O ZNACZENIU RZETELNEGO UDOKUMENTOWANIA SYSTEMU BEZPIECZEŃSTWA INFORMACYJNEGO DLA ZARZĄDZANIA RYZYKIEM INFORMACYJNYM

KRZYSZTOF LIDERMAN

WOJSKOWA AKADEMIA TECHNICZNA
WYDZIAŁ CYBERNETYKI

Wstęp

Zarządzanie ryzykiem to systematyczne stosowanie polityki, procedur i praktyki zarządzania do ustalania kontekstu ryzyka, jego identyfikowania, analizowania, wyznaczania, postępowania z ryzykiem oraz monitorowania i komunikowania ryzyka (definicja za PN-IEC 62198 [8]). Zagadnienia zarządzania ryzykiem nabierają coraz większego znaczenia w działalności biznesowej organizacji na całym świecie, czego przykładem jest pojawienie się nowej specjalności zawodowej „menedżera ryzyka"[1] oraz różnego rodzaju stowarzyszeń tej grupy zawodowej (jak np. FERMA – ang. *Federation of European Risk Management Associations*). Można chyba stwierdzić, że obecnie mamy do czynienia ze swoistą modą na widzenie wszystkich aspektów działalności biznesowej organizacji przez pryzmat ryzyka. Ma to przełożenie również na problematykę bezpieczeństwa informacyjnego, niezmiernie istotną we współczesnych, wysoce zinformatyzowanych organizacjach różnego rodzaju. Obecną modę na ryzyko poprzedziła moda z przełomu XX/XXI wieku na „widzenie" działalności biznesowej przez pryzmat procesów biznesowych – przykładem są chociażby zmiany zachodzące w kolejnych wydaniach serii norm z zakresu jakości, tj. ISO/IEC 900x.

Dobrym przykładem uzasadniającym stwierdzenie o nowym paradygmacie postrzegania działalności biznesowej są zmiany wprowadzone w 2010 roku do ustawy o ochronie informacji niejawnej [14] oraz treść normy [6]. Norma ta jest przeznaczona dla kadry kierowniczej organizacji oraz jej personelu w celu przedstawienia modelu oraz ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymywania i doskonalenia systemu zarządzenia bezpieczeństwem

[1] Przynajmniej w krajach innych niż Polska – w Polsce jest to specjalność nieformalna, nie ujęta w Rozporządzeniu Ministra Pracy i Polityki Społecznej z dnia 27 kwietnia 2010 r. w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy oraz zakresu jej stosowania (publikacja: Dz.U. z 2010 r., nr 82, poz. 537).

informacji (dalej w skrócie SZBI). Do podstawowych elementów takiego modelu należą (za normą [6], podkreślenia własne):

- *system zarządzania bezpieczeństwem informacji* (SZBI) – ta część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. SZBI obejmuje strukturę organizacyjną, polityki, działania planistyczne, zakresy odpowiedzialności, praktyki, procedury, procesy i zasoby;
- *deklaracja stosowania* (ang. *statement of applicability*) – dokument, w którym opisano cele stosowania zabezpieczeń oraz zabezpieczenia, które odnoszą się i mają zastosowanie w SZBI danej organizacji, oparte o rezultaty i wnioski z procesów szacowania i postępowania z ryzykiem.

Jak można zauważyć, kluczowym elementem proponowanego w normie modelu jest zarządzanie ryzykiem. Gdy mowa o analizie ryzyka w kontekście bezpieczeństwa informacyjnego, należy mieć na uwadze m.in. jej związki z analizą ryzyka biznesowego oraz zależności między osobami zaangażowanymi w ocenę (i zarządzanie) ryzyka biznesowego i ryzyka związanego z bezpieczeństwem informacji przetwarzanych, przesyłanych i przechowywanych w systemach teleinformatycznych organizacji, a także zakresy odpowiedzialności tych osób.

Dla menedżera zajmującego się ryzykiem biznesowym, ryzyko związane z przetwarzaniem informacji w systemach informacyjnych (w tym w teleinformatycznych) organizacji, będzie tylko jednym z wielu mogących mieć wpływ na osiąganie celów biznesowych wyznaczonych przez kadrę zarządzającą. Dla osoby odpowiedzialnej za bezpieczeństwo informacyjne i, w szczególności, teleinformatyczne[2] i zwykle będącej tzw. *właścicielem ryzyka IT* w kontekście całościowego ryzyka biznesowego, to „ryzyko IT" jest jedyne i najważniejsze, ponieważ ma wpływ na skuteczne zarządzanie bezpieczeństwem informacyjnym (co jest podstawowym zadaniem służbowym takiej osoby).

Zarządzanie ryzykiem (na potrzeby bezpieczeństwa informacyjnego) ma na celu:

- wykazanie, którego ryzyka i jak można uniknąć, stosując rozwiązania organizacyjne i techniczne w zakresie przetwarzania, przesyłania i przechowywania informacji w systemach informacyjnych organizacji;
- zapewnienie optymalnego, ze względu na koszty i znane/zadane ograniczenia, stanu ochrony takich informacji;
- zminimalizowanie ryzyka szczątkowego tak, aby stało się akceptowalne.

Pożądany poziom odporności na zagrożenia zapewnia zwykle tzw. *system bezpieczeństwa informacyjnego*, na który składają się powiązane i oddziałujące na siebie w różny sposób elementy[3] organizacyjne, techniczne (w tym programowe)

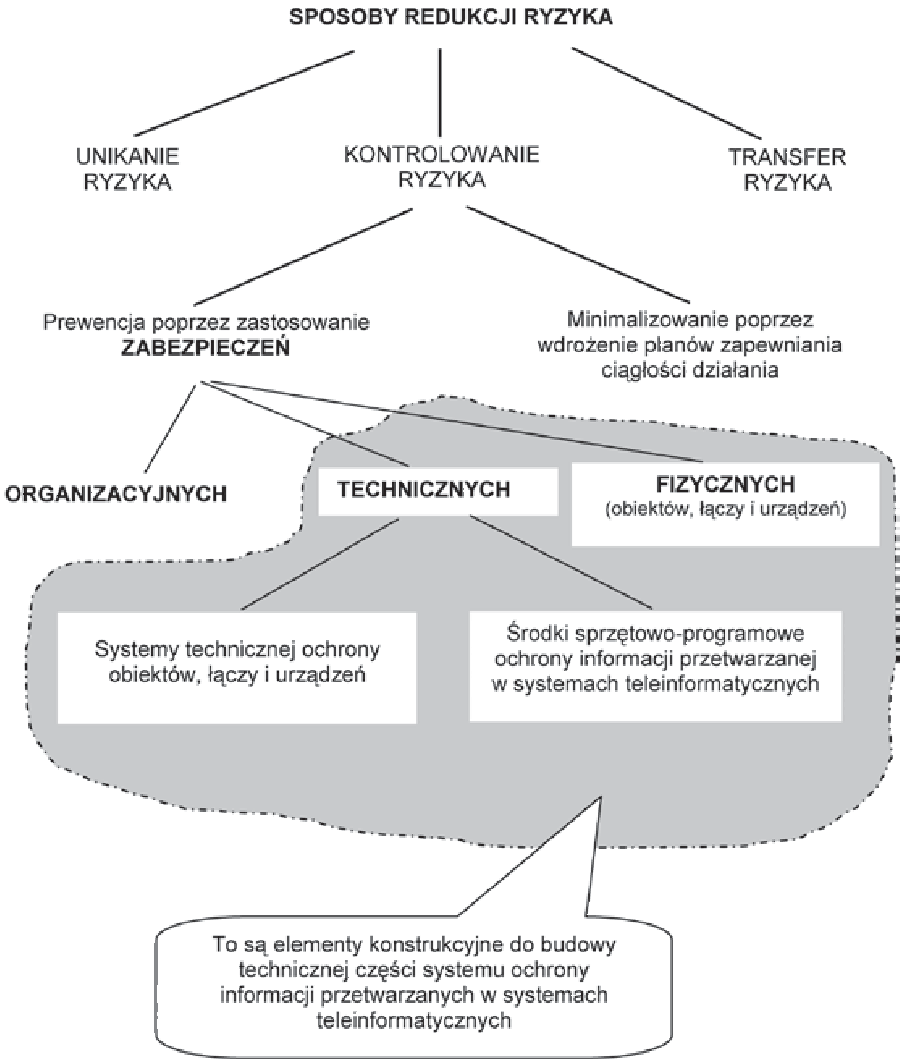
[2] Na przykład pełnomocnika ds. bezpieczeństwa lub administratora bezpieczeństwa teleinformatycznego.

[3] Nazywane zwykle zabezpieczeniami.

i ludzkie. Z perspektywy zarządzania ryzykiem, system ten służy do minimalizowania (redukcji) ryzyka – patrz rysunek 1.

Taki system, dla wszystkich wymienionych elementów składowych, powinien być dobrze udokumentowany. Jest to niezbędne dla:

- właściwej implementacji a potem eksploatacji zabezpieczeń (czyli, z perspektywy zarządzania ryzykiem, środków do minimalizacji ryzyka),
- utrzymania pod kontrolą zmian w tym systemie (czyli, z perspektywy zarządzania ryzykiem, minimalizacji ryzyka związanego z wprowadzeniem nie rozpoznanych podatności na zagrożenia),
- spełnienia wymogów różnych przepisów prawnych, które w sposób jawny nakładają obowiązek posiadania przez organizacje (o ile są przez nie przetwarzane i przechowywane określone klasy informacji) dokumentów nazywanych „polityka bezpieczeństwa", „instrukcje i procedury bezpieczeństwa" lub podobnie (patrz przykład 1). Czyli – z perspektywy zarządzania ryzykiem – minimalizacji ryzyka prawnego.



Przykład 1:

I. Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. *w sprawie minimalnych wymagań dla systemów teleinformatycznych*: § 3.
   1. Podmiot publiczny opracowuje, modyfikuje w zależności od potrzeb oraz wdraża politykę bezpieczeństwa dla systemów teleinformatycznych używanych przez ten podmiot do realizacji zadań publicznych.
   2. Przy opracowywaniu polityki bezpieczeństwa, o której mowa w ust. 1, podmiot publiczny powinien uwzględniać postanowienia Polskich Norm z zakresu bezpieczeństwa informacji.

II. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 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):

   § 3. 1. Na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „instrukcją".
   2. Dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej.
   3. Dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

   § 4. Polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności:
   1. wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym 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.

***

Uważam, że system bezpieczeństwa może być w pełni udokumentowany przez następujące, dobrze opracowane i poprawnie wdrożone[4] dokumenty:

1. „Politykę bezpieczeństwa informacyjnego" – zawiera najważniejsze, ogólne ustalenia dotyczące działania organizacji w zakresie ochrony informacji i zasad jej przetwarzania; powinien być udostępniany wszystkim zainteresowanym.

[4] „Wdrożone" oznacza, że dokumenty te muszą zostać wprowadzone w organizacji odpowiednim zarządzeniem naczelnego kierownictwa oraz muszą zostać wykonane odpowiednie czynności administracyjne, jak np. szkolenia, zakupy czy zmiany w obiegu dokumentów oraz techniczne, jak np. instalacja sprzętu komputerowego i oprogramowania.

2. „Plan bezpieczeństwa informacyjnego" – zawiera szczegóły budowy systemu bezpieczeństwa informacyjnego; powinien być udostępniany zgodnie z zasadą „wiedzy koniecznej".
3. „Instrukcje i procedury bezpieczeństwa teleinformatycznego" – zawiera zasady i sposób postępowania w zakresie bezpieczeństwa teleinformatycznego dla osób korzystających z systemów teleinformatycznych; dokument do użytku wewnętrznego.
4. „Plan zapewniania informacyjnej ciągłości działania" – zawiera instrukcje i procedury postępowania w przypadku wystąpienia tzw. zdarzeń kryzysowych naruszających informacyjną ciągłość działania; dokument do użytku wewnętrznego, podlegający specjalnej ochronie.

Podstawowym z wymienionych czterech dokumentów jest „polityka bezpieczeństwa informacyjnego". W dalszej części artykułu, ze względu na ograniczone ramy publikacji, zostanie bardziej szczegółowo opisany tylko ten dokument. Informacje nt. planu zapewniania ciągłości działania zainteresowany Czytelnik znajdzie w publikacjach [1] i [2] oraz w normach i standardach [3, 4, 7, 10, 11].

1. Dokument „polityka bezpieczeństwa informacyjnego"

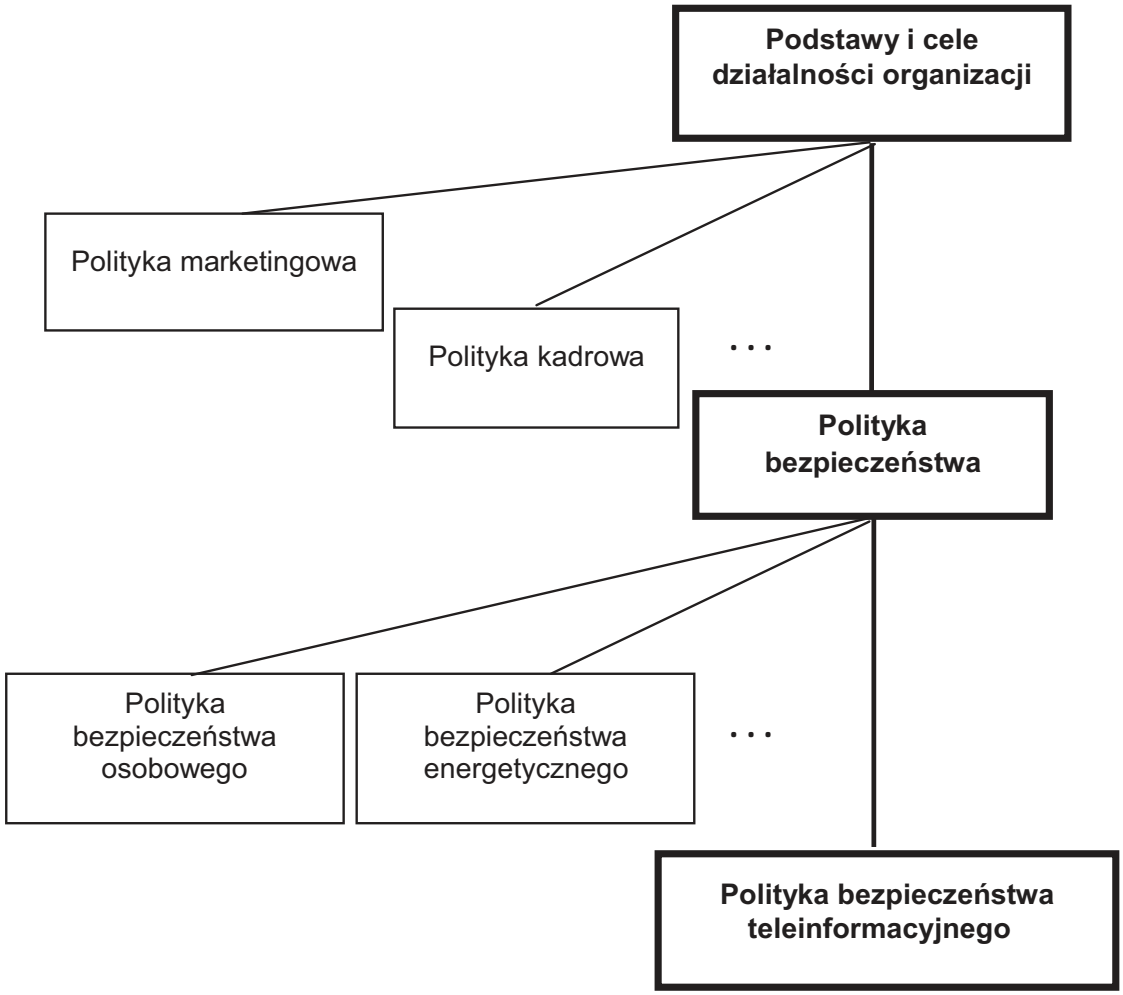
Potocznie termin „polityka" określa zorganizowane działania mające doprowadzić do osiągnięcia założonego celu(-ów)[5]. Na terenie konkretnej organizacji realizowane są zwykle różnorodne działania określane mianem „polityki", np.: polityka finansowa, polityka kadrowa, polityka marketingowa itd. (por. rys. 2). Zwykle te działania (określane tutaj mianem polityki) są wzajemnie powiązane, a zasady przeprowadzenia tych działań są spisane w odpowiednich dokumentach zatytułowanych „Polityka...". Podstawą dla wszelkiego rodzaju polityk realizowanych na terenie organizacji jest zazwyczaj jej statut, zawierający podstawę prawną i cele działalności[6].

Zdaję sobie w pełni sprawę z tego, że tak prymitywna definicja polityki może razić politologów czy przedstawicieli nauk społecznych. Jednak w dziedzinie, w której stosuję to pojęcie (bezpieczeństwo informacyjne), jest ono tak interpretowane. Uważam także, że jest ono zgodne z uznanymi interpretacjami – patrz znaczenie 3 w podanej w przypisie 5 definicji. Warto zwrócić także uwagę, że w języku angielskim opisywane pojęcie to „policy", nie mające odpowiednika w języku polskim,

[5] **Polityka** (gr. *politiké* 'sztuka rządzenia państwem', *tá politiká* 'sprawy publiczne, rządzenie') **1.** prowadzenie przez administrację rządową, samorządową działań zmierzających do określonej organizacji społeczeństwa w państwie oraz kierowania nim w kontaktach międzypaństwowych. **2.** działalność ugrupowań politycznych i społecznych mająca na celu zdobycie i sprawowanie władzy w państwie celem realizacji własnych celów programowych; także ogół działań prowadzonych dla osiągnięcia tego celu. **3.** *przen.* konsekwentne działanie w stosunku do jakiejś osoby lub grupy.
Na podstawie *Słownika Wyrazów Obcych,* Wydawnictwa Europa, M. Jarosz i zespół pod red. nauk. I. Kamińskiej-Szmaj, 2001.

[6] Często w tym kontekście pisze się o „misji" (ang. *mission*) organizacji.

różniące się od „politics" odpowiadającego rozumieniu polityki przez politologów i humanistów (polityka międzynarodowa, polityka obronna państwa itp.).



Rys. 2. „Polityki" w organizacji
Źródło: opracowanie własne

Dokumenty zatytułowane „Polityka..." wytwarza się m.in. w celu spełnienia wymogów różnych przepisów prawnych, które w sposób jawny nakładają obowiązek posiadania przez organizację takich dokumentów. Niestety, informacje zawarte w takich przepisach, a dotyczące konstrukcji i zawartości wymienionych dokumentów, są zwykle bardzo ogólnikowe, a nieraz także sprzeczne. Chaos w tym zakresie pogłębiają jeszcze różne interpretacje terminu „polityka". Normy i standardy odpowiednie dla bezpieczeństwa teleinformatycznego często ten chaos pogłębiają. Dlatego proponuję przyjęcie następujących ustaleń:

1) politykę (rozumianą jako sposób i zakres działania) kształtuje naczelne kierownictwo organizacji;
2) polityka w zakresie bezpieczeństwa informacyjnego jest realizowana przez ogół pracowników organizacji;
3) polityka w zakresie bezpieczeństwa teleinformatycznego jest nadzorowana przez osoby, które takie zadanie mają wpisane w swój zakres obowiązków

(głównie dotyczy to kierownictwa działów IT i osób z komórek organizacyjnych lub stanowisk związanych z bezpieczeństwem);

4) żeby politykę można było skutecznie realizować (czyli prowadzić działania mające doprowadzić do określonego celu – w tym przypadku zapewnienia odpowiedniego poziomu bezpieczeństwa informacyjnego) oraz nadzorować i w razie potrzeby aktualizować, polityka powinna być spisana w postaci dokumentu zatytułowanego (zwykle) „Polityka bezpieczeństwa informacyjnego”[7];
5) dokument, o którym mowa w punkcie 4), musi być wdrożony (por. przypis 4).

Dokument „Polityka bezpieczeństwa informacyjnego” (dalej w tekście PBI) to opis najważniejszych, ogólnych zamiarów działań i deklaracji najwyższego kierownictwa organizacji w zakresie zapewniania w niej odpowiedniego poziomu bezpieczeństwa informacyjnego. Przeznaczony jest do uzasadnienia zaufania klientów i partnerów biznesowych do powierzenia swoich informacji tej organizacji oraz stanowi podstawę do opracowania szczegółowych rozwiązań organizacyjnych i technicznych w zakresie ochrony informacji. PBI powinna być dokumentem jawnym, ogólnie dostępnym i powinna zawierać następujące informacje[8]:

1) słownik używanych pojęć i skrótów, w tym definicję bezpieczeństwa informacji oraz ról w systemie (właściciel, użytkownik, operator, administrator itp.);
2) wykaz dokumentów normatywnych (przepisów prawnych, jak np. ustawy, oraz standardów i norm technicznych), z których zapisami jest zgodny system ochrony informacji w organizacji[9] (patrz przykład 6.3);
3) wykaz aktów normatywnych, zgodnie z którymi należy rozstrzygać kwestie nieujęte w PBI i dokumentach pochodnych;
4) zakres (terytorialny i organizacyjny) i cel PBI;
5) deklarację priorytetów wartości dla organizacji, np.: życie i zdrowie klientów, życie pracowników i ich rodzin, zasoby powierzone, zasoby niezbędne dla utrzymania ciągłości działania itd.;
6) cel(-e) budowania systemu ochrony informacji;
7) deklarację zarządu organizacji odnośnie do środków finansowych przeznaczanych na bezpieczeństwo informacyjne;
8) opis zasobów informacyjnych organizacji, w tym:
   - specyfikację grup informacji podlegających szczególnej ochronie,
   - wymagany poziom ochrony dla każdej z grup informacji,

[7] W dalszej części termin „polityka” (domyślnie: w zakresie bezpieczeństwa informacyjnego) będzie używany wyłącznie jako nazwa dokumentu wymienionego w tym punkcie.

[8] Zapisy na temat polityki bezpieczeństwa informacyjnego oraz zawartości dokumentu, w zasadzie zgodne z przedstawionymi tutaj poglądami autora, można znaleźć także w normie PN-ISO/IEC-17799:2007, punkty: 5.1.1, 5.1.2, 6.1.1, 6.1.2.

[9] Wtedy w tekście PBI muszą być umieszczone zapisy wymagane prawem i, w razie umieszczenia takich odwołań, warunki zgodności z podstawowymi normami bezpieczeństwa.

- w razie potrzeby – system klasyfikacji i kategoryzacji informacji,
- znaczenie poszczególnych systemów informacyjnych (w szczególności teleinformatycznych) organizacji dla realizacji zadań statutowych,
- opis otoczenia informacyjnego organizacji, z dokładnym wskazaniem miejsc wejścia i wyjścia informacji do/z jej systemów informacyjnych,
- zasady dokumentowania systemu ochrony informacji;

9) ogólną zasadę podjęcia stosownych działań (także spoza zakresu kompetencji) oraz odstąpienia od działania (także należącego do obowiązków), z inicjatywy własnej lub na wezwanie (także w przypadku braku podległości służbowej) – w przypadku stwierdzenia zagrożenia interesów organizacji, w szczególności wartości priorytetowych dla organizacji (patrz punkt 5);
10) obowiązki i zakresy odpowiedzialności kierownictwa i pracowników organizacji w procesie ochrony zasobów informacyjnych oraz konsekwencje w przypadku nieprzestrzegania zasad zawartych w PBI;
11) ogólne zasady organizacyjne dotyczące dokumentu PBI, np.:
    - zapis o nadrzędności wobec innych dokumentów z zakresu bezpieczeństwa,
    - kto odpowiada za dokument PBI,
    - kto, kiedy i w jakim trybie może zmienić zapisy w PBI,
    - sposób przeglądu i aktualizacji PBI,
    - powiązania z regulacjami prawnymi i wewnętrznymi organizacji;
12) zasady nadawania uprawnień do działania na zasobach informacyjnych, w tym:
    - kto (na jakim stanowisku służbowym) i w jakim zakresie ma prawo do występowania o nadanie pracownikom uprawnień do zasobów informacyjnych,
    - kto, kiedy i w jakim zakresie ma prawo do występowania o nadanie uprawnień do zasobów informacyjnych w sytuacjach doraźnych (np. konsultantom zewnętrznym) lub wyjątkowych (np. w przypadku śmierci odpowiedzialnego za zasób pracownika lub żądania uprawnionych organów: policji, GIODO, kontroli skarbowej itd.),
    - sposób przekazywania i przechowywania informacji uwierzytelniających i autoryzacyjnych,
    - wzór (jako załącznik do PBI) dokumentu o nadanie uprawnień lub wskazanie aplikacji, za pomocą której takie zadanie jest realizowane w systemie informatycznym;
13) zasady dostępu do zasobów informacyjnych organizacji;
14) zasady przetwarzania informacji w systemach teleinformatycznych (zwykle poprzez odwołanie do innych dokumentów szczegółowych typu instrukcje i procedury) oraz przechowywania zbiorów informacyjnych (w tym komputerowych nośników informacji);

15) zasady ochrony zasobów informacyjnych niezbędnych do realizacji kluczowych procesów biznesowych;
16) zasady nadzoru nad wykorzystaniem zasobów informacyjnych zgodnie z obowiązującym prawem i wewnętrznymi przepisami organizacji;
17) zasady usuwania informacji z nośników komputerowych i niszczenia dokumentów papierowych;
18) koncepcję szkolenia pracowników organizacji w zakresie ochrony informacji;
19) zarys systemu kontroli, w tym audytów, w toku normalnej pracy organizacji;
20) ogólne wytyczne do sposobu reakcji na zdarzenia naruszające bezpieczeństwo informacyjne oraz wskazanie dokumentów zawierających szczegóły postępowania w takich przypadkach;
21) załączniki różne (np. schemat klasyfikacji informacji, schemat organizacyjny, wzory dokumentów itp.).

Warunkami i działaniami, bez których osiągnięcie sukcesu w opracowywaniu i wdrażaniu polityki bezpieczeństwa nie wydaje się możliwe, są:

1) świadomość najwyższej kadry kierowniczej znaczenia bezpieczeństwa informacyjnego dla działalności biznesowej organizacji;
2) chęć i jawna deklaracja najwyższej kadry kierowniczej wsparcia działań podnoszących poziom bezpieczeństwa informacyjnego, w tym zapewnienia odpowiednich środków finansowych;
3) sformułowanie celu budowy systemu bezpieczeństwa;
4) powołanie zespołu ds. zarządzania bezpieczeństwem informacyjnym, który będzie opracowywał (bądź nadzorował opracowanie) politykę bezpieczeństwa informacyjnego dla swojej organizacji;
5) podjęcie decyzji co do sposobu budowy (lub zmiany) systemu bezpieczeństwa informacyjnego – własnymi siłami organizacji lub wynajęcie do wykonania tej pracy wyspecjalizowanego zespołu z zewnątrz organizacji (rozwiązanie częściej spotykane);
6) zidentyfikowanie kluczowych dla działania organizacji procesów biznesowych (i związanych z nimi systemów teleinformatycznych);
7) zidentyfikowanie grup informacji, których ochrona jest szczególnie pożądana i określenie wymaganego poziomu ich ochrony (również ze względu na spełnienie wymagań ustawowych);
8) wstępne oszacowanie możliwych kosztów strat w przypadku utraty poufności, integralności lub dostępności informacji (również pod względem naruszenia przepisów prawnych państwowych lub resortowych, np. naruszenie przepisu o ochronie danych osobowych).

Należy zwrócić uwagę, że dla punktów 1-5 wymagane jest zaangażowanie najwyższego kierownictwa organizacji. W realizację punktów 6-8, wykonywanych najczęściej pod kierunkiem zewnętrznych ekspertów, są także zaangażowani przed-

stawiciele najwyższego kierownictwa, jako kompetentne osoby mające prawo do zajmowania oficjalnego stanowiska w imieniu organizacji.

Określenie niezbędności systemów teleinformatycznych w wypełnianiu zadań służbowych można przeprowadzić, stosując np. następującą opisową skalę ocen:

- **wspomagające** – zadania służbowe przy niewielkim dodatkowym nakładzie sił i środków mogą być wykonane innymi środkami (np. ręcznie);
- **ważne** – zadania służbowe mogą być wykonane innymi środkami tylko znacznym dodatkowym nakładem sił i środków;
- **zasadnicze** – ze względu na dużą ilość informacji, zadania służbowe mogą być wykonane innymi środkami tylko częściowo;
- **niezbędne** – zadania służbowe nie mogą być wykonane bez wykorzystania systemów teleinformatycznych.

Oszacowanie pożądanego poziomu ochrony informacji dotyczy wymaganej siły zabezpieczeń zastosowanych w konkretnych systemach teleinformatycznych i zwykle jest określane na podstawie skutków biznesowych (jako wynik tzw. *business impact analysis*), które miałyby miejsce, gdyby tych zabezpieczeń nie było. Poziom ten można określić na przykład według następującej skali:

- **bardzo wysoki** – gdy błędy w ochronie informacji przetwarzanych w systemach teleinformatycznych organizacji prowadzą do jej bankructwa lub wywierają szerokie niekorzystne skutki społeczne lub gospodarcze;
- **wysoki** – gdy błędy w ochronie informacji przetwarzanych w systemach teleinformatycznych organizacji naruszają zdolność do działania jej kluczowych elementów, a szkody z tego wynikłe dotyczą jej i podmiotów trzecich;
- **średni** – gdy błędy w ochronie informacji przetwarzanych w systemach teleinformatycznych organizacji przynoszą straty tylko tej organizacji;
- **niski** – jw., ale gdy straty są niewielkie.

W niektórych przypadkach (patrz przykład 2) poziomy ochrony mogą być jawnie wyspecyfikowane w przepisach prawnych. Natomiast cele budowania bezpieczeństwa teleinformatycznego będą zwykle następujące:

- zapewnienie dobrej marki organizacji na rynku;
- zapewnienie ciągłości pracy w organizacji;
- zapewnienie realizacji wymagań przepisów prawnych np. o ochronie tajemnicy przedsiębiorstwa;
- zagwarantowanie niezawodności procesów biznesowych z punktu widzenia zarówno ich terminowości (dostępność informacji), dokładności (integralność informacji), jak i poufności.

Przykład 2:

Wymagania bezpieczeństwa wynikające z rozporządzenia MSWiA 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):

1. Zróżnicowanie wymaganego poziomu ochrony przetwarzania danych w zależności od kategorii przetwarzanych danych oraz występujących zagrożeń:
   - **poziom podstawowy** – gdy **nie są** przetwarzane dane, o których mowa w art. 27^{10} ustawy, oraz żadne z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych **nie jest połączone** z siecią publiczną;
   - **poziom podwyższony** – gdy **są** przetwarzane dane, o których mowa w art. 27 ustawy oraz żadne z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych **nie jest połączone** z siecią publiczną;
   - **poziom wysoki** – gdy przynajmniej jedno z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych jest połączone z siecią publiczną.

   W rozporządzeniu są wyspecyfikowane stosowane obligatoryjnie środki ochronne, bez określenia sposobu implementacji tych środków.

   Na poziomie wysokim wymagane jest stosowanie środków ochrony kryptograficznej nie tylko wobec danych osobowych przesyłanych w publicznej sieci telekomunikacyjnej, ale również wobec informacji wykorzystywanych do uwierzytelniania się w systemie.
2. Obowiązek prowadzenia dokumentacji przetwarzania danych osobowych:
   - polityki bezpieczeństwa;
   - instrukcji zarządzania systemem informatycznym.
3. W odniesieniu do przetwarzania danych osobowych przez instytucje i organy ustanowione przez lub na podstawie traktatów ustanawiających Wspólnoty Europejskie, dodatkowo obowiązują wymagania wynikające z przepisów prawa UE.

***

Wdrożenie w organizacji dokumentów opisujących system bezpieczeństwa (patrz przypis 4) jest jednym z etapów wdrażania systemu bezpieczeństwa informacyjnego. W skład tego etapu wchodzą m.in. dwa przedsięwzięcia organizacyjne:

1) wprowadzenie do użytku w organizacji, odpowiednim zarządzeniem naczelnego kierownictwa, dokumentów opisujących system bezpieczeństwa informacyjnego,
2) przeprowadzenie szkolenia personelu organizacji (podstawą szkolenia są ww. dokumenty).

---

[10] Art. 27 ust. 1 (ust. 2 precyzuje, kiedy takie przetwarzanie jest dopuszczalne):
„Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym".

Kształtowanie świadomości kierownictwa i pracowników w zakresie bezpieczeństwa informacyjnego uważa się za jeden z kluczowych elementów zapewniania tego bezpieczeństwa. Praktyczne wskazówki dotyczące prowadzenia szkoleń z ochrony informacji niejawnych[11] i bezpieczeństwa informacyjnego można sformułować następująco:

1. Szkolenia personelu powinny obejmować cały związany z systemami informacyjnymi personel – od członków zarządu do zwykłego użytkownika systemu teleinformatycznego. Wymóg przeszkolenia dotyczy także pracowników okresowych (np. praktykantów, pracowników outsourcingowych itp.).
2. Merytoryczną podstawą szkolenia są wdrożone w organizacji, wymienione we wstępie niniejszego rozdziału, dokumenty (głównie dokument „Instrukcje i procedury...").
3. Szkolenie powinno być przeprowadzone, zanim zostaną w pełni wdrożone techniczne i organizacyjne przedsięwzięcia związane z systemem bezpieczeństwa.
4. Szkolenia powinny być powtarzane w regularnych odstępach czasu.
5. Tematyka szkolenia powinna uwzględniać również zagadnienia ogólne, takie jak:
   - cele wdrażania systemu bezpieczeństwa informacyjnego,
   - wybrane elementy obowiązującej w organizacji koncepcji bezpieczeństwa informacyjnego (w szczególności wskazanie osób odpowiedzialnych za poszczególne elementy tego bezpieczeństwa),
   - sposoby postępowania w przypadkach naruszania bezpieczeństwa.
6. Wszyscy pracownicy powinni poświadczyć własnoręcznym podpisem odbycie szkoleń z zakresu bezpieczeństwa informacyjnego, a fakt odbycia szkolenia powinien być odnotowany w aktach personalnych pracownika.
7. Szkolenia z podstaw bezpieczeństwa informacyjnego powinny zawierać elementy ochrony informacji niejawnych (w szczególności obowiązujący w organizacji system klasyfikowania informacji), nie pomijając informacji o konsekwencjach karnych i dyscyplinarnych ponoszonych przez pracownika naruszającego zasady tego bezpieczeństwa.

Dla osiągnięcia pożądanych rezultatów, szkolenia prowadzone są zwykle w następujących grupach:

1) najwyższej kadry kierowniczej organizacji;
2) personelu kierowniczego średniego szczebla;
3) pracowników biurowych;
4) personelu technicznego i pomocniczego;
5) administratorów sieci, serwerów, stacji roboczych i systemów.

[11] W przypadku informacji niejawnych w rozumieniu ustawowym, tryb i zakres prowadzonych szkoleń jest szczegółowo regulowany odpowiednimi przepisami.

Najwyższą kadrę kierowniczą należy przeszkolić, ponieważ to ona decyduje, na co i jak wydać pieniądze organizacji. W szczególności to spośród niej będzie się rekrutował tzw. *właściciel ryzyka* (tutaj: informacyjnego). Kadra ta powinna zatem zostać przekonana o słuszności inwestowania w „bezpieczeństwo" oraz muszą jej zostać dostarczone niezbędne informacje do podejmowania prawidłowych decyzji w zakresie bezpieczeństwa informacyjnego, w tym minimalizacji ryzyka. Poza tym, to na VIP-owskich notebookach znajdują się zwykle informacje szczególnie wrażliwe.

Personel kierowniczy średniego szczebla należy przeszkolić, ponieważ to on będzie w dużej mierze decydował o powodzeniu organizacyjnej strony przedsięwzięć bezpieczeństwa. To kierownicy komórek organizacyjnych występują o nadanie uprawnień w systemie dla podległych pracowników (a zatem powinni znać zasady „wiedzy koniecznej" i „minimalnego środowiska pracy"), to oni bezpośrednio nadzorują tzw. politykę „czystego biurka" i „czystego ekranu", to oni decydują o skierowaniu swoich pracowników na szkolenia itd. To personel kierowniczy średniego szczebla jest w głównej mierze nosicielem szczególnie groźnego dla skuteczności systemu bezpieczeństwa „syndromu kelnera": „Bezpieczeństwo sieci i komputerów? To nie ja (my), to dyrektor działu IT i jego ludzie!".

Szczególną uwagę należy zwrócić także na podnoszenie kwalifikacji przez administratorów technicznych w zakresie zarządzanych przez nich systemów i urządzeń. Im bowiem więcej administrator wie o systemie (urządzeniu, oprogramowaniu), tym lepiej może zrozumieć jego działanie i skuteczniej nim zarządzać, również pod względem bezpieczeństwa informacyjnego.

Przykład 3:

Kształtowanie świadomości w zakresie bezpieczeństwa teleinformatycznego według normy PN-ISO/IEC 27001:2007 (załącznik A.6.2.1: Szkolenie i kształcenie w zakresie bezpieczeństwa informacji): „Wszyscy pracownicy instytucji, a jeśli to konieczne, także użytkownicy – osoby trzecie – pochodzący spoza instytucji, powinni przejść właściwe, okresowo uaktualniane, przeszkolenie w zakresie polityk i procedur obowiązujących w instytucji, zanim zostanie im przyznany dostęp do informacji lub usług".

Norma PN-ISO/IEC-17799:2007 precyzuje w punkcie 6.2.1: „Przeszkolenie takie obejmuje wymagania bezpieczeństwa, odpowiedzialność prawną i zabezpieczenia wewnętrzne, jak również przeszkolenie w zakresie prawidłowego korzystania z urządzeń przetwarzania informacji, np. procedur rejestrowania w systemie, używania pakietów oprogramowania".

Podsumowanie

Znaczenie dokumentu „Polityka bezpieczeństwa informacyjnego" wynika z faktu, że jego posiadanie:

– świadczy o „należytej staranności" organizacji w zakresie ochrony informacji i daje **podstawy do rzetelnego zarządzania ryzykiem informacyjnym**;

- stanowi podstawę zaufania potencjalnych klientów lub partnerów biznesowych do powierzenia swoich dóbr informacyjnych takiej organizacji;
- dla audytora stanowi dowód, że koncepcja ochrony informacji jest przemyślana i spisana;
- dla inżynierów budujących system ochrony informacji (lub, patrząc na problem z perspektywy zarządzania ryzykiem, system minimalizacji ryzyka) zawiera podstawowe wymagania projektowe i operacyjne (wytyczne) na taki system;
- dla pracowników zaangażowanych w ochronę informacji stanowi podstawowy zbiór zasad pozwalających im na skuteczne pełnienie obowiązków służbowych;
- jest wymagane przez przepisy prawa (np. ustawę o ochronie danych osobowych i stosowne rozporządzenie) – patrz przykład 1.

Do efektywnego zarządzania ryzykiem potrzebne będą także pozostałe, wymienione pod koniec rozdziału 1, dokumenty:

- instrukcje i procedury z zakresu bezpieczeństwa teleinformatycznego są niezbędne do minimalizowania ryzyka związanego z błędami ludzkimi i proceduralnymi;
- „Plan bezpieczeństwa informacyjnego" jest niezbędny do minimalizowania ryzyka niewłaściwego zaprojektowania systemu ochrony oraz ryzyka jego niewłaściwej eksploatacji;
- „Plan zapewniania informacyjnej ciągłości działania" jest niezbędny do minimalizowania ryzyka związanego z wystąpieniem zdarzeń naruszających ciągłość pracy systemu informacyjnego lub integralność albo dostępność zbiorów danych.

ABOUT SIGNIFICANT RELIABLE INFORMATION SECURITY SYSTEM DOCUMENTATION FOR INFORMATION RISK MANAGEMENT

Summary: The paper presents author's view for significant reliable information security system documentation for information risk management. It presents an outline of activity assembled on information risk management. It explains the way of understanding the term "policy" in information security area. In details there is described the content of information security policy document.

Keywords: information risk management, information security, information security policy.

LITERATURA

[1] Liderman K., *Plan ciągłości działania elementem dokumentowania ładu korporacyjnego*, [w:] Gonciarski W., Zaskórski P. (red.), *Wybrane koncepcje i metody zarządzania na początku XXI wieku***,** WAT, Warszawa 2009, s. 147-159.
[2] Liderman K., *Bezpieczeństwo informacyjne*, PWN, Warszawa 2012.
[3] BS 25999-1: 2006: *Business continuity management. Code of practice*.
[4] BS 25999-2: 2007: *Specification for business continuity management*.

[5] PN-ISO/IEC-17799:2007: *Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji*.
[6] PN-ISO/IEC 27001:2007: *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*.
[7] PN-ISO/IEC 24762:2010: *Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie*.
[8] PN-IEC 62198:2005: *Zarządzanie ryzykiem przedsięwzięcia – Wytyczne stosowania*.
[9] PN-ISO/IEC 27005:2010: *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*.
[10] NFPA 1600: *Standard on Disaster/Emergency Management and Business Continuity Programs*, 2007 Edition.
[11] NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, June 2002.
[12] Rozporządzenia MSWiA 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).
[13] Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. *w sprawie minimalnych wymagań dla systemów teleinformatycznych* (Dz.U. z 2005 r., nr 212, poz. 1766).
[14] Ustawa z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnej* (Dz.U. z 2010 r., nr 182, poz. 1228).