowania w sytuacjach kryzysowych, wykaz procedur i instrukcji określających zarządzanie grupą informacji).

POZIOM III

Polityki bezpieczeństwa systemów przetwarzania informacji chronionych – wypełnienie założeń dokumentów z poziomu I i II (cel i zakres systemu oraz jego schemat, kryteria bezpieczeństwa systemu i zasady zarządzania nim, zasady reagowania w sytuacjach kryzysowych i przeprowadzania audytów bezpieczeństwa).

Wskazane polityki mogą być prezentowane w postaci:

- regulaminów: dokumenty opisujące zasady ochrony informacji, prawa i obowiązki pracowników oraz zasady korzystania z poszczególnych środków technicznych przetwarzających informacje;
- instrukcji: zestaw szczegółowych dokumentów związanych z zarządzaniem bezpieczeństwem informacji, które wynikają z dokumentu PBI;
- procedur: opisujące szczegółowo postępowanie w określonych przypadkach zarówno w normalnym toku działania instytucji, jak i w sytuacjach kryzysowych związanych z incydentem bezpieczeństwa.

[①] *Układ ten jest na ogół zgodny z metodyką TISM, którą uznano jako reprezentatywną dla instytucji w środowisku naukowym, np. jednostek badawczo-rozwojowych (jbr).*

Dokumenty poziomu II (jako uszczegółowienia wymagań) i poziomu III PBI (jako spełnienie wymagań bezpieczeństwa) powinny być ściśle ze sobą powiązane, nawzajem się uzupełniać i wynikać z dokumentów poziomu I PBI, które te wymagania określają. Ich forma może być różna i dostosowana do potrzeb i wymogów danej instytucji.

Zaprezentowany układ jest dostosowany do potrzeb IŁ-PIB, odpowiada zadaniom i celom działania oraz zasobom Instytutu, jego otoczeniu i funkcjonowaniu w warunkach konkurencyjności oraz gospodarki rynkowej.

Oczywiście nie jest to pełen zbiór problemów, należy bowiem pamiętać o tym, że może on być inny dla każdej instytucji, ale zawsze powinien odpowiadać jej potrzebom.

Strategia jako główny składnik PBI instytucji

Opracowywane PBI większości instytucji zawierają strategie ochrony i bezpieczeństwa informacji danej organizacji. Jest to stanowisko słuszne i dlatego – dla przejrzystości funkcjonowania PBI danej organizacji – powinno być powszechnie stosowane.

Strategia ochrony i bezpieczeństwa informacji powinna ujmować swoisty zamiar zarządu organizacji, wyrażający się poglądem i stanowiskiem w przedmiotowym problemie. Uważa się, że strategia jako główny składnik PBI powinna prezentować podstawę osiągnięcia spójnej ochrony informacji oraz sposoby osiągnięcia celów w zakresie ochrony informacji instytucji.

Podstawą osiągnięcia spójnej ochrony informacji może być m.in. rozpoznanie grup informacji, systemów oraz obszarów ich przetwarzania, które będą podlegać ochronie. Natomiast w zakresie wyznaczonych celów ochrony informacji, na przykładzie IŁ-PIB, strategia powinna wskazywać sposoby ich osiągania przez:

- wprowadzenie podziału na informacje jawne i chronione;
- określenie informacji, stanowiących tajemnicę instytucji jako podlegających ochronie ze względu na ich dobro, interes i pozycję na rynku;
- określenie informacji chronionych ze względu na wymogi prawne;
- możliwość nadawania każdej informacji chronionej odpowiedniej klauzuli tajności;
- wprowadzenie podziału informacji chronionych na grupy i zarządzanie nimi;
- określenie organizacyjnych i technicznych wymogów bezpieczeństwa przetwarzania grup informacji chronionych;
- utworzenie struktur organizacyjnych odpowiedzialnych za zarządzanie bezpieczeństwem i przetwarzaniem informacji;
- zarządzanie ciągłością przetwarzania informacji;
- standaryzację procedur postępowania oraz opracowanie niezbędnej dokumentacji, tj. zasad zarządzania bezpieczeństwem grup informacji i systemów ich przetwarzania;
- wdrożenie rozwiązań technicznych, zapewniających wymagany poziom bezpieczeństwa przetwarzanych informacji – inwestycje w infrastrukturę sieci i systemów informatycznych oraz fizyczne zabezpieczenie obszarów przetwarzania informacji chronionych;

– efektywne propagowanie zasad bezpieczeństwa informacji wśród kierownictwa i pracowników instytucji;
– cykliczne szkolenie pracowników w zakresie bezpieczeństwa informacji.

W celu dostosowania do zmian prawnych, potrzeb instytucji, postępu w zakresie rozwoju technologii i usług teleinformatycznych, strategia ochrony informacji instytucji powinna być na bieżąco aktualizowana.

Podsumowanie

Polityka bezpieczeństwa informacji prezentuje swoisty zbiór metod i zasad ochrony oraz zapewnienia bezpieczeństwa informacji, jako głównego zasobu w instytucji. Umożliwia ona zorganizowane i bezpieczne gromadzenie, przetwarzanie, przesyłanie i przechowywanie informacji, sprawne i kontrolowane jej zarządzanie, a także ochronę i bezpieczeństwo. Jest ona zbiorem dokumentów i stosownie do potrzeb instytucji powinna być ciągle odnawiana (aktualizowana). Przede wszystkim jednak PBI powinna być dokumentem czytelnym i zrozumiałym dla wszystkich pracowników instytucji. Powinien też nią szczególnie interesować się zarząd instytucji.

Bibliografia

[1] Barczak A., Sydoruk T.: *Bezpieczeństwo systemów informatycznych zarządzania*. Warszawa, BELLONA, 2003
[2] Białas A.: *Podstawy bezpieczeństwa systemów teleinformatycznych*. Gliwice, Wydawnictwo: Pracownia komputerowa Jacka Skalmierskiego, 2002
[3] Cole E., Krutz R. L., Conley J.: *Bezpieczeństwo sieci. Biblia.* Warszawa, Helion, 2005
[4] Filar W., Roman W., Koponski J.: *Założenia polityki bezpieczeństwa systemów i sieci teleinformatycznych*. W: Materiały z konferencji: *Bezpieczeństwo Systemów i Sieci Teleinformatycznych NetSec'99*, Katowice, 1999
[5] ISO/IEC TR 13335-3:1998 *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych* – Część 3: *Techniki zarządzania bezpieczeństwem systemów informatycznych*
[6] Kaeo M.: *Tworzenie bezpiecznych sieci*. Warszawa, Mikom, 2000
[7] Kifner T.: *Polityka bezpieczeństwa i ochrony informacji*. Gliwice, Helion, 1999
[8] Kowalewski M. i in.: *Aspekty bezpieczeństwa systemów teleinformatycznych*. Warszawa, Instytut Łączności, 2005
[9] Molski M., Opala S.: *Elementarz bezpieczeństwa systemów informatycznych*. Warszawa, Mikom, 2002
[10] PN-EN ISO 9001:2001 *System zarządzania jakością. Wymagania*
[11] PN-EN ISO 14001:2005 *Systemy zarządzania środowiskowego. Wymagania i wytyczne stosowania*
[12] PN-I-13335-1:1999 *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych*
[13] PN-ISO/IEC 15408-1:2002 *Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych* – Część 1: *Wprowadzenie i model ogólny*

[14] PN-ISO/IEC 15408-3:2002 *Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych* – Część 3: *Wymagania uzasadnienia zaufania do zabezpieczeń*

[15] PN-ISO/IEC 17799:2007 *Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji*

[16] PN-ISO/IEC 27001:2007 *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*

[17] Stokłosa J., Bilski T., Dankowski T.: *Bezpieczeństwo danych w systemach informatycznych*. Warszawa-Poznań, PWN, 2001

[18] Strebe M.: *Podstawy bezpieczeństwa sieci*. Warszawa, Mikom, 2005

[19] Szamański B.: *Integracja systemu zarządzania bezpieczeństwem informacji zgodnie z BS 7799 (ISO/IEC 17799) ze zintegrowanymi systemami zarządzania (ISO 9001, ISO 14001, PN 18001)*. W: Materiały z konferencji: *Enigma 2001*, Warszawa, 2001

[20] *TISM – Total Information Security Management*. Dokumentacja ver. 1.4 RC 1. Materiały firmy ENSI

Marian Kowalewski

Doc. dr hab. inż. Marian Kowalewski (1951) – absolwent WSOWŁ (1975); nauczyciel akademicki, pracownik naukowy i prorektor ds. dydaktyczno-naukowych w Wyższej Szkole Oficerskiej Wojsk Łączności (1975–1997); pracownik naukowy Instytutu Łączności w Warszawie (od 1997), zastępca dyrektora ds. naukowych i ogólnych IŁ (1997–2004), kierownik projektu TETRA w IŁ (od 2002); organizator oraz współorganizator wielu seminariów i konferencji naukowych; autor wielu podręczników i skryptów akademickich, artykułów, prac naukowo-badawczych dotyczących problematyki telekomunikacyjnej; zainteresowania naukowe: planowanie i projektowanie oraz efektywność systemów telekomunikacyjnych.
e-mail: M.Kowalewski@itl.waw.pl

Anna Ołtarzewska

Mgr Anna Ołtarzewska (1955) – absolwentka Wydziału Rewalidacji i Resocjalizacji Akademii Pedagogiki Specjalnej w Warszawie (2002); absolwentka Wydziału Strategiczno-Obronnego Akademii Obrony Narodowej w Warszawie (2003); długoletni pracownik Instytutu Łączności w Warszawie (od 1978); zainteresowania naukowe: techniki przetwarzania informacji, sztuka i technika negocjacji, wspomaganie decyzji, polityka bezpieczeństwa, bezpieczeństwo teleinformatyczne i ochrona danych, rynek telekomunikacyjny.
e-mail: A.Oltarzewska@itl.waw.pl